2017

글로벌 법제 동향 모니터링 및 이슈 분석 보고서

GLOBAL LEGAL ISSUES (III-1)

한국법제연구원

KOREA LEGISLATION RESEARCH INSTITUTE

2017

글로벌 법제 동향 모니터링 및 이슈 분석 보고서

GLOBAL LEGAL ISSUES (Ⅲ-1)

한국법제연구원

KOREA LEGISLATION RESEARCH INSTITUTE

CONTENTS

2017

글로벌 법제 동향 모니터링 이슈 분석 보고서

KOREA LEGISLATION RESEARCH INSTITUTE

GLOBAL LEGAL ISSUES (Ⅲ-1)

ISSUE 01

공공행정 / 규제개혁분야

공공행정 및 규제분야 글로벌 법제 이슈 동향 및 시사점

최 승 필
한국외국어대학교 법학전문대학원 교수

최승필 교수는 한국은행에서 Economist로 재직하였으며, 독일 Würzburg 대학교에서 경제행정법으로 박사학위를 취득하였다. 현재 한국외대 법학전문대학원 교수로 재직 중이며, 주요 연구활동분야는 행정법, 금융규제법, 환경법이다.

ISSUE
01
공공행정 / 규제개혁분야

공공행정 및 규제분야 글로벌 법제 이슈 동향 및 시사점

최 승 필 한국외국어대학교 법학전문대학원 교수

Abstract

양성평등은 공적부문에서 중요한 이슈 중의 하나이다. 『OECD 공공생활에서 양성평등에 대한 권고』는 공공정책과 예산의 설계, 개발, 집행, 평가 등에서 양성평등이 이루어져야 하며, 이를 위해 책임성 및 감독체계를 강화할 필요가 있음을 강조하고 있다. 고용에 있어서도 양성평등이 달성되도록 적절한 수단이 필요하다.

『OECD 규제정책에 대한 이해관계자의 참여에 관한 최적관행』은 규제정책의 중요한 요소로서 이해관계자의 참여와 개방적이고 포용적인 정책형성이 필요함을 강조하고 이해관계자의 참여가 주는 장점을 제시하면서 동시에 이해관계자 참여가 극복해야 할 과제도 아울러 제시하고 있다. 그리고 최적관행은 이해관계자의 참여는 영향에 따라 비례적으로 이루어져야 함을 언급하고 있다. 이해관계자의 참여의 예로 미국의 NPRM, 유럽연합의 Better Regulation 등이 들고 있다.

『유럽연합 공공부문 최적관행을 위한 거버넌스』는 거버넌스와 책임성의 체계를 설명하고

유럽의 공공부문 개혁구조를 정치적 우선순위의 설정과 재원의 배분, 인력정책, 감사와 재무관리 및 통제로 나누어 제시하고 있다. 한편 최적관행의 수행을 위해 감사기능이 필요함을 언급함과 동시에 투명성과 석명의무 달성을 위해 연차보고서 작성의 중요성을 강조하고 있다.

『OECD 수준높은 행정서비스를 위한 공적영역 종사자의 역할』은 최근의 공공부문 채용동향과 제한사항, 좋은 인사정책의 방향을 제시하고 있다. 특히 단순히 비용만을 고려한 다운사이징의 문제점과 함께 이를 방지하기 위한 안을 설명하고 있다. 아울러 공공부문의 가치사슬을 통해 공공부문의 영향이 시민들에게 어떠한 영향을 미치고 있는지를 나타내고 있다.

『유럽연합의 전자정부 액션플랜 2016-2020』은 전자정부의 효율성과 효과성 그리고 개방성, 포용성에 대한 논의를 소개하고 있다. 그리고 구체적인 액션플랜으로 원칙으로서 디지털, 원칙으로서 '단 한번(only-once)' 등을 제시하고 있다. 아울러 각 분야별로 2016년 이후 유럽연합 전자정부의 디지털 변환 추진계획 로드맵을 제시하고 있다.

『유럽연합은 2016년 5월 유럽연합 개인정보보호규칙』을 마련하고 2018년 5월 시행을 앞두고 있다. 주요한 특징으로는 이를 지침에서 규칙으로 전환하여 연합내의 통일성을 강화하였고, 개인정보의 활용성은 높이되, 정보주체의 개인정보통제권을 강화하였다.

『OECD 복지영역에서 공공서비스의 변화를 위한 디지털 정부전략』에서는 복지에서 공공영역간 경계 변화가 있음을 소개하고 복지서비스에 디지털 기술을 결합하여 보다 효과적이고 효율적인 복지서비스를 제공할 수 있음을 보여주고 있다. 특히 단순한 디지털화와 전자정부 그리고 디지털 정부 개념에서 복지서비스가 어떻게 달라지는 지를 표로 정리하고 있다.

중국은 2016년 11월 7일 제12기 전인대 상무회의에서 『네트워크안전법』을 제정 결의하였고 2017년 6월 1일부터 시행중이다. 주요한 구성은 네트워크 안전지원 및 촉진, 네트워크 운영안전, 네트워크 정보안전, 모니터링 조기경보 및 응급대처, 법적책임, 부칙으로 구성되었다.

공공부문 및 규제분야의 중요한 흐름 중 하나는 기술혁신과 관련된 사항으로 규제를

간소화 하거나 신기술의 발전에 대응하기 위한 스마트 규제에 주안을 두고 있다. 특히 금융선진국들은 핀테크를 포함한 규제분야에서 피규제자의 규제부담을 줄여주기 위해 RegTech 기술의 활용에 많은 노력을 기울이고 있다.

RegTech와 관련하여서는 『영국금융행위규제원의 RegTech』, 『호주증권투자위원회의 RegTech』, 우리 『금융보안원에서 제시한 RegTech 기술』, 『UNCTAD의 RegTech』, 『Deloitte 컨설팅이 제시한 RegTech Universe』, 『IIF가 제시한 금융서비스에서 RegTech의 활용』을 소개·설명하였다. RegTech는 최근 제4차산업혁명 그리고 핀테크와 관련하여 매우 관심 있게 논의되고 있음에 따라 가장 많은 분량을 할애하여 다양한 기관과 다양한 측면의 이슈를 조명하였다.

주요하게 다루었던 내용은 RegTech의 개념, RegTech의 활용분야, 관련기술, RegTech 활용의 장점과 극복해야 할 장애물을 살펴보았다. 마지막으로 실제로 규제와 가장 밀접한 규제보고 및 컴플라이언스 분야에서 현존하는 RegTech의 종류와 해당 서비스를 제공하는 기업을 Deloitte의 자료를 기반으로 간추려 정리하였다.

Ⅰ. 양성평등

■ 공공생활에서 양성 평등에 대한 권고 (OECD Recommendation of the Council on Gender Equality in Public Life 2015, 2016년 OECD에서 출간)

○ 공공정책과 예산의 디자인, 개발, 이행, 평가에서의 양성평등

– 양성평등에 대한 확고한 리더십이 있어야 하며, 정치적으로는 상위레벨, 정부에서는 적절한 레벨에서 이에 대한 관심을 가져야 한다. 구체적으로 합리적인 액션플랜(action plan), 정책의 우선순위, 일정별 계획, 기대효과, 정책수행의 대상을 특정해야 한다. 관련 정부부처는 물론 비정부기구(NGO)의 이해관계자도 참여할 필요가 있다.

– 효과적인 이행, 협조 그리고 지속가능성을 위해 명확한 역할을 특정하고 의무를 부과하며, 주요 정부기관과 감독당국의 책임성과도 연관시켜야 한다. 양성평등과 민감하게 연관된 프로그램과 정책에 대해서 개발, 이행 및 모니터링이 실시되어야 하며, 통계는 각 성별로 분리된 숫자를 보여주어야 한다.

– 양성평등과 관련한 연수와 지식을 제고할 프로그램을 운영해야 하며, 정부부처 내에서 양성평등과 관련하여 종적(vertical) 또는 횡적(horizontal) 거버넌스를 확립할 필요가 있다. 그리고 여기에는 비정부기구까지 연계할 필요가 있다.

– 조달, 공공컨설팅 및 서비스 등 공공거버넌스의 다양한 국면에서 성별이 주는 영향에 대해 통합적 증거 기반적 평가가 이루어져야 하며, 예산의 모든 단계에서 성별 측면에서의 통합적 고려가 이루어져야 한다.

○ 양성평등에 대한 책임성 및 감독체계의 강화 그리고 양성평등 이니시어티브의 확립

– 양성평등전략의 이행에 대한 모니터링과 정책형성과정에서 젠더(gender) 이슈의 통합 그리고 정기적인 보고, 감사, 측정이 수반되어야 한다. 이에 관련되는 부서로는 독립위원회, 최고감사기구, 옴부즈만 등을 들 수 있다.

– 양성평등 이행에 있어서 증거에 기반한 그리고 시스템적인 조치단계가 필요하고,

이행평가체계를 갖추고 책임성체계를 구축해야 한다. 아울러 데이터 수집과 가능하고 효과적이고 적시에 접근이 가능한 이행정보가 확보될 수 있도록 촉진해야 하며, 데이터 수집에 있어서는 이해관계자들과의 협력이 필요하다.

○ 공적영역에서 젠더의 균형을 확보하기 위해 필요한 조치를 고려

- 중앙정부와 지방자치단체(지방정부)의 각 레벨에서 여성의 참여를 촉진해야 하며, 이는 의회, 사법부 그리고 기타 영역에서도 마찬가지이다.
- 정치권 고위레벨에서 양성평등에 대한 노력이 있어야 하며, 그 일환으로 성별 균형이 잡힌 의회(의원)의 구성이 필요하다. 의회 및 행정부 등에서 양성평등을 촉진하기 위해서 자발적 또는 강제적 조치를 고려할 필요가 있는데 예로서 자발적 쿼터의 부여를 들 수 있다.
- 행정부, 사법부 등 고위공무원직에 남녀가 동등한 접근이 가능하도록 적절한 조치를 도입해야 한다. 예를 들어 일정한 비율 등 목표를 정하거나 쿼터를 설정해야 한다. 그러나 이때도 투명하고 능력위주의 원칙이 적용되어야 함은 물론이며, 동시에 공개경쟁, 명확한 인재채용기준을 제시할 필요가 있다.
- 공공기구의 고위레벨에서부터 일과 삶의 균형 그리고 가족 친화적인 업무환경을 만들 수 있도록 노력해야 한다. 즉 젠더이슈를 고려한 작업환경을 구현할 필요가 있다. 따라서 전통적인 근로시간 개념들을 재고할 필요가 있으며, 가족과 직업인으로서 의무를 조화시킬 수 있는 방안을 발전시켜야 한다.
- 체계적인 모니터링을 실시해야 한다. 모니터링의 대상은 각각 다른 직업그룹으로서 이들로부터 각각 다른 데이터를 수집하고 이를 바탕으로 양성평등 목표와 정책적 우선순위를 재평가할 필요가 있다.

○ 공적고용영역에서 양성평등을 제고할 수 있도록 적절한 수단을 도입

- 공적고용영역에서 유연성, 투명성, 공정성이 확보되고 공정한 급여, 동등한 기회가 남녀에게 주어져야 한다. 남녀 간 급여의 차이에 대해서 원인별로(cause-specific)

보다 이해할만한 조치가 필요하며, 구체적으로는 급여의 평등과 형평을 확보하기 위한 법 그리고 규정을 마련할 필요가 있다.

- 능력 중심의 채용과 양성평등에 대해 긍정적인 정책과 관행은 공공부문의 각 직역에서 남녀평등을 유도할 수 있으며, 암묵적 장벽(일종의 유리천장)을 제거할 수 있다. 독립성을 갖춘 이의제기 시스템을 확보할 필요도 있으며, 근본적으로는 공공부문의 관리자들에게 양성평등의 의미를 보다 더 적극적으로 알릴 필요가 있다.

Ⅱ. 규제정책에 대한 이해관계자 참여

■ 규제정책에 대한 이해관계자의 참여에 관한 OECD 최적관행 (OECD, Best Practice Principles on Stakeholder Engagement in Regulatory Policy, 2016)[1)]

○ 규제정책의 중요한 요소로서 이해관계자의 참여와 개방되고 포용적인 정책 형성

- 규제정책의 목적은 공공의 이익을 달성하기 위한 것이며, 이는 이해관계자들의 참여를 통해 달성할 수 있다. 여기에서 이해관계자들(stakeholders)이라 함은 시민, 기업(중소기업, 수출·수입업자, 잠재적 투자자를 포함), 거래조합, 시민단체, 공공단체 등을 모두 포함하는 개념으로서, 이해관계자를 모두 포용하는 것은 열린 정부 정책과도 일관성을 갖는다.
- 열려있는 그리고 포용적인 정책은 이해관계자의 참여를 통해 이루어지는데, 다음과 같은 점을 요소로 한다.

• 정부가 전문가 영역을 독점해서는 안 되며, 다른 이해관계자들도 가치 있는 정보를 가지고 있다는 점을 인식하고 그들의 수요와 전문적 의견을 피력하도록 촉진

1) 관련된 기존의 권고로는 The 2015 OECD Indicators of Regulatory Policy and Governance, The 2012 OECD Council Recommendation on Regulatory Policy and Governance, The 2008 OECD Guiding Principles for Regulatory Quality and Performance, OECD Best Practice Principles for Regulatory Policy, The APEC-OECD Integrated Checklist on Regulatory Reform이 있음.

- 정책과 서비스에 대한 대응성을 강화하고 유저 중심적 사고의 출발
- 모든 관련된 사람들이 참여할 수 있도록 하고 장애인 또는 소외계층 등에 대한 배려

– 이러한 열려있는 그리고 포용적인 정책은 혁신적인 아이디어와 새로운 input을 가능하게 하고 솔루션에 상응하는 문제에 대한 증거도 제공한다. 또한 정책과 서비스가 실제 수요를 반영할 수 있게 해주고, 정부에 대한 시민의 신뢰증진 및 사회적 응집력과 자본력을 강화한다.

○ 이해관계자의 참여가 주는 장점과 장애물

– 이해관계자는 규제 거버넌스 사이클의 모든 국면에서 통합적인 존재라고 할 수 있다. 이해관계자의 참여는 규제의 효율성과 효과성을 제고할 수 있으며 이를 통해 공공의 이익을 보호함과 동시에 불필요한 규제부담을 줄일 수 있다. 한편, 이해관계자는 규제성과와 규제모니터링에서도 핵심적인 존재이다. 이해관계자는 규제의 형성뿐만 아니라 규제의 평가과정에도 참여해야 한다.

– 이해관계자의 참여는 정부에게 가용할 수 있는 정보를 제공해 준다. 즉 규제의 개선을 위해서는 경험적 정보와 이를 분석한 결과가 필요하기 때문이다. 또한 이해관계자의 참여는 투명성의 수준도 제고한다.

– 이해관계자의 참여는 규제의 질을 제고한다. 정책토론에서 전문적 견해, 외부적 시각, 대안적 아이디어를 제공하고, 이를 통해 반대의견이 제시됨으로써 규제자가 균형을 유지할 수 있도록 해준다. 또한 의도하지 않았던 결과와 실제 현실에서의 문제점도 제시해주고 있다. 규제에 대해서는 규제편익분석이 이루어지는 바, 이러한 이해관계자들로부터의 정보는 해당 분석 중 질적 부문에서 활용이 가능하다.

– 이러한 장점에도 불구하고 이해관계자의 참여는 극복해야 할 몇 가지 장애물이 있다. 첫째, 조직화된 이해관계나 이익단체의 압력이 작용할 가능성이 있다. 둘째, 광범위한 사회 전 부문의 참여가 어려우며, 특정그룹의 의견이 전달되기 어려울 수 있다. 셋째,

이해관계자의 개입이 늦어질 경우 이미 결정이 상당히 진전되었고 변화의 가능성이 없을 수 있음. 결국 낮은 참여율을 보일 수 있다. 넷째, 너무 잦은 참여 – 특히 학문적 논쟁 또는 불충분하고 불정확한 계획들 그리고 정보들로 인해 '협의피로(consultation fatigue)'가 나타날 수 있다. 실제로 이해관계자들의 참여가 바라는 목표를 달성하기 위해서는 이러한 장애를 극복하는 것은 필수적이다.

○ 정부는 얼마나 열려있고 균형잡힌 협의를 할 것인가에 대해서 명확한 정책을 제시.

- 어떻게 이해관계자를 참여시킬 것인가를 명확히 해야 하며, 이해관계자의 참여를 통해서 얻을 수 있는 정책목표 역시 명확해야 한다. 이해관계자 참여에 대한 강력한 리더십이 발휘되어야 하며, 효과성과 효율성도 고려하여야 한다.
- 미국의 행정절차법(APA)에서 규정하고 있고 'notice and comment' 는 이해관계자 참여의 좋은 모델 중 하나이다. 모든 미국의 agency는 규제를 신설하거나 개선하는 입법을 할 때 이해관계자에게 알리고 의견을 수렴한다. 이러한 입법의 과정을 NPRM (Notice of Proposed Rulemaking)이라고 부르는데, 의견을 수렴하는 방식의 주요한 경로는 Federal Register이다.
- 유럽연합의 2015 Better Regulation Guidelines도 이해관계자의 참여를 규정하고 있으며, 회원국인 덴마크의 경우, 2012년부터 좋은 규제를 위해 비즈니스포럼을 개최하여 기업부문의 이해관계를 청취하고 반영하고 있다.
- 호주는 호주생산성위원회(Australian Productivity Commission)를 통해 공공설문제도(public inquiries)를 운영하고 있다. 이 제도는 호주의 경제적 성과나 공동체의 복지를 위해 중요한 정책이나 규제이슈에서 호주정부의 요청으로 해당 위원회가 공공설문을 실시한다.

○ 이해관계자의 참여는 해당 규제가 주는 중요성과 영향에 비례적으로 참여의 정도가 결정.

○ 이해관계자의 참여를 위해서는 이해관계자들에게 가장 관련되고 적시적인 정보가 제공되어야 하며, 이해관계자들이 자신들의 의견을 제출할 수 있도록 시간을 부여해야 한다. 그리고 이를 위해 명확한 시간 스케쥴을 제시해야 한다.

○ 정부는 이러한 이해관계자 참여정책을 정기적으로 평가해야 한다. 그리고 이러한 평가를 통해 보다 적합한 방법을 모색할 수 있다.

Ⅲ. 공공부문 최적관행

■ **유럽(집행)위원회의 최적관행을 위한 거버넌스 (European Court of Auditors, Governance at the European Commission best practices? 2016)**

○ 거버넌스와 책임성 체계(Government and Accountability Framework)

- 이해관계자는 의도하고 있는 결과를 정의를 해두고 이를 달성하기 위해 노력해야 하며, 이는 책임성과도 연결된다. 책임성은 거버넌스의 중요한 요소이다. 공공부문은 스스로의 의사결정에 책임을 져야 하며, 그 방식의 예로서, 공공펀드를 통해 지원을 할 경우 일종의 공적 스튜어트쉽((stewardship)을 발휘해야 하고, 성과를 측정하고, 적절한 형태의 외부감사를 받아야 한다.

○ 유럽위원회의 공공부문 개혁의 구조는 크게 3가지 축으로 나누어진다. 첫째, 우선목표의 설정과 예산의 투입, 둘째, 인력정책의 현대화, 셋째, 감사, 재무관리 및 통제의 개선이다. 전 유럽위원장이었던 프로디 개혁안의 3개 축은 공공부문 개혁의 출발점인데 이를 소개하면 다음과 같다.

〈프로디(전 집행위원장) 개혁안(White Paper)의 3개 축〉

축	정치적 우선순위의 설정과 재원의 배분	인력정책	감사, 재무관리 및 통제
목표	정치적 우선순위의 설정과 재원의 배분에 대한 보다 효과적인 방법의 모색	리쿠르트로부터 퇴직까지 현대화된 인력정책의 실시	재무관리, 효과성 및 책임성의 개선

출처 : European Court of Auditors(ECA) based on COM(2000) 200/final/2

- 이러한 프로디 개혁안을 축으로 하여 새로운 방안을 모색하는 것이 현재의 위원회의 개혁방안이다. 정치적 우선순위의 설정과 재원의 배분에 대해서 새로운 계획과 모니터링 수단의 개선을 지속적으로 추진한다.
- 재무관리, 통제 및 감사에 대해서 최적관행을 설립할 필요가 있다. 위원장에게 재무관리로부터 집행상황의 체크까지의 책임을 부여하고, 연간활동보고서에 각 부문별 수장이 적절한 내부통제시스템과 재원에 대해서 밝히도록 하고 있다. 각 부문은 별도의 감사시스템을 가지고 감사결과를 위원장에게 직접 보고한다. 한편, 각 업무의 담당자와 라인에 대해서 그 책임을 명확히 정의해줄 필요가 있다.

○ 공공부문의 최적관행을 위해서 감사위원회(Audit Committee) 또는 이와 동등한 기능을 가진 조직을 설치할 필요가 있다. 감사위원회는 운영 리스크를 관리하는 기구의 업무를 감사차원에서 지원할 수 있으며, 효과적인 통제환경을 유지하고 재무 그리고 비재무적 성과에 대해 보고를 실시한다.

- 감사위원회의 역할은 리스크 관리 및 내부통제의 적절성 및 효과성 개선지원, 굿 거버넌스(Good Governance)의 원칙과 그 원칙이 적용되는 것을 촉진, 내부통제 시스템의 지원, 외부통제기능의 수행, 건전한 내부통제와 리스크 관리에 대한 교육, 조직에 윤리적 거버넌스의 가치가 내재화 될 수 있도록 하는 기능 등이다.

○ 연차보고서는 투명성과 석명의무를 충족하는 주요한 수단이다. 연차보고서의 내용에 대해서 항목별로 다음과 같은 비교를 제시하였다. 유럽연합의 통합보고서, 공공기금으로서 유럽투자기금, 정책금융기관으로서 유럽투자은행을 상정하고 있으며, 대외비교를 위해 미국과 프랑스의 재무보고서를 함께 비교하였다.

〈일부 공공부문의 연차보고서[2]와 항목에 대한 개관〉

	EU 2014 통합계정 보고서	유럽투자기금 2015 연차보고서	유럽투자은행 2015 재무보고서	미국 2015 재무보고서	프랑스 2014 재무보고서
발생주의회계	O (공개)	O	O	O	O
주요지표요약	O	O	O	O	O
독립적 감사의견 제시	O	O	O	O	△(별도공개)
예산과 성과비교	O	△	△	O	O
거버넌스 구조와 이슈분석	요약본 공개	O	O	O	O
최고의사결정권자의 서문 또는 보고 메세지	△	O	△	O	△
비전형적 거래 또는 활동리스크	△	×	×	O	×
비전형성 수준의 측정	△	×	×	O	×
연 단위 활동에 대한 정보보고	△	O	O	O	O
장기예측과 지속가능성 보고	×	△	△	O	O
감사위원회의 결론	×	O	O	△	요약본

2) 제시된 연차보고서는 EU 2014 consolidated accounts, European Investment Fund 2015 Annual report, European Investment Bank 2015 Financial report, US 2015 Financial Report, Comptes de l'État 2014 (France) 임. 이하 표에서는 국문으로 표현.

Ⅲ. 공공부문 인력관리

■ **수준높은 행정서비스를 위한 공적영역 종사자(공무원 등)의 역할 (OECD, Engaging Public Employees for a High-Performing Civil Service, 2016)**

* 필자 주 : 최근 정부의 공공부문 일자리 창출과 관련하여 예산상 제약의 문제 및 해당 공무원의 역할 및 관리에 대한 논의가 있었다. OECD의 보고서는 이와 관련하여 일부 적절한 참고를 제공하고 있다.

○ 이행에서 성과로 : 최근의 동향과 공공채용의 제한요소

- 오늘날 공공행정은 증가하는 각 부문 간 연결, 관할을 넘어서는 현상, 예측 불가능한 행정환경에 노출되어 있다. 글로벌화, 기술진보, 고령화 그리고 가치변화의 상황에 직면하고 있으며, 이러한 빠른 변화는 조직과 인력에 대해 보다 유연하고 변화에 열려있기를 요구하고 있다.
- 인력, 급여의 축소, 채용동결, 연수정책의 축소, 단기근로, 임시적 해고, 인센티브 안식년 등의 조치를 통해 비용절감을 하는 방식이 있으나 이러한 방식은 인력을 단지 숫자와 비용으로 보는 시각으로 타당한 숫자와 받아들일 수 있는 비용을 찾는 것이 핵심관건이다.
- 과거와 달리 새로운 개혁적 노력은 공공직역 종사자의 동기와 헌신에 인력관리의 초점을 맞추고 있다. 따라서 얼마나 많은 사람이 투입되고 얼마나 많은 비용이 드는가가 아니라 어떤 사람이 어떤 능력으로 기여할 수 있고 그들이 최대의 성과를 낼 수 있는 방법이 무엇인지를 찾아내는데 주안을 두어야 한다.
- 증거기반적 개혁 전략을 마련해야 하며, 다양한 행정수요와 기대에 부응할 수 있는 방안이 모색되어야 한다. 그리고 여기에 고려되어야 하는 것이 효율성, 생산성, 공공부문의 혁신, 공공부문에 대한 시민의 신뢰, 각 공공기관별 리더십에 대한 소속 종사자들의 신뢰 등이다.

– 인사개혁을 위해서는 모든 공공부문 종사자들에 대한 서베이를 실시하여 이를 반영할 필요가 있다. 서베이의 결과 좋은 인사정책으로 평가받는 사례에서 공통적으로 찾아볼 수 있는 요소는 다음과 같다.

- 조직의 최고 리더십으로부터 명확한 정책 및 추진
- 소통의 향상 및 스태프들이 적극적으로 아이디어를 개진
- 각 단계별 담당자들 간 협력의 원활
- 전체적 그리고 미래지향적 인사정책, 전략과 수단의 존재

○ 예산제약, 비용절감조치와 행정서비스의 개혁

– 인사정책은 하나의 틀인바, 그 틀은 7가지 요소로 구성되어 있는데, 채용, 급여시스템, 연수시스템, 비용절감조치, 근로시간, 직업안정성, 고용의 형태가 있다.

– 단순히 비용측면에 집중한 다운사이징의 문제점을 지적하면 다음과 같다. (Box. 2.4. Responsible restructuring)

- 명확한 장단기 목표의 부재 /비용절감을 위한 선택적 노력의 부재
- 마지막 수단으로 다운사이징을 사용하기 보다는 최초 수단으로 다운사이징의 사용
- 선별적 다운사이징의 부재
- 공적 임무를 수행하는 방법의 변화에 대한 모색 부재
- 구조조정과정에 근로자의 관여부재
- 열려있고 진실된 소통부재
- 구조조정된 사람들에 대한 서투른 관리
- 다른 이해관계자들에 대한 영향 평가 무시
- 다운사이징에 대한 평가 부재

– 위와 같은 오류를 방지하기 위해서는 다음의 안이 제시될 수 있다. (Box.2.4. Responsible restructuring)

> • 남는 사람과 떠나는 사람을 고려하고 분석하는데 투자가 이루어져야 하며, 고객인 시민들에 대한 조직의 능력을 고려하여 다운사이징을 결정
> • 안정이 가져다주는 장점을 고려
> • 최종의사결정전에 소속 종사자들에게 정책내용 고지
> • 단기목표를 달성하기 위한 수단으로 다운사이징 사용 금지
> • 공정한 구조조정 / 구조조정 절차에 대한 정기적인 소통
> • 남는 사람들에게 왜 남았는지를 설명하고, 장래 새로운 인력고용의 이유 설명
> • 직원과 관리자에 대한 연수의 지속
> • 변화해야 한다는 관점에서 모든 인사정책에 대한 검토

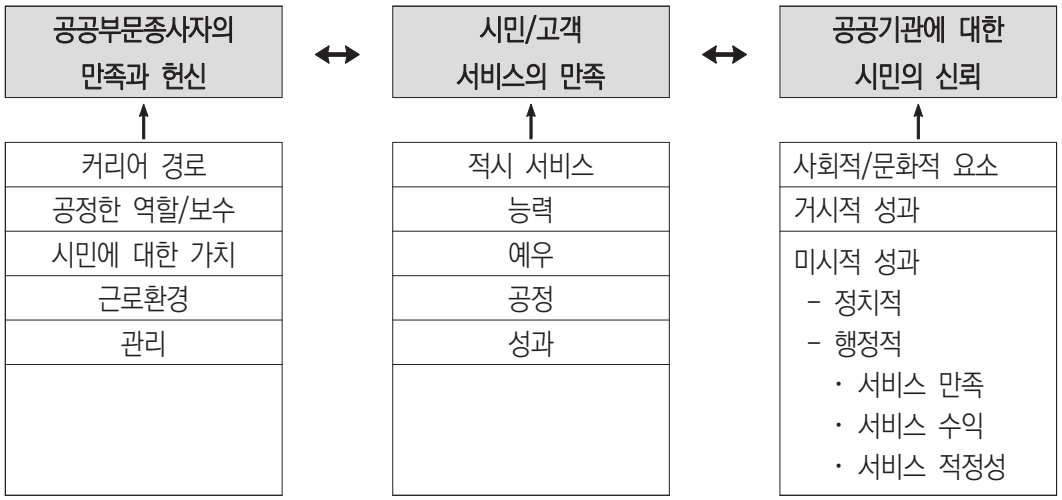
○ 혁신, 생산성 그리고 지속가능성 개혁에 대한 공공서비스의 연계

– 공공서비스 종사자들이 혁신과정에 직접 참여할 수 있도록 해야 한다. 당사자들이 혁신에 직접 참여할 경우, 그들 스스로가 아이디어를 직접 제공할 수 있다. 또한 피드백과 지원을 통해서 혁신에 대해 스스로 자기주도적이 될 수 있으며, 기존의 소모품적(burnout) 입장에서 보다 적극적으로 일할 수 있는 계기를 마련할 수 있다. 그리고 일과 가정 그리고 삶이 균형을 갖출 수 있도록 해야 혁신에 참여가 가능하다.

– 공공부문의 가치들은 공공서비스로 연계되는 체인구조를 이루고 있다. 표로 나타내면 다음과 같다.[3)]

3) 해당 보고서에서 제시하고 있는 표의 출처는 Heintzman, R. and B. Marson (2005), People, service, trust : is there a public sector service value chain, International Review of Administrative Sciences, Vol. 71, No. 4, pp. 549-575.

〈공공부문 가치사슬〉



Ⅳ. 디지털 정부

■ **유럽연합 전자정부 액션플랜 2016–2020 – 정부의 디지털변환을 촉진하기 위하여 (EU eGovernment Action Plan 2016–2020 – Accelerating the digital transformation of government[4])**

* 필자 주 : 디지털 정부는 기존의 전자정부를 뛰어넘어 디지털 기술을 통한 행정의 효율성, 규제의 스마트화 그리고 시민의 역동적 참여와 평가가 통합적으로 이루어지는 구조이다. 제4차 산업혁명과 관련하여 신기술들이 속속 개발되고 있으며, 이는 공공부문의 변화를 가져올 것으로 예상되어 해당 주제를 소개한다.

○ 전자정부를 통하여 효율성과 효과성을 제고하고 상시적으로 공공서비스의 향상을 목표로 하고 있다. 2020년까지 유럽연합의 행정기구와 공적기관들은 개방적이고, 효율적이며, 포용적이고, 경계가 없이 사용자 친화적인 디지털 서비스를 제공할 것을 목표로 하고 있다.

4) COM(2016) 179 final, 2016.4.19

- 행정기구 간 또는 행정기구 안에서 그리고 경계를 넘어선 데이터 공개와 서비스는 사업과 시민의 자유로운 이동을 촉진하고 효율을 증진한다.

○ 액션플랜은 몇 가지 전제가 되는 기본적인 원칙들을 가지고 있다. 이를 소개하면 다음과 같다.

- 원칙으로서 디지털로서 우선적으로 고려되는 옵션으로서 행정서비스의 디지털화(과거 디지털화는 대안 내지는 선택의 영역이었음)이다.
- 원칙으로서 '단 한번'('once-only')은 행정청이 시민과 기업으로부터 단 한번 정보 제공을 받고 정부내에서 공유하도록 하는 것을 의미한다. 과거 우리의 경우도 각기 다른 기관에서 같은 보고서를 중복하여 제출하도록 함으로써 규제부담이 늘었던 경험이 있다.
- 포용성과 접근성으로 공공행정은 디지털 공공서비스를 디자인해야 하는데, 이때 원칙으로 포용성을 고려해야 하며, 노령층과 장애인 등 각각의 다른 수요를 가진 사람들을 배려해야 한다.
- 개방성과 투명성으로 행정청 간에는 정보와 데이터를 공유해야 하며, 시민과 기업이 자신의 데이터를 통제하고 수정할 수 있도록 해야 한다. 아울러 사용자들이 그들과 관련된 행정절차를 모니터링할 수 있도록 해야 한다.
- 탈경계로서 행정청은 관련된 디지털 서비스를 경계를 넘어서 제공해야 한다. 오늘날은 지역적 경계뿐만 아니라 업무영역 간에도 경계가 사라지고 있으므로 종적 및 횡적으로 통합된 서비스가 필요하다.
- 호환성: 공공서비스는 단일시장 내에서 동일한 기준으로 적용되어야 한다.
- 신뢰성과 보안 : 모든 이니시어티브는 법적 체계 내에서 개인정보 및 프라이버시 보호 그리고 IT보안과 관련한 법적 프레임을 갖춘 컴플라이언스 체계를 갖추어야 하며, 이는 디지털서비스에서 신뢰를 제고하는 중요한 전제조건이라고 할 수 있다.

〈유럽연합의 전자정부의 디지털변환 추진계획 로드맵〉

유럽위원회(Commission)은 아래와 같은 사항을 추진할 계획임	목표년
1. 회원국이 완전한 전자조달과 전자계약등록을 할 수 있도록 지원	2019
2. 전자ID와 전자서명을 포함한 전자신원확인·인증·신용서비스(eIDAS : electronic Identification, Authentication and trust Service)의 촉진	2016
3. 국경 간 디지털 서비스의 장기적 지속가능성의 확보	2018
4. 유럽 호환성프레임(Interoperability Framework)의 개선 및 이를 지원할 수 있는 회원국 행정의 확보	2016-2019
5. 공공조달을 위한 ICT 표준의 유럽판 카탈로그의 원형을 개발하기 위한 협력	2017
6. 행정의 원칙으로서의 디지털('digital by default') 원칙과 절차의 간소화를 위한 오직 한번('once-only')의 원칙을 공유	2016-2019
7. Single Digital Gateway를 위한 제안의 제출	2017
8. 유럽 전자사법포털(e-Justice Portal)을 만들어 법적 이슈에 대한 정보의 제공	2016
9. 회원국의 기업 등록에 대해 강제적 연결	2017
10. 파산정보에 대한 전자연결시스템 구축	2019
11. 기업의 라이프 사이클을 고려한 디지털 솔루션의 활용 촉진	2017
12. 부가가치세의 지불과 등록을 위한 단일 전자메커니즘의 확대를 위한 법적근거마련	2016
13. 기업부문에 'Once Only' 원칙의 적용을 위한 파일럿 프로그램의 실시	2016
14. 해상운송과 디지털화된 전자문서의 보고를 위한 단일 창구의 설치	2018
15. 사회안전(Social Security)정보의 전자적 교환시스템의 설치	2019
16. 직업이동성(Job Mobility) 포털의 개발	2017
17. 국경 간 전자의료서비스의 개발	2016-2018
18. 국경 간 활동에 있어서 시민을 위한 'once-only' 원칙의 적용가능성 평가	2019
19. INSPIRE(European Spatial Data Infrastructure) 지침 데이터 인프라의 구축과 배치	2018

■ **유럽연합 개인정보보호규칙(General Data Protection Regulation, 2016/679, GDPR)**

○ 제정 및 시행일자 : 2016년 5월 제정, 2018년 5월 시행예정이다.

○ 제정목적 : 자연인의 개인정보를 보호하고, 유럽연합 내에서의 개인정보의 자유로운 이동 보장 목적으로 한다.

○ 주요특징

- 연합의 개인정보보호에 대해서는 기존에는 지침(Directive)의 형태로 규율하였으나 금번에는 규칙(Regulation)의 형식으로 제정함으로써 각 개별 회원국가의 변용과정이 불필요하며, 연합 내에서의 개인정보보호규제수준을 통일적으로 직접 규정하고 있다.[5)]
- 규칙은 정보주체의 개인정보 사용방식에 대한 통제권을 강화하는데 주안을 두고 있다. 규칙의 배경에는 개인정보를 자산으로 인식하고 적극적으로 활용하되, 활용을 하는 자에게 엄격한 책임을 부담하게 함으로써 활용하되, 책임이 있는 개인정보체계를 구축하려는 입법적 의도가 있다.

○ 개념의 분류

- 개인정보를 식별되었거나 식별할 수 있는 자연인에 관한 모든 정보로 개념정의하고 있다. 규칙은 민감정보라는 별도의 개념을 정의하고 강화된 규제수준을 도입. 민감정보는 인종, 민족, 정치적 견해, 종교, 신념, 노조가입여부, 생체정보, 건강, 성관련 정보를 의미하며. 해당 정보에 대해서는 원칙적으로 정보주체의 명시적 동의 없이 처리를 금지하고 있다. (제9조 1)

5) 지침은 규율대상에 대한 대강의 외연적 입법을 연합차원에서 하고, 구체적인 사항은 회원국이 입법을 통해 구현. 적용방식은 회원국의 입법을 통해 적용. 그러나 규칙은 모든 사항을 연합이 정함에 따라 회원국의 입법이 불필요하며, 규칙이 모든 유럽시민에게 직접 적용

○ 규칙의 주요구성은 다음과 같다.

장	내용
제1장	일반규정
제2장	원칙
제3장	정보주체의 권리
제4장	통제자(컨트롤러)와 개인정보취급자(프로세서)
제5장	제3국 및 국제기구로의 개인정보 이전
제6장	독립적 감독기구
제7장	협력 및 일관성
제8장	구제제도, 책임, 제재
제9장	특정 정보처리 상황에 대한 규정
제10장	위임법과 이행법
제11장	최종규정

○ 정보주체의 권리를 다음과 같이 규정하고 있다.

– 정보를 제공받을 권리, 정보를 열람할 권리, 정보를 정정할 권리, 잊힐 권리, 정보처리를 제한할 권리, 개인정보이동권, 프로파일링 권리, 기타 관련 조치에 반대할 권리 등(제13조 내지 제22조)

○ 컨트롤러(controller)는 개인정보 처리의 목적과 수단을 정하는 주체이며, 자연인, 공공기관, 에이전시, 기타 단체 등이 컨트롤러가 될 수 있다. 그리고 프로세서는 컨트롤러의 지시에 따라 개인정보를 처리하는 자를 말한다. (제4조 (7), (8))

○ 개인정보 활용 기업의 의무으로서, 개인정보처리활동의 기록(종업원 수 250명 이상 기업이 대상)(제30조), 적정한 기술적·조직적 조치(제25조), 개인정보영향평가(제35조), 행동강령 및 인증제도를 실시할 것을 권장(제40조)하고 있다.

○ 과징금의 부과

- 과징금의 최대 상한은 전 세계 연간매출액 4% 또는 2천만 유로 중 높은 금액이다. 한편 전 세계 연간매출액 2% 또는 1천만 유로 중 높은 금액이 부과되는 경우가 있는 바, 그 대상은 컨트롤러 또는 프로세서의 의무위반, 인증기관 의무위반, 모니터링 기구의 의무위반, 감독기구가 내린 명령 또는 정보처리의 임시적 또는 확정적 제한 위반, 위법한 개인정보이동 등이다.

■ 복지영역에서 공공서비스의 변화를 위한 디지털 정부 전략(OECD, Digital Government Strategies for Transforming Public Services in the Welfare Areas, 2016)

* 필자 주 : 복지는 현대국가에서 가장 중요한 국가임무 중 하나이다. 우리나라도 재정과 행정소요의 상당부분이 복지에 투입되고 있다. 따라서 복지 역시 새로운 기술사회의 추세에 따라 디지털 기술을 활용하여 효율성과 편리성을 제고해야 할 필요가 있어 해당 논의를 선정하여 소개하였다.

○ 디지털 변환은 정보 및 통신기술이 공공서비스에 적용되는 것을 의미하며 정부에서는 행정의 디지털화 그리고 전자정부 더 나아가 디지털 정부로 변화하게 된다. 즉, 디지털 정부는 현재까지로는 공공부문 디지털화의 마지막 단계라고 할 수 있다.

- 디지털 및 통신기술은 정부의 활동과 데이터/정보관리 능력을 향상시키게 되며 이를 통해 복지서비스에서의 효율성과 생산력을 증가시키게 된다. 디지털화는 표준화 프로세스를 통해 정부의 행정자체 및 시민에 대한 직접서비스에서 비용을 절감하는 효과를 가져온다.

○ 복지에서의 공공영역 간 경계에도 변화가 있다. 정치적 위임(mandate)은 보다 정밀한 업무의 우선순위와 서비스 수준을 가지고 있으며, 공급자의 입장에서는 핵심적 능력과 업무수행 전략을 제고한다. 반면, 사용자의 입장에서는 서비스의 최적가치를 구현하기 위해 사용자의 관여가 증가하고 있다. 그리고 행정의 파트너십의 입장에서는 민간과 공공의 통합적 인센티브의 혁신적 이용이 새로운 변화의 트랜드로 나타나고 있다.

○ 정책입안자들은 디지털 기술을 활용하여 효율성과 생산성을 증가시키고 서비스의 질을 제고시킬 수 있다. 서비스의 질은 적시성, 대응성 그리고 개인화된 서비스를 의미한다. 그러나 이러한 과정에서 정책입안자들은 각기 다른 이해관계자들의 이익 간 균형을 맞추어야 하는 딜레마에 빠질 수 있다.

- 프라이버시와 개방성(openness)간 균형 : 공공서비스의 혁신정책은 적절한 정보보안 및 프라이버시 보호와 개인정보를 활용하여 개인화된 맞춤서비스의 제공이라는 두 개의 목표사이에서 딜레마에 빠질 수 있다. 즉, 관련된 복지를 통합하여 맞춤형으로 제공하기 위해서는 각 영역을 넘어선 개인정보의 공유가 이루어져야 하는데 이는 프라이버시 보호와 상충관계(trade-off)관계를 형성한다.
- 디지털화의 속도(pace) : 얼마나 빨리 디지털화를 시킬 것인가도 고려해야 하는 이슈이다. 정부부문에서 디지털화를 너무 빨리 실시할 경우 시민들은 준비가 안 된 채 디지털화된 복지서비스를 수용해야 한다. 따라서 정부는 정책목표에 부합한 디지털화와 시민의 변화 수용성간 균형을 찾아야 한다. 디지털 정부는 정부의 목표가 될 수 있으나 시민에 대한 서비스의 경우 시민의 수용가능성이 있어야 하므로 반드시 빠른 조기 디지털화가 바람직한 것은 아니다.

〈디지털 변환의 요소(The element of digital transformation)〉

	정보와 통신기술		
	디지털화	전자정부 (E-government)	디지털정부 (Digital Government)
변화경로	• 범정부적 활동과 데이터/정보관리의 향상을 위한 디지털기술의 활용	• 보다 나은 정부를 위해 디지털 기술을 사용하며, 특히 인터넷의 사용이 중심	• 디지털기술과 사용자 선호를 통합. 새로운 공공가치의 창출을 위한 정부현대화의 일부
	• 효율과 생산성 향상 중심	• 개인별 맞춤형 서비스에서 효율성과 생산성 향상	• 효율성과 생산성에 거버넌스, 개방성, 투명성, 연계성을 추가하여 지향
	• 정부중심적. 사용자는 서비스의 수동적 수혜자	• 사용자와 시민 중심적. 사용자는 복지서비스의 제공에 참여.	• 사람 지향적 서비스로서 수요 지향적.

	공공서비스		
직접 행정서비스 제공을 돕는 행정기관의 내부적 활동과 행정서비스의 내부적 핵심기능	• 정부의 내부프로세스 개선 • 직접 행정서비스의 전달을 지원하는 내부프로세스의 개선	• 내부 프로세스의 혁신적 변화 • 서비스 전달체계의 혁신	• 내부프로세스의 변환 • 서비스 디자인과 전달 체계의 변환
직접행정서비스로서 시민복지 제공과 공공정책의 성과 지원	• 개인 데이터베이스와 정보시스템 • 표준화된 서비스 전달체계 • 표준화된 서비스	• IT 시스템과 데이터베이스 통합 • 시스템 간 조화	• 데이터공유 : 데이터와 정보/클라우드/데이터분석 • 정보공유와 서비스 그리고 조화지원을 위한 ICT 플랫폼의 채택 • 개인이 수요에 부응한 맞춤형 혁신적 서비스/ 유비쿼터스 서비스 (모바일 정부)

○ OECD는 디지털 정부전략에 대해 다음과 같이 권고하고 있다.[6)]

– 공공신뢰의 유지를 위한 시민의 참여와 열린 정부가 필요하다. 그 구성요소를 살펴보면 다음과 같다.

- 정부프로세스와 운영에서 투명성, 개방성 그리고 포용성을 확보
- 공공, 민간 그리고 시민사회의 이해관계들이 정책의 형성과 공공서비스개발 및 서비스 전달체계에 참여할 수 있도록 촉진
- 공공부분에서 데이터 중심의 문화 정착

6) OECD, Digital government strategies for transforming public services in the welfare areas, 2016, p. 54, Box 7. OECD Recommendation of the council on digital government strategies. 이 전략은 2014년에 OECD에서 이미 발표한 바 있음.

– 보다 좋은 결과와 조화(Collaboration)를 위한 거버넌스 개선이 필요하다.

- 디지털 보완과 프라이버시 이슈를 해결할 수 있는 리스크 관리를 반영. 이를 위해 효과적이고 적절한 보안조치를 채택해야 하며 이를 통해 정부서비스에 대한 신뢰를 제고할 수 있음.
- 디지털 전략에 대한 리더십과 정치적 관심을 확보. 이를 위해 디지털 정부전략에 대한 장관급의 협력 체제를 촉진하고 관련 기관 그리고 지방자치단체와의 협력 체제를 장려.
- 중앙정부와 지방자치단체를 그리고 정책영역을 관통하는 관련 디지털 기술의 활용
- 효과적인 조직적 프레임웍과 거버넌스 프레임웍을 확보함으로서 디지털 정부전략의 수행에 있어서 협력체제 유지
- 국가 간 협력의 강화

– ICT 투자의 성과(return)를 달성하기 위한 능력 강화가 필요하다.

- 재원확보를 유지할 수 있는 명확한 사업사례들을 개발하고 디지털 기술 프로젝트의 이행에 포커스를 맞춤.
- 프로젝트의 이행에 대한 모니터링 및 관리를 위한 제도적 능력의 확보
- 디지털 스킬, 직무 프로파일, 기술, 계약, 내부기관 간 협약 등 현존하는 자산의 평가를 기초로 한 디지털 기술의 채택. 이를 통해 효율성을 제고하고 혁신을 지원.
- 일반적 그리고 분야별 특정한 법적 그리고 규제적 프레임웍을 확보

○ 디지털 전략을 수행하기 위해 의사결정권자가 확인해야 할 체크리스트로는 다음을 들 수 있다.

- 거버넌스 프레임웍의 명확화
- 명확한 장기비전
- 프로젝트를 이행할 능력을 갖춘 팀
- 베타테스트 혹은 파일럿 프로그램을 통한 실험

- 견조한 사업사례 개발
- 사용자그룹으로부터의 주요한 코멘트를 받아 반영
- 시작단계부터 공무원들과 공동 수행
- 분야별 전문가 그룹의 참여
- 지방자치단체의 참여
- 소통네트워크의 형성
- 지식과 경험의 공유
- 좋은 복지정책을 지원하기 위한 증거의 확보와 이용 가능한 데이터의 이용
- 프로젝트 수행 자료의 정리
- 영향지수를 포함 명확한 평가체계의 채택

■ 중국 사이버안전 규제 - 네트워크안전법(中华人民共和国网络安全法) 제정

○ 네트워크안전법은 중국의 네트워크 안전보장, 네트워크 공간 간 주권과 국가안전, 사회공공이익 수호, 공민과 법인 기타 조직의 권익보호, 경제사회 정보화발전을 촉진하는 것을 목적으로 한다. 중국의 전자상거래 및 전자금융은 매우 빠른 속도로 성장하고 있으나, 외형적 성장에 비해 사이버보안에 대한 인프라는 부족하다. 따라서 이를 보완하기 위하여 네트워크안전법을 제정하였다. 2016년 11월 7일 제12기 전인대 상무회의 24차 상무회의에서 제정을 하였고, 2017년 6월 1일부터 시행 중이다.

- 네트워크안전법을 통하여 네트워크 안전과 관련한 영업의 진입규제, 행위규제, 국가의 의무, 제재의 대상 및 수준 등을 규정하고 있다.

○ 주요구성을 살펴보면, 총 7장 79조로 구성되어 있다. 제1장은 총칙, 제2장은 네트워크 안전지원 및 촉진, 제3장은 네트워크 운영안전, 제4장은 네트워크 정보안전, 제5장은 모니터링 조기경보 및 응급대처, 제6장은 법적책임, 제7장 부칙이다.

○ 네트워크 운영자는 정보보호조치 수립, 관리하고 있는 개인정보 유출시 즉시 조치를 실시하고 사용자 및 감독당국에 보고(제40조, 제42조). 네트워크 안전과 관련한 민원을 적시에 수리 및 처리(제49조)의 책임을 진다.

○ 국가적 네트워크 안전시스템의 설계에 대해서는 네트워크안전에 대한 조기경보체제의 구축(제51조, 제52조), 네트워크 안전위험평가 및 응급조치훈련의 실시(제53조), 안전사고 발생 시 적시에 시민들에게 주의 공지(제55조) 조항을 두고 있다. 한편, 네트워크안전등급보호제도의 실시를 실시하고 있는 바, 그 구체적 내용으로 국가표준 및 업종표준을 제정(제15조), 네트워크 안전책임자 지정, 네트워크보호를 위한 기술조치, 데이터 분류 및 암호화를 두고 있다. 중요시설 또는 특정 분야에 대한 보호를 강화하고 있는 바, 통신, 정보서비스, 금융, 공공서비스, 전자정부 등 중요영역에 대해서는 보호수준 강화 및 중점보호(제31조) 조치를 하고 있다.

○ 중국 내에서 영업을 영위하던 중 취득한 개인정보와 중요데이터는 국내보관이 원칙이나, 단, 업무적 필요로 인해 국외제공이 필요한 경우에는 안전평가를 거쳐야 한다.

○ 네트워크시스템 운영자가 네트워크안전법에 부여된, 인프라 구비의무, 리스크 평가 등 의무를 이행하지 않은 경우, 의도적으로 악성프로그램을 설치하여 네트워크의 안전을 침해 한 경우, 타인의 네트워크에 불법적으로 침입하여 데이터를 절취하거나 이를 방조한 경우 등에 대해서는 각각의 처벌수위를 달리하여 과태료에서부터 형사처벌까지 제재를 정해두고 있다.

Ⅴ. RegTech

■ **영국 금융행위규제원(FCA : Financial Conduct Authority)의 RegTech (FCA Supporting the development and adoption of RegTech, Call for Input, Nov. 2015)**

○ RegTech에 대해서는 아직 OECD 등 국제기구차원에서의 권고는 없다. 다만 핀테크와 관련하여 금융 선진국들에서 RegTech에 대한 논의가 이루고지고 있음을 확인할 수 있었다. 그 중 가장 적극적인 입장을 보이고 있는 국가는 영국으로, 영국 FCA의 사례를 검토하였다.

- RegTech는 금융분야에서 시작했지만 금융에 국한되는 사항은 아니며 규제전반에서 활용성이 매우 높다.

○ 금융위기 이후 감독당국은 새로운 금융규제기준을 맞추기 위하여 금융기관에 대해 많은 양의 보고서 제출을 요구하고 있다. 아울러 보고서의 적시보고의무도 부과하고 있어 기업들의 보고부담이 커지고 있다. 따라서 감독당국과 기업 모두 이러한 규제조치를 보다 효율적으로 운영하기 위하여 혁신적 기술을 활용할 필요성을 느끼고 있다. 그리고 새로운 기술의 활용은 기업의 입장에서 감독당국의 규제요구에 보다 잘 부응하고 규제비용 역시 절감할 수 있는 장점이 있다.

○ RegTech와 관련하여 몇 가지 활용 가능한 기술적 요소로는 다음을 들 수 있다.

- 컴플라이언스와 리스크 평가기능이 내재화된 실시간 시스템으로 컴플라이언스와 리스크 기술이 금융회사 사무운영의 효율성 및 효과성을 제고할 수 있다. 예컨대, 거래감시, 금융범죄리스크 모니터링, 돈세탁방지, 고객프로파일링과 행위 리스크 모니터링에 활용이 가능하다.

– 빅데이터 기술도 활용성이 높으며, 비쥬얼화와 로보툴도 유용하다. 온라인상에서 비쥬얼화와 로보어드바이스 툴은 보다 낮은 가격으로 효율적, 효과적인 전달체계를 제공할 수 있도록 해준다. 그리고 이러한 기술은 금융회사들이 규제와 이에 대한 책임을 보다 잘 이해하는데 활용될 수 있다.

– 소프트웨어통합툴로서, 개별 금융회사의 소프트웨어와 감독당국의 소프트웨어 간 통합을 통해 직접 규제보고 시스템을 연결한다. 이를 통해 별도로 수작업을 하지 않더라도 보고서의 정확성은 제고할 수 있으며, 반면, 기업의 규제이행비용은 감소한다. 이외에 클라우드 기술도 활용분야이다.

○ RegTech의 개발과 활용을 위해서 다음의 질문을 던져볼 필요가 있는데, 이는 FCA가 RegTech의 본격적인 활용을 위해 금융회사들에게 보낸 설문의 내용이기도 하다.

- 어떤 RegTech가 금융회사와 감독당국 간 보다 낮은 비용 및 행정부담을 주면서 보다 쉽게 연결해 줄 수 있는가 ?
- FCA가 RegTech의 개발과 적용을 위해 무슨 역할을 해야 하고 무슨 방법이 가장 적합한 것인가 ?
- RegTech의 적용과 혁신에 장애가 되는 특정한 규제룰(regulatory rule)과 또는 정책이 있는가 ?
- RegTech의 적용과 혁신을 위해 도입이 필요한 특정하나 규제룰과 정책이 있는가 ?
- 현재 있는 규제컴플라이언스 또는 규제보고사항 중 어느 분야가 RegTech의 가장 이익을 볼 수 있을 것인가 ?

* 필자 주 : 기술기반적 재화 및 서비스의 제공은 복잡성을 특징으로 함에 따라 규제요소가 증가하고 있다. 신기술산업에서 규제완화는 대체적인 흐름이다. 그리고 규제수요와 규제완화의 중간적 역할을 해주는 것이 RegTech라고 할 수 있다. 최근 각국은 기술변화에 능동적으로 대응하고 규제효율성을 높이기 위해 순수 자율규제 또는 규제된 자율규제를 적극 활용하고 있다. RegTech는 자율규제와 기업내부의 컴플라이언스 감독당국의 규제를 연계하는 효율적 기제로 작동할 수 있다.

■ **호주 증권투자위원회(ASIC)의 RegTech 정책[7)]**

○ RegTech의 정의와 의미

– 호주 증권투자위원회(ASIC : Australian Securities and Investment Commission Act)는 RegTech를 "규제 및 컴플라이언스의 요구사항을 효과적으로 해결하기 위한 새로운 기술의 사용"으로 정의하고 있다. 증권투자위원회는 RegTech를 통해 관련 산업과 커뮤니케이션을 확대하고 이를 통해 규제시간과 비용을 절감할 수 있을 것으로 기대하고 적극적인 행보를 보이고 있다.

○ RegTech의 활용분야

– RegTech가 활용될 수 있는 금융규제분야로는 고객확인의무를 포함한 고객신분확인, 거래분석을 통한 거래사기방지, 돈세탁방지, 내부 컴플라이언스 중 자동화 가능한 부분(컴플라이언스 데이터의 수집 및 분석), 모니터링 및 이상징후 경고 등이 있다.

– 증권투자위원회는 RegTech의 적극적인 활용뿐만 아니라 관련 산업 자체를 육성할 계획을 가지고 있다. 즉, 단순히 감독조치의 일환으로 RegTech를 활용하는 것에서 벗어나 산업을 육성하려는 것으로 규제를 대하는 새로운 발상으로 받아들여지고 있다.

■ **RegTech 적용가능 기술 (금융보안원, 금융규제 이행을 위한 RegTech의 필요성 및 향후과제, 보안연구부 2017-008, 2017.3.13.)**

○ 금융보안원에서 발간한 보고서에 따르면 다음의 사항을 RegTech에 활용할 주요 기술로 보고 있는 바, 활용기술에 대한 예시는 RegTech를 실제 활용하는데 중요한 요소라는 점에서 소개한다.

7) http://asic.gov.au/for-business/your-business/innovation-hub/regtech/(2017.9.30. 방문)

주요기술	세부내용
Data Mining	Machine Learning 기반의 데이터 마이닝 기술을 통해 대량의 비정형데이터를 분석하고 이를 통해 의심스러운 거래를 적발하고 내부통제 등에 활용
Machine Learning	분석된 데이터를 바탕으로 위험을 예측하고 실시간 거래 감시 등에 활용
Robotics	로봇을 통해 데이터 전송 및 저장 등 IT 프로세스를 자동제어
Cloud Computing	실시간 리스크 관리, 위험분석 등 고성능의 컴퓨팅 인프라가 필요한 경우 클라우드 컴퓨팅을 활용
Biometrics	지문, 홍채 등 바이오인증 기술을 결합하여 신원 확인
Visual Analytics	분석된 대용량 데이터를 이해하기 쉽게 효율적으로 시각화하여 탐색 및 보고
Blockchain	규제준수관련 문서 송부, 저장 등에 블록체인을 활용함으로써 추적, 감사기능을 제공

출처 : 금융보안원, 금융규제 이행을 위한 RegTech의 필요성 및 향후과제, 보안연구부 2017-008, 2017.3.13.

○ RegTech와 관련하여 2016년 9월부터 홍콩 증권선물위원회는 금융데이터 분석업무를 위한 RegTech 파일럿 프로그램을 진행 중이며, 싱가포르 통화청은 2016년 5월에 도입한 규제샌드박스와 RegTech를 연계하기 위해 포럼 등을 개최[8]하는 등 금융산업과 관련하여 금융이 발달한 국가를 중심으로 RegTech논의가 활발하게 이루어지고 있다.

■ **UNCTAD의 RegTech(UNCTAD Multi-year Expert Meeting on Trade, Service and Development, Geneva 18-20, July 2017 발표자료 - Fintech Inclusion, Fintech, and RegTech)[9]**

8) 금융보안원, 전게자료, 10면

9) 당시 회의의 3세션 자료로서 Zürich 대학교 법과대학의 교수이면서 영국 캠프리지대학교 리스크연구센터에 소속되어 있는 Kern Alexander 교수의 발표 ppt임.

○ RegTech의 의의

– RegTech는 혁신적인 기술과 규제 간 연결로서 금융서비스를 포함한 산업을 관통하는 규제요구를 해결하기 위한 것으로 보고 있다. 따라서 규제와 컴플라이언스가 있는 모든 사업영역에서 RegTech 솔루션은 적용이 가능하다.

– RegTech를 위한 툴과 기술(Tools and techniques for RegTech)을 소개하면 다음과 같다.[10)]

- 빅데이터 어플리케이션과 기술
- 데이터 마이닝과 고급 분석 툴
- 비쥬얼화 툴
- 생체인식과 소셜미디어 분석
- 실시간 그리고 시스템 내재적 컴플라이언스와 리스크 평가 툴
- 소프트웨어 통합 툴
- 예측 코딩(coding)
- 열린 플랫폼과 네트워크

○ 규제기관들의 RegTech 사용의지도 매우 높음. 대표적인 예로 영국의 금융행위규제원을 들 수 있다. 영국 금융행위규제원은 보다 좋은 규제를 위해서 새로운 기술에 대해 지식을 공유하고 대화하며 조화를 이루는 활동을 장려하겠다고 발표한 바 있다. 금융행위규제원은 금융소비자보호 업무가 주된 업무로서 금융소비자보호부문에서 보다 효과적인 경쟁을 촉진하기 위하여 RegTech를 사용하고 있으며, 특히 컴플라이언스 부문에서 RegTech 활용노력이 가시적으로 나타나고 있다. – "우리는 컴플라이언스가 진입장벽이 되기를 원치 않는다."

○ RegTech가 극복해야 할 과제도 있다. RegTech가 활성화되기 위해서는 기밀성, 보안성, 유지보수, 안정성, 데이터 질이 확보되어야 한다. 특히 암호와 보안기술이 뒷받침되어야 한다. 또한 기술적 규제시스템의 안정성도 장기적인 RegTech의 발전에

10) Kern Alexander 교수가 BBVA Research의 Digital Economy Outlook, Feb. 2016을 인용.

중요하다. 기술규제가 수시로 변할 경우 지속적 규제기술 개발이 어려우며, 이를 채택한 규제체제도 영향을 받게 되기 때문이다.

- 보안성 및 기밀성 확보를 위해서 블록체인 기술의 활용이 가능(RegTech와 Blockchain의 접점)하며, 규제자도 참여하는 블록체인을 통해 데이터 보고서 등을 규제자에게 자동으로 제출하도록 한다. 그러나 이러한 체제는 정보의 완전한 투명성, 직접성, 즉시성도 아울러 확보해야 한다.

○ AI와 Machine Learning을 통한 규제변화의 자동적 적용 가능성이 있다. 로봇을 통한 일상적 컴플라이언스의 수행과 복잡한 규제절차에 대한 대체물로서 '스마트계약(smart contract : 기술과 규제상황을 종합적으로 고려한 규제계약)' 의 활용가능성도 검토 필요가 있다.

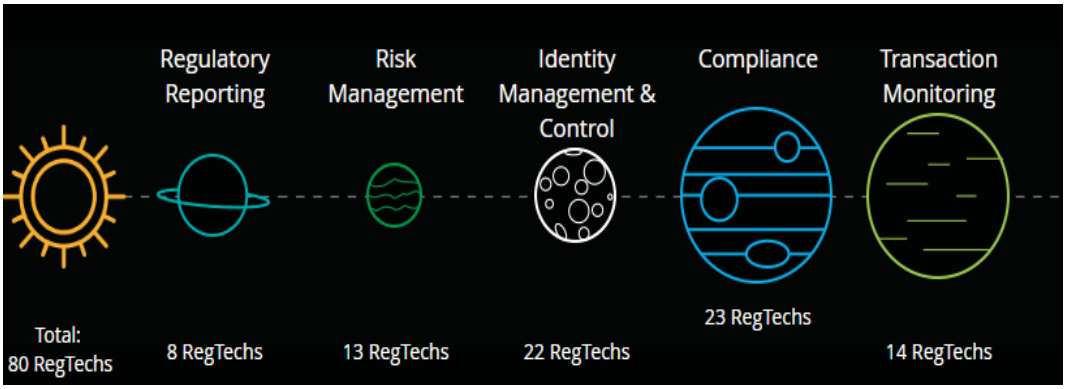
■ Deloitte RegTech Universe[11)]

○ 세계적인 컨설팅 그룹인 딜로이트(Deloitte)는 딜로이트 RegTech Universe라는 도식을 만들어 RegTech의 분야별 적용기술을 설명하고 있다. 이는 주로 기술과 활용에 대한 사항으로 실제 RegTech 기술이 어느 정도까지 왔고, 규제와 관련하여 구체적으로 어디에 활용되고 있는지를 보여주고 있다.

- RegTech Universe는 개념에 그치고 있는 RegTech 기술이 실제로 어떻게 구현이 되고 있는가를 잘 보여주고 있다. 각각의 기술이 이미 상용화 서비스되고 있으며, 각 기술들은 대상 법령상의 규제요건을 반영하여 솔루션 또는 서비스를 제공하고 있다.

  * 필자 주 : RegTech의 구현현황은 향후 우리가 RegTech에 대한 정책구현과 규제설계에서 참고할 만한 사항이다. 향후 연구에서는 관련 법령에서 요구하고 있는 규제의 내용 및 보고서를 분석하여 해당 솔루션과 대응시켜볼 필요가 있다. 더 나아가 RegTech를 통해 얻어진 정보를 기반으로 행정청이 자동의사결정을 하는 것도 고려해 볼 수 있다. 법리적으로는 행정의 자동화결정 법리가 적용될 수 있다.

11) https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html(2017.9.2. 방문)



- 전체 152가지 적용기술이 있는데 규제보고단계에서는 20가지 기술, 리스크 관리에서는 27가지 기술, 신원관리 및 통제에는 39가지 기술, 컴플라이언스에는 40가지 기술 그리고 거래 모니터링에는 19가지 기술이 사용될 있는 것으로 분류하고 있다. 이들 기술은 각각의 회사가 가지고 있는 기술을 의미한다.

○ 규제보고 및 컴플라이언스 분야에 대한 기술동향을 정리하면 다음과 같다.

- 유니버스에는 이외에 리스크 관리, 신원관리 및 통제 등 다양한 분야들도 있지만 규제와 직접 관련성이 있는 분야만을 소개하였다.
- 규제보고(Regulatory reporting)는 관련 법령에 의해 해당 기업에게 거래 및 자산현황 등 보고의무를 부여하고 있는 경우 웹 또는 클라우드를 통해 감독당국의 시스템과 연결하여 자동화된 규제보고시스템을 운영하는 것을 의미한다.

〈규제보고〉

회사명	국가	기술
28MSEC	미국	실시간 보고와 멀티데이터 구조를 가진 이질적 데이터 분석
Abide Financial	미국	데이터 프로세싱과 관련 감독당국들에 대하여 데이터를 배분하기 위한 단일 솔루션

회사명	국가	기술
Accudelta	이탈리아	규제보고와 분배를 위한 데이터 관리 솔루션
Arkk Solutions	영국	보고 소프트웨어
Cappitech	이스라엘	매입과 매도에 대한 거래 및 보고 솔루션
Commcise	영국	위원회 관리와 보고 솔루션
DeltaconX	스위스	규제소프트웨어 솔루션으로 EMIR, REMIT 그리고 MiFID II에서 요구하고 있는 규제요구사항을 제공
Funds-Axis	영국	투자컴플라이언스 모니터링, 리스크 분석과 규제보고기술
Fundsquare	룩셈부르크	펀드산업에서 주문관리와 정보서비스
Hexanika	미국	빅데이터 분석에 기초한 규제보고툴, 실시간 규제보고와 클라우드 서비스
Lombard Risk	영국	규제보고자동화시스템과 규제당국의 보고요구에 부응한 범상품적 집단관리시스템
Quan Template	지브롤터	분산데이터수집과 AI를 통한 정보분석과 규제보고서의 자동생산
REGIS-TR	룩셈부르크	유럽연합의 규제보고요구사항에 따라 보고대상 거래에 대한 중앙거래정보보관
RegTek Solutions	미국	규제보고서 생산을 위한 클라우드 기반 솔루션
Silverfinch	영국	PRIIPS와 Solvency II에 대한 보험사업자 및 자산관리사를 연결하는 펀드데이터 유틸러티
Taleo Reporting	룩셈부르크	펀드에 대한 규제보고. 포괄하는 규제법령은 CRDIV, FATCA, CRS, Solvency II, AIFMD, EMIR, MIFID II, MIFIR, PRIIPs임
TRADEcho	영국	사전·사후거래보고 시스템
TransFICC	영국	파생상품시장 등에서 기업이 규제컴플라이언스를 할 수 있도록 거래 솔루션
Treamo	오스트리아	재무부에 대한 보고 및 EMIR 보고서를 위한 클라우드 기반 SaaS 솔루션
Vizor	이탈리아	금융당국이 웹기반 데이터 제출포탈과 실시간 확인을 통해서 금융회사를 감독할 수 있도록 한 시스템

컴플라이언스는 규제체제의 가장 일선에 있는 것으로 그 중요성이 제고되고 있다. 이에 대한 RegTech는 40개에 달하나 규모가 기업을 중심으로 20개를 선정하여 정리하였다.

〈컴플라이언스〉

회사명	국가	기술내용
Aesthetic Integration	영국	규제컴플라이언스를 위한 금융알고리즘 분석
Aprivacy	캐나다	정보보안 및 경로추적 서비스. 전자재무보고서 및 문서공유
AssetLogic	룩셈부르크	투자데이터와 문서의 중앙보관
AxiomSL	미국	통합리스크 관리와 규제컴플라이언스 플랫폼
Behavox	영국	컴플라이언스 보고 및 평가툴 제공, 직원 모니터링 및 리스크 스코어링
ClearMash	이스라엘	선행적 컴플라이언스와 거버넌스와 규제 인텔리전스를 위한 실시간 지식정보제공 솔루션
Comply365	미국	실시간 데이터 분석, 감사와 탄력적 보고, 규제컴플라이언스 추적을 위한 SaaS 솔루션 제공
Continuity Control	미국	컴플라이언스 관리 프로세스의 지속적 자동화, 작업흐름 솔루션 제공, 규제경보(regulatory alert)
CUBE	영국	컴플라이언스 규제 감시와 리스크 평가
Darktrace	영국	사전적으로 미확인된 데이터 보안에 대한 위협을 탐지
Datactics	영국	리스와 컴플라이언스 데이터 관리
Droit	미국	금융상품거래에 대한 실시간 그리고 자동화된 규제 컴플라이언스 인텔리전스
Drooms	독일	기밀문서 및 제3자의 접근 차단을 위한 최고수준의 안전 솔루션
GRC Solutions	영국	온라인 법적 컴플라이언스 연수와 컴플라이언스 리뷰
Neota Logic	미국	법적 컴플라이언스 애플리케이션
Netguardians	스위스	자동화된 컴플라이언스 관리 소프트웨어 및 실시간 인간행동분석을 통해 사기방지
Qumram	스위스	디지털 감사시스템으로 온라인, 모바일 그리고 사회관계망을 대상
TheMarketTrust	룩셈부르크	규제기술솔루션
Vigitrust	이탈리아	클라우드 기반 리스크 및 컴플라이언스 포털
WordFlow	호주	법령을 모바일에 최적화된 형태로 전환할 수 있는 툴로서 이를 각 개별법령과 연결

■ **금융서비스에서의 RegTech의 활용 – 컴플라이언스와 보고를 위한 솔루션 기술 (IIF : Institute of International Finance, RegTech in Financial Service – Technology Solutions for Compliance and Reporting, March 2016)**

○ 컴플라이언스와 규제보고영역에서 RegTech 솔루션의 개발로 얻을 수 있는 장점으로는 리스크 데이터의 집적, 모델링 및 시나리오분석과 예측, 지급결제거래의 모니터링, 고객과 법인의 신원확인, 금융기관의 내부문화와 행동에 대한 모니터링, 금융시장에서의 거래, 새로운 규제의 확인 및 해석 그리고 규제적용이다.

○ RegTech의 활용을 위해 적용해야 하는 기술분야로 다음을 들 수 있다.

- 기계학습(Machine Learining : 컴퓨터가 스스로 학습할 수 있도록 하는 기술), 로보틱스, 인공지능
- 암호화기술 : 금융회사, 고객, 감독기관이 정보를 공유하기 위한 암호화
- 생체인식(Biometrics) : 신원확인기능의 자동화로 자금세탁방지를 위한 'KYC (Know-Your-Customer) 프로세스'에 적용
- 블록체인과 분산원장
- APIs(Application Programming Interface)
- 공유된 유틸리티와 클라우드 – 암호화기술 : 금융회사, 고객, 감독기관이 정보를 공유하기 위한 암호화

○ 금융회사에 RegTech를 적용하는데 있어서 입법과 규제면의 문제점들은 첫째, 데이터 프라이버시와 데이터 보호규범이다. 특히 데이터 활용에 있어서 개인프라이버시의 보호는 데이터 공유의 문제와 충돌 가능성이 높다. 또한 데이터 보안 요구사항을 충족과 만약 데이터를 분산 저장하는 것이 의무화된 경우 집적 사용과 충돌 가능성이 있다.

– IT 인프라에 대한 Basel 239's(BCBS 239 compliance) 원칙에 따르면 시스템적으로 중요한 글로벌 은행과 국내은행은 리스크 데이터의 중앙집중화와 자동수집기능을 가지고 있어야 하는데 이 원칙과 기술구현과의 조화가 필요하다.

- 중요한 IT와 리스크 인프라의 복구와 정리에 관한 규범과의 조화 필요하며, 고객 확인을 위한 특별한 신원확인방법을 채택하고 있는 KYC 규범이 있는 경우 해당 규범과의 조화도 필요하다.

O 데이터 호환 및 공유 및 통합을 위한 데이터 조화성(harmonization)과 데이터 개념의 일치성이 중요해진다. 데이터 호환 및 공유 그리고 통합을 위해서는 데이터가 서로 조화를 이루어야 하는 바, 이를 위해서는 관련기관 간 데이터 표준을 정할 필요가 있으며, 표준의 내용으로는 정의, 표현, 포맷 또는 교환데이터 등이 있다.

- 각 데이터별 포괄범위도 일치시킬 필요가 있다. 예를 들어 '소매(retail)'의 정의에 대해서 유동성 비율기준 또는 자본적정성 기준이 다른 정의와 기준을 사용하고 있는 바, 만약에 고객으로 받은 돈이 1백만 유로를 넘지 않는 경우 바젤 유동성 규제(Basel liquidity regulation)상 소상업은행(small business bank)은 소매은행으로 분류하나, 바젤 자본규제(Basel capital regulation)상으로는 이러한 고객으로부터 펀딩된 돈이 소상업은행을 구분하는 기준이 되지 않는다. 즉, 감독당국이 자동으로 보고서를 받고 모니터링하기 위해서는 감독규정상의 데이터 포괄범위는 물론 시장과 감독당국 간 데이터의 포괄범위를 일치시킬 필요가 있다는 것이다.

참고문헌

IIF, Institute of International Finance, RegTech in Financial Service - Technology Solutions for Compliance and Reporting, March 2016

OECD, Recommendation of the Council on Gender Equality in Public Life 2015, 2016

OECD, Best Practice Principles on Stakeholder Engagement in Regulatory Policy, 2016

OECD, Engaging Public Employees for a High-Performing Civil Service, 2016

OECD, Digital Government Strategies for Transforming Public Services in the Welfare Areas, 2016

European Court of Auditors, Governance at the European Commission best practices ? 2016

EU, eGovernment Action Plan 2016-2020 - Accelerating the digital transformation of government

EU, General Data Protection Regulation, 2016/679, GDPR

FCA, Supporting the development and adoption of RegTech, Call for Input, Nov. 2015

UNCTAD, Multi-year Expert Meeting on Trade, Service and Development, Geneva 18-20, July 2017 Presentation ppt - Fintech Inclusion, Fintech, and RegTech

금융보안원, 금융규제 이행을 위한 RegTech의 필요성 및 향후과제, 보안연구부 2017-008, 2017.3.13.

中國 中华人民共和国网络安全法

http://asic.gov.au/for-business/your-business/innovation-hub/regtech/ (2017.9.30. 방문)

https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html(2017.9.2.방문)

부 록

〈부록〉 개인정보보호규칙

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC [1].

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council [2] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

[1] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

[2] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council [1]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council [2], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [1] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be

[1] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or

Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [1] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data

[1] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their

further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes

by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [1], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

[1] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given

his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the

nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data

protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out

and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of

protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council [1] as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the

[1] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the

processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the

possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance

with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first

seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council [1] should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate

[1] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council [1] leaves intact and in no way affects the level of protection of natural persons with regard to the

[1] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council [1] should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council [2] provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement

[1] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

[2] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 [1].

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council [2], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

[1] OJ C 192, 30.6.2012, p. 7.
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(1) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific

processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council [1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council [1].

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

2017

글로벌 법제 동향 모니터링 이슈 분석 보고서

KOREA LEGISLATION RESEARCH INSTITUTE

GLOBAL LEGAL ISSUES (Ⅲ-1)

ISSUE 02

국제경제분야

서비스무역규범 논의 현황 및 국내규제 규율에 관한 동향 분석

고 준 성
산업연구원 선임연구위원

고준성 박사는 1992년 고려대학교에서 법학박사학위를 취득하였고, 법무부에서 국제통상분야 실무를 경험한 후 산업연구원(KIET)에서 국제산업협력실장 등을 역임하고 현재는 선임연구위원으로 재직 중이다. 주요 연구활동 분야는 국제통상·투자법이며, 특히 FTA 규범 및 정책에 집중하고 있다.

ISSUE
02
국제경제분야

서비스무역규범 논의 현황 및 국내규제 규율에 관한 동향 분석

고 준 성 산업연구원 선임연구위원

Abstract

최초의 서비스무역규범인 WTO GATS는 서비스무역을 규율하는 총칙규범으로서 골격적인 내용을 담고 있고, 따라서 핵심규정에 대한 추가적인 부속협정이 필요한 상황이지만, 아직까지 아무런 구체적인 성과가 없다. 다만, 거의 유일하게 국내규제(domestic regulation)와 관련하여 1998년 회계부문 국내규제규범 채택과 2012년 국내규제규범초안 마련 그리고 2016년 서비스무역원활화협정 인도 제안서 등의 제한적인 성과가 있었다. 특히, 미국 주도하에 추진된 서비스무역협정(Trade in Services Agreement: TiSA) 협상에서는 국내규제부속서안을 마련하였고, 2016년 2월 정식 서명된 환태평양전략적경제동반자협정(Trans-Pacific Strategic Economic Partnership Agreement: TPP협정) 안에는 모범규제관행 규정을 포함하는 규제일관성챕터(제25장)와 투명성규정(제26장의 일부)이 채택되었고, 현재 일시 중단된 범대서양무역투자동반자협정(Transatlantic Partnership Trade and Investment Agreement: TTIP) 협상에서는 EU가 모범규제관행 챕터와 규제협력 챕터를 제안하였고, 투명성 챕터안이 포함되어 있다.

국가가 갖는 국내규제의 권한에 대해 WTO 등 국제기구와 무역협정에서 이를 국제적으로 규율하고자 하는 배경은 그러한 국내규제가 무역자유화(시장개방)의 효과를 제한하거나 상쇄할 수 있기 때문이다. 또한 국가들 간의 상이한 국내규제 자체가 무역자유화에 장애로서 작용할 수 있기 때문이다. 이 점에서 미국이나 EU는 다양한 국제기구와 자신들이 협상하는 무역협정에서 규제일관성, 규제협력 또는 좁게 모범규제관행 등의 제하에 국내규제를 규율하는 규정의 도입에 큰 관심을 갖고 있다. 그런데, 향후 우리가 체결하는 무역협정 안에 이러한 국내규제 규율이 포함될 경우 우리의 국내규제 규율 법 및 정책에 직간접적인 영향을 미치는 점에서 이에 대한 면밀한 대응이 요구된다.

Ⅰ. 들어가며

종전의 GATT체제는 오직 국경을 넘어 교역되는 상품만이 그 규율 대상이었으나, 1986년 개시된 Uruguay Round(UR) 다자간무역협상의 결과 1993년 타결된 UR 최종 문서의 일부로서 서비스무역에 관한 일반협정(General Agreement on Trade in Services: GATS)이 포함되었고, 이로써 상품무역과 마찬가지로 서비스무역도 새로운 다자간 무역규범인 WTO협정의 일 부속서인 GATS의 규율을 받게 되었다. 그런데 GATS는 불과 29개의 조문으로 구성된 총칙규정이어서 핵심 규정이라 할 수 있는 서비스무역 관련 긴급세이프가드조치(GATS 10조)나 보조금(GATS 15조) 및 정부조달(GATS 13조) 등에 대한 실체적 규정이 없고, 따라서 이를 후속 협상 과제로서 규정하였다.

본고 Ⅱ장에서는 서비스무역규범과 관련하여 WTO 출범 이후 논의를 소개하고, 최근의 현황을 살펴보고자 하며, III장에서는 WTO 서비스무역규범 협상에서 거의 유일하게 성과를 거두고 있는 국내규제(domestic regulation)와 관련하여 WTO 밖에서의 이에 관한 논의 현황 및 성과를 소개하고, 그 정책적 시사점을 모색해 보고자 한다.

Ⅱ. WTO체제하에서의 서비스무역규범 논의 현황

1. 그간의 서비스무역규범 논의 개관

GATS에서의 mandate에 따라 WTO 출범 이후 WTO 서비스무역이사회 산하에 설치된 GATS 규범작업반(Working Party on GATS Rules: WPGR)은 서비스무역에 대한 긴급세이프가드(emergency safeguard measures), 서비스 보조금(service subsidies) 및 정부 서비스조달에 대한 구체적인 규범 제정 작업을 맡아 수행하고 있다. 그러나 이들 이슈에 대한 규범 제정에 있어 제반 난제로 인해 2017년 현재까지 아무런 성과를 거두지

못하고 있고, 향후 타결 전망 역시 매우 불투명하다.

한편, GATS 제6조(국내규제) 4항에서는 자격요건과 절차, 기술표준 및 면허요건과 관련된 조치가 서비스무역에 불필요한 장벽(unnecessary barriers to trade in services)이 되지 않도록 보장하기 위하여 서비스무역이사회는 자신이 설치할 수 있는 기관을 통해 모든 필요한 규율을 수립, 개발해야 한다고 규정한다. 이와 관련 1993년 12월 15일 채택된 "전문직 서비스에 관한 결정"[1]에서는 GATS 제6조 4항에 규정된 작업계획을 즉시(immediately) 시행하고, 이를 위해 "전문직서비스작업반(Working Party on Professional Services: 'WPPS')"을 설치할 것과 WPPS가 특히 회계분야에서의 다자간 규율 제정을 우선적으로 수행할 것을 권고하였다.

이에 따라 WTO 서비스무역이사회는 1998년 12월 14일 "회계분야 국내규제에 관한 규범(Disciplines on Domestic Regulation in the Accountancy Sector: '1998년 회계분야 규범')"[2]을 채택하는 성과를 거두었다. 동 규범을 채택하면서 서비스무역이사회는 동 규범이 WTO 회원 중 자국의 양허표를 통해 회계분야에 대한 시장개방 약속을 포함한 회원국들에 대해서만 적용된다. 그런데, 동 규범은 진행 중인 서비스협상의 타결 전에 GATS의 일부분으로 통합된 이후 시행된다고 명시하였다.[3] 이에 따라 1998년 채택된 회계분야 규범은 아직 적용되고 있지 못하다. 다만, 동 이사회 결정에 포함된 현상유지(standstill) 규정에 따라 상기 규범이 채택된 1998년 12월 이후 WTO 회원들은 동 규범에 저촉되는 회계분야에서의 국내규제를 도입하는 것이 금지된다.

2. GATS 국내규제작업반에서의 국내규제규범 논의 현황

1999년 2월 개최된 WPPS 회의에서 국내규제에 관한 일관되고 통합된 규범 마련을 위해 WPPS의 개편 필요성이 제기되었고,[4] 이에 따라 WTO 서비스무역위원회는 1999년 4월

1) WTO, The Results of the Uruguay Round of Multilateral Trade Negotiations: The Legal Texts, 462-463 (1994).
2) WTO, S/L/64 (dated on Dec. 17, 1998).
3) WTO, S/L/63 (dated on Dec. 15, 1998).

26일 논의 대상을 전문직서비스에 한정한 WPPS를 폐지하고, 대신에 WPPS의 기존 논의 영역을 포함하여 보다 광범위한 범주를 규율 대상으로 하는 국내규제에 관한 규범 논의를 수행하기 위하여 "국내규제 작업반(Working Party on Domestic Regulation: 이하 'WPDR')"을 설치하기로 결정하였다. 동 작업반은 2011년 4월 "Draft: Disciplines on Domestic Regulation"('2011년 국내규제규범 초안')가 포함된 "Progress Report"(경과보고서)[5]를 작성하는 성과를 거두었다.

2011년 경과보고서에 따르면 2011년 국내규제규범 초안은 조문에 따라 그 진전 성과가 3가지 카테고리(사실상 합의, 단일의 대안 및 복수의 대안 대립)로 차이가 있다. 이를 규율 분야별로 나누어 살펴보면, 먼저 GATS 제6조 4항에 따른 자격요건(qualification requirements) 및 절차, 면허(licensing) 및 절차와 기술표준(technical standard) 등 5개의 국내규제 구성 요소와 관련하여서는 일부 규정이 사실상 단일 조문에 합의하였고, 일부 규정은 단일안이 마련되었거나 복수의 대안이 검토 중에 있는 등 상당한 진전을 거두었다. 이는 상술한 5개의 국내규제 구성 요소들에 관한 사안들은 대체로 기술적인 성격을 가진 것이어서 상대적으로 합의 도출이 용이했던 것으로 보여진다. 다만, 기술표준에 관한 성과가 다른 요소들에 비해 낮은 것이 주목된다.

다음으로 WPDR에서의 국내규제의 국제적 규율의 틀을 구성하는 원칙들(basic principles)에 관한 논의의 경우 크게 국내규제에 대한 다음의 4개 기본원칙 즉, 필요성(necessity), 투명성(transparency), 동등성(equivalency), 국제표준(international standards)을 중심으로 논의가 이루어져 왔고, 이 중에서도 필요성 심사와 투명성 이슈가 핵심 이슈로서 다루어졌다. (i) 투명성(transparency)은 새로운 규제를 도입하거나 기존 규제를 강화하는 과정에서 서비스 규제에 대한 예측 가능성과 안정성을 보장해 주는 핵심 수단이 될 뿐만 아니라 양허의 실효성을 제고하고 서비스무역에 있어 불필요한 규제를 예방하는데 중요한 수단이 된다. 2011년 국내규제 규범 초안 제13항에 따르면 각 회원국은 면허요건 및 절차, 자격요건 및 절차 그리고 기술표준에 대해 일반적으로 적용되는 조치는 물론 이들 조치에

4) WTO, S/WPPS/M/25 (dated on March 5, 1999).
5) WTO, S/W/PDR/W/45 (dated on Apri 14, 2011).

관한 상세 정보를 인쇄 또는 전자수단을 통해 즉시 공표해야 한다고 규정하면서 그러한 정보에 포함되는 대상을 구체적으로 열기한다. 공표가 곤란한 경우 다른 방법을 통해 당해 정보를 일반이 이용할 수 있도록 해야 한다. (ii) 필요성 심사(necessity test)는 국내규제가 특정한 정당한 목적을 달성하는데 필요한 이상으로 무역을 제한하거나 부담이 되는 것이어서는 아니 된다는 필요성을 판단하기 위한 기준에 관한 것으로서 국내규제가 서비스무역에 대해 불필요한 장벽이 되지 않도록 보장하기 위한 국내규제의 국제적 규제를 위한 핵심장치 중의 핵심이라 할 수 있다. 그런데, "필요성 심사"와 관련하여서는 그러한 필요성 심사 형태의 규범적 기준을 국내규제 규범에 포함시켜야 할 것인지의 여부에 대해서조차 아직 합의를 이루지 못하고 있다. (iii) 동등성 원칙은 서비스공급자가 외국에서 취득한 관련 자격 및 경험을 고려해 주도록 규정한다. (iv) 국제표준과 관련하여 기술표준이 요구되고, 관련 국제표준이 존재하거나 그 채택이 임박한 경우 그러한 국제표준이 국가의 정책목적을 달성함에 있어 효과가 없거나 부적절한 경우를 제외하고는 자국의 기술표준을 입안함에 있어 그러한 국제표준을 고려하도록 규정한다.

한편, 2001년 국내규제 규범 초안 마련 이후 이에 관한 논의가 계속되어 오고 있고, 2017년 3월 14-17일 간 국내규제작업반(WPDR)과 서비스이사회 회의에서는 그간의 국내규제 규범 협상을 진전시키기 위해 WTO 회원들로부터의 국내면허절차 및 기술표준이 무역에 불필요한 장벽이 되어서는 아니되도록 보장하기 위한 것에 관한 4건의 신규 또는 개선 제안을 논의한 상황이다.

3. GATS 국내규제작업반에서의 서비스무역원활화협정 논의 현황

인도는 2016년 9월 23일자 Communication[6]을 통해 "서비스무역원활화협정(Trade Facilitation Agreement for Services: 'TFS 협정')의 추진을 제안하였다. 동 Communication은 WTO 국내규제작업반(WPDR) 회원들에게 회람되어, 2017년 3월 14-17일 간 WPDR과 서비스이사회 회의에서도 논의되었다.

6) S/WPDR/W55, 27 Sept. 2016.

(1) TFS협정 추진 배경 및 동기[7)]

인도는 추진 제안서에 따르면 서비스는 국내 및 국제 거래에 있어 상당하고도 증가하는 비중을 차지한다. 그러나 서비스무역 거래는 수많은 국경 장벽과 국경 너머의 장벽(behind-the-border barriers) 그리고 절차적 난관에 직면하여 있고, 이는 전체적인 서비스무역의 역량을 실현하는데 장애가 되고 있다. 이러한 장애는 특히 전 세계 중소기업 및 소규모 수출업자들이 서비스무역에서 받을 수 있는 혜택을 제한하고 있음을 지적한다.

이와 관련 WTO 회원들에 의해 2014년 채택되어 2017년 발효된 무역원활화협정(Trade Facilitation Agreement: TFA)은 상품무역과 관련하여 중요한 기념비적 성과이다. TFA의 목적은 상품의 이동, 양도 및 통관절차는 물론 통관 준수 이슈에 있어 협력을 촉진하기 위한 것이다. TFA와 마찬가지로 서비스무역에 있어서도 상응하는 협정에 대한 필요가 존재한다. 이는 TFS협정도 서비스무역에 대한 불필요한 규제 및 행정적 부담으로 발생하는 거래비용의 감소를 가져 올 수 있기 때문이다. TFS협정은 서비스무역의 촉진과 관련된 핵심 이슈들 가령, 투명성(transparency), 간소화절차(streamlining procedures) 및 병목 제거(eliminating bottlenecks) 등을 다루어야 할 것이다. 또한 제안하는 TFS 협정의 적용 범위는 모든 서비스공급방식을 넘어 서비스무역에 영향을 미치는 회원들의 조치를 포함해야 할 것이다. 아울러 TFA의 경우와 마찬가지로 TFS 협정 역시 개도국 및 최빈개도국(Least Developed Countries: LDCs)에 대한 특별하고 차별적인 대우에 관한 규정을 포함해야 할 것이며, 이들을 위한 기술지원과 역량배양 지원을 위한 이슈들을 다루어야 할 것이다.

(2) TFS 협정에 포함되어야 할 요소(규정) 예시[8)]

TFS 협정은 상품에 대한 TFA에 기초하되, 필요한 적절한 변경과 변형을 하여 입안될 수 있다. 협정의 일부 규정은 4가지 서비스공급방식 모두에 관련된 범분야(cross-cutting) 이슈가 될 것이지만, 다른 일부 규정은 공급방식 중 특정 공급방식에만 적용될 수도 있다.

7) S/WPDR/W55, 27 Sept. 2016, p.1.
8) S/WPDR/W55, 27 Sept. 2016, pp.1-2.

TFS 협정에 포함되어야 할 규정을 제시해 보면, 먼저 모든 공급방식에 적용되어야 할 이슈로서 (i) 무역데이타의 자동화 및 국제전자교류 등을 포함한 정보의 공표 및 이용, (ii) 서비스 무역에 영향을 미치는 일반적으로 적용되는 모든 조치의 적용에 있어 투명성, (iii) 서비스무역에 영향을 미치는 조치의 합리적이고, 객관적이며 공평한 방식으로의 집행 보장, (iv) 관계 당국들 간에 있어 협의 및 협력, (v) 서비스 무역에 영향을 미치는 조치의 시행 이전 단계에서의 의견 개진 기회, (vi) 서비스공급자로부터의 신청에 대한 고려 및 이의제기와 재심에 관한 절차와 기한, (vii) 서비스 공급에 대한 조세, 수수료, 요금 및 기타 부과금에 대한 규율, (viii) 개도국 및 최빈국에 대한 특별하고 구별된 대우, (ix) 제도적 장치를 예시하였다.

다음으로 특정 공급방식과 관련 규정들을 공급방식별로 제시해 보면, (i) 모드 1과 관련하여 모드 1 서비스의 의미있는 공급 보장을 위한 국경간 정보의 자유로운 이동의 원활화를 예시한다. (ii) 모드 2와 관련하여 외국에서의 의료 및 관광서비스의 이용에 적용될 국경간 보험 교환성(cross border insurance portability) 등을 통한 모드 서비스 공급의 촉진과 가령, 의료서비스, 교육서비스, 관광 등을 이용하기 위하여 다른 국가에 입국하고자 하는 소비자에 대한 비자처리수수료 등과 같은 임시 입국 서류, 절차 및 기한을 간소화하기 위해 노력할 것을 예시한다. (iii) 모드 3과 관련하여 상업적 주재의 설립을 위한 단일창구해결(single window clearance)과 같은 조치를 포함하여 모드 3 서비스 공급의 원활화 그리고 모드 3 서비스 공급자에 부과되는 수수료에 관한 규율을 예시한다. (iv) 모드 4와 관련하여 일시 입국 및 체류 절차의 간소화와 모드 4 약속 카테고리에 해당하는 고용허가 및 임시 입국에 있어 명료화를 통한 모드 4 서비스의 공급 촉진 그리고 임시 입국 등과 관련한 과세, 수수료/요금, 차별적 급여 요건, 사회보장 기여와 관련된 조치들이 외국서비스 공급자에게 부당하게 불이익을 초래하지 않도록 보장하기 위하여 이들 조치들에 대한 규율을 예시한다.

끝으로 인도 정부는 TFA와 마찬가지로 잘 짜여진 TFS 협정은 WTO 모든 회원들에 있어 서비스무역의 가능성을 실질적으로 증대시켜 줄 것이라고 확신한다. 다만, 모든 회원들의 주요 관심사를 효과적으로 다룰 수 있는 틀을 개발하기 위해 TFS 협정 개념에 대한 면밀한 검토가 요구됨을 언급하였다.

Ⅲ. 국내규제 규율에 관한 최근 동향 분석

앞서 언급하였듯이 WTO GATS는 서비스무역을 규율하는 총칙규범으로서 골격적인 내용을 담고 있고, 따라서 핵심규정에 대한 추가적인 부속협정이 필요한 상황이지만, 구체적인 성과가 없다. 다만, 거의 유일하게 국내규제와 관련하여 제한적인 성과가 있음을 살펴보았다. 그런데, 미국의 주도하에 추진된 서비스무역협정(Trade in Services Agreement: TiSA) 협상과 2016년 2월 정식 서명된 환태평양전략적경제동반자협정(Trans-Pacific Strategic Economic Partnership Agreement: TPP협정) 그리고 현재 일시 중단된 범대서양무역투자동반자협정(Transatlantic Partnership Trade and Investment Agreement: TTIP) 협상에서 국내규제와 관련된 챕터들이 제안되거나 도입되는 큰 진전이 있었는바 아래에서는 이들 내용을 살펴보고자 한다.

본장의 논의대상인 "국내규제"(domestic regulation)의 개념과 관련하여 WTO GATS에서는 직접적인 정의를 하고 있지 아니하다. 대신, GATS 제6조 1항에서는 시장개방을 약속한 분야에 있어 국가에 의한 "서비스무역에 영향을 미치는 일반적으로 적용되는 모든 조치"라고 언급하고 GATS 제6조 4항에서는 국내규제를 보다 구체적으로 "자격요건과 절차, 기술표준 및 면허요건과 관련된 조치"를 가리킨다고 규정한다.

1. TiSA협상에서의 국내규제 논의 현황

WTO 출범 후 2000년대 초반 개최된 최초의 다자간무역협상인 도하개발아젠다(DDA) 협상의 일 분야로서 DDA 서비스 협상이 달리 진전을 보이지 못하면서, WTO 회원국 중 서비스무역 자유화에 관심이 많은 국가들로 구성된 "Really Good Friends of Services"라 불리는 16개국 그룹이 서비스무역 자유화를 위해 WTO GATS와는 별도의 서비스무역협정을 추진하기 위하여 2011년 말 일련의 모임을 가졌으며, 이 모임은 미국과 호주가 주도하였다. 이후 소위 복수국간 "서비스무역협정"(TISA') 협상이 2013년 4월 제네바에서 공식

개시되었고, 2016년 기준 우리나라를 포함하여 24개 WTO 회원[9]이 참가하고 있다. TiSA협상은 수많은 회의를 거쳐 2016년 6월 기준 TISA 본문(core-text)과 17개에 달하는 부속서의 상당 조문이 타결되고, 일부 조문이 미결 상태인 가운데 협상 타결을 시도하였으나 2016년 말 미국의 트럼프 대통령 당선 이후 협상이 중단된 상태이다.

TiSA에서 국내규제 규율은 TiSA 본문(Core-text)상의 국내규제 조항과 별도의 국내규제부속서(Annex on Domestic Regulation: DR부속서)에서 규정한다. TiSA는 협상 중이어서 구체적인 내용을 공표할 수 없는바, DR부속서의 주요 규율 사항을 소개하면, 국내 규제 주권 인정, 규정의 적용대상, 서비스무역 영향 조치의 합리적, 객관적, 공평한 시행, 실체적 의무로서 필요성 심사와 절차적 공정성 등, 잠정적인 실체적 의무로서 서비스무역 다자협상 결과의 반영 약속, 행정결정에 대한 재심 절차 보장, 합리적 인가신청 기간, 검사 주기 등, 전자양식 도입, 사본 접수 원칙, 인가수수료, 처리일정 제공, 신속한 신청 처리, 합리적 기간 내 신청처리, 주무당국의 신청 정보 제공, 거부된 신청의 처리, 인가 효력, 기술표준 채택 절차의 투명성, 인가 정보의 투명성 등을 포함하고 있다.

2. TPP협정의 규제일관성 챕터의 주요 내용[10]

브루나이, 칠레, 뉴질랜드, 싱가포르, 미국, 호주, 페루, 베트남, 말레이시아, 멕시코, 캐나다, 일본 등 12개 국가가 참여하여 2015년 10월 타결되고, 2016년 2월 서명된 TPP협정안에는 국내규제와 관련하여 규제일관성(Regulatory Coherence) 챕터(제25장)가 포함되어 있는 바 주요 내용을 소개하면 다음과 같다.

(1) 적용대상 규제조치의 정의 및 범위

먼저 적용대상 규제 조치(covered regulatory measure)란 본 장에 따라 각 당사국이

9) (아시아 및 대양주) 우리나라, 일본, 대만, 홍콩, 파키스탄, 호주, 뉴질랜드; (미주) 미국, 캐나다, 멕시코, 코스타리카, 파나마, 콜롬비아, 페루, 칠레, 파라과이, 우루과이; (유럽 및 중동) EU, 스위스, 노르웨이, 아이슬란드, 터키, 이스라엘 등

10) 본 내용은 필자가 연구책임자로 참여하여 집필한 비공개 정부연구용역 "국내·외 모범규제관행 동향조사 및 정책시사점 연구"(2017)을 재활용하여 작성하였음을 밝혀둔다.

결정한 규제 조치를 말하고, 규제 조치(regulatory measure)란 본 협정의 적용 대상이 되는 모든 사안과 관련하여 규제 당국에서 도입하였고 의무적으로 준수해야 하는 일반적으로 적용되는 조치를 말한다.[11] 다음으로 적용 대상 규제 조치의 범위와 관련하여 협정에서는 각 당사국이 신속하게, 그리고 해당 당사국의 본 협정 발효일로부터 1년 이내에 자국의 적용 대상 규제 조치의 범위를 정하고 공개하고, 적용 대상 규제 조치의 범위를 정할 때 상당한 적용 범위를 달성하는 것을 목표로 해야 한다고 규정한다.[12]

(2) 규제 일관성 촉진을 위한 장치

1) 조정 및 검토 절차 또는 메커니즘

모든 당사국은 규제 조치 개발 과정과 연계된 부처 간 협의 및 조정을 확대하는 국내 메커니즘을 통하여 규제 일관성이 촉진될 수 있음을 인정하고, 이에 따라 각 당사국은 제안된 적용 대상 규제 조치에 대한 효과적인 부처 간 조정 및 검토가 원활하게 이루어지도록 노력한다. 이를 위하여 각 당사국은 국가 또는 중앙 조정 기관(national or central coordinating body)을 설립 및 유지하는 것을 검토해야 한다.[13]

또한 모든 당사국은 상술한 절차나 메커니즘이 각 당사국의 개발 수준 및 정치적, 제도적 구조상의 차이를 포함한 상황에 따라 다를 수 있다는 것을 인정한다. 그러나 당사국들이 (i) 적용대상 규제 조치의 개발이 협정 제25.5조(핵심 모범 규제관행의 이행)에 명시된 관행을 포함하되 이에 한정되지 않는 모범 규제관행에 부합하는 정도를 결정하기 위하여 제안된 적용 대상 규제 조치를 검토하고, 그러한 검토를 기초로 한 권고안(recommendation)을 제시할 능력, (ii) 잠재적 중복(overlap and duplication)을 파악하고 부처 간에 불합치하는 요건이 발생하지 않도록 국내 부처 간 논의와 조정을 강화할 능력, (iii) 체계적인 규제 개선을 위하여 권고안을 제시할 능력 그리고 (iv) 검토한 규제 조치, 체계적인 규제 개선을 위한 모든 제안 그리고 제1항에 언급된 절차와 메커니즘에 대한 최근의 변경사항에 대해

11) TPP협정 제25.1조.
12) TPP협정 제25.3조.
13) TPP협정 제25.4조 1항.

공개적으로 보고할 능력을 가지고 있고, 따라서 각 당사국은 해당 절차나 메커니즘에 대한 기술을 포함하고 일반에게 공개될 수 있는 문서를 작성해야 한다.[14]

2) 핵심 모범 규제관행(Core Good Regulatory Practices)의 시행

첫째, 모든 당사국은 목표 달성을 위한 최선의 조치를 고안하는 과정에서 제안된 적용 대상 규제 조치를 개발할 때, 그 조치가 해당 당사국이 정한 경제적 영향 또는 적절한 경우 기타 규제 영향의 기준을 초과한다면 관련 규제 당국에게 자국 법과 규정과 합치하게 규제 영향 평가(regulatory impact assessment)를 실시하도록 장려해야 한다. 규제 영향 평가는 가능한 영향을 가늠하기 위하여 다양한 절차를 포함할 수 있다.[15] 둘째, 당사국 간 제도적, 사회적, 문화적, 법적, 개발 상황의 차이가 특정한 규제적 접근을 초래할 수 있음을 인식하면서, 당사국이 실시하는 규제 영향 평가에는 (i) 문제의 성격 및 의의에 대한 기술을 포함한 규제 제안의 필요성 평가, (ii) 일부 비용과 혜택은 계량화 및 금전적 환산이 어렵다는 것을 인식하여 관련 리스크 및 분배상의 영향(distributive impacts) 등 조치에 따르는 비용과 혜택을 포함하는 실행가능한 대안을 법과 규정에 합치하며 실행가능한 한도에서 검토, (iii) 적절한 경우 그 비용과 혜택 그리고 리스크 관리의 가능성에 대한 참조를 포함하여 선택된 대안이 정책 목적을 효율적으로 달성한다고 결론을 내린 근거의 설명 그리고 (iv) 특정 규제 기관의 권한(authorities), 위임(mandate) 및 재원(resource)의 범위 안에서 관련 과학, 기술, 경제 및 기타 정보 등 가장 합당하게 획득할 수 있는 기존 정보의 이용 등에 관한 요소를 포함되어야 한다.[16] 셋째, 당사국은 규제 영향 평가를 실시할 때, 제안된 규제가 중소기업에 미치는 잠재적 영향을 고려할 수 있다.[17] 넷째, 각 당사국은 일부 조치가 기술적 사안을 다루고 있고, 이를 이해하고 적용하기 위해 관련 전문지식이 필요하다는 사실을 인정하며, 신규 적용 대상 규제 조치를 평이하게 기술하는 한편, 명확, 간결, 체계적이며, 쉽게 이해할 수 있도록 해야 한다.[18] 다섯째, 각 당사국은 자국의 법과

14) TPP협정 제25.4조 2항.
15) TPP협정 제25.5조 1항.
16) TPP협정 제25.5조 2항.
17) TPP협정 제25.5조 3항.
18) TPP협정 제25.5조 4항.

규정에 따라, 관련 규제 당국이 신규 적용 대상 규제 조치에 관한 정보에 대중이 접근 가능하도록 하고, 실현 가능한 경우 이 정보를 온라인상에 게시해야 한다.[19] 여섯째, 각 당사국은 해당 당사국의 정책 목적 달성을 위하여 더욱 효과적인 규제 체제를 만들기 위하여 당사국이 이행한 특정 규제 조치에 대한 수정, 간소화, 확장 또는 폐지가 필요한 지 여부를 결정해야 한다. 이를 위해 각 당사국이 적절하다고 간주하는 시간적 간격을 두고 적용 대상 규제 조치를 검토해야 한다.[20] 일곱째, 각 당사국은 해당 당사국의 규제 당국이 향후 12개월 이내에 공표할 것으로 합당하게 예측되는 모든 적용 대상 규제 조치에 대한 연례 공지를 해당 당사국이 적절하다고 간주하고 자국의 법과 규정과 합치하는 방법으로 제공해야 한다.[21] 여덟째, 각 당사국은 자국 법에 합치하며 적절한 한도에서 적용 대상 규제 조치를 기획할 때, 관련된 자국의 규제 기관이 다른 당사국의 규제 조치 및 국제적, 지역적 및 기타 포럼에서의 관련된 진전 상황을 고려할 것을 장려해야 한다.[22]

3) 규제일관성위원회

당사국은 각 당사국의 정부 대표들로 구성된 규제일관성위원회(Committee on Regulatory Coherence: 위원회)를 설립한다. 위원회는 본 장의 이행 및 운영과 관련된 사안을 고려한다. 위원회는 본 장에서 적용되는 사안 및 본 협정의 다른 장에서 적용된 규제 일관성과 관련된 사안과 관계된 분야별 잠재 이니셔티브와 협력 활동을 포함한 향후 우선순위를 확인한 것을 고려한다. 위원회는 향후 우선순위 확인에 있어 다른 위원회와 실무 그룹 그리고 본 협정 하에 수립된 모든 부속 기관의 활동을 고려하고, 활동이 서로 중복되지 않도록 이들 기관들과 조정한다. 위원회는 규제 협력에 관한 위원회의 업무가 기타 관련 부문에서 논의 중인 이니셔티브에 부가 가치를 제공하고 그러한 노력의 저해나 중복을 방지하도록 보장한다. 각 당사국은 다른 당사국의 요청이 있을 시 제27.5조(연락창구[contact point])에 따른 본 장의 이행에 관하여 정보를 제공하기 위하여 연락창구를 지정하고 통지한다. 위원회는

19) TPP협정 제25.5조 5항.
20) TPP협정 제25.5조 6항.
21) TPP협정 제25.5조 7항.
22) TPP협정 제25.5조 8항.

본 협정의 발효일로부터 1년 이내에 그리고 그 이후에는 필요한 경우에 회합한다. 끝으로 위원회는 본 협정의 혜택을 더욱 증진하기 위하여 이사회(Commission)에 본 장의 규정을 개선하기 위한 권고를 할 것인지의 여부를 고려하는 관점 하에서 본 장의 이행에 관한 당사국들의 경험과 더불어 제25.4조(조정 및 검토 절차 또는 메커니즘) 제1항에 언급된 절차나 메커니즘 유지에 관한 모범 규제관행 및 모범 관행 분야의 진전 상황을 본 협정의 발효일 이후 최소한 5년에 한 번씩 고려한다.[23]

4) 이해관계자의 참여

위원회는 당사국의 이해관계자(Interested Persons)가 규제 일관성의 향상과 관련된 사안에 관한 조언을 할 수 있는 기회를 지속적으로 제공하기 위하여 적절한 메커니즘을 구축한다.[24]

5) 이행 통지

첫째, 각 당사국은 투명성의 목적상 그리고 본 장의 협력과 역량 배양을 위한 기초가 될 수 있도록 해당 당사국의 본 협정 발효일로부터 2년 내에 그리고 그 이후에는 최소한 4년에 한 번씩, 제27.5조(접촉창구)에 따라 지정된 접촉창구를 통해 본 협정의 이행 사항을 위원회에 통지한다.[25] 둘째, 각 당사국은 최초 통지 시 해당 당사국의 본 협정 발효일 이후 이행 단계에 대하여 기술한다. 또한 본 장의 이행을 위한 계획을 기술하고, 여기에는 (i) 제25.4조(조정 및 검토 절차 및 메커니즘)에 따른 제안된 적용 대상 규정 조치에 대한 효과적인 부처 간 조정 및 검토를 촉진하기 위한 절차나 메커니즘의 수립, (ii) 관련 규제 당국이 제25.5조(핵심 모범 규제관행의 이행) 1항 및 2항에 따라 규제 영향 평가를 실시하도록 장려, (iii) 제안된 적용 대상 규제 조치가 제25.5조(핵심 모범 규제관행의 이행) 4항 및 5항에 따라 작성되고 이용될 수 있도록 보장, (iv) 적용 대상 규정 조치를 제25.5조(핵심

23) TPP협정 제25.6조 1항-7항.
24) TPP협정 제25.8조.
25) TPP협정 제25.9조 1항.

모범 규제관행의 이행)에 따른 검토 그리고 (v) 제25.5조(핵심 모범 규제관행의 이행)에 따라 도입이 예상되는 적용 대상 규제 조치에 관한 정보를 당사국의 연례 공지를 통한 일반에의 제공 등을 포함해야 한다.[26] 셋째, 각 당사국은 제25.9조 2항상의 통지를 포함하여 이전의 통지 이후 해당 당사국이 취한 조치들과 본 장을 이행하기 또한 본 장의 준수를 개선하기 위해 취하고자 계획한 조치들을 후속 통지에서 기술한다.[27] 넷째, 위원회는 본 장의 이행 및 운영과 관련된 사안을 고려할 때, 제1항에 따른 당사국의 통지를 검토할 수 있다. 그러한 검토 중에 당사국들은 해당 당사국의 통지의 특정 측면에 대하여 질의하거나 논의할 수 있다. 위원회는 그러한 통지에 관한 검토 및 논의를 제25.7조(협력)에 따른 지원을 제공하기 위하여 지원 및 협력 활동의 기회를 확인하기 위한 기초로서 이용할 수 있다.[28]

6) 협력

모든 당사국은 본 장의 원활한 이행과 그로부터 발생하는 혜택을 극대화하기 위하여 협력한다. 협력 활동은 각 당사국의 필요를 고려하되, (i) 다른 당사국과의 정보 공유, 대화 또는 회합, (ii) 중소기업과 다른 당사국을 포함한 이해관계자와의 정보 공유, 대화 또는 회합, (iii) 연수 프로그램과 세미나 그리고 기타 관련된 지원, (iv) 규제 당국 간의 협력 강화와 기타 관련된 활동 그리고 (v) 당사국이 합의하는 기타 활동을 포함할 수 있다.[29] 나아가 모든 당사국은 규제 사안에 관한 당사국들 간 협력이 증진될 수 있기 위해서는 무엇보다도 각 당사국의 규제 조치가 중앙에 집중되어 이용될(centrally available) 수 있게 보장되어야 함을 인정한다.[30]

26) TPP협정 제25.9조 2항.
27) TPP협정 제25.9조 3항.
28) TPP협정 제25.9조 4항.
29) TPP협정 제25.7조 1항.
30) TPP협정 제25.7조 2항.

(3) 다른 장과의 관계 및 분쟁해결 조항의 비적용

본 장과 본 협정의 다른 장이 상충하는 경우 다른 장이 상충하는 부분에 대해 우선 적용된다.[31] 또한 어떠한 당사국도 본 장(章)에 의해 발생한 사안에 대해 제 28장(분쟁해결)에 따른 분쟁 해결에 의존하여서는 아니 된다.[32]

3. TTIP협상에서의 EU제안 모범규제관행 챕터

거대 경제권인 EU와 미국은 2013년 TTIP협상을 개시하여 진행하여 왔으나 이 역시 2016년 말 트럼프의 대통령 당선 이후 협상이 사실상 중단된 상태이다. TTIP협상에서 EU는 국내규제와 관련하여 모범규제관행(Good Regulatory Practices) 챕터를 제안하였는바, 주요 내용을 소개하면 다음과 같다.

(1) 모범규제관행챕터의 의의 및 적용범위

1. 당사국들은 무역과 투자를 촉진하는 가운데 높은 보호 수준에 기초한 공적정책의 목표를 달성하기 위해, 모범 규제 원칙 및 관행에 대한 당사국들의 공동의 책임(shared commitment)을 재확인 한다.

2. 이 장의 어떠한 규정도 당사국의 다음의 권리에 영향을 미치지 아니한다:

(a) 당사국의 모범 규제의 틀 및 원칙에 따라 공적정책의 목표를 달성하기 위한 각각의 규제 또는 행정 절차에서 정한 기한에 따라 지체 없이 행해진 조치를 채택, 유지, 적용할 권리.

(b) 자국의 관할권 내에서, 예컨대 위험평가 및 위험관리의 영역에서, 의사결정을 규율하는 당사국의 근본적 원리를 적용할 권리.[33]

31) TPP협정 제25.10조.
32) TPP협정 제25.11조.
33) EU에 대해서는, 그러한 원칙들은 EU 기능조약에서 뿐만 아니라 EU 기능조약 제289조에 따라 채택된 규정 및 지침에서 확립된 것도 포함한다.

3. 이 장은 EU와 미국에 대해 의무만을 부과한다.

이장의 목적상 a) "규제 행위(regulatory acts)"는 일반적 적용가능성이 있는 행위를 의미한다.[34] 규제 행위라 함은,

EU에 대해서는 i. EU 기능조약 제289조에 따라 채택을 위해 제안된 규정과 지침; ii. EU 기능조약 제290조와 제291조에 따라 각각 위임 및 지시된 행위

미국에 대해서는 i. (이 장의 제5조와 관련하여) 미국 의회의 구성원이 제안한 법률안 초안(Draft bills introduced by Members of Congress in Congress (with respect to Article 5 of this chapter); ii. 미국 행정부가 미국 의회에 제안한 법률안 초안; iii. 법률 또는 정책을 이행, 해석, 상세히 규정하거나, 조직, 절차, 관행적 요건을 구체화하는, 일반적 적용가능성과 장래의 효력을 갖는 기관의 설명(agency statements)

이 협정의 적용 대상이 되는 어떤 사안에 대해서도 b) "규제 당국(regulatory authorities)"은 다음을 의미한다. i. EU에 대해서는 EU 집행위원회; ii. 미국에 대해서는 중앙정부 수준에서 규정을 제정할 수 있는 모든 당국으로서 규제 행위를 할 수 있는 집행부와 독립 관청을 포함

(2) 내부 조율(Internal coordination)

각 당사국은 모범 규제 관행을 촉진하기 위한 목적으로 투명성 계획, 이해관계인 협의, 효과 분석 및 규제 행위의 사후평가(retrospective evaluations)를 포함하는 내부 조율 절차 또는 체계를 유지하여야 한다.

(3) 규제 절차에 대한 설명(Description of Regulatory Processes)

각 당사국은 일반 공중이 규제 행위의 개발에 대한 의견(input)을 제출할 수 있도록 허용하는 적용 가능한 지침, 규정 또는 절차를 포함한 규제 행위를 개발 및 검토할 자국의 규제당국이 채택한 규제 절차 및 체계에 대한 설명이 대중에게 이용 가능하도록 하여야 한다.

34) 보다 명확히 하기 위해서, 개별 자연인 또는 법인을 다루는 조치에는 적용되지 않는다.

(4) 조기 정보(Early information)

1. 각 당사국은 최소한 1년에 1회 계획 중인 주요[35] 규제 행위의 목록을 대중에게 이용 가능하도록 하여야 한다.

2. 영향평가 중인 계획된 주요 규제 행위에 대해 각 당사국은 가능한 한 조기에, 계획된 이해관계자와의 협의 및 무역과 투자 그리고 중소기업에 미칠 잠재적 영향을 포함한, 채택에 이르기까지의 계획과 시점에 관한 정보를 대중에게 이용 가능하도록 하여야 한다.

(5) 이해관계자 협의

1. 규제 행위를 준비할 때, 각 당사국은 자국의 각각의 규정과 절차를 따라 다음의 행위를 하여야 한다.

a. 어떤 자연인 또는 법인에게도 의견(input)을 제출할 합리적인 기회를 차별 없이 제공.

b. 자연인 또는 법인, 또는 타방 당사국이 자신의 이익이 상당하게 영향을 받을 것인지 여부 또는 그 영향의 정도에 대해 접근하는 것을 허용하기 위해, 예상되는 새로운 규제 행위에 관한 충분한 상세정보를 제공하는 규제 행위 초안 또는 협의 문서의 공표

2. 각 당사국은 가능한 경우 의사의 연락을 위해 전기적 수단을 사용하고 전용의 단일 웹 포털을 사용할 것을 추구한다.

3. 각 당사국은 자국이 수신한 의견을, 비밀정보의 보호나 개인정보 또는 부적절한 정보의 보류에 필요한 범위를 제외하고(except to the extent necessary to protect confidential information or withhold personal data or inappropriate content), 대중에게 이용 가능하도록 하여야 한다.

4. 제안된 또는 최종의 규제 행위[36]를 공표할 때 각 당사국은 협의 절차의 결과에 대한 설명을 대중에게 이용 가능하도록 하여야 한다.

35) 각 당사국의 규제당국은 "주요" 규제 행위를 정의한다.

36) 보다 명확히 하기 위해서, 이러한 의무는 별도의 그러나 같은 시기의(contemporaneous) 서류의 발간을 통해 이행될 수 있다.

(6) 기존 규제의 틀에 대한 의견 수집(Feedback)

각 당사국은 어떤 자연인 또는 법인도 관련 규제 당국에게 기존 규제의 틀에 대해, 어떤 규제의 틀이 건강, 환경, 복지, 안전 또는 다른 공공 정책적 목표를 달성하는데 비효율적인지 여부 또는 간소화 및 부담의 감축에 대한 제안을 포함하여, 의견을 제출할 수 있는 기회를 제공하여야 한다.

(7) 규제 영향 평가(Regulatory Impact Assessment)

1. 각 당사국은 계획된 규제 행위에 대해, 자국의 개별적인 규정과 절차에 따라, 영향 평가를 실시할 의도를 재확인 한다.

2. 제1항에 따른 규제 영향 평가를 실시할 때에는, 각 당사국은 다음을 보장하여야 한다.

a. 제안된 규제 행위의 필요성 및 규제 행위가 해결하고자 하는 문제의 성격과 중요성에 대한 고려.

b. 만약 규제 행위의 목적을 달성할 수 있는 경우, 실행 가능한 규제 그리고 비규제적 대안(규제하지 않는 것을 포함)에 대한 조사.

c. 해당 대안이 단기 및 장기적 사회, 경제, 환경에 미칠 잠재적 영향 평가 및 예상되는 비용 및 편익(어떤 비용 및 편익은 수량화 하기 어려운 점을 고려하여, 양적, 질적, 혹은 양자 모두)

3. 제1항에 따른 규제 영향 평가를 실시할 때에는, 중소기업의 발전에 규제 행위가 미칠 영향에 대해 특별한 주의를 기울여야 한다.

4. 제1항에 따른 규제 영향 평가의 전반적인 틀 내에서, 규제 당국은 고려중인 선택사항이, 다른 어떤 측면 중에서도, 아래 사항들을 평가하여야 한다.

a. 국제적으로 합의된 규제 관련 문서와의 연관성.

b. 타방 당사국이 동일한 사안에 대해 규제 행위를 도입하였거나 도입할 계획이 있는 경우, 규제에 접근하는 타방 당사국의 방식에 대한 고려.

c. 국제무역 및 투자에 미치는 영향.

5. 규제 영향 평가의 결과는 늦어도 규제 행위의 제안 또는 최종 규제 행위까지는

공표되어야 한다.

6. 당사국들은 규제정책 분석[37]에 적용된 방법론 및 경제적 추정뿐만 아니라, 국제무역 및 투자에 미치는 영향 평가에서의 자국의 관행에 관한 이용 가능한 관련 증거 및 자료에 관한 정보의 교류를 촉진하여야 한다.

(8) 사후평가(Retrospective Evaluation)

1. 각 당사국은 규제의 틀에 관한 정기적 사후평가를 촉진하기 위한 절차와 체계를 유지하여야 한다.

2. 각 당사국은 계획된 사후평가에 관한 경험의 교환과 정보의 공유를 촉진하여야 한다.

3. 각 당사국은 모든 사후평가의 결과를 대중에게 이용 가능하도록 하여야 한다.

(9) 규제정보 관리를 위한 데이터베이스[38]

4. 국내규제의 국제적 규율 논의 배경, 평가 및 정책적 시사점

(1) 서비스무역규범에서의 국내규제 규율 논의 배경 및 의의

1) WTO GATS에서의 국내규제의 규율 배경 및 의의

GATS 전문에서는 국가의 정책 목표(national policy objectives)를 충족시키기 위하여 자기 나라 영토 내의 서비스 공급을 규제하고, 신규 규제를 도입할 수 있는 회원국의 국내규제 권한을 인정한다. 그러한 국가 정책목표로는 소비자 보호, 소득이나 주거지와 관계없이 특정 서비스에 대한 형평한 이용(가령, 통신, 교통 및 보건서비스 경우), 시장지배나 반경쟁관행의 방지, 국민보건 등 다양하기 마련이다. 가령, 의사와 같은 전문직서비스에

37) 어떤 정보의 교환도 비밀정보의 교환에 관하여 합의된 규정을 준수하여야 할 필요가 있으며, 비밀정보 보호 및 지시재산권에 의해 보호받는 정보에 관한 각 당사국의 법체계에 합치하여야 한다.

38) 구체 내용은 제시되어 있지 아니하다.

대한 면허 제도에 따른 규제는 '환자라는 소비자의 보호' 내지 국민보건이라는 정책목표에 해당될 것이다.

한편 GATS는 서비스무역 자유화를 위해 목표로 하고 있다. 이를 위해 GATS 하에서 WTOP 회원이 자국의 구체적 약속양허표를 통해 특정 서비스분야(업종)에 대해 시장개방을 약속하였다. 그렇지만, 이와 같이 GATS 하에서 특정 서비스분야(업종)의 개방을 약속한 경우라 할지라도 각 회원국이 해당 서비스분야(업종)에 국내규제를 갖고 있거나 새로이 이를 도입하는 경우 그러한 국내규제가 시장개방을 통해 서비스를 공급할 수 있게 된 다른 회원국 서비스공급자의 비즈니스에 영향을 미칠 수 있다. 환언하면, 각 회원국의 양허표를 통해 시장개방이 이루어진 서비스분야(업종)에서도 합법적으로 도입, 시행되는 다양한 형태의 국내규제가 그러한 개방된 서비스분야(업종)에 있어 자유로운 무역(서비스공급)에 중대한 장벽으로 작용할 수 있다.

요컨대, 국가정책의 정당한 목적(legitimate objective)을 달성하기 위한 국내규제는 인정되나 이러한 규제가 서비스무역에 중대한 장벽으로 작용할 수 있는 경우가 발생할 수 있는 점에서 서비스통상규범에서의 국내규제에 대한 일정한 규율의 필요성이 제기된다. 이를 위하여 GATS 제6조(국내규제) 1항에서는 구체적 약속이 행하여진 분야에 있어 각 회원국이 서비스무역에 영향을 미치는 일반적으로 적용되는 모든 조치가 합리적이고 객관적이며 공평한 방식으로(in a reasonable, objective and impartial manner) 시행되도록 보장할 것을 요구한다. GATS 제6조 4항에서는 자격요건과 절차, 기술표준 및 면허요건과 관련된 조치가 서비스무역에 불필요한 장벽(unnecessary barriers to trade in services)이 되지 않도록 보장하기 위한 규율을 수립할 것을 요구하며, 그러한 국내규제의 규율에 있어 (a) 서비스를 공급할 자격 및 능력과 같은 객관적이고 투명한 기준에 기초할 것, (b) 서비스의 질을 보장하기 위하여 필요한 정도 이상의 부담을 지우는 것이 아닐 것, (c) 허가절차의 경우 그 자체가 서비스공급을 제한하는 조치가 아닐 것을 보장할 것으로 목표로 제시한다.

2) TPP협정에서의 규제일관성 챕터의 도입 배경 및 의의

정부는 공정한 경쟁, 소비자 안전, 환경 보호, 작업장의 안전 및 다른 정당한 정책적 목적을 위해 이에 대한 규제 권한과 책임을 갖고 있다. 그런데 규제 환경 및 제도가 국가에 따라 큰 차이가 있다. 가령, 미국의 경우 투명성, 공평성 및 적법절차를 보장하기 위해 규칙제정 절차가 잘 만들어져 있다. 또한 미국은 관련 이슈를 담당하는 상이한 기관들에 의해 규제간의 충돌을 초래할 수 있는 내부 결정을 방지하고 기관들이 규제할 책임을 맡고 있는 이해관계자들에 의해 부당하게 영향을 받는 것을 방지하기 위한 정부 부처들 간에 있어 잘짜여진 조정제도가 마련되어 있다.[39] 반면에 국가가 갖는 국내규제 권한을 둘러싸고 특히 중복적이거나 과도한 국내규제 또는 신규 국내규제의 도입이나 운영에 있어 투명성의 결여 등으로 인해 외국의 상품이나 서비스공급자 또는 투자자가 상당한 장벽에 직면하게 하는 경우가 적지 않음도 사실이다. 또한 아시아-태평양 권역 국가들의 규제 환경 및 제도는 상당히 다양하여 이 지역 정부들은 상이한 규제 우선순위를 가질 수 있고 따라서 특정 규제 이슈들에 대해 다른 결론을 내릴 수 있다.

그러나 이들 국가들은 신뢰할만하고 객관적인 데이터에 기초한 규제를 개발하고, 자신들의 시장에 있어 상충되는 요건을 회피하며, 정책목적을 달성하기 위해 요건이 가능한 가장 효과적인 방법으로 충족될 수 있도록 하며, 최적의 결과를 도출하는 의사결정이 될 수 있도록 공중의 의견 개진을 보장하는 점에 있어 공통된 이익을 가진다. 또한 이들 국가는 새로운 도전에 대처하기 위한 적절한 규제방법에 대한 정보를 교환하고 협조하는데 관심을 공유한다. 이는 TPP 경제가 보다 통합되어 가고 기업들이 국경을 넘어 생산과 공급망을 관리하며 근로자들이 이러한 생산과 공급망이 지원하는 일자리에 보다 많이 의존하게 되는 경우 특히 중요하다.[40]

이러한 배경에서 미국 정부는 TPP협정 안에 "규제일관성" 챕터의 도입을 추진하였고, 이는 아시아 태평양 지역에서 활동하는 자국 기업들에게 TPP 회원국 내에서 개방된, 공정한 그리고 예측 가능한 규제 환경을 촉진함으로써 회원국들 간의 무역을 보다 원활하고

39) https://medium.com/the-trans-pacific-partnership/regulatory-coherence-6672076f307a#.g9ptcnmls
40) https://medium.com/the-trans-pacific-partnership/regulatory-coherence-6672076f307a#.g9ptcnmls

효율적으로 만들어 이를 통해 이들 간의 무역과 투자를 촉진하기 위한 것이 주된 목적이었다.[41]

이 점에서 TPP 규제일관성 챕터에서도 (i) 당사국 간 상품 및 서비스 무역의 증대 그리고 투자의 증대를 촉진하는 측면에서 규제 일관성을 통하여 본 협정의 혜택을 지속하고 향상하는 것의 중요성을 인정하고 이를 위하여 규제 조치의 개발에 있어 이해관계자로부터의 의견 반영 및 당사국들 간의 규제 협력 및 역량 배양 개발의 중요성을 인정한다.[42] 이와 더불어 해당 당사국이 적절하다고 간주하는 수준에서 각 당사국의 규제의 우선순위(regulatory priorities)를 확인하고 이러한 우선순위를 처리하기 위하여 규제 조치를 수립하고 시행할 각 당사국의 주권과 공공 정책의 목적 달성에서 규제의 역할의 중요성 역시 함께 인정한다.[43] 더불어, TPP 규제 일관성 챕터에서의 규제 일관성을 촉진하기 위한 장치로서 (i) 조정 및 검토 절차 또는 메커니즘, (ii) 핵심 우수 규제 관행(Core Good Regulatory Practices: GRP)의 시행, (iii) 규제 일관성위원회 설치, (iv) 이해관계자의 참여, (v) 이행 통지, (vi) 협력에 대해 규정한다. 이와 관련 제25장의 목적상 규제 일관성이란 국내 정책 목적 달성을 촉진하기 위하여 규제조치를 기획, 설계, 공표, 이행 및 검토하는 과정에서, 그리고 그러한 정책 목적을 발전시키고 국제 무역 및 투자, 경제 성장과 고용을 증진하기 위한 범정부적인 노력에서 모범 규제관행(good regulatory practices: GRP)의 이용을 의미한다.[44]

(2) TPP 규제일관성 챕터의 평가

TPP협정에서 처음 도입된 규제 일관성 챕터는 정부가 갖는 합법적인 권한인 국내규제로 인한 국제 무역 및 투자에의 부정적 영향을 최소화하기 위하여 한편으로 당사국의 국내 차원에서 모든 당사국 정부로 하여금 규제 조치 개발 과정과 연계된 부처 간 협의 및 조정을 확대하기 위한 정부 기관들 간의 조정과 효과적인 기관 상호간 협의 메커니즘(mechanism

41) https://ustr.gov/tpp/outlines-of-TPP.
42) TPP협정 제25.2조 2항 가,라,마호.
43) TPP협정 제25.2조 2항 나,다호
44) TPP협정 제25.2조 1항.

for effective interagency consultation)을 수립할 것과 핵심 모범규제관행(Core Good Regulatory Practices)의 시행을 권장한다. 특히, 후자와 관련하여 제안된 적용 대상 규제조치에 대한 규제 영향 평가(regulatory impact assessment)를 실시할 것, 규제가 명료하고 간결하게 입안되도록 보장할 것, 일반이 신규 규제조치에 대한 정보에 접근할 수 있도록 보장할 것, 기존 규제조치에 대해서는 당해 조치가 그 도입 목적을 달성하기 위한 가장 효과적인 조치인지를 판단하기 위해 정기적으로 심사할 것 등을 요구한다. 그런데, 이들 규정은 미국의 규제절차의 핵심 요소라 할 수 있는 투명성, 공평성, 적법절차 및 조화로운 규제 접근을 보장하기 위한 정부 부처들 간의 협력과 같은 제반 원칙을 수용한 것이라는 점이 주목된다.[45] 다만, 규제 일관성 챕터가 TPP 당사국들의 보건, 안전, 노동 및 환경 보호, 국가안보, 재정 건전성 및 그 밖의 공익적 사유를 위한 규제 권한에는 영향을 미치는 것은 아니다.

다른 한편으로 당사국들 간의 국제 차원에서 규제일관성위원회의 설치, 이행의 통지 및 국제 협력에 대해 규정하고 있음도 주목된다.

이와 같이 이해관계자의 의견 반영 기회와 더불어 모범 규제관행을 기초로 입안되고 시행되며 부처 간에 조정되는 일관된 규제절차는 아시아-태평양 시장에서 활동하는 TPP 참가국 기업들에게 공개되고, 공정하며 예측 가능한 기회를 만들어 줌에 있어 매우 중요한 요소가 될 것이다. 다만, 규제 일관성 챕터가 무역 및 투자와 관련된 구체적인 규제 이슈들을 다루는 것이 아니라 TPP 참가국들이 규제를 개발하는 전반적인 절차 내지 시스템을 대상으로 하는 것임을 유의할 필요가 있다.[46] 또한 TPP 규제 일관성 챕터가 각 참가국의 자신의 규제 우선순위를 정하고, 이러한 우선순위에 대처하기 위해 자신이 적절하다고 판단하는 조치를 입안하고 시행할 권한을 재확인하고 있음에도 불구하고, 당해 챕터가 향후 모범 규제 관행의 영향력을 확산하는데 기여할 것으로 기대된다.

45) USTR, The Trans-Pacific Partnership: Detailed Summary of U.S. Objectives(이하 'USTR 2015'), 2015, p.34.
46) https://medium.com/the-trans-pacific-partnership/regulatory-coherence-6672076f307a#.g9ptcnmls

(3) TPP 및 TTIP에서의 국내규제 규율(모범규제관행 포함)에 대한 평가 및 시사점

먼저 1994년 이후 APEC, OECD 등과 같은 국제기구에서 모범규제관행에 대해 그리고 APEC-OECD 합동 회의에서는 보다 큰 틀에서 규제개혁에 관해 국제적 논의를 추진하게 된 배경은 역내 국가들 간의 상이한 기준, 기술규정 및 적합성 제도로 인해 무역과 투자에 미치는 부정적 영향을 줄이고, 개선된 표준 및 적합성 운영을 통해 시장접근을 촉진하고, 고양하기 위한 것이었다. 이에 대해 최근 TPP나 TTIP 협상에서의 모범규제관행(GRP)을 포함한 규제 일관성 내지 규제협력에 관한 규정의 도입을 추진하는 취지는 무역 및 투자에 있어 국가의 국내규제가 갖는 부정적 영향을 줄이거나 제거하기 위한 것이라는 점에서 차이가 있다. 즉, GRP를 포함한 국내규제 규율 논의의 추진 배경이 최초 기술규제에 대한 대응으로부터 비롯되어 최근의 무역협정 협상에서는 기술규제를 포함한 국내규제 전반을 대상으로 확대되었다는 점이 주목된다. 이는 GATS와 FTA에서의 무역자유화가 상품무역 이외에 서비스무역을 포함하게 된 것과 긴밀한 관계가 있다. 앞서 지적하였듯이 국내규제가 존재하는 서비스시장 개방은 실질적인 개방 효과가 나타나지 않을 수 있기 때문이다.

다음으로 TPP 협정 규제 일관성챕터에서는 핵심 모범규제관행(GRP)으로서 규제영향평가, 규제정보 공개 및 제공 등을 규정하면서 이밖에도 조정 및 검토절차, 이해관계자의 참여, 규제 일관성 위원회, 이행 통지, 규제당국 간 관련 정보 공유 및 대화 등 협력에 대해 규정한다. 이에 대해 EU가 TTIP 협상에서 제안한 모범규제관행 제안에 따르면 내부 조율 체계 유지, 규제절차에 대한 설명, 조기 정보 제공, 규제행위 입안시 이해관계자와의 협의, 기존 규제에 대한 의견 수렴, 규제영향평가, 규제의 사후평가, 규제정보관리 데이터베이스 구축 등 TPP 규제 일관성챕터상의 다양한 장치를 포함하고 있어 사실상 규제 일관성의 다른 버전이라 볼 수도 있다. 이와 같이 TTP나 TTIP 협상은 물론 APEC이나 OECD와 같은 국제기구 논의에서의 모범규제관행의 구성 요소를 보면 서로 차이가 있는바, 이는 GRP의 구성요소는 확정된 것이 아니라 일종의 non-exhaustive list로서 이해하여 할 것이며, 따라서 필요하다면 새로운 구성 요소가 얼마든지 추가될 수 있다. 다만, (i) 규제 도입 단계에서의 정보 교환 및 통보, (ii) 규제 입안 활동에 있어 국내규제당국들 간의 내부 조정 (iii) (비용 편익 분석 등) 규제 영향 평가, (iv) 투명성, (v) 규제 도입 단계에서의 (국내 및 해외) 이해관계자의 참여(공중 협의 또는 공중 참여) 등이 GRP의 핵심요소(core

elements)로서 언급된다. 따라서 이들 요소의 보장이 향후 GRP에 관한 국제규범 논의(협상)에서 핵심 쟁점이 될 것이다.

한편, TTIP협상에서는 EU가 제안한 모범규제관행챕터 이외에 규제협력챕터가 함께 논의되고 있고, TTIP 규제협력챕터에 대한 EU 제안을 보면 투명성 및 공중 참여 등 GRP의 구성요소를 포함하여 규정하고 있다. 환언하면, 모범규제관행 챕터가 규제협력(Regulatory Cooperation) 챕터의 대체규정에 상당하는 것이 될 수 있다. 사실 체약국들 간의 규제협력은 모범규제관행을 확산, 전파하는 효과적인 수단으로서 규제당국들 간의 대화, 정보 공유, 규제 정보 제공을 위한 단일의 온라인 창구 설치에서 특정 협정 협상에 이르기까지 광범위하며, GRP의 구성 요소를 포함하기도 한다. 일반적으로 규제협력은 모범규제관행의 요소들을 포함하고 이밖에도 규제당국들 간의 다양한 협력 장치를 포괄하는 보다 광의의 개념이기는 하나 앞에서 언급하였듯이 GRP나 규제협력 모두 (기술)규제의 무역장벽적 효과를 방지 또는 완화하기 위한 수단이라는 점에서 동일하고 이들 두 수단의 구성요소들에 대한 법적 제한이 있는 것도 아니어서 양자 간의 구분 실익 자체가 큰 의미가 없다. 다만, 2016년 서명된 TPP에서 모범규제관행 대신에 규제협력에 보다 가까운 규제일관성 챕터를 도입한 점이나 TTIP 협상에서 EU가 GRP 챕터와 함께 규제협력 챕터를 제안한 점 등에 비추어 보면, 좁은 범위의 GRP보다는 보다 넓은 범위의 규제협력이나 규제일관성 타이틀 하의 국내규제 규범의 이용이 보다 선호될 것으로 보여진다.

〈표 1〉 TPP 및 TTIP 협정에서의 국내규제 규율 관련 규정 비교

TPP협정	TTIP협정안
■ 규제 일관성챕터(제25장) - 조정 및 검토절차 - 핵심모범규제관행 시행 · 규제영향평가 · 규제정보의 온라인상 게시 · 1년내 도입 규제 정보 사전 제공 - 규제일관성위원회 - 이해관계자의 참여 - 이행통지 - 관련 정보공유, 대화 등 협력	■ EU 제안 모범규제관행챕터 - 내부 조율 체계 유지 - 규제절차에 대한 설명 - 조기 정보 제공 - 규제행위 입안시 이해관계자와의 협의 - 기존 규제에 대한 의견 수렴 - 규제영향평가 - 규제의 사후평가 - 규제정보관리 데이터베이스 구축

■ 투명성규정(제26장 부패방지 및 투명성 챕터 일부) - 협정 적용대상 행정결정의 공표 - 제안된 규정의 관보 또는 웹사이트 게재 및 온라인 단일 포털에 통합과 적용 사안 공표 - 행정절차에 있어 합리적인 통지 및 의견 개진 기회 제공 - 재심 및 불복청구 보장	■ EU 제안 규제협력챕터 - 전문 - 목적 및 일반원칙 - 정의 - 범위 - 규제협력 규율 총칙 - 규제양립성 촉진 구체적 활동 - 투명성 및 공중 참여 - 중앙 이외 수준에서의 규제협력 - 입법제안 - 분쟁해결의 비적용 - 부속서: 이행을 위한 제도적 장치 ■ 투명성챕터안

다른 한편으로 미국 및 EU가 최근 추진하였던 TPP나 TTIP 협상에서 기존의 WTO 무역에 대한 기술장벽협정(TBT협정)이나 이에 기초한 FTA TBT 챕터와는 별도로 모범규제관행을 포함한 규제 일관성 내지 규제협력 챕터를 도입하고자 하는 또 다른 배경은 기술규제에 있어 조화(harmonization) 내지 상호인정(mutual recognition)을 통한 무역장벽적 효과를 제거 내지 완화하는 것이 갖는 한계를 인식하고, 대신에 무역 및 투자에 부정적 영향을 미치는 기술규제를 방지하기 위한 보다 효과적인 장치로서 기술규제를 포함한 국내규제입법절차에 있어 투명성, 규제영향평가, 이해관계자의 참여 등의 보장을 인식한 것으로 보아야 할 것이다. 더욱이 규제 일관성 챕터나 규제협력 챕터는 상품 관련 국내 기술규제는 물론 서비스 관련 제반 국내규제에도 함께 적용되는 것이어서 그 효과가 훨씬 넓기 때문이다. 이러한 점에서 향후 미국과 EU가 주도하는 무역협정에서는 모범규제관행을 포함한 규제 일관성 챕터 내지 규제 협력 챕터의 도입에 큰 이해관계를 갖고 협상의 우선순위를 둘 가능성이 크다. 향후 우리가 체결하는 무역협정 안에 이러한 국내규제 규율이 포함될 경우 우리의 국내규제 규율 법 및 정책에 직간접적인 영향을 미치는 점에서 이에 대한 면밀한 대응이 요구된다.

부 록

〈부록 1〉 COMMUNICATION FROM INDIA

CONCEPT NOTE FOR AN INITIATIVE ON TRADE FACILITATION IN SERVICES

WORLD TRADE ORGANIZATION

S/WPDR/W/55

27 September 2016

(16-5137) Page: 1/2

Working Party on Domestic Regulation Original: English

COMMUNICATION FROM INDIA

CONCEPT NOTE FOR AN INITIATIVE ON TRADE FACILITATION IN SERVICES

The following communication from the delegation of India, dated 23 September 2016, is being circulated to the Members of the Working Party on Domestic Regulation.

---

1 BACKGROUND AND MOTIVATION

1.1. Services occupy a significant and growing share of domestic and international transactions. However, trade flows in services remain subject to numerous border and behind-the-border barriers as well as procedural bottlenecks, which are impediments to the realization of the full potential of services trade. These impediments particularly limit the benefits of trade in services especially for small and medium enterprises and small exporters worldwide.

1.2. The Trade Facilitation Agreement ("TFA"), adopted by WTO Members in 2014, was a significant milestone in relation to trade in goods. Its overall purpose is to expedite the movement, release and clearance of goods as well as co-operation on customs compliance issues. Like the TFA, there is need for a counterpart agreement in services, an Agreement on Trade Facilitation in Services ("TFS Agreement"), which can result in reduction of transaction costs associated with unnecessary regulatory and administrative burden on trade in services. The TFS Agreement will address the key issues that are pertinent to facilitating trade in services, such as transparency, streamlining procedures, and eliminating bottlenecks.

1.3. The scope of the proposed TFS Agreement would encompass measures by Members affecting trade in services across all modes of supply.

1.4. Importantly, the TFS Agreement, as in the case of the TFA, will also contain provisions for special and differential treatment for developing countries and LDCs and address related issues of technical assistance and support for capacity building.

2 ILLUSTRATIVE ELEMENTS OF A TFS AGREEMENT

2.1. The TFS Agreement could be based on the TFA in goods, with suitable modification and adaptation to the services context, as required.

2.2. Some of the issues would be cross-cutting issues relevant for all modes of supply of services, and others would be specific to each mode of supply.

2.3. An illustrative list of such elements is provided below:

2.1 CROSS-CUTTING ISSUES

- Publication and availability of information, including automation and international electronic exchange of trade data.
- Transparency in application of all measures of general application affecting trade in services.
- Ensuring administration of measures affecting trade in services in a reasonable, objective and impartial manner.
- Consultations and cooperation among relevant authorities.
- Opportunities to comment before entry into force of measures affecting trade in services.
- Procedures and timelines for consideration of applications from service suppliers, as well as for appeal and review.
- Disciplines on taxes, fees, charges and other levies on supply of services.
- Special and Differential Treatment for developing country Members and LDCs.
- Institutional arrangements.

2.2 MODE-SPECIFIC ISSUES

Mode 1:

- Facilitation of free flow of data across borders for ensuring meaningful supply of Mode 1 services.

Mode 2:

- Facilitation of supply of Mode 2 services, including through cross border insurance portability for availing of medical or tourist related services in a foreign country.
- Endeavour to streamline temporary entry formalities, such as visa processing fees, procedures and timelines for consumers seeking entry into another country to avail of services (such as medical services, education services, tourism, etc.).

Mode 3:

- Facilitation of supply of Mode 3 services, including through measures such as single window clearance for setting up commercial presence.
- Disciplines on charges applicable on Mode 3 service suppliers, in order to ensure that these do not unfairly disadvantage foreign service suppliers.

Mode 4:

- Facilitation of supply of Mode 4 services through simplification of procedures for temporary entry and stay, and clarity in respect of work permits and visas as relevant for the categories of the Mode 4 commitments.
- Disciplines on measures relating to taxation, fees/charges, discriminatory salary requirements, social security contributions in relation to temporary entry, etc. in order to ensure that these do not unfairly disadvantage foreign service suppliers.

3 CONCLUDING COMMENTS

India firmly believes that like the TFA, a well-structured TFS will significantly enhance the potential for trade in services for all Members. This concept requires careful deliberation in order to enable the development of a framework that can effectively address the main concerns of all Members. India looks forward to comments and suggestions from all Members on this critical concept and to developing the elements for the same.

〈부록 2〉 TPP CHAPTER 25 REGULATORY COHERENCE

CHAPTER 25

REGULATORY COHERENCE

Article 25.1: Definitions

For the purposes of this Chapter:

covered regulatory measure means the regulatory measure determined by each Party to be subject to this Chapter in accordance with Article 25.3 (Scope of Covered Regulatory Measures); and

regulatory measure means a measure of general application related to any matter covered by this Agreement adopted by regulatory agencies with which compliance is mandatory.

Article 25.2: General Provisions

1. For the purposes of this Chapter, regulatory coherence refers to the use of good regulatory practices in the process of planning, designing, issuing, implementing and reviewing regulatory measures in order to facilitate achievement of domestic policy objectives, and in efforts across governments to enhance regulatory cooperation in order to further those objectives and promote international trade and investment, economic growth and employment.

2. The Parties affirm the importance of:

(a) sustaining and enhancing the benefits of this Agreement through regulatory coherence in terms of facilitating increased trade in goods and services and increased investment between the Parties;

(b) each Party's sovereign right to identify its regulatory priorities and establish and implement regulatory measures to address these priorities, at the levels that the Party considers appropriate;

(c) the role that regulation plays in achieving public policy objectives;

(d) taking into account input from interested persons in the development of regulatory measures; and

(e) developing regulatory cooperation and capacity building between the Parties.

Article 25.3: Scope of Covered Regulatory Measures

Each Party shall promptly, and no later than one year after the date of entry into force of this Agreement for that Party, determine and make publicly available the scope of its covered regulatory measures. In determining the scope of covered regulatory measures, each Party should aim to achieve significant coverage.

Article 25.4: Coordination and Review Processes or Mechanisms

1. The Parties recognise that regulatory coherence can be facilitated through domestic mechanisms that increase interagency consultation and coordination associated with processes for developing regulatory measures. Accordingly, each Party shall endeavour to ensure that it has processes or mechanisms to facilitate the effective interagency coordination and review of proposed covered regulatory measures. Each Party should consider establishing and maintaining a national or central coordinating body for this purpose.

2. The Parties recognise that while the processes or mechanisms referred to in paragraph 1 may vary between Parties depending on their respective circumstances (including differences in levels of development and political and institutional structures), they should generally have as overarching characteristics the ability to:

(a) review proposed covered regulatory measures to determine the extent to which the development of such measures adheres to good regulatory practices, which may include but are not limited to those set out in Article 25.5 (Implementation of Core Good Regulatory Practices), and make recommendations based on that review;

(b) strengthen consultation and coordination among domestic agencies so as to identify potential overlap and duplication and to prevent the creation of inconsistent requirements across agencies;

(c) make recommendations for systemic regulatory improvements; and

(d) publicly report on regulatory measures reviewed, any proposals for systemic regulatory improvements, and any updates on changes to the processes and mechanisms referred to in paragraph 1.

Each Party should generally produce documents that include descriptions of those processes or mechanisms and that can be made available to the public.

Article 25.5: Implementation of Core Good Regulatory Practices

1. To assist in designing a measure to best achieve the Party's objective, each Party should generally encourage relevant regulatory agencies, consistent with its laws and regulations, to conduct regulatory impact assessments when developing proposed covered regulatory measures that exceed a threshold of economic impact, or other regulatory impact, where appropriate, as established by the Party. Regulatory impact assessments may encompass a range of procedures to determine possible impacts.

2. Recognising that differences in the Parties' institutional, social, cultural, legal and developmental circumstances may result in specific regulatory approaches, regulatory impact assessments conducted by a Party should, among other things:

(a) assess the need for a regulatory proposal, including a description of the nature and significance of the problem;

(b) examine feasible alternatives, including, to the extent feasible and consistent with laws and regulations, their costs and benefits, such as risks involved as well as distributive impacts, recognising that some costs and benefits are difficult to quantify and monetise;

(c) explain the grounds for concluding that the selected alternative achieves the policy objectives in an efficient manner, including, if appropriate, reference to the costs and benefits and the potential for managing risks; and

(d) rely on the best reasonably obtainable existing information including relevant scientific, technical, economic or other information, within the boundaries of the authorities, mandates and resources of the particular regulatory agency.

3. When conducting regulatory impact assessments, a Party may take into consideration the potential impact of the proposed regulation on SMEs.

4. Each Party should ensure that new covered regulatory measures are plainly written and are clear, concise, well organised and easy to understand, recognising that some measures address technical issues and that relevant expertise may be needed to understand and apply them.

5. Subject to its laws and regulations, each Party should ensure that relevant regulatory agencies provide public access to information on new covered regulatory measures and, where practicable, make this information available online.

6. Each Party should review, at intervals it deems appropriate, its covered regulatory measures to determine whether specific regulatory measures it has implemented should be modified, streamlined, expanded or repealed so as to make the Party's regulatory regime more effective in achieving the Party's policy objectives.

7. Each Party should, in a manner it deems appropriate, and consistent with its laws and regulations, provide annual public notice of any covered regulatory measure that it reasonably expects its regulatory agencies to issue within the following 12-month period.

8. To the extent appropriate and consistent with its law, each Party should encourage its relevant regulatory agencies to consider regulatory measures in other Parties, as well as relevant developments in international, regional and other fora when planning covered regulatory measures.

Article 25.6: Committee on Regulatory Coherence

1. The Parties hereby establish a Committee on Regulatory Coherence (Committee), composed of government representatives of the Parties.

2. The Committee shall consider issues associated with the implementation and operation of this Chapter. The Committee shall also consider identifying future priorities, including potential sectoral initiatives and cooperative activities, involving issues covered by this Chapter and issues related to regulatory coherence covered by other Chapters of this Agreement.

3. In identifying future priorities, the Committee shall take into account the activities of other committees, working groups and any other subsidiary body established under this Agreement and shall coordinate with them in order to avoid duplication of activities.

4. The Committee shall ensure that its work on regulatory cooperation offers value in addition to initiatives underway in other relevant fora and avoids undermining or duplicating such efforts.

5. Each Party shall designate and notify a contact point to provide information, on request by another Party, regarding the implementation of this Chapter in accordance with Article 27.5 (Contact Points).

6. The Committee shall meet within one year of the date of entry into force of this Agreement, and thereafter as necessary.

7. At least once every five years after the date of entry into force of this Agreement, the Committee shall consider developments in the area of good regulatory practices and in best practices in maintaining processes or mechanisms

referred to in Article 25.4.1 (Coordination and Review Processes or Mechanisms), as well as the Parties' experiences in implementing this Chapter with a view towards considering whether to make recommendations to the Commission for improving the provisions of this Chapter so as to further enhance the benefits of this Agreement.

Article 25.7: Cooperation

1. The Parties shall cooperate in order to facilitate the implementation of this Chapter and to maximise the benefits arising from it. Cooperation activities shall take into consideration each Party's needs, and may include:

(a) information exchanges, dialogues or meetings with other Parties;

(b) information exchanges, dialogues or meetings with interested persons, including with SMEs, of other Parties;

(c) training programmes, seminars and other relevant assistance;

(d) strengthening cooperation and other relevant activities between regulatory agencies; and

(e) other activities that Parties may agree.

2. The Parties further recognise that cooperation between Parties on regulatory matters can be enhanced through, among other things, ensuring that each Party's regulatory measures are centrally available.

Article 25.8: Engagement with Interested Persons

The Committee shall establish appropriate mechanisms to provide continuing opportunities for interested persons of the Parties to provide input on matters relevant to enhancing regulatory coherence.

Article 25.9: Notification of Implementation

1. For the purposes of transparency, and to serve as a basis for cooperation and capacity building activities under this Chapter, each Party shall submit a notification of implementation to the Committee through the contact points designated pursuant to Article 27.5 (Contact Points) within two years of the date of entry into force of this Agreement for that Party and at least once every four years thereafter.

2. In its initial notification, each Party shall describe the steps that it has taken since the date of entry into force of this Agreement for that Party, and the steps that it plans to take to implement this Chapter, including those to:

(a) establish processes or mechanisms to facilitate effective interagency coordination and review of proposed covered regulatory measures in accordance with Article 25.4 (Coordination and Review Processes or Mechanisms);

(b) encourage relevant regulatory agencies to conduct regulatory impact assessments in accordance with Article 25.5.1 (Implementation of Core Good Regulatory Practices) and Article 25.5.2;

(c) ensure that covered regulatory measures are written and made available in accordance with Article 25.5.4 (Implementation of Core Good Regulatory Practices) and Article 25.5.5;

(d) review its covered regulatory measures in accordance with Article 25.5.6 (Implementation of Core Good Regulatory Practices); and

(e) provide information to the public in its annual notice of prospective covered regulatory measures in accordance with Article 25.5.7 (Implementation of Core Regulatory Practices).

3. In subsequent notifications, each Party shall describe the steps, including those set out in paragraph 2, that it has taken since the previous notification, and those that it plans to take to implement this Chapter, and to improve its adherence to it.

4. In its consideration of issues associated with the implementation and operation of this Chapter, the Committee may review notifications made by a Party pursuant to paragraph 1. During that review, Parties may ask questions or discuss specific aspects of that Party's notification. The Committee may use its review and discussion of a notification as a basis for identifying opportunities for assistance and cooperative activities to provide assistance in accordance with Article 25.7 (Cooperation).

Article 25.10: Relation to Other Chapters

In the event of any inconsistency between this Chapter and another Chapter of this Agreement, the other Chapter shall prevail to the extent of the inconsistency.

Article 25.11: Non-Application of Dispute Settlement

No Party shall have recourse to dispute settlement under Chapter 28 (Dispute Settlement) for any matter arising under this Chapter.

〈부록 2〉 TTIP– EU proposal for Chapter: Good Regulatory Practices

*This **TEXTUAL PROPOSAL** is the European Union's proposal for legal text on "Good Regulatory Practices" in TTIP. It was tabled for discussion with the US and made public on 21 March 2016. The actual text in the final agreement will be a result of negotiations between the EU and US.*

TTIP- EU proposal for Chapter: Good Regulatory Practices

Article 1 - General Provisions

1. The Parties reaffirm their shared commitment to good regulatory principles and practices to achieve public policy objectives based on a high level of protection, while facilitating trade and investment.

2. Nothing in this Chapter shall affect the rights of each Party to:

   (a) adopt, maintain and apply measures without delay, in accordance with deadlines under its respective regulatory or administrative procedures, to achieve its public policy objectives, in accordance with its regulatory framework and principles;

   (b) apply its fundamental principles governing decision-making in its jurisdiction, for example in the areas of risk assessment and risk management.[1]

3. This Chapter shall only impose obligations on the European Union and the United States.

Article 2 - Definitions

For the purposes of this Chapter:

a) "regulatory acts' means acts of general applicability[2]:

for the EU:

i. proposed Regulations and Directives submitted for adoption pursuant to Article 289 of the Treaty on the Functioning of the European Union;

ii. Delegated and Implementing acts pursuant to Articles 290 and 291, respectively of that Treaty.

for the US:

i. Draft bills introduced by Members of Congress in Congress (with respect to Article 5 of this chapter)

[1] For the EU, such principles include those established in the Treaty on the Functioning of the European Union as well as in Regulations and Directives adopted pursuant to Article 289 of the Treaty on the Functioning of the European Union.
[2] For greater certainty, this does not apply to measures addressed to individual natural or legal persons.

EU-US TTIP Negotiations

ii. Draft bills proposed by the US Administration to Congress

iii. agency statements of general applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organisation, procedure, or practice requirements of an agency;

in respect to any matter covered by this Agreement.

b) "regulatory authorities" means:

i. for the EU, the European Commission;

ii. for the US, any rule-making authority at the central level of government, including any Executive Branch or independent agency that develops regulatory acts.

Article 3 – Internal coordination

Each Party shall maintain internal coordination processes or mechanisms in order to foster good regulatory practices, including transparent planning, stakeholder consultation, impact assessments and retrospective evaluations of regulatory acts.

Article 4 - Description of Regulatory Processes

Each Party shall make publicly available a description of the processes and mechanisms employed by its regulatory authorities to develop and to review regulatory acts, including the applicable guidelines, rules or procedures which allow the public to provide input to the development of regulatory acts.

Article 5 – Early information

1. Each Party shall make publicly available at least once a year a list of planned major[3] regulatory acts. Such list shall provide information on the scope and objectives of the regulatory acts.

2. For planned major regulatory acts undergoing impact assessment each Party shall make publicly available, as early as possible, information on planning and timing leading to their adoption, including on planned stakeholder consultations and potential for significant impacts on trade, investment and on small and medium sized enterprises (SMEs).

[3] Regulatory authorities of each Party define "major" regulatory acts.

EU-US TTIP Negotiations

*This **TEXTUAL PROPOSAL** is the European Union's proposal for legal text on "Good Regulatory Practices" in TTIP. It was tabled for discussion with the US and made public on 21 March 2016. The actual text in the final agreement will be a result of negotiations between the EU and US.*

Article 6 – Stakeholder Consultations

1. When preparing regulatory acts, each Party shall, in accordance with its respective rules and procedures:

    a. offer a reasonable opportunity for anynatural or legal person, on a non-discriminatory basis, to provide input;
    b. publish either draft regulatory acts or consultation documents that provide sufficient details about a possible new regulatory act to allow natural or legal persons and the other Party to assess whether and how their interests might be significantly affected;
    c. consider the contributions received.

2. Each Party should make use of electronic means of communication and seek to use dedicated single access web portals, where possible.

3. Each Party shall make publicly available any comments it receives, except to the extent necessary to protect confidential information or withhold personal data or inappropriate content.

4. In publishing a proposed or final regulatory act[4] each Party shall endeavor to provide a publicly available explanation of the results of the consultation process.

Article 7 - Feedback on the existing regulatory framework

Each Party shall offer the opportunity for any natural or legal person to submit views to the relevant regulatory authority on improvements to existing regulatory frameworks, including whether a regulatory framework has become ineffective at protecting health, environment, welfare, safety or other public policy objectives, or suggestions for simplification and burden reduction.

[4]For greater certainty, this obligation may be met by publication of a separate but contemporaneous document.

EU-US TTIP Negotiations

*This **TEXTUAL PROPOSAL** is the European Union's proposal for legal text on "Good Regulatory Practices" in TTIP. It was tabled for discussion with the US and made public on 21 March 2016. The actual text in the final agreement will be a result of negotiations between the EU and US.*

Article 8 – Regulatory Impact Assessment

1. Each Party affirms its intention to carry out, in accordance with its respective rules and procedures, a regulatory impact assessment for planned regulatory acts.

2. When carrying out a regulatory impact assessment in accordance with paragraph 1, each Party shall ensure that it:

   a. considers the need for the proposed regulatory act and the nature and the significance of the problem the regulatory act is intended to address;
   b. examines feasible regulatory and non-regulatory alternatives (including the option of not regulating), if any, that would achieve the objective of the regulatory act;
   c. assesses potential short and long term social, economic, and environmental impacts of such alternatives and the anticipated costs and benefits (quantitative, qualitative, or both, recognising that some costs and benefits are difficult to quantify).

3. When carrying out a regulatory impact assessment in accordance with paragraph 1, special attention shall be given to the impact of the regulatory act in development on SMEs.

4. Within the overall framework of their regulatory impact assessments in accordance with paragraph 1, the regulatory authority shall, among other aspects, assess how the options under consideration:

   a. relate to relevant internationally agreed regulatory documents[5];
   b. take account of the regulatory approaches of the other Party, when the other Party has adopted or is planning to adopt regulatory acts on the same matter[6];
   c. have an impact on international trade or investment.

5. The findings of regulatory impact assessments shall be published no later than the proposed or final regulatory acts.

6. The Parties shall promote the exchange of information on available relevant evidence and data, on their practices in assessing impacts on international trade or

[5] For greater certainty, only regulatory documents adopted by international bodies or fora in which both Parties' regulatory authorities participate and to which they have agreed can be considered as "internationally agreed regulatory documents" for the purposes of this provision.
[6] For greater certainty, this is an obligation for regulatory authorities to examine the approaches of the other Party on their merits, but not to a particular result.

EU-US TTIP Negotiations

investment, as well as on the methodology and economic assumptions applied in regulatory policy analysis[7].

Article 9 – Retrospective Evaluation

1. Each Party shall maintain procedures or mechanisms to promote periodic retrospective evaluations of regulatory frameworks.
2. The Parties shall promote the exchange of experience and share information on planned retrospective evaluations.
3. Each Party shall make publicly available the results of any such retrospective evaluations.

[Article 10 Placeholder for a provision on Regulatory repository]

Article 11 – Non-application of dispute settlement

Chapter XX (Dispute Settlement) does not apply to this Chapter.

***

[7] Any exchange of information needs to respect the rules to be agreed on the exchange of confidential information and needs to be consistent with each Party's legal framework as to confidential information and information protected by intellectual property rights.

2017

글로벌 법제 동향 모니터링 이슈 분석 보고서

KOREA LEGISLATION RESEARCH INSTITUTE

GLOBAL LEGAL ISSUES (Ⅲ-1)

ISSUE 03

보건/재난분야

재난 구호 및 질병 관리 관련 글로벌 쟁점

장 원 경
이화여자대학교 스크랜튼학부 교수

장원경 교수는 2009년에 미국 인디애나대학교 법과대학 및 행정환경대학에서 박사학위를 취득하였으며, 현재 이화여자대학교 스크랜튼학부 교수로 재직 중이다. 관심 분야는 기초법학 및 공공정책학으로 법의식 및 법문화, 공공갈등관리, 생명윤리 및 의료윤리 등에 관한 연구를 수행하고 있다.

ISSUE
03
보건/재난분야

재난 구호 및 질병 관리 관련 글로벌 쟁점

장 원 경 이화여자대학교 스크랜튼학부 교수

Abstract

2016년도에 국제 사회에서 이루어진 재난 구호와 관련된 논의 중 가장 핵심적인 것은 인도주의적 구호활동 중 수집하여 사용하게 되는 디지털 데이터에 관한 것으로, 2016년 5월에 터키 이스탄불에서 개최되었던 인도주의 정상회의(World Humanitarian Summit)에서도 데이터의 책임감 있는 사용이 강조되었다. 국제연합의 인도주의 업무 조정국(UN OCHA)은 '데이터 책임'이라는 개념을 제시하며, 재난현장에 대한 구호 및 지원에서 활용되고 있는 디지털 데이터에 관한 최소한의 기준을 발표하고 이러한 기준을 준수할 것을 제안하고 있다. 한편, 공중 보건 및 질병 관리와 관련하여 국제 사회에서 2016년에 논의된 정책 중 가장 흥미로운 것은 세계보건기구(WHO)에서 발표한 '식품안전에 관한 위험 커뮤니케이션 지침'이다. 식품의 안전에 관한 문제는 공중 보건과 직결되는 중요한 쟁점이며, 특히 최근에는 사람들의 활발한 국제적인 이동 및 광범위한 농산물 및 공산품의 유통으로 식품 안전에 관한 알려지지 않은 새로운 유형의 위험이 발생 가능성이 높아지고 있다. 이러한 점을 강조하며 WHO는 식품안전에 관한 쟁점이 발생한 경우에 정부 부처가 취하여야 하는 위험 커뮤니케이션의 기본 원칙 및 고려 사항을 자세히 제시하고 있다.

Ⅰ. 재난 구호

1. 개요

재난 구호와 관련하여 2016년도에 국제연합의 인도주의 업무 조정국(UN OCHA, United Nations Office for Coordination of Humanitarian Affairs)은 인도주의적 구호활동 과정에서 수집되어 사용되는 데이터와 관련하여 '데이터 책임(data responsibility)'이라는 새로운 개념을 제시하고, 데이터 책임 구축의 필요성 및 핵심 내용을 발표하였다. UN OCHA는 지난 몇 년 동안 인도주의적 구호활동에 새로운 디지털 기술을 활용하여 구호 및 지원의 효율성을 높이는 방안을 고민하면서 동시에 개인정보의 보호도 강조하여 왔다. 그러나 이제 단순히 개인정보 보호의 차원을 넘어서, 데이터 수집 이전 단계에서부터 데이터와 관련하여 발생할 수 있는 위험 및 위해를 파악하고, 데이터 수집이 필요한 경우에 반드시 준수하여야 할 최소한의 기준을 마련하여 따르도록 제안하고 있다.

2. 인도주의적 구호 활동에서 데이터 책임의 구축[1)]

(1) 인도주의적 데이터 생태계의 형성

소셜 미디어 및 휴대전화의 설문조사 기능이 화재, 지진, 태풍, 홍수 등의 재난 현장에서 상황을 신속하고 정확하게 파악하고 적절한 구조 및 지원을 제공하기 위한 수단으로 활용되고 있다. 그러나 동시에 이러한 새로운 형태의 데이터의 등장으로 데이터 수집, 분석, 집계 및 공유에 대한 우려가 제기되고 있다. 특히 재난 현장에서 인도주의적 구호활동 기관의 도움을 많이 필요로 하는 사람들은 사회·경제적으로 취약한 사람들일 가능성이 높고, 이러한 사람들에 대한 디지털 데이터가 손쉽게 생성되어 사용되고 있는 상황이다.

1) United Nations Office for the Coordination of Humanitarian Affairs, Building Data Responsibility into Humanitarian Action, OCHA Policy and Studies Series 018 (May 2016)의 내용을 번역, 요약한 것이다.

이러한 데이터를 생산하고 소비하는 사람들은 다양하고 복잡한 "인도주의적 데이터 생태계(humanitarian data-ecosystem)"를 형성하고 있다. 데이터 생태계는 인도주의적 구호활동 기관 및 구호활동과 연관된 사람들, 구조 및 지원을 필요로 하는 사람들 및 공동체로 구성되어 있으며, 이러한 생태계를 통하여 재난으로 인하여 피해를 입은 사람들 및 공동체의 휴대전화 기록, 소셜 미디어 게시물, 위성 이미지, 감지 데이터, 금융 거래 등의 데이터가 밀집된 망을 형성하고 있다. 인도주의적 데이터 생태계를 통하여 형성된 데이터 중 가중 중요한 유형의 데이터는 재난으로 인하여 피해를 입은 사람들의 시간별 및 공간별 활동에 관한 정보, 즉 "시간-공간 메타 데이터(spatiotemporal metadata)"이다. 이러한 데이터는 재난으로 인하여 피해를 입은 사람들의 이동 경로를 이해하여 적절한 구조 및 지원을 제공하는데 활용될 수 있지만, 동시에 이러한 사람들에게 위해를 가하기 위한 수단으로 악용될 수 있다.

따라서 새로운 도구와 기법을 활용하여 데이터를 생성 및 사용하는 과정에서 발생할 수 있는 위험을 예견하고 이러한 위험을 완화할 수 있는 프레임워크를 구축하여야 할 필요성이 제기되고 있다. 즉, 적절한 데이터 보안 체계를 개발하고, 데이터와 관련한 윤리적 기준을 설정하며, 개인정보 보호의 보장 방안을 체계화하는 것이 인도주의적 데이터 생태계 전체의 총체적인 책임으로 인식되기 시작하였다.

(2) 데이터 사용의 잠재적인 위험 및 위해

인도주의적 구호활동의 효율성을 높이기 위하여 최근 여러 기관 및 단체는 데이터를 통합하려는 시도를 하고 있다. 여러 기관 및 단체에서 수집하여 통합하는 방식으로 생성된 디지털 데이터를 활용하는 것은 구호 요청과 관련된 잠재적인 신호의 포착 및 도움을 필요로 하는 사람들에 대한 집중적인 구호와 지원에 있어서 효율적이다. 하지만 동시에 데이터를 수집하여 처리하고 사용하는 데이터 수명주기의 모든 단계에 상당한 위험이 내포되어 있다. 예를 들어, 데이터의 수집 및 사용 과정에서 개인정보를 포함한 데이터의 유출과 같은 전통적인 형태의 위험에서부터 위기 상황에서 급박하게 이루어지는 데이터의 수집 및 처리 과정에서 발생하는 보안 문제 등 인도주의적 구호활동이라는 특수한 상황에서 발생 가능한

다양한 위험이 존재한다. 또한 이미 재난의 발생으로 취약한 상태에 놓여있는 사람들이 이러한 데이터의 착취 및 유출로 인하여 새로운 유형의 위협에 직면할 수 있고, 구호활동 중 활용되는 디지털 데이터로 인하여 특정한 구호와 지원에서 배제되어 더 심각한 위험에 노출될 수 있는 가능성도 있다. 이러한 잠재적인 위험 및 위해를 감소시키기 위하여서 인도주의적 구호활동 기관의 책임감 있는 데이터 사용이 절실한 상황이다.

(가) 민감한 데이터

민감한 데이터를 수집하고 사용하는 과정에는 항상 다양한 유형의 위험이 발생할 가능성이 있으나, 인도주의적 구호활동과 관련하여 개인적으로 민감한 데이터 또는 인구 통계학적으로 민감한 데이터를 다루는 경우에는 특히 더 그러하다. 재난 현장의 긴급하고 모호한 상황에서, 데이터 오남용의 두려움으로 도움을 필요로 하는 개인이 자신의 기본적인 권리를 행사하지 못할 수 있고, 부적절한 데이터 사용으로 보안, 비밀유지 및 프라이버시에 대한 우려를 낳을 수 있다. 이러한 잠재적인 위험 및 위해는 장기적으로 데이터 공유에 대한 저항을 높여 인도주의적 구호활동 자체를 침해할 정도의 파급 효과까지도 낳을 수 있다. 최소한의 데이터 책임(data responsibility)에 관한 지침도 없이 임기응변으로 이루어지고 있는 데이터 공유 관행으로 프라이버시 침해, 데이터에 대한 소유권 및 이미 재난으로 인하여 취약한 인구 집단에 대한 잠재적인 위해 가능성이 제기되고 있다.

(나) 크라우드소싱으로 수집된 데이터

인도주의적 구호활동 기관은 재난 현장에서 크라우드소싱 및 여러 가지 형태의 소셜 미디어를 활용하여 그 이전에는 상황을 파악하기 어려웠던 지역에 대한 접근을 시도하고 있다. 데이터 처리 기술을 지닌 자원봉사자들과 협력하여 위기상황에 대응할 수 있는 디지털 네트워크를 구축하고, 시민들의 참여를 독려하여 재난 현장에 대한 실질적인 데이터를 확보할 수 있게 되었다. 그러나 크라우드소싱으로 수집된 정보는 불완전하고 부정확할 수 있다는 문제점을 지니고 있다. 즉, 참여의 용이성 및 장벽이 없다는 사실이 크라우드소싱 데이터를 정보 수집의 강력한 메커니즘으로 만드는 반면, 바로 그 사실로 인하여 정보의

질에 관한 문제가 제기되고 있는 것이다. 크라우드소싱으로 수집된 정보는 상당한 잡음 및 쓸모없는 정보가 포함되어 있고, 스팸, 악의적인 사용자, 상업적인 정보 또는 소문으로부터 생성된 정보가 포함되어 있기도 하다. 또한 많은 데이터가 이차적인 출처에서 나오기 때문에 데이터의 정확성을 검증하기 어려울 수 있다. 따라서 크라우드소싱으로 수집된 데이터는 구호활동을 계획하는 과정에서 다른 정보를 보완하는 정도로 신중하게 사용되어야 한다.

(다) 편견 및 디지털 차별

데이터가 생성되고, 수집되고, 처리되고, 분석되는 과정에서 사회적·경제적·문화적 편견의 대상이 되는 공동체에 대한 사회적·경제적 불평등이 더욱 심화될 수 있다. 데이터에 기초한 구호활동으로 디지털 기술에 대한 접근이 어렵거나 숙달되지 못한 사람들은 정보 수집 과정에서 소외될 수 있고, 이렇게 편향된 정보 수집은 재난으로 인하여 피해를 입은 인구 집단을 잘못 대표하는 데이터를 구축하여 구호 및 지원과 관련한 의사소통 및 실행 단계에서 커다란 문제를 야기할 수 있다. 결국 이러한 제한으로 디지털 차별(digital discrimination)이 발생하게 되는데, 디지털 기술을 활용할 수 있는 공동체와 비교하여 인터넷이나 다른 소셜 미디어에 대한 접근이 제한적인 사회적·경제적으로 취약한 공동체에 대한 정보 수집이 늦어져, 복구 과정에서 기존의 사회적·경제적 불평등이 강화될 수 있다는 것이다. 적절한 정책적인 판단에 기초한 개입 없이 테크놀로지와 데이터에만 의존하여 이루어지는 인도주의적 구호활동은 디지털 차별을 야기하여, 특정한 인구 집단 또는 지역 공동체에 대한 지원 및 구호를 지연시킬 뿐만 아니라 장기적으로 사회적·경제적 불평등을 심화시킬 것이다.

(3) 데이터 책임의 구축 및 구현 절차

디지털 데이터의 활용으로 인도주의적 구호활동 기관의 역할 및 운영방식이 변화함에 따라, 각 기관은 데이터와 관련하여 발생할 수 있는 위험을 최소화하기 위한 노력을 하여야 한다. 데이터 책임(data responsibility)은 데이터 프라이버시 또는 데이터 보호보다 더 포괄적인 개념으로, 데이터 책임 프레임워크는 최소한 다음의 네 단계 절차를 의미한다.

1. 데이터가 생성되고 공유되는 상황 및 목적에 대한 평가

- ▸ 데이터 사용과 관련하여 어떠한 이득이 예측되는가?
- ▸ 누가 데이터에 접근할 수 있는가?
- ▸ 어떠한 데이터가 부적절하게 사용될 수 있는가?
- ▸ 데이터의 부적절한 사용에 대한 위협이 어떻게 발생할 수 있는가?

2. 데이터 목록의 작성 및 저장

- ▸ 데이터는 어디에 저장되고, 누가 관리하는가?
- ▸ 데이터는 나중에 어디에 보관하는가?
- ▸ 누가 장래에 데이터에 접근할 수 있는가?
- ▸ 데이터에 대한 접근을 모니터링하는가?

3. 데이터 수집 전, 데이터의 사용과 관련한 위험 및 위해 요소에 대한 사전 평가

- ▸ 수집하려는 데이터가 다른 데이터와 결합되면 개인을 식별할 수 있는가?
- ▸ 수집하려는 데이터가 그대로 공개되면 어떠한 일이 발생하는가?
- ▸ 재난으로 인하여 피해를 입은 사람들에게 고의적으로 위해를 가하기 위하여 누가 데이터를 사용할 수 있는가?
- ▸ 데이터에 대한 분석이 잘못 해석되면 구호활동 전체에 좋지 않은 영향을 미칠 수 있는가?

4. 위험 및 위해 요소를 완화하기 위한 전략의 개발

- ▸ 의사 결정 분지도(decision tree)를 활용하여 데이터 처리 정책 및 시나리오를 개발한다.
- ▸ 데이터에 대한 접근을 제한한다.
- ▸ 기술적인 해결 방안을 마련한다.
- ▸ 데이터를 다루는 직원을 교육시킨다.

(4) 데이터 책임 구축을 위한 최소한의 기준 및 핵심 역량

인도주의적 구호 활동에서 데이터의 수집 및 분석, 사용에 관한 공통의 기준이 확립되지 않은 상황에서 적십자(Red Cross)의 국제위원회, 스탠바이 태스크포스(Standby Taskforce) 등은 개별적으로 데이터와 관련한 지침을 마련하여 사용하고 있다. UN은 「전산화된 개인 정보 파일에 관한 규제를 위한 지침(Guidelines for the Regulation of Computerized Personal Data Files)」을 채택하고, 국제기관 및 단체에 데이터 보호의 원칙을 적용할 것을 촉구하고 있다. 이러한 상황에서 인간애, 중립성, 공평성, 독립성이라는 인도주의적 활동의 기본원칙에 기초하여, 데이터 책임을 위한 최소한의 기준을 채택하고 이러한 기준을 준수할 수 있는 기관의 역량을 키우는 것이 필수적이다.

(가) 데이터 책임의 최소한의 기준

인도주의적 구호활동 기관이 디지털 데이터를 다루는데 있어서 구축하여야 하는 데이터 책임의 최소한의 기준에는 다음의 핵심적인 요소가 반드시 포함되어야 한다.

- 필요성에 대한 확인: 모든 유형의 인도주의적 구호활동과 마찬가지로, 데이터에 기초한 구호활동은 이러한 유형의 개입이 필요한지 여부를 명확히 확인한 후 이루어져야 한다. 단순히 데이터가 존재하기 때문에 사용되어서는 안 되고, 그 목적이 분명하고 명확하여야 한다.

- 핵심 역량에 대한 평가: 인도주의적 구호활동을 하는 기관이 데이터를 책임감 있게 사용할 수 있는 핵심적인 역량을 지녔는지 여부에 대한 판단이 반드시 포함되어야 한다. 예를 들어, 안전한 인프라, 데이터와 관련한 행동 기준, 잠재적인 위험 및 위해 요소를 감소시키기 위한 지침 등이 갖추어져 있는지 판단하여야 한다. 이러한 핵심 역량에 대한 평가는 프로젝트의 설계 단계에서 이루어져야 하고, 프로젝트의 운영 중간에 이루어져서는 안 된다.

▸ 취약한 사람들에 대한 위험 관리: 인도주의적 구호활동 기관이 데이터를 사용하거나 또는 사용하지 않음으로써 발생할 수 있는 위험은 상황에 따라 달라질 수 있다. 또한 구호활동과 관련된 데이터는 재난 종료 이후에 취약한 특정한 사람들에게 영향을 미칠 수 있다. 따라서 인도주의적 구호활동 기관은 ① 데이터 사용으로 인하여 발생할 수 있는 위험과 이득을 비교하여 데이터 사용의 필요성을 분명히 하고, ② 데이터 사용의 위험 요소를 미리 파악하여 관리하여야 한다.

▸ 법규 및 윤리지침의 준수: 인도주의적 구호활동에서 이루어지는 데이터 수집은 관련 국내 및 국제 법규를 준수하여야 할 뿐만 아니라, 일반적으로 수용된 윤리지침도 준수하여야 한다. 현재 규제환경이 매우 파편화되어, 여러 국가의 국경을 넘나들며 이루어지는 인도주의적 구호활동에 어떠한 법이 적용되는지 여부를 판단하는 것이 쉽지 않다. 따라서 인도주의적 데이터 생태계에 국제적으로 수용된 통일된 데이터 책임의 접근방식을 적용하여 인도주의적 구호활동과 관련된 데이터를 보호하여야 한다.

(나) 데이터 책임 구축을 위한 핵심 역량

데이터 책임의 최소한의 기준을 준수하기 위하여서는 다음과 같은 역량이 요구된다.

▸ 과정으로서의 책임: 데이터 책임은 단순히 프로젝트의 초기 단계의 어느 한 시점에 고려하여야 할 문제가 아니라 인도주의적 구호활동의 운영 전반에 걸쳐서 필요한 통합적이고 반복적인 과정이다. 데이터 책임의 구현 절차에 따라 각 단계에서 최소한의 기준을 적용하여 실행하고 평가할 수 있는 숙련된 인력이 확보되어야 한다.

▸ 밝은 선(bright line) 규칙 및 붉은 버튼(red button) 대응: 인도주의적 구호활동 기관은 데이터를 배포하거나 테크놀로지에 기초한 특정한 개입을 시도하기 전에 허용되는 행위와 허용되지 않는 행위를 분명히 구분하는 밝은 선 규칙을 개발하고 준수하여야 한다. 또한 프로젝트를 즉시 중단할 필요성이 있는 상황에 해당하는 "붉은 버튼" 순간을 파악하고 대응방안을 미리 마련하여야 한다.

▸ 투명성: 데이터에 기초한 개입을 한 인도주의적 구호활동 기관은 해당 프로젝트에 관한 정보를 정확히 기술하고 관련 정보를 공공에 공개하여야 하며, 특정한 사람들이 피해를 입었거나 정보통신 관련 인프라에 피해가 발생한 경우에 그 내용을 공개하여야 한다. 또한 책임감 있는 구호활동 기관은 데이터와 관련한 표준운영지침을 다른 기관과 공유하여야 한다.

▸ 피드백(feedback) 고리: 데이터 사용과 관련하여 책임감 있는 구호활동 기관은 핵심적인 이해관계자들과 피드백 고리를 구축하여야 하는데, 특히 재난의 피해를 입은 사람들 및 구호활동을 하는 다른 조직 등과 이러한 관계를 형성하여야 한다. 데이터 관련 작업의 속도가 매우 빠르고 상황이 급속하게 변화할 수 있는 여건에서, 피드백 고리를 만들어 기관의 관리 역량을 키우는 것이 필수적이다. 또한 내부적인 피드백 고리도 만들어 프로젝트가 진행되는 동안 데이터 관련 업무를 모니터링하여야 한다.

3. 시사점

인도주의적 구호활동에서 데이터에 관한 논의는 이제까지 개인정보 보호에 초점을 맞추어 이루어져 왔다. 즉, 새로운 정보통신 기술을 사용하여 데이터를 수집하는 경우에 데이터 수집의 대상이 되는 사람들에게 미칠 영향을 고려하여 심의 절차를 도입하는 방안 및 긴급한 상황에서 간소한 절차에 따라 심의를 받은 후 나중에 사후승인을 받는 방안 등이 논의되었다. 그러나 최근 인도주의적 구호활동에 디지털 데이터의 수집 및 사용이 필수적인 것으로 인식되면서, UN OCHA는 '데이터 책임'이라는 새로운 개념을 제시하고 있다. 데이터 책임은 개인정보 보호 또는 프라이버시 보호의 개념을 넘어 인도주의적 구호활동 기관의 디지털 데이터에 대한 윤리 의식을 높이고 책임감 있는 데이터 수집 및 사용을 촉구하는 것이다. 이러한 접근방식의 변화는 디지털 데이터에 대한 인식 자체를 변화시켜 무분별한 데이터의 수집 및 사용으로 인하여 발생할 수 있는 피해를 최소화하는데 기여할 것이다.

Ⅱ. 질병 관리

1. 개요

국제연합(UN, United Nations) 산하의 공중 보건 및 질병 관리와 관련한 전문 기구인 세계보건기구(WHO, World Health Organization)는 2016년도에 '식품안전에 관한 위험 커뮤니케이션 지침(Risk Communication Applied to Food Safety Handbook)'을 발표하였다. WHO는 매일 섭취하는 식품의 안전에 관한 문제가 공중 보건과 직결되는 쟁점이라는 점을 강조하며, 식품안전에 관한 위험이 발생한 경우에 공중 보건에 책임이 있는 정부 부처가 취하여야 하는 커뮤니케이션 절차를 상세히 제시하고 있다. 특히 WHO는 사람들의 국제적인 이동이 활발하여지고 이와 더불어 광범위한 농산물 및 공산품이 유통되고 있는 상황에서 식품안전에 관한 알려지지 않은 새로운 유형의 위험이 발생할 가능성이 높다는 점을 인식하고, 위험 커뮤니케이션의 기본 원칙 및 고려 사항을 자세히 안내하고 있다.

2. 식품안전에 관한 위험 커뮤니케이션[2)]

(1) 식품안전에 관한 위험 커뮤니케이션의 정의 및 중요성

(가) 식품안전에 관한 위험 커뮤니케이션의 정의

일반적인 위험분석 프레임워크가 식품안전과 관련하여서도 적용되는데, 위험분석 프레임워크는 다음의 세 가지 요소로 구성된다.

▸ 위험평가(risk assessment): 위험요소를 양적 또는 질적으로 평가하여 특징을 판단하는데 사용되는 프로세스를 의미한다.

2) World Health Organization, Risk Communication Applied to Food Safety Handbook (2016)의 내용을 번역, 요약한 것이다.

- ▸ 위험관리(risk management): 선택 가능한 통제조치를 평가하고 선택하여, 적절한 수준으로 보호하는데 필요한 통제를 구현하는 것을 의미한다.
- ▸ 위험 커뮤니케이션(risk communication): 위험 평가자, 위험 관리자, 소비자, 기타 이해관계자 사이에 위험 및 위험과 관련된 요소에 대한 정보와 의견을 교환하는 것을 의미한다.

위험 커뮤니케이션은 위험분석의 필수적인 구성요소로, 사람들이 정보에 기초한 판단을 하고, 이해관계자들 사이에 상호 이해를 촉진하며, 위험평가와 위험관리에 관한 정보를 제공하는 역할을 수행한다.

(나) 식품안전에 관한 위험 커뮤니케이션의 중요성

식품안전과 관련한 위험요소에 사람들은 상시적으로 노출되어 있는데, 그 노출의 빈도와 정도는 식품사슬(food chain) 전반에 걸쳐 실시되는 정책적인 통제, 소비자들의 식습관, 대체가능한 식품공급 가능성 등에 따라 달라진다. 따라서 식품안전에 관한 위험 커뮤니케이션이 효과적으로 이루어지면, 다음과 같은 사항이 개선될 것이다.

- ▸ 사람들의 육체적인 안녕
- ▸ 식품 공급 및 규제 시스템에 대한 사람들의 신뢰
- ▸ (동물 및 식물을 포함한) 사람들이 살아가고 있는 생활환경
- ▸ (사회적·경제적·심리적 요소를 포함한) 사람들의 전반적인 삶의 질

(다) 식품안전에 관한 위험 커뮤니케이션의 목표

식품안전에 관한 위험 커뮤니케이션의 전반적인 목표는 사람들이 식품안전과 관련된 판단을 내리는데 필요한 정보를 제공함으로써 사람들의 건강을 보호하려는 것이다. 이러한 정보는 사람들이 특정한 식품을 섭취할 것인지 여부, 특정한 식품에 포함되어 있는 위험을 줄이기 위하여 식품을 어떻게 다룰 것인지, 그리고 특정한 식품에 포함되어 있는 위험에

노출된 경우에 어떻게 자신을 보호할 것인지에 대한 결정을 내리는데 도움이 된다. 특히, 임산부, 영아, 노인, 면역체계가 약한 환자 등 특정한 유형의 위험에 취약한 사람들에게 식품의 위험 및 이득에 관한 정보를 제공하여 정보에 기초한 판단을 내릴 수 있도록 도우려는 것이다.

효과적인 식품안전에 관한 위험 커뮤니케이션을 위하여 소비자를 포함한 모든 이해관계자들의 이해와 대화의 촉진이 필수적이다. 특정한 쟁점에 의하여 영향을 받거나 영향을 미칠 수 있는 개인 또는 집단, 예를 들어 정부, 기업, NGO, 대학, 연구소, 미디어 등의 이해관계자들과의 의사소통을 통하여 위험 커뮤니케이션의 목표 달성에 필요한 적절한 정보를 얻고, 커뮤니케이션의 주요 대상자(target audience)에 대한 이해를 넓힐 수 있다. 소비자, 취약한 인구 집단, 식품의 생산·저장·운반·분배를 담당하는 사업자, 식품안전 관련 쟁점을 다루는 NGO 등 위험 커뮤니케이션이 특히 목표로 하고 있는 주요 대상자들이 필요로 하는 메시지를 전달하는 방식으로 위험 커뮤니케이션의 효과를 극대화하여야 한다.

(라) 효과적인 위험 커뮤니케이션이 어려운 이유

일반적으로 효과적인 위험 커뮤니케이션이 어려운 이유는 다음과 같다.

- ▸ 커뮤니케이션의 모든 대상자를 파악하고 그들의 위험인식, 우려, 커뮤니케이션 욕구 등을 파악하여야 한다는 점
- ▸ 식품안전에 관한 위험과 관련된 정보 및 이러한 위험을 평가하고 관리하는 기관에 대한 신뢰를 구축하고 유지하여야 한다는 점
- ▸ 불확실성이 어디에 존재하고 있는지에 대하여 알리고 이러한 불확실성을 줄이기 위한 노력을 하여야 한다는 점
- ▸ 외부 환경의 변화에 따라 위험 커뮤니케이션을 조정하여 위험의 현재 상태를 반영하여야 한다는 점
- ▸ 과학적인 전문가와 커뮤니케이션의 주요 대상자 사이의 지식의 차이를 파악하여야 한다는 점

- 각각의 커뮤니케이션 대상자(예를 들어, 사회적으로 소외된 취약한 사람들)와의 효과적인 의사소통을 저해하는 요소를 파악하여야 한다는 점
- 동일한 식품안전에 관한 쟁점을 전달하는 여러 개인 및 기관 사이의 위험 커뮤니케이션 메시지를 조정하여야 한다는 점
- 명확하고 시의 적절하게 커뮤니케이션을 하여야 한다는 점
- 커뮤니케이션의 의도하지 않은 결과를 최소화하여야 한다는 점

또한 효과적인 위험 커뮤니케이션을 어렵게 하는 구조적인 문제가 있는 경우도 있다. 예를 들어, 어떠한 국가에는 식품의 위험성을 파악하고 그 위험을 평가하는 전문가가 없는 경우도 있고, 관련 정부 부처 사이에 식품안전에 관한 위험 커뮤니케이션의 일차적인 책임이 어디에 있는지 불분명한 경우도 있다.

(마) 위험에 대한 인식의 중요성

식품안전에 관한 위험 커뮤니케이션을 실시하기 위하여서는 위험평가 단계에서 파악되는 위험 및 위험인식에 대한 고려가 중요하다. 위험요소(hazard)는 건강에 유해한 영향을 미칠 수 있는 가능성을 지니고 있는 생물학적, 화학적, 물리적 요소를 의미한다. 위험(risk)은 위험요소로부터 나타날 수 있는 유해한 영향의 가능성 및 이러한 영향의 심각성을 의미한다. 위험인식(risk perception)은 특정한 위험의 특성, 가능성, 심각성에 대한 사람들의 판단을 의미한다. 어떠한 위험물질의 경우에는 제한된 노출로 인하여 사람들에게 실질적으로 미칠 수 있는 위험의 정도는 매우 낮으나, 공공의 위험인식 및 사회적인 우려는 매우 높을 수 있다. 위험인식에 영향을 미칠 수 있는 요소가 다음의 〈표〉에 제시되어 있다.

〈표〉 위험인식에 영향을 미치는 요소

요소	위험인식의 증가	위험인식의 감소
자연적으로 발생하는지 여부에 대한 인식	자연적으로 발생하지 않은 경우/인간이 유발한 경우	자연적으로 발생한 위험요소
통제에 대한 인식	통제 불가능한 경우	개인적으로 통제 가능한 경우
과학적 지식	위험이 과학적으로 알려져 있지 않은 경우	위험이 과학적으로 알려져 있는 경우
친숙한 정도	새로운 위험	친숙한 위험
노출에 대한 자발성	비자발적으로 노출된 경우	노출을 스스로 선택한 경우
대형 참사로 이어질 가능성에 대한 인식	많은 사람들이 동시에 영향을 받는 경우	사람들이 장기간 영향을 받아온 경우
결과의 심각성	(실제 발생가능성과 상관없이) 심각한 결과를 유발할 수 있는 경우	결과가 심각하지 않을 경우
결과의 즉시성	결과가 즉시 발생할 경우	결과의 발생이 지연될 경우
영향을 받는 사람	취약한 사람들 (예를 들어, 영아, 유아, 임산부)	취약하지 않은 사람들
위험과 이득의 분배에 대한 인식	위험과 이득이 불공평하게 분배되는 경우	위험과 이득이 공평하게 분배되는 경우
윤리적 및 도덕적 우려	위험이 윤리적 또는 도덕적으로 잘못된 것으로 보이는 경우 (예를 들어, 사기)	윤리적 또는 도덕적 우려가 없는 경우

사람들의 위험인식에서 가장 중요한 것은 기술적으로 위험이 어떻게 측정되는지와 상관없이, 사람들이 위험을 어떻게 인식하느냐에 따라서 사람들의 태도 및 행동이 달라진다는 점이다. 따라서 위험에 대한 사람들의 인식을 파악하고 대응하는 것이 효과적인 위험 커뮤니케이션에서 필수적이다. 기존의 위험 커뮤니케이션 메시지는 주로 과학적 사실에 초점을 맞추고 있으나, 이러한 메시지는 특정한 사회·문화에서 사람들의 위험에 대한 인식 및 위험에 대한 수용 정도에 대한 아무런 통찰도 제공하지 못한다는 문제가 있다. 따라서 위험

커뮤니케이션 담당자는 식품안전의 어떠한 요소가 사람들의 인식 형성에 어떠한 영향을 미치는지를 적극적으로 파악하여야 한다.

(바) 식품안전에 관한 위험 커뮤니케이션의 활용

위험 커뮤니케이션은 모든 유형의 식품안전에 관한 위험에 적용될 수 있으나, 식품안전과 관련된 특정한 쟁점에 따라 다른 유형의 커뮤니케이션 전략 및 방법이 요구된다. 식품안전과 관련하여 응급상황이 발생한 경우에 신속한 대응이 필수적이다. 식품안전과 관련한 응급상황으로는 식품을 매개로 한 질병이 발생한 경우, 식품이 오염되어 사람들의 건강을 위협하는 경우 등을 들 수 있다. 이러한 경우에 메시지는 직접적이고 자주 그리고 긴급하게 전달되어야 한다. 그러나 대부분의 응급상황에서 이해관계자들과 관련 위험에 대하여 의견을 교환할 시간이 충분하지 않고, 위험의 정도와 미칠 수 있는 영향의 범위에 대한 정보도 완전하지 않을 것이다. 따라서 위험 커뮤니케이션 담당자는 의사소통 과정에서 이러한 불확실성에 대응할 수 있어야 한다.

지속적인 식품안전과 관련된 쟁점의 경우에는 지속적인 의사소통이 필요한데, 위험에 관한 구체적인 정보를 적절한 시기에 또는 일정한 시간을 두고 특정한 사람들에게 배포하는 등의 방법으로 대처할 수 있다. 예를 들어, 햄버거의 적절한 조리법과 관련한 쟁점을 여름에 발표하는 방법으로 메시지 전달의 효율성을 높일 수 있다. 또한 사회적인 관심이나 우려를 유발하는 진행 중인 식품안전에 관한 쟁점의 경우에는 일관된 의사소통이 요구된다. 예를 들어, 생명공학, GMO, 식품에 적용되는 나노기술의 잠재적인 위험과 이득이 사회적으로 계속하여 논의될 수 있도록 하여야 하며, 이해관계자들과의 의사소통을 통하여 위험관리에 관한 사회적인 우선순위를 파악하여야 한다.

(사) 이해관계자와 주요 대상자 파악의 필요성

위험 커뮤니케이션의 목표를 달성하기 위하여서는 모든 이해관계자와 주요 대상자가 파악되어야 하고, 관심이 있는 모든 이해관계자들이 위험 커뮤니케이션 과정에 접근 가능하여야 한다. 식품안전에 관한 위험 커뮤니케이션 과정에 이해관계자를 포함시키는 것에는 다음과 같은 장점이 있다.

▸ 식품안전에 관한 위험과 관련한 지식의 차이를 확인할 수 있다.
▸ 이해관계자의 위험에 관한 인식 및 우려를 이해한다.
▸ 이해관계에 따라 형성된 잠재적인 의사소통의 장벽을 확인하고, 가장 선호하는 정보의 소스(information source)와 가장 적합한 의사소통의 채널을 파악한다.
▸ 커뮤니케이션의 의도하지 않은 결과를 파악하고 대응방안을 모색한다.

이해관계자와 협력적인 절차를 구축하게 되면, 다음과 같은 장점이 있다.

▸ 더 많은 아이디어가 생산될 수 있다.
▸ 협력하지 않았으면 인지하지 못하였을 우려를 파악할 수 있다.
▸ 다양한 관점을 살펴볼 수 있다.
▸ 잠재적인 동의를 형성하고 커뮤니케이션 노력에 대한 지지를 얻을 수 있다.
▸ 여러 정부 부처(예를 들어, 보건, 농업, 교역) 및 다양한 이해관계자들 사이에 식품안전에 관한 책임을 공유하고 의사소통에 있어서 협력을 촉진한다.

이러한 이유에서 이해관계자와 주요 대상자를 파악하고 식품안전에 관한 위험 커뮤니케이션 과정에 이러한 사람들이 참여할 수 있도록 독려하는 것이 매우 중요하다.

(2) 위험 커뮤니케이션의 원칙

(가) 정보 및 규제기관에 대한 신뢰

신뢰는 효과적인 위험 커뮤니케이션에 필수적인데, 사람들은 자신이 신뢰하지 않는 정보를 믿거나 따르지 않을 것이며, 그 결과 위험관리가 효율적으로 이루어지기 어렵고 잠재적으로 보건, 환경, 식품교역 및 경제에 심각한 영향을 미치게 될 것이다. 일반적으로 사람들은 해당 분야의 전문지식과 어느 정도의 경력을 지니고 있는 사람 또는 기관을 신뢰하는 경향이 있다. 그러나 전문지식만을 가지고 이러한 신뢰를 확보하는 것은 충분하지 않다. 예를 들어, 식품안전과 관련하여 특정한 이해관계를 지니고 있는 전문가의 의견은 사람들의 신뢰를

얻기 어려울 것이다. 일반적으로 다음과 같은 정보를 사람들은 훨씬 더 신뢰하는 경향이 있다.

- ▸ 선입견이 있거나 자신의 이득을 위한 견해를 제시할 명백한 이유가 없는 경우
- ▸ 사람들의 가치와 우려를 공감하고 공유하는 경우
- ▸ 특정한 결정이 공중의 보건을 보호하기 위한 것이라는 사실을 충분히 설명하는 경우

따라서 식품안전 및 식품안전에 관한 위험과 관련된 정보에 대한 신뢰를 높이기 위하여 공개적이고 솔직하고 명료하게 정보를 전달하여야 한다. 어느 정도의 신뢰가 형성되어 있는 경우라도 정보의 과장, 부인, 또는 왜곡이 드러나는 경우에는 공공의 신뢰를 잃는 것은 물론 사회적·경제적으로 심각한 결과를 초래하게 될 것이다. 따라서 개방성과 투명성, 대응성과 적시성에 따라 신뢰를 구축하고 유지하는 것이 위험 커뮤니케이션에서 필수적이다.

(나) 식품안전에 관한 위험 커뮤니케이션의 원칙

(a) 개방성과 투명성

개방성(openness)은 모든 식품안전과 관련된 이해관계자들에게 참여할 수 있는 기회를 보장하는 것을 의미한다. 여기에서 이해관계자는 위험에 영향을 받은 사람들과 그러한 위험 발생에 잠재적인 책임이 있는 사람들을 의미한다. 위험평가, 위험관리, 위험 커뮤니케이션은 개방된 방식으로 수행되어야 하며, 적절한 시점에 이해관계자들에게 이러한 절차에 참여하여 자신의 의견을 제시할 수 있는 기회가 주어져야 한다. 그러나 항상 이러한 의견을 반영하여 공동으로 위험관리 결정을 내려야 한다는 의미는 아니며, 위험관리 결정에 이해관계자들이 제시한 의견의 어떠한 부분이 어떠한 이유로 고려되었는지 여부 등을 명확히 밝히는 것만으로도 개방성을 충족하였다고 볼 수 있다.

투명성(transparency)은 의사결정 과정에서 관련 정보에 대한 공공의 검토를 허용하는 것을 의미한다. 그러나 정보의 완전한 공개가 언제나 가능한 것은 아닌데, 비밀보호 및 소유권 정보 보호 등에 관한 적법한 우려가 있을 수 있기 때문이다. 이러한 경우에 투명성에

관한 원칙은 일관되고 명확하게 설명되어야 한다. 만약 투명성에 대한 제한이 불필요한 비밀유지의 변명으로 보이는 경우에는 사람들의 불신을 낳을 것이다.

개방성과 투명성은 서로 교환 가능한 개념이 아니다. 위험 커뮤니케이션 담당자는 투명하지 않지만 개방적일 수 있고, 그 반대의 경우도 가능하다. 예를 들어, 어떠한 기관은 관련 정보를 매우 투명하게 웹사이트에 공개하지만, 의사결정 과정에 이해관계자들의 참여를 허용하지 않을 수 있다. 또한 어떠한 개방된 조직은 많은 이해관계자들과 기꺼이 상호작용하지만, 이해관계자들의 의견이 어떻게 반영되었는지에 대하여 공개하지 않을 수 있다. 따라서 원활한 위험 커뮤니케이션이 이루어지기 위하여서는 개방성과 투명성을 모두 갖추어야 한다. 예를 들어, 이해관계자들의 절차 참여를 허용하였으나 합의에 도달하지 못한 경우에는 그 사실조차도 투명하게 공개하는 것이 바람직하다.

(b) 적시성과 대응성

적시성(timeliness)은 시간적으로 적절한 때에 의사소통을 하는 것으로 이러한 커뮤니케이션은 공중 보건의 보호, 신뢰의 구축 및 유지, 소문 및 잘못된 정보 방지를 위하여 필수적이다. 식품안전에 관한 위험과 관련된 많은 논란은 위험 그 자체보다는 '왜 우리에게 조금 더 빨리 내용을 전달하지 않았는가'라는 질문에 초점을 맞추고 있다. 심지어 거의 제공할 정보가 없는 상황에서조차도 규제기관이 어떻게 사건을 조사하고 언제 정보를 제공할 것인지에 대하여 알리는 것이 바람직하다. 또한 시의성과 투명성을 충족시키기 위하여서는 식품안전에 관한 위험과 관련한 불확실성에 대하여 커뮤니케이션하여야 한다. 어떠한 점이 불확실한지 반드시 설명되어야 하며, 이러한 불확실성에 대응하여 어떠한 조치를 취하고 있으며, 이러한 불확실성으로 인하여 발생할 수 있는 결과에 대한 정보가 제공되어야 한다.

대응성(responsiveness)은 식품안전에 책임이 있는 사람들이 커뮤니케이션 과정에서 주요 대상자의 욕구와 기대에 대응하는 정도를 의미한다. 예를 들어, 사람들은 자신의 우려를 이해하지 못하고 단지 위험평가에 관한 기술적인 정보만을 전달하는 메시지는 신뢰하지 못할 것이다. 따라서 대응성 있는 위험 커뮤니케이션을 하기 위하여 커뮤니케이션의 주요 대상자가 알고자 하는 정보 및 위험관리와 관련하여 기대하는 바를 명확히 이해하고

메시지에 이러한 내용을 포함시키는 것이 중요하다. 위험 커뮤니케이션 담당자는 계획하거나 예측하지 못한 사건의 발생을 포함하여 외부 환경의 변화에 유연하게 대처하여야 하며, 상황에 따라 해당 메시지를 적절히 수정하여야 한다.

(다) 계획의 중요성

계획은 효과적인 식품안전 관련 위험 커뮤니케이션의 수행 과정에서 핵심적이다. 물론 모든 가능한 쟁점을 예측하고, 준비하고, 계획을 세우기는 어렵지만, 미리 우선순위를 정하고 계획을 세우는 것은 신속하고 효과적인 커뮤니케이션에 기여할 것이다. 가장 기본적으로 식품안전에 관한 위험 커뮤니케이션 계획은 식품안전에 관한 쟁점이 발생하기 전, 발생한 동안, 발생한 후에 누가, 무엇을, 어떻게 할 것인지를 명확히 하는 것이다. 이러한 계획을 세울 때 고려하여야 할 점은 식품안전과 관련하여 응급상황인지 여부에 따라 달라지는데, 응급상황에서는 단시간에 더 많은 수의 관련 정부 부처 및 기관과 의논을 하여 공동으로 대응방안을 마련하여야 할 것이다.

다음의 절차에 따라 커뮤니케이션 담당자는 식품안전에 관한 위험 커뮤니케이션을 준비하여야 한다.

1. 식품안전과 관련된 여러 쟁점 중에서 발생할 가능성이 높은 순위의 쟁점을 파악하고, 이와 관련한 정보를 수집한다.
2. 효과적인 의사소통을 위하여 필요한 커뮤니케이션 활동을 파악한다.
3. 커뮤니케이션 활동에 도움이 될 만한 사람과 기관에 대한 정보를 수집하고, 장단점을 파악한다.
4. 커뮤니케이션의 주요 대상자를 파악하고 이해하고, 이해관계자들과 의견을 교환한다.
5. 메시지를 작성하고 배포한다.
6. 커뮤니케이션의 결과를 모니터링하고 평가한다.

(3) 식품안전에 관한 위험 커뮤니케이션의 실시 전에 고려하여야 할 사항

(가) 식품안전 쟁점의 본질에 대한 이해

(a) 연관된 위험 및 이득의 본질에 대한 이해

다음의 정보를 수집하는 과정에서 특정한 식품안전 쟁점과 관련된 위험과 이득의 본질을 파악할 수 있을 것이다.

- ▸ 누가 그리고 무엇이 영향을 받을 수 있는가?
- ▸ 어떠한 정도로 영향을 받을 수 있는가?
- ▸ 어떠한 결과를 야기할 것인가?
- ▸ 어떠한 가능성이 있는가?
- ▸ 어떠한 시간적인 프레임에서 발생할 것인가?

식품안전에 관한 위험 발생의 가능성과 심각성을 이해하는 것은 다양한 이해관계자들과의 사이에 위험 커뮤니케이션 전략을 결정하는데 있어서 매우 중요하다. 예를 들어, 위험에 대한 대중의 관심이 매우 낮고 위험이 현실화되어 부정적인 상황이 발생할 가능성은 매우 낮으나 그 잠재적인 결과가 심각한 경우에, 관련 정부 부처의 웹사이트에 위험과 관련된 충분한 정보를 제공하는 것이 적절한 방법일 것이다. 그러나 이러한 경우에 위험요소를 모니터링할 수 있는 이해관계자들과 대화를 나누고 부정적인 상황의 발생 가능성을 최소화하려는 노력을 할 필요가 있다.

또한 식품안전에 관한 위험이 발생하면 누가 그리고 무엇이 영향을 받을 수 있는지에 대한 이해에 바탕을 두고 위험 커뮤니케이션의 대상을 결정하여야 한다. 특히 중요한 것은 특정한 위험에 취약한 인구 집단 및 그들이 위험에 잠재적으로 노출된 정도를 파악하는 것이다. 일반적으로 취약한 인구 집단으로 영아, 유아, 노인, 임산부, 질병 또는 영양부족으로 면역체계가 약한 사람들을 들 수 있으며, 이러한 사람들에게 특별히 초점을 맞춘 커뮤니케이션이 이루어져야 할 것이다.

위험 커뮤니케이션 담당자는 사람들의 위험에 대한 용인의 정도를 조사하여야 한다. 특정한 식품 섭취로 인하여 발생할 수 있는 위험과 이득의 정도에 대한 판단은 다양한 요인에 의하여 사람마다 다를 수 있다. 따라서 사람들마다 위험에 대한 용인의 정도가 다를 수 있음을 인정하고 커뮤니케이션의 주요 대상자에 따른 적절한 전략을 검토하여야 한다.

(b) 위험의 본질

위험 커뮤니케이션 담당자는 특정한 식품안전 쟁점과 관련된 위험의 본질에 대하여 과학적으로 명확히 이해하여야 하고, 이와 더불어 사람들이 여러 가지 유형의 위험에 어떻게 대응하는지도 이해하여야 한다. 즉, 위험에 노출된 정도(노출된 시간과 양)와 위험의 특성(화학적 위험 또는 생물학적 위험)이 사람들의 대응방식에 많은 영향을 미칠 것이다.

생물학적 위험의 경우에는 잠재적인 위험을 평가할 때 질병을 유발할 정도로 소비되어야 하는 병원균의 양에 대하여 이해하는 것이 중요하다. 건강한 성인은 오염된 날 음식(예를 들어, 채소 또는 생선)을 섭취하여 일정한 정도의 위험에 노출되었더라도 임상적으로 질병이 발생하지 않을 수 있다. 그러나 취약한 인구 집단에 해당하는 사람들이 노출된 경우, 많은 수의 사람들이 동시에 노출된 경우, 위험에 노출된 정도가 심한 경우, 소량 노출되었더라도 질병이 유발될 수 있는 경우, 위험요소가 자연적으로 발생하지 않았다고 여겨지는 경우에 사람들의 우려의 정도는 높아질 것이다. 이러한 경우에는 위험 커뮤니케이션에서 이러한 우려를 직접적으로 언급하며 위험의 심각성에 대하여 명확히 의사소통하는 것이 반드시 필요하다.

화학적 위험의 경우, 소량의 특정한 독소(예를 들어, 납)가 신체에 장기간 축적되어 장기적으로 문제를 발생시킬 수 있다. 이러한 장기적인 영향은 일반적으로 심각하게 인식되지 않는 경향이 있는데, 사람들이 정보에 기초한 판단을 내릴 수 있도록 위험 커뮤니케이션 메시지에 이러한 내용이 포함되어야 한다. 또한 위험이 잘 알려져 있지 않거나 위험의 정도가 수량화되지 않는 경우에, 이러한 지식의 불확실성이나 부족도 위험 커뮤니케이션에서 다루어져야 한다.

(c) 이용 가능한 데이터의 질과 확실성에 대한 평가

식품안전 쟁점과 관련된 위험 및 이득에 관한 데이터가 규칙적인 위험 분석 과정에서 제공될 수도 있지만, 심각한 위험을 예방하거나 감소시키기 위하여 긴급하게 위험 커뮤니케이션이 필요한 상황에서는 완전하지 못하고 불확실한 데이터가 일반적이다. 위험에 관한 데이터가 불확실한 상황에서 효과적으로 의사소통을 하기 위하여 위험 커뮤니케이션 담당자가 불확실성에 대하여 정확히 이해하고 있는 것이 필수적이다. 이러한 경우에 위험평가 담당자는 위험평가를 진행하는 동안 발생한 불확실성을 문서화하고 위험관리 담당자 및 위험 커뮤니케이션 담당자와 적절히 의사소통하여야 한다. 또한 이해관계자들 및 커뮤니케이션의 주요 대상자들이 위험평가의 한계를 이해하고 적절한 판단을 내릴 수 있도록, 일반인들이 이해할 수 있는 기술적이지 않은 용어로 메시지를 작성하여야 한다.

(d) 위험과 관련하여 취할 수 있는 조치에 대한 이해

위험 커뮤니케이션 담당자는 사람들이 위험요소에 노출되는 것을 방지하기 위하여 스스로 어떠한 조치를 취할 수 있는지 이해하고 명확히 알려주어야 한다. 사람들이 개인적으로 위험요소에 대하여 통제할 수 있는지 여부는 매우 중요한데, 이러한 개인적인 통제가 어려운 경우에는 위험을 줄이기 위하여 규제기관이 구조적으로 취하고 있는 조치에 대하여 명확히 전달하여야 한다.

식품안전에 관한 위험을 효과적으로 관리하기 위하여서는 위험을 줄이기 위하여 무엇을 하여야 하고, 누가 그렇게 할 수 있는 위치에 있는지에 대하여 정확히 파악하여야 한다. 예를 들어, 깨끗한 물에 쉽게 접근할 수 없는 경우에, 음식을 조리하는 사람들에게 손을 씻도록 독려하는 캠페인을 하는 것은 효과적이지 못하다. 이러한 경우에 커뮤니케이션은 음식을 조리하는 사람들이 일하는 장소를 소유하고 있거나 통제하는 사람들을 대상으로 이루어져야 할 것이다. 또한 식품안전에 관한 특정한 위험관리가 성공적으로 이루어지기 위하여 위험관리와 관련한 권고를 준수한 사람들에게 주어지는 긍정적 또는 부정적 인센티브(예를 들어, 보상 또는 법적 제재)를 분명히 하여야 한다.

(e) 의도하지 않은 결과에 대한 예측 및 대응

발생할 수 있는 의도하지 않은 결과에 대하여 파악하고, 예측하고, 감소시키기 위한 노력도 수반되어야 한다. 예를 들어, 특정한 식품안전 관련 위험에 영향을 받은 저소득 계층의 사람들에게 적절한 대안을 제시하지 않고 특정한 식품이 오염되었다거나 건강에 유해할 수 있다는 사실만을 알리는 것은 공중 보건의 보호에 아무런 실익도 없이 단순히 사회적 우려만을 유발할 뿐이다. 따라서 효과적이지 못한 식품안전에 관한 위험 커뮤니케이션으로 부터 발생할 수 있는 식품 소비의 의도하지 않은 변화에 대하여 고려하는 것이 중요하다.

(나) 주요 대상자의 욕구에 대한 이해

식품안전 쟁점의 본질에 대한 이해는 성공적인 위험 커뮤니케이션을 계획하고 실행하는데 있어서 반드시 필요한 요소이나 전부는 아니다. 식품안전 쟁점의 본질에 대한 이해만큼 중요한 것이 커뮤니케이션의 주요 대상자에 대한 이해이다. 언제 대상자들이 수월하게 의사소통할 수 있고, 어떠한 유형의 정보를 필요로 하는지에 대하여 고찰하기 위하여 확인하여야 할 사항은 다음과 같다.

- ▸ 주요 대상자가 위험에 대하여 현재 얼마나 알고 있는가?
- ▸ 현재 알고 있는 지식에 기초하여 주요 대상자가 어떻게 행동하고 있는가?
- ▸ 어디에서 지식의 격차가 나타나고 있으며, 이러한 지식의 격차를 좁혀야 할 필요가 있는가?
- ▸ 주요 대상자는 어떠한 우려를 하고 있으며, 위험에 관한 인식은 어떠한가?

(a) 주요 대상자의 문화적·사회적·경제적 배경

적절한 위험 커뮤니케이션을 결정하기 위하여서 위험 커뮤니케이션 담당자는 주요 대상자의 문화, 신념, 사회적·경제적 지위를 고려하여야 한다. 위험 커뮤니케이션 담당자가 고려하여야 할 사항은 다음과 같다.

▸ 문화 및 사회에서 음식의 특별한 의미: 특정한 사회 및 문화권에서는 특정한 음식 및 음식을 준비하는 과정에 특별한 의미가 부여되어 있을 수 있다. 음식을 준비하고 섭취하는 관행은 그 사회 및 문화권에 살고 있는 사람들의 정체성과 관련되어 있기 때문에 식품안전에 관한 위험 커뮤니케이션을 할 때 상당히 주의하여야 한다. 예를 들어, 어떠한 문화권에서는 음식에 직접 손을 대어 음식을 준비하는 것이 전통적인 방식인데, 위생을 이유로 장갑을 착용하도록 권고하는 것은 그들의 요리 관행이 깨끗하지 않다는 비판으로 인식될 수 있다.

▸ 성 역할: 특정한 사회 또는 문화권에서는 식품의 구입 및 음식의 조리 등에 관한 성 역할 및 책임이 구분되어 있다. 많은 문화권에서 일반적으로 여성들이 가족이 먹을 음식을 결정하고 준비하는데 있어서 일차적인 책임을 지니고 있다. 이러한 경우에 특정한 식품안전에 관한 위험 커뮤니케이션은 여성들을 대상으로 이루어져야 할 것이다. 그러나 문화적 또는 종교적 전통으로 남성이 음식의 선택과 관련한 주요한 결정을 하는 사회도 있다. 따라서 식품안전과 관련하여 주요한 책임이 있는 사람들을 파악하고 적절한 커뮤니케이션 전력을 세워야 한다.

▸ 언어: 문화적·언어적으로 다양한 사회에서는 여러 종류의 언어로 위험 커뮤니케이션이 실시되어야 한다. 다양한 언어로 의사소통을 하기 위하여서는 많은 기술과 자원이 필요하기 때문에 일반적으로 많은 수의 사람들이 사용하는 언어로 의사소통이 이루어지는 경향이 있다. 그러나 한 가지 언어로 식품안전과 관련한 필수적인 정보에 대하여 의사소통을 하게 되면, 다른 언어를 쓰는 사람들이 정보부족으로 유해한 상황에 노출될 수 있고, 규제기관이 이러한 사람들의 보건에 신경을 쓰고 있지 않다는 의미로 해석될 수 있다. 따라서 위험 커뮤니케이션 메시지를 전달하는 언어도 고려되어야 한다.

▸ 읽기 능력: 식품안전에 관한 위험이 문서로만 전달되는 경우에, 읽기 능력이 부족한 많은 커뮤니케이션 대상자들에게 위험 관련 내용이 충분히 전달되지 않을 수 있다.

따라서 커뮤니케이션 대상자들의 읽기 능력을 파악하여 다양한 방식으로 식품안전에 관한 위험과 관련한 관한 정보를 제공하여야 할 것이다. 예를 들어, 라디오 방송, 텔레비전 방송, 팟캐스트, 이미지, 노래, 연극 등의 정보 전달 방식을 활용할 수 있을 것이다.

(b) 주요 대상자에게 접근하는 방법

식품안전에 관한 위험 커뮤니케이션은 주요 대상자들에게 적절한 방식으로 접근할 수 있는 경우에만 효과가 있다. 따라서 각각의 주요 대상자들이 선호하는 정보의 소스(source), 의사소통 채널 등을 이해하는 것이 중요하다.

- 정보의 소스 및 대변인의 특성: 효과적인 의사소통을 위하여서 위험 커뮤니케이션 담당자는 주요 대상자들이 신뢰하는 정보의 소스에 대하여 파악하여야 한다. 가장 신뢰를 받는 정보의 소스가 반드시 가장 많이 활용되는 정보의 소스는 아니라는 점을 기억하고, 위험 관련 정보를 전달하기에 적절한 정보의 소스를 찾아내어 협력하여야 한다. 또한 규제기관은 신뢰에 기초하여 주요 대상자와 효과적으로 의사소통할 수 있는 대변인을 선택하여야 한다. 성공적인 위험 커뮤니케이션을 위하여서는, 기술적으로 위험과 관련된 쟁점을 명확히 이해하고, 확신 있게 관련 내용을 전달하며, 행동 및 태도로 다른 사람들에게 신뢰를 줄 수 있는 사람이 대변인으로 선정되어야 한다. 위험에 관한 전문적인 지식과 원활한 의사소통 기술을 동시에 지니고 있는 사람을 찾기 어려운 경우에는, 이러한 능력을 지닌 사람들로 구성된 팀을 만들어 위험 커뮤니케이션을 진행할 수도 있을 것이다.

- 의사소통 채널 및 방식: 커뮤니케이션의 주요 대상자들에게 접근하기 위하여서는 적절한 의사소통 채널 및 방식을 이용하여야 한다. 모든 주요 대상자들이 동일한 의사소통 채널에 접근 가능하거나 이용 가능한 것은 아니다. 예를 들어, 웹사이트는 대부분의 사람들의 인터넷 접근 가능성이 제한된 개발도상국가에서는 활용되기 어려울 것이다. 그러나 이러한 국가에서도 특정한 유형의 전문가를 중심으로 정보를 확산시키려는 경우에는 웹사이트를 활용할 수 있을 것이다.

(다) 위험의 역사적·정치적 배경 및 미디어 환경

특정한 식품안전 쟁점에 대응하는데 필요한 정보의 유형을 결정하기 위하여, 위험 커뮤니케이션 담당자는 식품안전 쟁점이 발생한 역사적·정치적 배경 및 미디어 환경을 고려하여야 한다. 식품안전 쟁점과 관련된 배경을 더 완전히 이해하기 위하여서는 관련 역사를 인식하는 것이 필수적이다. 예를 들어, 어떠한 회사의 특정한 식품제품에서 식품안전에 관한 위험 쟁점이 두 번째로 발생한 경우에, 위험 그 자체에 대한 의사소통 이외에도 동일한 문제가 반복하여 발생한 이유 및 장래의 대처방안 등에 대하여 설명하여야 한다. 또한 식품안전 쟁점과 관련하여 정치적인 견해, 과학적인 판단, 소비자 단체 또는 NGO의 주장 등이 엇갈리는 경우에, 위험 커뮤니케이션 담당자는 다양한 이해관계자들의 견해에 언제 어떻게 대응할 것인지 고려하여야 한다.

식품안전 쟁점과 관련하여 이미 발행된 미디어 보도의 내용, 톤, 분량 등도 위험 커뮤니케이션 전략을 결정하는데 있어서 중요하다. 미디어에서 식품안전 쟁점을 어떻게 보도하였느냐에 따라서 사람들이 위험에 관하여 알고 있는 내용 및 위험에 대한 태도가 달라질 수 있다. 따라서 미디어 보도 내용을 분석하여, 위험 커뮤니케이션에서 어떠한 내용을 다룰 것인지, 위험의 본질을 설명하기 위하여 어떻게 접근할 것인지 등을 결정하여야 한다.

(라) 식품안전 관련 위험 커뮤니케이션 담당자의 책임

특정한 식품안전에 관한 위험이 발생한 상황에서 위험 커뮤니케이션 담당자의 책임을 명확히 할 필요가 있다. 관련 자원이 충분하지 않은 상황에서 공중 보건에 미치는 영향 및 대중의 우려의 정도를 고려하여 어떠한 정도의 개입과 노력이 적절한지 여부에 대하여 결정하여야 한다. 공중 보건에 심각한 결과를 초래할 수 있는 즉각적인 위협이 제기된 경우에, 적절한 경고를 작성하여 많은 사람들에게 신속하게 배포하여야 할 윤리적 의무 및 법적 책임이 커뮤니케이션 담당자에게 있다. 반면에, 공중 보건에 미치는 영향이 적고 사람들이 관련 쟁점에 관심이 없는 상황에서, 커뮤니케이션 담당자의 책임을 분명히 하는 것은 오히려 더 어려울 수 있다. 따라서 이러한 경우에는 관련 쟁점에 대하여 궁금해 하는

사람들이 쉽게 정보를 찾을 수 있도록 보도 자료를 배포하거나 웹사이트에 게시하는 등의 방법을 활용할 수 있을 것이다.

위험 커뮤니케이션 담당자가 대응하기 어려운 쟁점은 과학적 위험평가의 정도와 공공의 위험인식이 일치하지 않는 경우이다. 공중 보건에 미치는 영향은 크지만 공공의 우려가 낮은 경우에, 위험 커뮤니케이션 담당자는 공중 보건을 보호할 윤리적 의무에 따라 관련 쟁점에 대한 공공의 인식을 높여야 할 것이다. 반면에, 공공의 우려가 공중 보건에 실질적으로 미치는 영향을 과도하게 넘은 경우에, 위험 커뮤니케이션 담당자는 사람들이 우려하는 이유를 찾아 적절하게 대응하면서 관련된 위험에 대한 과학적 평가 결과를 적절히 알리는 것이 중요하다. 하지만 이러한 경우에도 위험에 대한 공공의 인식이 반드시 수정되어 위험에 대한 과학적 평가 또는 전문가의 견해와 일치하여야 한다는 것을 의미하는 것은 아니다. 왜냐하면 특정한 식품안전에 관한 위험이 질병이나 죽음을 초래하지 않는다는 사실이 반드시 그러한 유형의 위험이 문화적으로 수용되어야 한다는 것을 의미하지는 않기 때문이다.

(4) 식품안전에 관한 위험 커뮤니케이션의 실시

(가) 주요 대상자에 대한 파악

위험 커뮤니케이션 담당자는 메시지를 작성하기 전에 커뮤니케이션의 주요 대상자에 대하여 이해하여야 한다. 주요 대상자를 파악하는 목적은 다음과 같다.

- 주요 대상자가 정보에 기초한 결정을 내리는데 필요한 정보의 제공
- 주요 대상자가 스스로 건강을 증진시키기 위하여 특정한 행위를 하도록 설득
- 주요 대상자와 적절히 의사소통하기 위한 대화를 개시

주요 대상자에 대한 파악은 일반적으로 이해관계자들과의 대화를 통하여 이루어지며, 다음과 같은 사항이 고려되어야 한다.

- 위험으로 인하여 누가 또는 무엇이 직접적으로 영향을 받았는가?

▸ 누가 쟁점에 긍정적·부정적 영향을 미칠 수 있는가? (예를 들어, 누가 위험을 효과적으로 최소화할 수 있으며, 해결방안을 제시할 수 있는가?)
▸ 누가 쟁점에 간접적으로 영향을 받았으며, 위험에 관하여 인지하고 있을 필요가 있는가? (예를 들어, 환자를 간병하는 사람)

동일한 식품안전에 관한 위험이라고 하더라도, 파악된 주요 대상자가 다른 경우에 주요 대상자에 따라 다른 메시지를 작성할 필요가 있다. 예를 들어, 집에서 혼자 생활하는 고령의 노인, 노인을 돌보는 사회복지사, 요양병원의 영양사에게는 대상자별로 적합한 의사소통 채널을 활용하여 필요한 메시지가 전달되어야 한다.

(나) 주요 대상자에 대한 이해

커뮤니케이션의 주요 대상자들은 모두 다른 정보에 대한 욕구를 지니고 있기 때문에, 위험 커뮤니케이션을 통하여 어떠한 정보를 어떠한 방식으로 획득하고자 하는지에 대한 이해가 필수적이다. 주요 대상자들의 정보에 대한 욕구를 조사하는 방법으로는 주요 대상자들 중 일부를 만나 작성한 메시지를 전달하고 반응을 살펴보는 방법, 설문조사와 같은 양적 연구를 실시하는 방법, 포커스 그룹과 같은 질적 연구를 실시하는 방법 등이 있다. 이렇게 주요 대상자들의 정보에 대한 요구를 조사할 때 다음과 같은 질문이 유용하다.

▸ 식품안전에 관한 위험에 관하여 주요 대상자는 어떻게 생각하고 있는가?
▸ 식품안전에 관한 위험에 관하여 주요 대상자는 어떠한 오해를 하고 있는가?
▸ 주요 대상자는 위험이 크거나 작다고 생각하고 있는가?
▸ 주요 대상자의 위험과 관련한 주요한 우려는 무엇인가?
▸ 주요 대상자는 누가 이러한 유형의 위험에 가장 취약하다고 생각하는가?
▸ 주요 대상자는 식품안전에 관한 위험과 관련한 정보를 어떻게 획득하는 것을 선호하는가? 과학자 등 전문가 집단, NGO, 미디어, 정부 부처 중 누구를 통하여 정보를 획득하고 싶어 하는가?

- ▸ 주요 대상자는 어떠한 소스(source)의 정보를 신뢰하는가? 과학자 등 전문가 집단, NGO, 미디어, 정부 부처 중 어떠한 소스의 정보를 신뢰하는가?
- ▸ 주요 대상자가 계획된 정보 소스와 채널에 접근 가능한가?
- ▸ 누가 주요 대상자의 의견에 영향을 미칠 수 있는 사람인가?

이러한 질문에 대한 대답은 커뮤니케이션의 주요 대상자와 커뮤니케이션 담당자 사이에 또는 주요 대상자들 사이에 어떠한 지식의 격차가 있고, 정보를 제공하여 이러한 격차를 좁힐 필요가 있는지 여부를 결정하는데 도움이 된다. 또한 특정한 사람들과 위험에 관한 의사소통을 하는데 적합한 정보 소스와 채널을 결정하는데 도움이 될 것이다. 예를 들어, 임산부에게 위험에 관한 특정한 정보를 전달하기 위하여서는 산부인과 전문의 또는 소셜 미디어 등을 활용할 수 있고, 고령의 노인에게 전달하기 위하여서는 사회복지사 또는 지역 라디오 채널 등을 활용할 수 있을 것이다.

(다) 이해관계자와의 상호작용

식품안전에 관한 위험 커뮤니케이션의 쟁점은 여러 정부 부처, 식품 관련 제조업자, 소비자 단체 등 다양한 이해관계자들과 직접적인 관련을 맺고 있다. 따라서 이해관계를 지니고 있는 다양한 집단 사이에서 의견을 조율하는 것은 위험 커뮤니케이션 과정에서 꼭 필요한 부분이다. 이러한 과정은 응급상황에서 특히 더 중요한데, 메시지가 매우 짧은 시간적 상황에서 작성되어야 하며 자주 수정될 필요가 있기 때문에, 더 광범위한 이해관계자들의 자문이 필수적이다. 이해관계자들과의 의견 조율이 적절히 이루어지지 않아 일관되지 않은 메시지가 대중에 전달되면, 사회적 혼란이 야기될 수 있다. 따라서 이해관계자들과 적절한 상호작용이 반드시 이루어져야 할 것이며, 이러한 상호작용에는 추가적으로 다음과 같은 장점이 있다.

- ▸ 상황에 대한 이해도를 높일 수 있다.
- ▸ 주요 대상자가 우려하는 점에 대한 피드백을 얻을 수 있다.

▸ 필요한 경우에, 관련 정보를 배포하는 과정에서 이해관계를 지닌 기관의 자원이나 신뢰도를 활용할 수 있다.

이해관계자들과의 의견 조율이 원활히 이루어지려면 상호간에 강력한 관계가 요구되는데, 이러한 관계는 식품안전에 관한 위험 쟁점이 발생한 긴급한 상황에서 형성되기는 어렵다. 따라서 일상적인 상황에서 식품안전과 관련하여 이해관계를 지니고 있는 집단을 파악하고, 일정한 관계를 유지하는 것이 중요하다. 이러한 이해관계를 지니고 있는 집단을 파악하는데 활용될 수 있는 기준은 다음과 같다.

▸ 위험을 줄이거나 늘릴 수 있는 결정을 하는 의사결정권자
▸ 위험에 의하여 가장 영향을 많이 받는 사람들과 그들을 대표하는 조직
▸ 신뢰 및 주요 대상자에 대한 접근의 측면에서 영향력이 큰 사람
▸ 위험 커뮤니케이션의 목적 달성을 도울 수 있는 사람
▸ 위험 커뮤니케이션의 목적 달성을 방해할 수 있는 사람

이해관계자의 시각 및 전문적인 견해는 효과적인 메시지 작성 및 배포에 도움이 될 수 있지만, 이해관계자들이 위험관리 및 위험 커뮤니케이션 과정에 부적절한 영향을 미쳐서는 안 된다. 이러한 과정에 이해관계자가 부적절한 영향을 미쳤을 수 있다는 인식만으로도 위험 커뮤니케이션 메시지에 대한 신뢰도는 떨어질 것이다.

(라) 정보의 불확실성

식품안전에 관한 위험과 관련한 정보가 불확실한 경우에, 대부분의 위험관리 담당자는 다음과 같은 이유로 모든 사실이 분명해질 때까지 위험과 관련한 쟁점에 관한 의사소통을 꺼리는 경향이 있다. 그러나 정보가 불확실한 경우라도 불확실성을 인정하면서 위험 커뮤니케이션을 실시하는 것이 바람직하다.

▸ 공황상태에 대한 공포: 위험에 관한 불확실한 정보는 대중의 공포수준을 공황상태까지 끌어올려 비이성적인 행동을 유도할 수 있다는 인식에 기초한다. 그러나 제한적이고 불분명한 정보라도 정보가 제공된 경우에 공포의 수준이 낮아진다는 것이 연구결과 드러나고 있다.

▸ 통제상실에 대한 공포: 위험분석의 결과를 대중에게 알리지 않음으로써 사회적으로 사람들을 통제할 수 있다는 믿음에서 나온 것이다. 그러나 사실상 위험과 관련한 쟁점은 이미 통제를 벗어나 있고, 불확실성을 이유로 대중과 소통하지 않음으로써 대중의 신뢰까지도 잃을 수 있다.

▸ 경제적인 손실에 대한 공포: 불확실한 정보로 의사소통을 하게 되면 해당 기업에 피할 수 없는 경제적인 손실을 가져온다는 사실에 기초한 것이다. 그러나 해당 시점까지 밝혀진 과학적인 정보가 확실한 경우에는 초기에 위험 커뮤니케이션을 함으로써 경제적인 비용을 오히려 줄일 수 있는데, 위험이 현실화되어 질병이 발생한 경우에 공중보건에서 부담하여야 하는 비용 및 정부와 기업을 상대로 한 소송비용까지 고려하면 위험 커뮤니케이션을 진행하는 것이 오히려 경제적으로 이득이 된다.

▸ 대체 식품의 부족: 식품안전에 관하여 쟁점이 된 식품을 대체할 식품이 없는 상황을 의미한다. 특히 사람들이 문제가 된 식품의 섭취를 멈추어 심각한 건강상의 이상이 발생할 수 있는 경우가 있을 수 있다.

정보가 불확실한 상황에서도 위험 커뮤니케이션을 통하여 주요 대상자들은 스스로 자신을 보호하는 조치를 취할 수 있고, 커뮤니케이션 담당자 또는 기관에 대한 신뢰를 제고할 수 있기 때문에, 위험 발생의 가능성을 인지한 경우에는 위험 커뮤니케이션이 실시되어야 한다. 특히 식품을 매개로 한 질병이 발생한 경우에 관련 정보가 확실하여 질 때까지 의사소통을 미루면, 더 많은 수의 사람들이 피해를 입을 수 있다. 따라서 위험 발생에 관하여 신속히

공공에 알리고, 위험의 원인을 아직 조사 중이라는 사실을 인정하고, 소비자 및 취약한 인구집단이 스스로를 보호하기 위하여 취할 수 있는 일반적인 식품안전 예방조치를 제시하여야 한다.

(마) 메시지 작성

위험 커뮤니케이션 메시지는 식품안전 쟁점의 본질 및 주요 대상자의 의사소통 욕구에 대한 이해에 기초하여 작성되어야 한다. 메시지를 작성할 때, 다음의 질문이 주요 대상자와의 관계에서 주요하게 고려되어야 할 것이다.

- ▸ 식품안전 관련 쟁점이 무엇인가?
- ▸ 주요 대상자에게 어떠한 위험이 있는가?
- ▸ 주요 대상자가 위험과 관련하여 어떠한 인식 및 우려를 지니고 있는가?
- ▸ 주요 대상자가 위험과 관련하여 스스로를 보호하기 위하여 무엇을 할 수 있는가?
- ▸ 위험에 관하여 어떠한 점이 알려져 있지 않거나 불확실한가?
- ▸ 불확실성을 줄이기 위하여 무엇을 하였는가?
- ▸ 위험관리를 위하여 무엇을 하였는가?
- ▸ 주요 대상자와 관련하여 고려하여야 할 다른 맥락이 있는가?

다음의 과정은 핵심적인 메시지 작성에 도움이 될 것이다.

1. 위험에 관한 사회적인 우려를 확인한다.
2. 대응하여야 하는 쟁점 및 쟁점에 대한 일반적인 인식을 파악하기 위하여 사회적인 우려를 분석한다.
3. 대응할 필요가 있는 일반적인 또는 특정한 우려에 대한 핵심 메시지를 작성한다.
4. 핵심 메시지에 포함된 사실 및 근거와 관련한 정보를 확인한다.
5. 메시지를 전달받을 주요 대상자 중 일부를 상대로 메시지를 테스트한다.
6. 주요 대상자에게 적절한 배포 방식을 확인하는 등 메시지의 전달방법을 계획한다.

위험 커뮤니케이션 메시지는 일반적으로 다음과 같은 정보를 전달하고 있어야 한다.

- ▸ 위험에 대한 묘사
- ▸ 주요 대상자 또는 소비자에 대한 조언
- ▸ 주요 대상자 또는 소비자에 대한 조언을 반복하는 인용 (전문가 집단, 정부 부처 등을 인용하여 조언을 반복)
- ▸ 위험을 최소화하기 위하여 취한 조치에 대한 설명
- ▸ 위험과 관련한 추가적인 상황에 대한 설명

이러한 메시지는 위험의 심각성 및 주요 대상자의 취약성, 위험을 최소화하기 위하여 사람들이 취하여야 하는 조치 등을 알려주어야 하며, 주요 대상자가 이해할 수 있는 일반적인 용어로 작성되어야 한다. 또한 내용을 전달하는데 있어서 시각적으로 도움이 될 수 있는 자료를 활용하는 것이 좋으며, 읽기 능력이 부족한 이민자 집단 등을 대상으로 한 메시지를 작성할 때에는 특히 더 그러하다.

메시지로 인하여 발생할 수 있는 의도하지 않은 결과를 예측하고 관리하기 위하여, 이해관계자들과 함께 메시지의 내용을 검토하고 주요 대상자들 중 일부에게 메시지를 먼저 전달하여 반응을 살펴보아야 한다. 메시지를 작성하는 동안 이해관계자들과 논의할 수 있는 기회가 없으면, 주요 대상자들에게 메시지를 전달하기 전에 이해관계자들에게 먼저 전달하여 발생할 수 있는 의도하지 않은 결과를 예측하여야 할 것이다.

(바) 커뮤니케이션 채널, 도구, 방법의 선택

특정한 커뮤니케이션 채널이 효과적인지 여부는 위험 커뮤니케이션의 목적, 메시지의 내용 및 긴급성, 주요 대상자의 접근 가능성 등에 따라 달라진다. 예를 들어, 웹사이트는 광범위한 대상자와 의사소통을 하여야 하고 피드백을 받을 필요가 없는 경우에 적합하다. 또한 식품안전에 관한 위험과 관련하여 응급상황이 발생한 경우에는 미디어를 통한 신속한 정보의 제공이 이루어져야 한다. 상황에 따라 다음에 제시된 다양한 커뮤니케이션 채널을 선택·조합하여 활용할 수 있을 것이다.

- 미디어
- 웹사이트
- 이메일
- 인쇄물
- 디지털 인쇄물
- 회의, 워크숍, 포커스 그룹
- 이해관계자들의 네트워크
- 소셜 미디어 (페이스북, 트위터)
- 블로그
- 팟캐스트
- 온라인 회의
- 설명회

(사) 미디어와의 상호작용

미디어와의 상호작용은 식품안전에 관한 위험 커뮤니케이션 전략의 필수적인 부분이다. 따라서 위험 쟁점에 관한 미디어 보도에 영향을 미치는 핵심적인 요소를 인식하는 것이 중요한데, 그 예는 다음과 같다.

- 공포
- 갈등
- 비난
- 은폐
- 다윗과 골리앗 (균형이 맞지 않는 경쟁적인 이해관계의 충돌)
- 시각적인 효과
- 사람들의 관심을 끄는 쟁점

식품안전에 관한 쟁점이 발생하기 전에 미디어와의 상호작용을 위하여 다음과 같은 준비를 하여야 한다.

- 식품안전 쟁점을 규칙적으로 다루는 신문기자를 파악한 후 일정한 관계를 맺고 유지한다. 사람들의 관심을 끄는 쟁점을 찾아 보도를 하는 신문기자와 커뮤니케이션의 주요 대상자에게 접근할 수 있는 신문기자를 모두 찾는 것이 중요하다.
- 미디어와 소통할 수 있는 대변인을 찾아서 훈련시킨다. 과학적 전문지식보다 의사소통의 기술이 더 중요하다는 것을 염두에 두어야 한다.
- 식품안전 쟁점에 관한 내용이 여러 미디어에 일관되게 보도될 수 있도록 배경자료를 준비하고, 보도와 관련하여 각각의 사람들이 어떠한 역할을 하는지 파악한다.
- 식품안전에 관한 위험이 특정한 사건으로 발생한 경우에 어떻게 미디어 대응을 할 것인지에 대한 계획을 핵심 이해관계자들과 함께 마련한다.

미디어와 상호작용 과정에서 미디어 대응의 효율성을 높이기 위하여 다음과 같은 조치를 취하여야 한다.

- 상황을 앞서서 주도한다.
- 주요 대상자에게 메시지를 전달할 수 있는 역량을 갖추고 있는 목표 미디어를 찾아내고, 그러한 미디어의 특성에 맞추어 보도 자료를 수정한다.
- 가능한 경우에 이해관계자들과 함께 미디어 대응방안을 조율한다.
- 미디어 이해관계자와 의사소통할 수 있는 다양한 방식을 검토한다.
- 미디어의 보도내용을 모니터링하고 오보가 있는 경우에는 가능한 빨리 바로 잡는다.

미디어 대응 이후에 다음과 같은 방식으로 미디어와 상호작용을 평가하는 것은 장래의 상호작용에 유용한 지침이 될 것이다.

- ▸ 식품안전 쟁점이 미디어에 보도된 내용을 검토하고 분석한다. 예를 들어, 메시지가 정확하게 반영되었는가? 주요 대상자와 관련하여 목표로 한 미디어에 관련 메시지가 보도되었는가?
- ▸ 미디어 대응을 통하여 얻은 교훈에 대하여 이해관계자들과 함께 논의한다.
- ▸ 미디어 대응에 대한 피드백을 받기 위하여 언론인들에게 자문을 구한다.

(아) 외국과의 상호작용

식품안전에 관한 위험과 관련하여 응급상황이 발생한 경우에, 이해관계를 지니고 있는 국가와 의사소통을 하는 것은 응급상황의 발생을 국제적으로 알리고, 국제적으로 필요한 자원을 동원하고, 집단적인 대응이 필요한 경우에 관련된 논의를 시작할 수 있게 한다. 또한 종합적인 위험평가를 실시할 수 있는 역량을 갖추고 있지 못한 국가의 경우에는 국제적인 지원을 받을 수 있다. 오염된 식품이 국제 시장에 유입된 것이 확실한 경우에 관련 국가의 식품안전과 관련된 정부 부처와 의사소통을 하는 것은 필수적이다. 또한 국내에서 생산하고 소비하는 식품에서 위험과 관련한 쟁점이 발생한 경우라도, 인터넷 구매 등 비공식적인 방식으로 다른 국가에 전달되었을 수도 있기 때문에 국가 간 정보 교환이 수반되어야 할 것이다. FAO와 WTO가 공동으로 관리하는 국제 식품안전 당국자 간 네트워크(INFOSAN, International Food Safety Authorities Network)를 활용하여 식품안전에 관한 위험에 대한 평가 및 관리, 위험 커뮤니케이션 과정에서 다른 국가와의 정보 교환 등이 원활하게 이루어질 수 있을 것이다.

(자) 모니터링 및 평가

식품안전에 관한 위험 커뮤니케이션은 단순히 메시지만을 전달하는 일방향 과정이 아니라, 주요 대상자가 궁금하여 하는 정보를 파악하고 그러한 정보를 제공하는 것이 적절한지를 판단하고, 메시지가 주요 대상자들에게 적절히 수용되고 이해되어 적절한 조치가 취하여졌는지를 확인하는 양방향 과정이다. 따라서 위험 커뮤니케이션 과정을 모니터링하고 의사소통의 노력을 평가하는 것은, 이러한 커뮤니케이션이 실행되는 동안 또는 그 이후에

의사소통에 의미 있는 변화를 가져올 수 있고, 장래에 유사한 상황이 발생한 경우에 필요한 교훈을 줄 수 있다.

식품안전에 관한 위험 커뮤니케이션을 모니터링하는데 필요한 질문은 다음과 같다.

1. 주요 대상자가 메시지를 전달받았는가?
   a. 전달받지 못하였다면, 왜 전달받지 못하였는가?
2. 주요 대상자가 메시지에 대응하였는가?
   a. 대응하였다면, 주요 대상자는 커뮤니케이션 담당자가 의도한대로 대응하였는가?
   b. 대응하지 않았다면, 왜 하지 않았는가?
   c. 어떠한 질문이나 우려가 있었는가?
3. 식품안전에 관한 위험에 관하여 이해관계자와 무엇을 의사소통하였는가?
   a. 의사소통한 정보에 있어서, 다른 이해관계자와 비교하여 심각한 정도의 차이가 있었는가?
4. 주요 대상자의 위험 인식에 어떠한 변화가 있었는가?
   a. 어떠한 쟁점이 새롭게 제기되어 식품안전에 관한 위험 인식에 변화가 발생하였는가?
5. 얼마나 많은 수의 미디어가 위험 커뮤니케이션 메시지를 다루었고, 얼마나 자주 다루었는가?

식품안전에 관한 의사소통 노력을 평가할 때 필요한 질문은 다음과 같다.

1. 주요 대상자의 의사소통 욕구에 변화가 있었는가?
2. 메시지가 수정될 필요가 있었는가?
   a. 수정될 필요가 있었다면, 어떻게 수정되었어야 하는가?
3. 다른 의사소통 채널이 필요하였는가?
   a. 다른 의사소통 채널이 필요하였다면, 어떠한 채널인가?
4. 메시지를 작성하고 배포하는데 있어서 이해관계자가 포함되었는가?

a. 포함되지 않았다면, 왜 포함시키지 않았고, 앞으로도 포함시키지 않을 것인가?

b. 포함되었다면, 적절한 이해관계자이었는가?

5. 미디어는 위험 커뮤니케이션 메시지를 정확히 보고하였는가?

6. 미디어가 효과적으로 사용되었는가?

7. 의사소통의 목표와 관련하여 이러한 노력이 잘 진행되었는가?

3. 시사점

우리나라에서는 2011년 가습기살균제 사건이 발생한 이후 공산품 및 농산물의 위험에 대한 정보가 제공되지 않아 피해가 발생하는 사례가 연속적으로 발생하고 있다. 2017년에 발생한 달걀 살충제 파동 및 유해 생리대 사건 등으로 식품 및 공산품에 대한 규제기관의 관리가 철저하지 못하고 소비자들에게 관련 정보가 충분히 제공되지 않아 소비자들이 국가기관의 보호를 제대로 받고 있지 못하는 인식이 팽배해져 있는 상황이다. 이러한 상황에서, 식품안전에 관한 쟁점이 발생한 경우에 위험 커뮤니케이션 담당자의 역할을 단계별로 상세히 제시하고 있는 WHO의 '식품안전에 관한 위험 커뮤니케이션 지침'은 우리나라 정부 부처의 대응 방식을 검토하고, 앞으로 유사한 쟁점이 발생한 상황에서 적용할 수 있는 기준으로 유용하게 활용될 수 있을 것이다.

글로벌 동향 모니터링

1. UN OCHA

- Building Data Responsibility into Humanitarian Action, OCHA Policy and Studies Series (May 2016).
- Leaving No One Behind: Humanitarian Effectiveness in the Age of the Sustainable Development Goals, OCHA Policy and Studies Series (2016).
- Understanding the Climate-Conflict Nexus from a Humanitarian Perspective: A New Quantitative Approach,OCHA Policy and Studies Series (May 2016).

2. WHO

〈Ageing〉

- Global Strategy and Action Plan on Ageing and Health (2016-2020) (2016).

〈Ebola Virus〉

- Clinical Care for Survivors of Ebola Virus Disease (2016).

〈Food Satety〉

- Evaluation of Certain Food Additives: Eighty-Second Report of the Joint FAO/WHO Expert Committee on Food Additives (2016).
- Evaluation of Certain Veterinary Drug Residues in Food: Eighty-First Report of the Joint FAO/WHO Expert Committee on Food Additives (2016).
- Risk Communication Applied to Food Safety Handbook (2016).
- Safety Evaluation of Certain Food Additives and Contaminants (2016).

〈Gender〉

▸ A Tool for Strengthening Gender-Sensitive National HIV and Sexual Reproductive Health (SRH) Monitoring and Evaluation Systems (2016).

▸ Strategy on Women's Health and Well-Being in the WHO European Region (2016).

〈Gender, Equity and Human Rights〉

▸ A Foundation to Address Equity Gender and Human Rights in the 2030 Agenda: Progress in 2014-2015 (2016).

〈HIV/AIDS〉

▸ Guideline Updates on HIV and Infant Feeding (2016).

〈Indoor Air Pollution〉

▸ Burning Opportunity: Clean Household Energy for Health, Sustainable Development, and Wellbeing of Women and Children (2016).

〈Injuries, Traffic〉

▸ Drug and Road Safety (2016).

▸ Post-Crush Response: Supporting Those Affected by Road Traffic Crashes (2016).

▸ Road Safety Mass Media Campaigns: A Toolkit (2016).

〈International Programme on Chemical Safety〉

▸ The Public Health Impact of Chemicals: Knowns and Unknowns (2016).

〈Ionizing Radiation〉

▸ Communicating Radiation Risks in Paediatric Imaging: Information to Support Healthcare Discussions about Benefit and Risk (2016).

〈Leprosy〉

- Global Leprosy Strategy 2016-2020: Accelerating towards a Leprosy-Free World (2016).
- Global Leprosy Strategy 2016-2020: Accelerating towards a Leprosy-Free World Operation Manual (2016).

〈Maternal〉

- Caring for Newborns and Children in the Community: Facilitator Guideliens for Conducting a Planning Workshop (2016).

〈Mental Health〉

- Group Interpersonal Therapy (IPT) for Depression (2016).
- mhGAP Intervention Guide for Mental, Neurological and Substance Use Disorders in Non-Specialized Health Settings, Version 2.0 (2016).

〈Nutrition〉

- Toxicological Evaluation of Certain Veterinary Drug Residues in Food (2016).
- WHO Guideline: Daily Iron Supplementation in Adult Women and Adolescent Girls (2016).
- WHO Guidelines: Daily Iron Supplementation in Infants and Children (2016).
- WHO Guideline: Fortification of Maize Flour and Corn Meal with Vitamins and Minerals (2016).
- WHO Guideline: Iron Supplementation in Postpartum Women (2016).
- WHO Guideline: Use of Multiple Micronutrient Powders for Point-of-Use Fortification of Foods Consumed by Infants and Young Children Aged 6-23 Months and Children Aged 2-12 Years (2016).

▸ WHO Guideline: Use of Multiple Micronutrient Powders for Point-of-Use Fortification of Foods Consumed by Pregnant Women (2016).

〈Rabies〉

▸ Moves to Consign Rabies to History (2016).

〈Sexual and Reproductive Health〉

▸ Child, Early and Forced Marriage Legislation in 37 Asia-Pacific Countries (2016).

▸ Companion of Choice During Labour and Childbirth for Improved Quality of Care (2016).

▸ Selected Practice Recommendations for Contraceptive Use, Third Edition (2016).

▸ WHO Recommendations on Antenatal Care for a Positive Pregnancy Experience (2016).

▸ WHO Guidelines on the Management of Health Complications from Female Genital Mutilation (2016).

〈Zika Virus〉

▸ Screening, Assessment and Management of Neonates and Infants with Complications Associated with Zika Virus Exposure in Utero (2016).

▸ WHO Guideline: Infant Feeding in Areas of Zika Virus Transmission (2016).

| 집필진 |

최승필 한국외국어대학교 법학전문대학원 교수
고준성 산업연구원 선임연구위원
장원경 이화여자대학교 스크랜튼학부 교수

| 기획 및 편집 |

한국법제연구원 글로벌법제연구실
한정미 연구위원
김형건 연구위원
최지연 부연구위원
왕승혜 부연구위원
김수홍 부연구위원
서승환 부연구위원
목희진 위촉연구원
홍현표 위촉연구원

2017 GLOBAL LEGAL ISSUES (Ⅲ-1)

2017년 11월 10일 인쇄
2017년 11월 17일 발행
발행인 이 익 현
발행처 한국법제연구원
세종특별자치시 국책연구원로 15(반곡동, 한국법제연구원)
전화 : 044-861-0300 FAX : 044-868-9913
등록번호 : 1981.8.11. 제2014-000009호
http://www.klri.re.kr
ISBN : 978-89-6684-767-9 93360

값 : 10,000원

KOREA LEGISLATION RESEARCH INSTITUTE

2017
GLOBAL LEGAL ISSUES (III-1)

93360
9 788966 847679
ISBN 978-89-6684-767-9
값 10,000원