# 개인정보 보호법 시행령 일부개정령(안)

# BSA | The Software Alliance 의견서

**2023 년 6 월 30 일**

**개인정보보호위원회 귀하**

개인정보보호법 시행령 일부개정안과 최근 개정된 개인정보보호법에 대해 BSA | The Software Alliance (**BSA**)[1]의 의견을 제공할 수 있는 기회를 얻게 되어 기쁩니다.

BSA 는 정부와 세계시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있는 연합체입니다. BSA 회원사들은 클라우드 스토리지 서비스, 고객 관리 소프트웨어, 인적 자원 관리 프로그램, ID 관리 서비스, 보안 솔루션 및 협업 소프트웨어 등 기업들에게 중요한 기술과 서비스를 개발하고 이를 제공하고 있습니다.

BSA 는 개인정보보호법의 발전을 위한 다수의 논의[2]에 적극적으로 참여해왔습니다. BSA 는 시행령 개정안이 시행을 앞둔 개인정보보호법에서 위임한 구체적인 사항을 규정하고 있다는 점을 주목하고 있습니다. 이와 관련하여 위원회의 그동안의 노고에 감사 말씀을 드리며,시행령 일부개정(안) (이하 '개정안')에 대해 다음과 같은 제안사항을 드립니다.

## "수탁자"의 소비자 대면의무 제외

**개정안과 개정된 개인정보보호법 은 '데이터 컨트롤러'와 '데이터 프로세서'로 지칭되는 개인정보 위탁자와 수탁자의 역할을 명확하게 구분하지 못하고 있습니다. BSA 는 위원회가 시행령 개정 또는 향후 개인정보법 개정을 통해 개인정보보호법에서 개인정보 위탁자와 수탁자의 고유한 역할을 인정하고, 소비자 대상 의무가 "수탁자"에게 적용되지 않도록 하시기를 제언드립니다.**

정보 주체에 대한 데이터를 수집하고 사용하는 방법과 이유를 결정하는 회사(위탁자)와 다른 회사를 대신하여 이러한 데이터를 처리하는 회사(수탁자)를 구별하는 것은 매우 중요합니다. 위탁자와 수탁자 모두 개인정보를 보호하는 데 있어 중요하지만 분명히 다른 역할을 수행하기 때문입니다. 이러한

[1] BSA 회원사 : Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] 참조: 개인정보보호법 시행령 개정안에 대한 BSA | The Software Alliance 의견서, 2020 년 5 월, https://www.bsa.org/kr/policy-filings/gaeinjeongbobohobeob-sihaenglyeong-gaejeongane-daehan-bsa-the-software-alliance-ui-uigyeonseo; 개인정보보호법 일부개정안, 2021 년 2 월, https://www.bsa.org/kr/policy-filings/gaeinjeongbobohobeob-ilbugaejeongbeoblyulan-2021-1ho 개인정보보호법 일부개정법률안 BSA | The Software Alliance 의견서, 2021 년 11 월 https://www.bsa.org/kr/policy-filings/gaeinjeongbobohobeob-ilbugaejeongbeoblyulan-bsa-the-software-alliance-uigyeonseo

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

이유로 전 세계의 개인정보보호법은 두 개의 서로 다른 실체를 명확히 구분하고 있으며, 개인정보 보호에 있어 서로 다른 역할을 반영하여 각각의 다른 책임을 부여하는 글로벌 합의를 반영하고 있습니다. 이러한 접근 방식을 채택한 데이터 보호법으로는 유럽연합의 일반 데이터 보호 규정(GDPR)[3], 캘리포니아의 소비자 개인정보 보호법(CCPA)[4], 일본의 개인정보 보호법(APPI)[5], 싱가포르의 개인 데이터 보호법(PDPA)[6] 등이 있습니다.

**개정된 개인정보보호법은 위탁자와 수탁자의 역할과 책임을 적절히 구분하지 못하고 있습니다. 특히, 개정된 개인정보보호법의 제 26 조 8 항은 '개인정보처리자(위탁자)'에게 적용되어야 하는 정보주체 대면의무를 수탁자에게 부과[7]하고 있습니다. 따라서, BSA 는 정보주체 대면 의무가 "수탁자"에게는 적용되지 않는다는 점을 명확히 해줄 것을 개인정보보호위원회에 제언 드립니다.**

정보주체 대면 의무를 부과해야 하는 기업은 개인정보처리자(위탁자)로, 개별 정보 주체와 직접적으로 교류하고, 정보수집의 대상과 시기, 이유를 결정하기 때문입니다. 반면, 수탁자는 일반적으로 개별 정보주체와 직접적으로 교류하지 않습니다. 대신, 수탁자자는 일반적으로 계약을 기반으로 위탁자의 지시에 따라, 위탁자를 대신하여 개인정보를 처리합니다. 해당 내용이 위탁자에 의해 결정되기 때문에 수탁자는 처리하는 개인정보의 특성이나 처리 목적에 대해 알지 못할 수 있습니다. 또한 수탁자는 위탁자를 위해 저장하거나 처리하는 개인정보에 접근하거나 위탁자가 지시한 것 이외의 목적으로 개인정보를 처리하는 것이 계약상 금지될 수 있습니다. 수탁자에게 정보주체 대면 의무를 부과할 경우, 수탁자가 검토하지 않아도 되는 상당한 양의 개인정보를 검토해야 하고, 법적 요건을 충족하기 위해 연락해야 하는 정보주체를 식별하기 위해 해당 개인정보에 접근하고 분석 해야하므로 의도치 않게 소비자의 개인정보가 훼손될 수 있습니다. 이로 인해 개인정보 보호 및 보안 문제까지 발생할 수 있으며, 특히 수탁자가 모르는 개인이나 신원을 정당하게 인증할 수 없는 주체에게도 개인정보를 제공해야 할 수도 있습니다. 이러한 중요한 권리와 의무가 의도치 않게 위원회의 개인정보보호를 훼손하는 방식으로 행사되지 않도록 하기 위해 정보주체와의 상호적용 의무는 위탁자에게 부과되어야 합니다.

**BSA 는 개정안이 개정된 개인정보보호법 상 위임하고 있는 항목에 대해서만 규정할 수 있다는 점을 잘 이해하고 있습니다. 향후 개인정보보호법이 추가로 개정 시, 제 26 조 8 항을 개정하여 다음 의무사항에서 "수탁자"를 제외시켜 주실 것을 요청드립니다.**

- **제15조부터 제25조(2), 제27조 및 제28조의 개인정보 처리 목적에 따라 부과되는 소비자 대면 의무. 위에서 언급한 바와 같이, 수탁자는 처리하는 개인정보의 특성 또는 그러한 처리가 수행되는 목적이 위탁자에 의해 결정되기 때문에 그러한 처리 목적에 대해 알지 못합니다.**
- **제33조에 따른 개인정보 영향 평가의 대상 및 제34조에 따른 정보 주체에게 위반 사실을 통지할 의무**
- **제35부터 제38조에 명시된 소비자 권리. 위에서 언급한 바와 같이 위탁자는 개별 정보주체와 상호 작용할 수 있는 가장 좋은 위치에 있는 반면, 수탁자는 이러한 데이터를 알 가능성이 낮고 신원을 인증하는 데 필요한 정보가 부족할 수 있습니다.**

---

[3] 유럽연합 개인정보보호법, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[4] 2018 년 캘리포니아 소비자 개인정보 보호법, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[5] 일본 개인정보 보호법, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

[6] 2012 년 싱가포르 개인정보 보호법, https://sso.agc.gov.sg/Act/PDPA2012.

[7] 여기에는 다음과 같은 의무가 포함됩니다. 제 22 조(동의를 받는 방법), 제 22 조의 2(아동의 개인정보 보호), 제 27 조(영업양도 등에 따른 개인정보의 이전 제한), 제 28 조의 8(개인정보의 국외 이전) , 제 28 조의 9(개인정보의 국외 이전 중지 명령), 제 34 조(개인정보 유출 등의 통지・신고), 제 35 조의 2(개인정보의 전송 요구), 제 36 조(개인정보의 정정・삭제) , 제 37 조(개인정보의 처리정지 등), 제 37 조의 2(자동화된 결정에 대한 정보주체의 권리 등)

**더불어, 개인정보위는 2020 년 12 월에 개정된 개인정보 처리 위탁 가이드[8] (이하 가이드)를 발표하여 제 26 조의 운영 등에 대한 추가 정보를 제공한 바 있습니다. 당사는 "개인정보처리자"와 "수탁자"의 서로 다른 역할을 반영하여 개인정보처리 위탁 가이드를 업데이트할 것을 제안 드립니다. 이와 관련하여, 참고를 위해 위탁자와 수탁자의 구별에 대한 BSA 의 입장문도 첨부 드립니다. [9]**

개인정보보호법의 정보주체 대면 의무는 개인정보를 효과적으로 보호하고 프라이버시를 유지함에 있어 매우 중요하지만, 이러한 의무가 소비자 개인정보를 처리하는 데 있어 매우 다른 역할을 하는 단체에 부적절하게 적용되지 않도록 위원회가 보장해야 합니다. 정보주체 대면 의무는 개인정보 보호 및 보안을 강화하는 것이 아니라 약화시킵니다. 따라서 이러한 동의 의무와 소비자 권리 요청에 대한 응답은 위탁자에게 적용되어야 하며, 수탁자에게는 위탁자의 지침에 따라 개인정보를 안전하게 처리해야 하는 책임이 부과되어야 합니다.

## 개인정보의 국외 이전 촉진

BSA 는 개인정보보호법 개정으로 개인정보의 국외 이전에 대한 추가적인 법적 근거가 마련되었다는 점을 높이 평가하고 있습니다. 특히 개정된 개인정보보호법 제 28 조의 8 에 따르면, 개인정보를 이전 받는 자가 위원회의 인증을 획득했거나, 위원회가 적절한 수준의 개인정보 보호 수준을 갖춘 것으로 인정한 국가 또는 국제기구인 경우 동의 없이 개인정보를 국외로 이전할 수 있도록 허용하고 있습니다. 이러한 의무를 이행하기 위해 시행령 개정안 제 29 조의 12 는 '국외 이전 전문위원회'(이하 전문위원회)가 개인정보 국외 이전 정책을 검토하도록 명시하고 있습니다.

**BSA 는 시행령 개정안에 따라 전문위원회가 기업 내 구속력 있는 규칙, 국제 트러스트마크 및 지역 인증과 같은 기타 제 3 자 인증 프로세스 및 데이터전송 메커니즘의 사용을 권장할 수 있도록 허용하여 국경 간 데이터 전송을 보다 유연하게 지원할 수 있도록 할 것을 권장합니다.** 이러한 메커니즘은 한국이 참여하고 있는 글로벌 및 APEC 국경간 프라이버시 규칙(CBPR), 유럽연합의 일반 개인정보 보호법(GDPR), 일본의 개인정보보호법 등 국경 간 데이터 흐름을 촉진하기 위한 다른 국제 개인정보 보호 프레임워크에 포함되어 있습니다. 예를 들어, 시행령 개정안에 따르면 위원회는 정보주체의 동의를 받을 필요 없이 개인정보를 국외로 이전할 수 있는 인증으로 글로벌 CBPR 인증의 사용을 권고할 수 있습니다.

개인정보처리자가 국외로 개인정보를 전송할 때 다양한 메커니즘을 사용할 수 있도록 허용하면 기업은 자신에게 가장 적합하고 적합한 메커니즘을 유연하게 결정할 수 있습니다. 반면, 시장별로 다른 여러 인증을 요구하면 글로벌 서비스를 제공하는 한국 기업과 외국 기업 모두에게 상당한 부담이 될 수 있습니다.

이와 관련하여 BSA 는 개정된 인정보보호법이 다음과 같은 경우 개인정보 이전 중단을 명령할 수 있는 권한(중단 명령)을 개인정보보호위원회에 부여하고 있다는 점에 주목하고 있습니다: (i) 개인정보 이전이 개인정보보호법을 위반하는 방식으로 이루어지거나 이루어질 것으로 예상되는 경우; 또는 (ii) 개인정보를 이전 는 자나 개인정보가 이전되는 국가 또는 국제기구가 이 법에 따른 개인정보 보호 수준에 비하여 개인정보를 적정하게 보호하지 아니하여 정보주체에게 피해가 발생하거나 발생할 우려가 현저한 경우

[8] 개인정보처리 위수탁 안내서(2020.12.개정), https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7040#LINK

[9]컨트롤러와 프로세서: 프라이버시 관리자의 분류 역사 https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf

BSA 는 시행령 개정안에 중지 명령을 내리기 전에 고려해야 할 사항들이 명시되어 있다는 점을 높이 평가하고 있으며,[10] 이러한 사항들은 권한 명령을 내릴 시기에 대한 명확한 지침으로 작용하길 기대하고 있습니다. 다만, 중지 명령은 개인정보 보호법 위반이 발생한 경우 향후 개인정보 전송을 방지하는 데 효과적일 수 있는 한편, 전송 속도를 고려할 때 현재 진행 중인 전송에 대해서는 어떻게 작용할지 예상하기 어려운 실정입니다. 따라서 **개인정보의 전송의 진행 중인 경우, 중지 명령이 실제로 어떻게 작용될지 대한 구체적인 내용을 규정해주시면 감사하겠습니다.**

## 국내 대리인 지정

개정안 제 32 조 3 은 국내 대리인을 지정해야 하는 법인의 범위를 명시하고 있습니다.[11]

BSA 는 시행령에서 규정하는 국내 대리인 지정 요건이 지나치게 광범위하지 않다는 점과 기업의 총 매출액과 취급하는 정보 주체의 수를 고려하고 있다는 점을 높이 평가하고 있습니다. 국내 대리인은 개인정보 보호 책임자의 의무와 기타 통지 및 보고 의무를 수행하여 기업이 개인정보 보호 의무를 준수하는 데 도움을 줄 것이라 생각합니다. 다만, 기업의 규모, 복잡성 및 개인 정보 처리량이 다양하다는 점을 고려할 때, 기업의 적합성과 조직 구조에 따라 개인정보보호책임자를 지정할 수 있도록 해야 합니다. **이를 위해 개인정보보호위원회는 기업이 국내 대리인을 선임할 때 최소 자격 요건이나 개인정보보호위원회가 요구하는 특정 자격증과 같이 지나치게 규범적인 기준을 적용하는 것을 지양하시기를 제안 드립니다.**

## 마치며

BSA의 의견이 개인정보보호법 시행령 개정안에 도움이 되기를 바라며, 의견서와 관련하여 궁금한 점이 있거나 추가적인 도움이 필요하면 언제든지 문의해 주십시오.

감사합니다.

Tham Shen Hong
아태지역 정책 매니저

[10] 전송된 개인정보의 유형과 규모, 위반의 중대성, 중지가 정보주체에게 이익이 되는지 여부 등이 고려 요소에 포함됩니다. 또한, 개인정보보호위원회는 중지 명령을 내리기 전에 전문위원회와 협의해야 합니다.

[11] 즉, 국내에 주소 또는 영업소가 없는 온라인 서비스 제공자로서 가) 직전 사업연도의 총 매출액이 1 조원 이상, 나) 전년도 말 기준 직전 3 개월간 그 개인정보가 저장, 관리되고 있는 국내 정보주체의 수가 일일 평균 100 만명 이상인 자, 다) 법 제 63 조 1 항에 따라 관계 물품, 서류 등 자료의 제출을 요구 받은 자로서 국내대리인을 지정할 필요가 있다고 위원회가 심의, 의결한 자를 의미합니다..

# 컨트롤러와 프로세서:
# 프라이버시 관리자의 분류 역사

현대의 개인정보보호법은 초기 개인정보 프레임워크를 뒷받침하는 핵심 원칙을 중심으로 제정되었습니다. 예를 들어, 선도적인 역할을 하는 개인정보보호법들은 전세계적으로 통지, 접근, 수정의 원칙을 포함하고 있습니다. 이러한 권한을 이행하기 위해 조직의 적절한 의무를 식별하여, 해당 정보의 컨트롤러로서 개인정보의 처리방법과 이유를 결정하는 회사, 그리고 해당 정보의 프로세서로서 다른 사람을 대신하여 정보를 처리하는 회사를 역시 구분하고 있으며, 전 세계의 개인정보보호 및 데이터보호법은 소비자의 개인 정보를 취급하는 데 있어서 각기 다른 역할을 반영하여, 다른 유형의 주체에게 다른 의무를 부과하고 있습니다.

컨트롤러와 프로세서의 개념은 40년 이상 존재해왔습니다. 이들의 역할은 OECD 프라이버시 가이드라인(OECD Privacy Guideline), 유럽평의회 조약 제108호(Convention 108), APEC 프라이버시 프레임워크, ISO27701을 포함한 글로벌 개인정보 및 데이터 보호 체계의 핵심 요소이기도 합니다.

## 컨트롤러와 프로세서의 역사

1980: OECD 프라이버시 가이드라인
전산화 된 데이터 처리에 의해 촉발되는 개인정보 보호 문제를 조사하고 공공정보실행원칙을 권고하는 미국 보건, 교육 및 복지부의 1973년 보고서를 포함한 이전의 노력을 바탕으로, OECD 프라이버시 가이드라인은 현대 개인 정보 보호법의 새로운 물결을 일으켰습니다. [1]

1980년에 채택된 OECD 프라이버시 가이드라인은 **"데이터 컨트롤러"**를 "당사자 또는 대리인의 해당 개인정보의 수집, 저장, 처리, 배포 여부에 관계없이 개인정보의 내용 및 사용에 대한 능력이 있는 자"로 정의하고 있습니다.*[2]

1980 가이드라인에 대한 논평은 "정보 컨트롤러"라는 용어가 매우 중요하다고 인정하고 있는데, 이는 이 용어가 "정보의 내용과 사용에 대해 결정할 수 있는 법적인 능력"을 가진 주체를 정의하기 때문입니다.*[3]

---

1981: 유럽평의회 조약 제108호*
1981년, 유럽평의회는 데이터 보호 분야에서 최초의 법적 구속력이 있는 국제 규범을 서명을 위해 개방했습니다. 조약 제108호는 **"파일 컨트롤러"**를 "보관해야 하는 개인정보의 종류 및 그에 적용할 작업"을 뿐만 아니라 자동화된 개인정보 파일의 목적을 "결정할 권한을 가진…개인"으로 정의했습니다.[4]

1995: EU 데이터 보호 지침
이전에 EU 회원국의 개인정보보호법의 기반이 된 1995 EU 데이터 보호 지침은 컨트롤러와 프로세서를 별도로 정의했습니다.[5] **컨트롤러**는 "개인정보 처리의 목적과 수단을 결정하는" 자연인 또는 법인으로 정의되었으며, **프로세서**는 "컨트롤러를 대신하여 개인정보를 처리하는" 자연인 또는 법인으로 정의되었습니다.

2005: APEC 프라이버시 프레임워크
APEC 프라이버시 프레임워크는 OECD 개인정보 지침을 기반으로 하며 APEC 지역 국가를 위한 개인정보 보호, 보안

및 데이터 흐름에 대한 지침을 제공합니다. 이는 2005년 APEC에 의해 승인되고 2015년에 갱신되었습니다. 프레임워크는 **컨트롤러**를 "개인 정보의 수집, 보유, 처리, 사용, 공개 또는 전송을 제어하는" 조직으로 정의하며, 여기에는 다른 사람이 데이터를 대신 처리하도록 지시하는 것도 포함됩니다.[6] 다른 조직의 지시에 따라 데이터를 처리하는 주체에는 적용되지 않습니다.

2011: APEC 국가 간 프라이버시 규칙 시스템
2011년, 모든 21개의 APEC 국가는 국가 간 프라이버시 규칙 (CBPR) 시스템을 승인하여, APEC 프라이버시 프레임워크를 구현하도록 설계된 정부 지원의 자발적 시스템을 구축했습니다.[7] CBPR 시스템은 **데이터 컨트롤러**에게만 해당됩니다. 2015년 APEC은 컨트롤러가 적격하고 책임 있는 **프로세서**를 식별할 수 있도록 별도의 개인정보 프로세서 인증제도 (Privacy Recognition for Processor, PRP) 시스템을 구축했습니다.[8]

2016: EU 일반 개인정보 보호법
EU 일반 개인정보 보호법은 1995년 지침을 대체하는 것으로, 개인정보 처리의 "목적과 수단을 결정하는" 주체로 **컨트롤러**의 정의와 "컨트롤러를 대신하여 개인정보를 처리하는" 주체로 **프로세서**의 정의를 유지하였습니다.[9] 이 법은 2016년에 채택되어, 2018년에 발효되었습니다.

2018: 유럽 평의회 제108조 현대화 개정 협약
2018년, 제108조 협약은 현대화되어 **컨트롤러**의 정의를 개정하고, 프로세서의 정의를 추가했습니다. 컨트롤러는 "정보 처리에 관한 의사결정 능력을 가진" 주체로, [10] **프로세서**는 "컨트롤러를 대신하여 개인정보를 처리하는" 주체로 정의했습니다.[11]

2019: 개인정보보호 경영시스템 (ISO27701)
2019년, 국제표준화기구는 개인정보보호 경영시스템 (ISO27701)을 발표하며 개인정보 관리를 위한 최초의 국제 표준을 설정하였습니다. ISO27701은 조직이 컨트롤러인지 프로세서인지 여부에 따라 개인정보 통제를 구현하는 의무를 할당합니다. **컨트롤러**는 "처리 목적과 수단" [12]을 결정하는 반면, **프로세서**는 고객을 대신하여 처리된 개인정보가 "문서화된 고객 지침에 명시된 목적으로만 처리되도록" 보장해야 한다는 것을 인정하고 있습니다.[13]

2023: US 개인정보보호 주(州)법
2023년부터 미국의 캘리포니아, 콜로라도, 코네티컷, 유타, 버지니아의 5개 주에서 소비자 개인정보보호법이 시행됩니다. 5개의 법 모두 처리 목적과 수단을 결정하는 **컨트롤러**/사업자와, 컨트롤러/사업자를 대신하여 개인정보를 처리하는 **프로세서**/서비스 제공자를 구분하고 있습니다.

2021년 3월 보고서에 따르면, OECD 설문조사에 응답한 국가의 84% 이상이 개인정보보호법에서 "정보 컨트롤러"를 정의하고 있습니다.[14]

## 컨트롤러와 프로세서: 세계적으로 채택된 분류 방안

전 세계의 개인정보보호법은 오랜 개인정보보호 체계에서 비롯되었으며, 컨트롤러와 프로세서의 차이를 인식하고 개인정보를 처리하는 데 있어서 각각의 다른 역할에 기반하여 다른 주체에게 다른 책임을 할당하고 있습니다. 아래의 표는 컨트롤러와 프로세서의 역할을 반영하는 국가 개인정보보호법을 가진 일부 국가를 보여줍니다.

| 관할권 | 컨트롤러 | 프로세서 |
|---|---|---|
| **브라질**[15] | **컨트롤러:** "개인정보의 처리에 관한 *의사결정을 담당하는* …자연인 또는 법인" | **프로세서:** "컨트롤러의 명의로 개인정보를 처리하는 … 자연인 또는 법인" |
| **케이맨 제도**[16] | **데이터 컨트롤러:** "단독 또는 타인과 공동으로 개인정보가 처리되거나 *처리될 목적, 조건, 방식을 결정*하는 자" | **데이터 프로세서:** "데이터 컨트롤러를 *대신하여* 개인정보를 처리하되, 의심의 여지를 없애기 위해 정보 컨트롤러의 고용인이 아닌" 자 |
| **유럽 연합**[17] | **컨트롤러:** "단독 또는 타인과 공동으로 *개인정보 처리의 목적과 수단을 결정하는…"* 자연인 또는 법인" | **프로세서:** "컨트롤러를 *대신하여* 개인정보를 처리하는" 자연인 또는 법인 |
| **페로 제도**[18] | **컨트롤러:** "단독 또는 타인과 공동으로 *개인정보 처리의 목적과 수단을 결정*하는" 자연인 또는 법인 | **프로세서:** "컨트롤러를 *대신하여* 개인정보를 처리하는" 자연인 또는 법인 |
| **홍콩**[19] | **데이터 사용자:** "단독 또는 타인과 공동으로 *정보의 수집, 보유, 처리 또는 사용을 통제*하는" 자 | **데이터 프로세서:**<br>(a)다른 사람을 *대신하여* 개인정보를 처리하는 자; 그리고<br>(b) *자신의 목적을 위해 정보를 처리하지 않는 자* |
| **코소보**[20] | **데이터 컨트롤러:** "단독 또는 타인과 공동으로 *개인정보 처리의 목적과 수단을 결정*하는" 자연인 또는 법인 | **데이터 프로세서:** "정보 컨트롤러를 *대신하여* 개인정보를 처리하는" 자연인 또는 법인 |
| **말레이시아**[21] | **정보 사용자:** "단독 또는 타인과 공동으로 개인정보를 처리하거나, 개인정보 처리에 대해 *통제 혹은 승인하지만, 데이터 프로세서가 아닌*" 자 | **데이터 프로세서:** "데이터 사용자를 *대신하여* 단독으로 개인정보를 처리하되, *자신의 목적을 위해 개인정보를 처리하지 않는*" 자 |

| 관할권 | 컨트롤러 | 프로세서 |
|---|---|---|
| **멕시코**[22] | **데이터 컨트롤러:** "개인정보 *처리를 결정하는*" 개인 또는 민간 법인 | **데이터 프로세서:** "데이터 컨트롤러를 *대신하여* 단독 또는 타인과 공동으로 개인정보를 처리하는" 개인 또는 법인 |
| **필리핀**[23] | **개인정보 컨트롤러:** "본인을 대신하여 개인정보를 수집, 보유, 처리, 사용, 이전 또는 공개하도록 *타인 또는 조직에 지시*하는 개인 또는 조직을 포함하여, *개인 정보의 수집, 보유, 처리 또는 사용을 통제*하는" 개인 또는 조직. 다른 사람이나 단체의 지시에 따라 기능을 수행하는 사람이나 단체는 제외함. | **개인정보 프로세서:** "개인정보 컨트롤러가 정보 주체와 관련된 개인정보의 처리를 *위탁*할 수 있는" 자연인 또는 법인 |
| **카타르**[24] | **컨트롤러:** "단독 또는 공동으로 *개인정보가 처리될 방법과 처리 목적을 결정*하는…" 자연인 또는 법인 | **프로세서:** "컨트롤러를 위해 개인정보를 처리하는" 자연인 또는 법인 |
| **싱가포르**[25] | **조직:** 개인, 회사, 협회 또는 개인의 단체, 법인 또는 비법인: (a) 싱가포르 법에 따라 설립 또는 승인되었거나, 또는 (b) 싱가포르에 거주하거나 사무실이나 사업장이 있는 경우 | **정보 중개인:** "*타 조직을 대신하여* 개인정보를 처리하되, 해당 조직의 피고용인은 포함하지 않는" 조직 |
| **남아프리카 공화국**[26] | **책임 당사자:** "단독 또는 타인과 공동으로 *개인정보 처리의 목적과 수단을 결정*하는" 공공/민간 단체 또는 그 외의 개인 | **운영자:** "해당 당사자의 직접적인 권한에 귀속되지 않고, 계약 또는 위임에 따라 책임 당사자를 위해 개인정보를 처리하는" 자 |
| **태국**[27] | **데이터 컨트롤러:** "개인정보의 수집, 이용, 또는 공개와 관련한 *결정의 권한과 의무를 가진*" 자 또는 법인 | **데이터 프로세서:** "*데이터 컨트롤러에 의해 또는 대신하여 주어진 명령에 따라* 개인정보의 수집, 이용, 공개와 관련하여 운용하는" 자 또는 법인 |
| **터키**[28] | **데이터 컨트롤러:** "*개인정보 처리의 목적과 수단을 결정*하는" 자연인 또는 법인 | **데이터 프로세서:** "데이터 컨트롤러의 승인에 따라 컨트롤러를 *대신하여* 개인정보를 처리하는" 자연인 또는 법인 |

| 관할권 | 컨트롤러 | 프로세서 |
|---|---|---|
| **우크라이나**[29] | **개인정보 소유자:** "*개인정보 처리의 목적, 해당 데이터의 구성 및 처리 절차를 결정*하는" 자연인 또는 법인 | **개인정보 관리자:** "개인정보 소유자 또는 법에 의해 소유자를 *대신하여* 개인정보를 처리할 수 있는 권한을 부여" 받은 자연인 또는 법인 |
| **영국**[30] | **컨트롤러:** "단독 또는 공동으로 *개인정보의 처리 목적과 수단을 결정*"하는 자연인 또는 법인 | **프로세서:** "컨트롤러를 *대신하여* 개인정보를 처리"하는 자연인 또는 법인 |

---

1 Dept. of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens (1973), https://aspe.hhs.gov/reports/records-computers-rights-citizens.

2 OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, § 1(a) (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

3 Id. at Explanatory Memorandum, § IIB, para. 40.

4 Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, art. 2(d), Jan. 28, 1981, ETS No. 108, https://rm.coe.int/1680078b37.

5 Directive 95/46/EC, art. 2(d)-(e), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML.

6 APEC, APEC Privacy Framework (2015), § II.10, https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf.

7 See APEC, 2011 Leaders' Declaration, https://www.apec.org/meeting-papers/leaders-declarations/2011/2011_aelm; http://cbprs.org/privacy-in-apec-region/.

8 See APEC Privacy Recognition for Processors ("PRP") Purpose and Background, https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf.

9 EU General Data Protection Regulation, art. 4(7)-(8), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

10 Council of Europe, Modernised Convention for the Protection of Individuals With Regard to the Processing of Personal Data, art. 2(d), May 17-18, 2018, ETS No. 108, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

11 Id. at art. 2(f).

12 Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines 1, 4-5, 29-55 (2019).

13 Id. at 43.

14 OECD, Report on the Recommendation of the Council Concerning Guidelines Governing Protection of Privacy and Transborder Flows of Personal Data, 16 (2021), https://www.oecd.org/sti/ieconomy/privacy.htm.

15 Law No. 13,709, Aug. 14, 2018, art. 5 VI-VII (as amended by Law No. 13,853, July 8, 2019, Official Journal of the Union [D.O.U.] July 9, 2019), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

[16] Data Protection Act (2021), § 2, https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf.

[17] EU General Data Protection Regulation, art. 4, 2016 O.J. (L 119), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

[18] Act on the Protection of Personal Data No. 80 (2020), §§ 6(6)-(7), https://dat.cdn.fo/media/opccxh1q/act-on-the-protection-of-personal-data-data-protection-act-act-no-80-on-the-7-june-2020.pdf?s=LA6lqXBchs1Ryn1Kp9h3KSPuFqg.

[19] Personal Data (Privacy) Ordinance, (1996) Cap. 486, § 2(1), https://www.elegislation.gov.hk/hk/cap486. See https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.

[20] Law No. 06/L-082 on Protection of Personal Data (2019), art. 3, §§ 1.11, 1.14, https://www.dataguidance.com/sites/default/files/law_no._06_l_-082_on_protection_of_personal_data_0.pdf.

[21] Act 709 Personal Data Protection Act 2010, § 4, https://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf.

[22] Federal Law on Protection of Personal Data Held by Private Parties, art. 3, XIV & IX, Official Gazette July 5, 2010, https://www.dataguidance.com/legal-research/federal-law-protection-personal-data-held.

[23] Data Privacy Act of 2012, Rep. Act No. 10173, §§ 3(h)-(i) (Aug. 15, 2012), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/#:~:text=11,.transparency%2C%20legitimate%20purpose%20and%20proportionality.

[24] Law No. 13 of 2016 Personal Data Privacy Protection, art. 1, https://www.dataguidance.com/sites/default/files/law_no._13_of_2016_on_protecting_personal_data_privacy_-_english.pdf.

[25] Personal Data Protection Act 2012, as amended, § 2(1), https://sso.agc.gov.sg/Act/PDPA2012.

[26] Protection of Personal Information Act, 2013, Act 4 of 2013, Chap. 1, https://popia.co.za/.

[27] Personal Data Protection Act, B.E. 2562 (2019), § 6, https://cyrilla.org/es/entity/sl9175q71u?page=1.

[28] Law on Protection of Personal Data No. 6698 (2016), art. 3(g), 3(i), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.

[29] Law of Ukraine on Personal Data Protection (2010) (as amended), art. 2, 4(4), https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.

[30] UK General Data Protection Regulation 2016 (as amended), c. 1, art. 4(7)-(8), https://www.legislation.gov.uk/eur/2016/679. See also UK Information Commissioner's Office, Who Does the UK GDPR Apply To?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.