The Software Alliance

BSA

Controllers and Processors: A Longstanding Distinction in Privacy

Modern privacy laws have coalesced around core principles that underpin early privacy frameworks. For example, leading data protection laws globally incorporate principles of notice, access, and correction. They also identify appropriate obligations for organizations in fulfilling these rights, making important distinctions between companies that decide how and why to process personal data, which act as controllers of that data, and companies that process the data on behalf of others, which act as processors of such data. Privacy and data protection laws worldwide also assign different obligations to these different types of entities, reflecting their different roles in handling consumers' personal data.

The concepts of controllers and processors have existed for more than forty years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27701.

The History of Controllers and Processors

1980: OECD PRIVACY GUIDELINES

The OECD Privacy Guidelines launched the modern wave of privacy laws, building on earlier efforts including a 1973 report by the US Department of Health, Education and Welfare that examined privacy challenges posed by computerized data processing and recommended a set of fair information practice principles.[1]

The OECD Guidelines, adopted in 1980, define a "**data controller**" as the entity "competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf."[2]

Comments to the 1980 Guidelines recognize "[t]he term 'data controller' is of vital importance" because it defines the entity "legally competent to decide about the contents and use of data."[3]

1981: COUNCIL OF EUROPE CONVENTION 108

The Council of Europe in 1981 opened for signature the first legally binding international instrument in the data protection field. Convention 108 defined a "**controller of the file**" as the person "competent . . . to decide" the purpose of automated files, as well as "which categories of personal data should be stored and which operations should be applied to them."[4]

1995: EU DATA PROTECTION DIRECTIVE

The 1995 EU Data Protection Directive, which previously formed the basis of privacy laws in EU member countries, separately defined both controllers and processors.[5] **Controllers** were defined as the natural or legal person that "determines the purposes and means of the processing of personal data," while **processors** were defined as a natural or legal person "which processes personal data on behalf of the controller."

2005: APEC PRIVACY FRAMEWORK

The APEC Privacy Framework builds on the OECD Privacy Guidelines and provides guidance on protecting privacy, security, and the flow of data for economies in the APEC region. It was endorsed by APEC in 2005 and updated in 2015. The Framework defines a **controller** as an organization that "controls the collection, holding, processing, use, disclosure, or transfer of personal information," including those instructing others to handle data on their behalf. It does not apply to entities processing data as instructed by another organization.[6]

2011: APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

All 21 APEC economies endorsed the Cross-Border Privacy Rules (CBPR) System in 2011, creating a government-backed voluntary system designed to implement the APEC Privacy Framework.[7] The CBPR system is limited to **data controllers**. In 2015, APEC created a separate Privacy Recognition for Processors ("PRP") System to help controllers identify qualified and accountable **processors**.[8]

2016: EU GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation replaced the 1995 Directive, maintaining the definition of **controller** as the entity that "determines the purposes and means" of processing personal data, and the definition of **processor** as the entity that "processes personal data on behalf of the controller."[9] It was adopted in 2016 and took effect in 2018.

2018: COUNCIL OF EUROPE MODERNIZED CONVENTION 108

Convention 108 was modernized in 2018, revising the definition of **controller** and adding a definition of processor. A controller is the entity with "decision-making power with respect to data processing."[10] A **processor** "processes personal data on behalf of the controller."[11]

2019: ISO 27701

The International Organization for Standardization published ISO 27701 in 2019, creating the first international standard for privacy information management. ISO 27701 allocates obligations to implement privacy controls based on whether organizations are controllers or processors. It recognizes that a **controller** determines "the purposes and means of processing"[12] while **processors** should ensure that personal data processed on behalf of a customer is "only processed for the purposes expressed in the documented instructions of the customer."[13]

2023: US STATE PRIVACY LAWS

In the United States, five new state consumer privacy laws will take effect in 2023, in California, Colorado, Connecticut, Utah, and Virginia. All five laws distinguish between **controllers** or businesses that determine the purpose and means of processing, and **processors** or service providers that handle personal information on behalf of the controller or business.

According to a March 2021 report, **more than 84%** of countries responding to an OECD questionnaire define "data controller" in their privacy legislation.[14]

Controllers and Processors: A Distinction Adopted Around the World

Privacy laws worldwide draw from longstanding privacy frameworks, recognizing the distinction between controllers and processors and assigning different responsibilities to these different entities based on their different roles in processing personal data. The chart below identifies some of the countries with national privacy or data protection laws that reflect the roles of controllers and processors.

JURISDICTION	CONTROLLER	PROCESSOR
Brazil[15]	**Controller:** A "natural person or legal entity . . . *in charge of making the decisions* regarding the processing of personal data."	**Processor:** A "natural person or legal entity . . . that processes personal data in the name of the controller."
Cayman Islands[16]	**Data Controller:** A "person who, alone or jointly with others *determines the purposes, conditions and manner* in which any personal data are, or are to be, processed …."	**Data Processor:** Any person "who processes personal data *on behalf of* a data controller but, for the avoidance of doubt, does not include an employee of the data controller."
European Union[17]	**Controller:** A natural or legal person that "alone, or jointly with others, *determines the purposes and means of processing* personal data…."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."
Faroe Islands[18]	**Controller:** A natural or legal person that "alone or jointly with others, *determines the purposes and means of the processing* of personal data."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."
Hong Kong[19]	**Data User:** A person who "either alone or jointly or in common with other persons, *controls the collection, holding, processing or use of the data.*"	**Data Processor:** A "person who: (a) Processes personal data *on behalf of* another person; and (b) *Does not process the data for any of the person's own purposes.*"
Kosovo[20]	**Data Controller:** A natural or legal person that "alone or jointly with others, *determines purposes and means of personal data processing.*"	**Data Processor:** A natural or legal person that "processes personal data for and *on behalf of* the data controller."
Malaysia[21]	**Data User:** A person "who either alone or jointly or in common with other persons processes any personal data or *has control over or authorizes* the processing of any personal data, but *does not include a data processor.*"	**Data Processor:** A person "who processes the personal data solely *on behalf of* the data user, and *does not process the personal data for any of his own purposes.*"
Mexico[22]	**Data Controller:** An individual or private legal entity "*that decides on the processing* of personal data."	**Data Processor:** The individual or legal entity that "alone or jointly with others, processes personal data *on behalf of* the data controller."
Philippines[23]	**Personal Information Controller:** A person or organization "*who controls the collection, holding, processing or use of personal information*, including a person or organization *who instructs another person or organization* to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes a person or organization who performs such functions as instructed by another person or organization."	**Personal Information Processor:** A natural or juridical person "to whom a personal information controller may *outsource* the processing of personal data pertaining to a data subject."
Qatar[24]	**Controller:** A natural or legal person "who, whether acting individually or jointly with others, *determines how Personal Data may be processed and determines the purpose(s)* of any such processing…."	**Processor:** A natural or legal person "who processes Personal Data for the Controller."
Singapore[25]	**Organisation:** Any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore or (b) resident, or having an office or a place of business, in Singapore.	**Data Intermediary:** An organisation "which processes personal data *on behalf of another organisation* but does not include an employee of that other organisation."

JURISDICTION	CONTROLLER	PROCESSOR
South Africa[26]	**Responsible Party:** A public or private body or any other person that "alone or in conjunction with others, *determines the purpose of and means for processing* personal information."	**Operator:** A person who "processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party."
Thailand[27]	**Data Controller:** A person or juristic person "*having the power and duties to make decisions* regarding the collection, use, or disclosure of the Personal Data."	**Data Processor:** A person or juristic person who "operates in relation to the collection, use, or disclosure of Personal Data *pursuant to the orders given by or on behalf of the Data Controller*."
Turkey[28]	**Data Controller:** A natural or legal person "who *determines the purposes and means of processing* personal data."	**Data Processor:** A natural or legal person "who processes personal data *on behalf of* the data controller upon its authorization."
Ukraine[29]	**Personal Data Owner:** A natural or legal person who "*determines the purpose of personal data processing, the composition of this data and the procedures for its processing.*"	**Personal Data Manager:** A natural or legal person who is "granted the right by the personal data owner or by law to process this data *on behalf of* the owner."
United Kingdom[30]	**Controller:** A natural or legal person that "alone or jointly with others, *determines the purposes and means* of the processing of personal data."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."

Endnotes

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=LA6IqXBchs1Ryn1Kp9h3KSPuFog.

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/sl9175g71u?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/.