



November 21, 2022

Federal Trade Commission
Office of the Secretary
6600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B)
Washington, DC 20580
Submitted electronically via www.regulations.gov

Re: Commercial Surveillance ANPR, R111004

Dear Chairwoman Khan,

BSA | The Software Alliance appreciates the opportunity to submit comments in response to the advance notice of proposed rulemaking (ANPR) by the Federal Trade Commission (FTC).

BSA is the leading advocate for the global software industry before governments and in the international marketplace.¹ Our members create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Enterprise software companies support organizations across the world, including SMEs and large companies; local and central governments; hospitals, schools and universities; and non-profits. By offering trusted and responsible business-to-business software, enterprise software companies enable other organizations to serve their customers.

Businesses entrust some of their most sensitive data — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Businesses depend on BSA members to help them protect the privacy of data they handle and our companies compete to provide privacy-protective and security-protective products and services. BSA members recognize that companies must earn consumers' trust and act responsibly with their data and BSA members' business models do not depend on monetizing users' personal information.

Our comments focus on four points that are fundamental to the questions posed in the ANPR:

- The United States needs strong privacy protections. BSA has urged Congress to pass a comprehensive national privacy law that requires consumers' data be handled responsibly.
- If the FTC proceeds with a rulemaking it should focus narrowly, and not duplicate the broad privacy and data security obligations that will be foundational to any national privacy law.

¹ BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, 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.

- Context matters. If the FTC proceeds with a rulemaking, any rule should account for the context in which consumers' personal data is collected and used. Different kinds of data-driven business models carry different kinds of risks for consumers.
- Different companies play different roles in handling consumers' data. If the FTC proceeds with a rulemaking, any rule should account for these different roles, including:
 - For privacy, the roles of controllers and processors
 - For security, the shared responsibilities of companies and service providers
 - For AI, the roles of developers and deployers

I. The United States Needs a Strong and Comprehensive National Privacy Law

Consumers deserve to know their personal data is being used responsibly. Consumers today share their personal data with countless businesses in the course of using everyday products and services, both online and offline. That data should be protected.

BSA has urged Congress to enact a strong, comprehensive federal privacy law that provides confidence to consumers that their data will be used responsibly — and ensures that companies that violate their obligations are subject to strong enforcement. We believe federal privacy legislation should achieve three goals: (1) establish consumers' rights in their personal data, including the right to access, correct, and delete that data; (2) impose strong obligations on companies to safeguard consumers' personal data and prevent misuse; and (3) provide strong, consistent enforcement.² In each of these areas, a federal privacy law can — and should — build on protections and obligations that states have advanced and enacted.

Enacting a federal privacy law would meaningfully contribute to US leadership on privacy issues globally and bring consistency to existing protections. More importantly, it would also create broad and long-lasting protections for consumers nationwide. Congress has made significant progress this year alone in advancing privacy legislation, including in the House of Representatives, where the Committee on Energy & Commerce passed the American Data Privacy and Protection Act (ADPPA) by an overwhelming vote. BSA has commended ADPPA's sponsors for their dedication to moving bipartisan privacy legislation through Congress, and we have urged lawmakers to continue working with stakeholders so that Congress can pass a comprehensive privacy bill into law.

II. Any Rulemaking Should Focus Narrowly

BSA supports the Federal Trade Commission's central role in protecting consumer privacy. The FTC has demonstrated that it is highly capable of overseeing and enforcing existing consumer privacy protections, as is evident from the more than 150 privacy and data security enforcement actions the agency has brought under Section 5 of the FTC Act.³ The FTC has also developed a deep understanding of the complexities of the digital economy and has generally observed the principle of bringing cases that remedy and deter harmful conduct, rather than punishing technical lapses. BSA believes that any national privacy law should strengthen the FTC's ability to do this important work and we have supported giving the FTC new tools and resources to carry out its mission. For example, BSA supports giving the FTC new authorities to enforce a national privacy law, including

² See Testimony of Victoria Espinel, President and CEO of BSA | The Software Alliance, before the Senate Committee on Commerce, Science and Transportation, at Hearing on Policy Principles for a Federal Data Privacy Framework in the United States, February 27, 2019, available at <https://www.commerce.senate.gov/services/files/1DEC81B-5947-4FEB-B3E1-E9DF65866321>.

³ See FTC, Privacy and Data Security Update 2020, at 2-3, available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

targeted rule-making authority, the ability to fine first-time violators, and additional funding and staff, which we recognize are key aspects of enforcing a national privacy law.

If the FTC chooses to proceed with a rulemaking, we urge the agency to focus its efforts narrowly — and not use the rulemaking process to adopt the type of broad privacy and data security rules that will be foundational to any comprehensive federal privacy law. A narrow approach can help to ensure the FTC’s work does not inadvertently create tension with important and ongoing Congressional efforts to develop national privacy legislation. Instead, if the FTC proceeds with rulemaking it can and should target specific unfair or deceptive practices that are prevalent in the marketplace. For example, if the FTC chooses to pursue a rulemaking it could focus narrowly on malicious practices that may present a high risk for the misuse of data, such as high-risk practices by some data brokers and the protection of vulnerable groups.

III. Any Rulemaking Should Focus on Context

The risks consumers face from the collection and processing of their data will vary tremendously based on how and why that data is being collected and processed. If the FTC moves forward with rulemaking, we urge the agency to ensure any rule recognizes that consumers’ data may be collected, shared and processed for a wide variety of purposes — many of which support products and services that consumers rely on and that benefit them. Put simply: context matters.

The technology landscape has grown larger and more complex over the last 20 years, as consumers, businesses and governments around the world have moved online to connect with friends and family, conduct business, and access and share information. Companies of all sizes and across all industries now collect personal data from consumers to power products and services on which consumers rely. For example, the collection of personal data is integral to services including telemedicine, distance learning, and virtual job training. At the same time, it can be difficult for consumers to understand the vast difference in data practices between different companies and different business models. Those different practices provide critical context for any rulemaking, which should avoid treating all types of data collection equally.

Although the ANPR focuses on what it calls “commercial surveillance,” the agency’s broad definition of that term sweeps in any “collection” of consumer data — without distinguishing between low-risk types of data collection that consumers understand and expect (like providing an address and payment information to a merchant to complete an online purchase) and non-obvious types of data collection that pose much higher risks (like when a merchant sells consumers’ personal data to a data broker, which could then resell the data and further monetize it for its own purposes).

We urge the FTC to recognize that different types of data collection and processing present different risks to consumers, and different benefits. We strongly encourage the agency to account for this context as it considers rules that address the collection and processing of consumers’ personal data. If the FTC proceeds with a rulemaking, we strongly recommend that the agency focus on high-risk scenarios, to avoid imposing broad obligations on low-risk uses of data that consumers expect.

IV. Any Rulemaking Should Recognize the Different Roles of Different Companies

If the FTC proceeds with a rulemaking, it must also ensure that any rule accounts for the different types of companies that play different roles in collecting, safeguarding, and responsibly using consumers’ personal data. Privacy and cybersecurity laws and frameworks have long focused on role-based responsibilities because defining the different roles that different companies play in handling consumers’ data ensures that laws and regulations can tailor obligations to those roles.

If the agency moves forward with rulemaking, we urge the FTC to ensure that:

- Any privacy rule accounts for the longstanding distinction between controllers of personal data (which decide how and why the data is used) and processors of that data (which process the data on behalf of a controller and pursuant to its instructions);
- Any security rule accounts for the roles of both an end-user company and its service providers; and
- Any rule on AI recognizes the distinct roles of companies that develop AI systems and companies that deploy AI systems.

A. Any Privacy Rule Should Recognize the Roles of Controllers and Processors

BSA supports strong data privacy laws. Our members have extensive experience with protecting personal data in compliance with data protection and privacy laws across the globe. Establishing a strong, comprehensive federal privacy law is a top priority for BSA.⁴

If the FTC adopts a privacy rule, it should account for the roles of both controllers and processors. Privacy laws worldwide reflect the longstanding distinction between companies that act as *controllers* of personal data (which decide how and why to collect consumers' personal data) and those acting as *processors* (which process the data on behalf of another business and pursuant to that business's instructions). To be clear, both controllers and processors have important, but distinct, roles in safeguarding consumers' personal data.

We urge the FTC to ensure any privacy-related rule reflects this longstanding and widespread distinction, which can help increase privacy protections.

- ***The distinction between controllers and processors reflects today's economy.*** A consumer today may interact with one company to buy clothes or order groceries — but those consumer-facing companies each rely on a network of processors to store, analyze, and process data in order to serve their customers. Both a consumer-facing company and its processors should safeguard consumers' personal information, but privacy-related obligations placed on these two different types of companies must be different in order to protect consumers' privacy. Indeed, applying consumer-facing obligations to processors can create privacy and security risks, such as requiring processors to seek consent from consumers they do not know or requiring processors to access more information than is necessary to provide a product or service.
- ***Privacy and data protection laws worldwide create strong obligations for both controllers and processors by distinguishing between the two roles.*** The distinction between controllers and processors is longstanding. Global privacy laws and data protection frameworks have recognized the distinct roles of controllers and processors for more than 40 years, dating back at least to the OECD's Privacy Guidelines. It is also widespread. All five state privacy laws in the United States distinguish between controllers and processors; the distinction is also reflected in international privacy standards and in data protection and privacy laws worldwide, including in Brazil, the European Union, Singapore, and more than a dozen other countries.⁵ Importantly, deciding if a company acts as a controller or a processor is fact-specific — and a single company may act as a controller for some business lines (such as

⁴ This section of BSA's comments addresses portions of the ANPR focused on the collection, use, retention, and transfer of consumer data (Questions 43-51), consumer consent (Questions 73-82), and notice, transparency and disclosure (Questions 83-92).

⁵ BSA | The Software Alliance, *Controllers and Processors: A Longstanding Distinction in Privacy*, available at <https://www.bsa.org/files/policy-filings/10122022controllerprodinction.pdf> and attached to this submission. In California, the state privacy law refers to these companies as businesses and service providers, while Colorado, Connecticut, Utah, and Virginia all use the terms controller and processor.

consumer-facing services for which the company decides how and why to collect consumers' data) and as a processor for others (such as enterprise services, where data is handled on behalf of a business customer and pursuant to contractual instructions). Recognizing these different roles helps to ensure consumers' data is protected when it is handled by both types of companies.

Fundamentally, the distinction between controllers and processors reflects the fact that processors work on behalf of other businesses and depend on the trust of their business customers.

That trust exists because a processor, by definition, acts on behalf of its business customers and does not process those customers' data for its own purposes. State and leading global privacy laws also require processors to adopt a range of safeguards in how they handle personal data, which strengthens this trust and further protects the data that processors handle for business customers. Contractual commitments between controllers and processors create another layer of safeguards and often limit when and why a processor may access data that a business customer stores on the processor's service, to better protect the privacy and security of that data. These limits help to ensure that a processor does not treat the business customer's data as its own. Instead, the data continues to belong to the business customer, which decides how and why it will be processed.

This trusted relationship is in stark contrast to other actors who are not limited in how they handle consumers' data. For example, while a processor must, by definition, act on behalf of a controller and pursuant to its instructions, third parties aren't so limited — and can decide to use consumers' data for its own purposes, such as monetizing the data. For example, an online merchant may rely on a network of processors to handle consumers' data, including a cloud storage company to securely store customer information collected by the merchant and a communications provider that customer service representatives use to update consumers about their orders. To qualify as processors, those companies must only process that data on behalf of the merchant and pursuant to its contractual instructions. If these processors violated that trust — and stopped acting on behalf of the business customer — they would no longer qualify as processors.⁶ In contrast, if the online merchant sold customers' personal data to a data broker, it is not so limited and could simply sell or monetize the data for its own purposes.

B. Any Security Rule Should Recognize the Roles of Companies and Service Providers

BSA supports strong data security laws. Our companies are leaders in providing secure software services and other businesses trust BSA members to securely handle their most sensitive information and to securely support their most critical business functions. We appreciate the FTC's focus on the importance of data security to consumers. Maintaining appropriate technical and administrative controls as part of a comprehensive, risk-based cybersecurity risk management program, with effective oversight, is critical to managing cybersecurity risk.⁷

If the FTC adopts a data security rule, it should recognize the shared responsibilities of companies and their service providers. Effective security programs assign appropriate responsibilities to companies and service providers relative to their role in, and level of control over, data that the companies handle. This model of shared responsibility has been successfully implemented in the financial services and other sectors and ensures that responsibility reflects the different roles of different companies involved in safeguarding consumers' personal data.

⁶ Under at least four state privacy laws, a company that purports to be a processor but stops processing data on behalf of a controller and pursuant to its instructions would no longer be deemed a processor but would be treated as a controller and subject to obligations imposed on controllers. See Colorado Privacy Act, 6-1-1305(7); Connecticut Public Act No. 22-15 Sec. 7(d); Utah Consumer Privacy Act, 13-61-301(3); Virginia Consumer Data Protection Act, 59.1-579.D.

⁷ This section of BSA's comments addresses sections of the ANPR focused on data security (Questions 31-36).

For example, to the extent any new rule addresses data breach reporting, the FTC should avoid placing obligations on service providers that are inconsistent with their role in handling data on behalf of a business customer. Any rule should support the continued reporting of incidents by service providers to their business customers, consistent with contractual arrangements. This could be done, for instance, by clearly stating that requirements to disclose cyber incidents to consumers apply to end-user businesses, which typically have a direct relationship with individual consumers whose data may be affected by an incident, and do not apply to service providers, which do not.

More broadly, if the FTC creates a new rule on data security, we strongly encourage the agency to leverage existing laws and frameworks. Data security is a heavily regulated space — and for good reason. We urge the FTC to recognize that the best way to strengthen security practices across industry sectors is by connecting any rule on data security to existing and proposed regulations, standards, and frameworks. For example, a rule may focus on ensuring companies benchmark their security practices to industry standard certifications or guidelines that are appropriate for the nature of their business and the types of data they process.

This approach can also ensure the agency supports a risk-based and technology-neutral approach to data security that is consistent with the FTC’s longstanding guidance on cybersecurity and leading compliance mechanisms, such as the NIST Cybersecurity Framework.⁸ For example, any rule on data breach notification should reflect this risk-based approach, including clearly stating that a breach of personal data that is unusable, unreadable, or indecipherable to an unauthorized party due to the use of methods such as encryption, redaction, access controls and other mechanisms, does not trigger security notification requirements. Similarly, incidents affecting personal data already in the public domain are not likely to cause high risk of identity theft or financial fraud.

C. Any AI Rule Should Recognize the Roles of Developers and Deployers

BSA supports the responsible use of AI. Our companies are leaders in the development of enterprise AI systems and are on the leading edge of providing businesses in every sector of the economy with the trusted tools they need to leverage the benefits of AI.⁹ From helping farmers protect their crops from the impact of climate change to enabling medical researchers searching for the next breakthrough, AI is used by a wide range of businesses today to benefit consumers.¹⁰ To give just one example, AI helps organizations stay ahead of hackers by predicting potential cybersecurity attacks, mitigating attacks in real time, managing access to resources, and encrypting sensitive data — all of which help companies secure consumers’ data from evolving threats.

For BSA members, earning trust and confidence in the AI and other software they develop is crucial. As a result, identifying ways to reduce the risk of bias in AI systems is a priority. BSA therefore set out to develop real, credible, and actionable steps to guard against the potential of AI systems producing unintended disparate impacts. The resulting framework — *Confronting Bias: BSA’s Framework to Build Trust in AI* — was released in June 2021 and is built on a vast body of research and informed by the experience of leading AI companies.

⁸ See, e.g., *Careful Connections, Keeping the Internet of Things Secure* (September 2020) at 3 (directing companies to “[t]ake a risk-based approach” to design security); *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), available at <https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc> (recognizing that “for most organizations . . . the [NIST] Framework may be well worth using solely for its stated goal of improving risk-based security” but that it can also “deliver additional benefits.”).

⁹ This section of BSA’s comments address sections of the ANPR focused on automated decision-making systems (Questions 53-64).

¹⁰ See *BSA, Artificial Intelligence in Every Sector*, available at <https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf> (providing examples of AI use in healthcare, security, infrastructure, agriculture, and other sectors).

If the FTC adopts a rule on AI, it should account for the different roles that different companies play in developing and deploying AI systems. A rule must reflect these different roles in order to effectively support responsible uses of AI systems.

- **AI Developers** are responsible for the design and development of AI systems. Because they design AI systems, developers will have the greatest insight into how an AI system was created, including decisions about how the AI system was trained.
- **AI Deployers** adopt and use AI systems. In many cases, an AI system can be used either for purposes that create low risks to individuals (e.g., helping a company optimize its logistics to more efficiently ship packages to consumers) or purposes that may create higher risks to individuals (e.g., helping a company make decisions about an individual's access to credit or educational opportunities). Because the company that deploys that AI system will have the most information about the purpose for which it is used, a deployer is often best positioned to assess those risks and to ensure resiliency of the system.

Any rule on AI should recognize that risk management is a collective responsibility. AI can be developed and deployed in many ways, and the ability to address and mitigate risks will differ among the different stakeholders involved in developing and deploying the AI system. In many instances, risks created by an AI system (including the risk of bias) may emerge at the intersection of system design decisions that were made by the system's developer and downstream decisions by the organizations that may deploy that system. While the precise allocation of risk management responsibilities will vary depending on the use case, as a general matter AI developers will be best positioned to provide information about the system's design and capabilities to enable the deployer to make informed deployment and risk mitigation decisions. Any rule on AI should leave flexibility in recognizing these different roles.

More broadly, any rule on AI should focus on high-risk uses of AI systems. The risks that AI systems may pose and the appropriate mechanisms for mitigating those risks are largely context- and role-specific. Many AI systems pose extremely low, or even no, risk to individuals or society. Imposing broad regulations on low-risk systems would have few advantages for consumers and potentially significant drawbacks. If the FTC adopts a rule on AI, it should avoid creating one-size-fits-all obligations for all AI systems, regardless of the level of risk posed by those systems. Instead, any new requirement should focus on high-risk scenarios, to address specific risks that may arise from particular uses of AI systems. In this respect, it will be important to carefully assess scenarios that could be deemed high-risk. Because of the profound impact that some AI systems can have on people's lives, the public should be assured that high-risk AI systems are being designed and deployed responsibly. For example, BSA supports requiring organizations to perform impact assessments on high-risk systems, which is an important mechanism to promote accountable uses of AI systems and to create strong market incentives for effective risk management.

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome the opportunity to further engage with the FTC on these important issues.

Sincerely,



Kate Goodloe
Senior Director, Policy
BSA | The Software Alliance



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 <i>determines the purposes, conditions and manner</i> in which any personal data are, or are to be, processed”	Data Processor: Any person “who processes personal data <i>on behalf of</i> 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, <i>determines the purposes and means of processing</i> personal data. . . .”	Processor: A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”
Faroe Islands ¹⁸	Controller: A natural or legal person that “alone or jointly with others, <i>determines the purposes and means of the processing of</i> personal data.”	Processor: A natural or legal person that “processes personal data <i>on behalf of</i> the controller.”
Hong Kong ¹⁹	Data User: A person who “either alone or jointly or in common with other persons, <i>controls the collection, holding, processing or use of the data.</i> ”	Data Processor: A “person who: (a) Processes personal data <i>on behalf of</i> another person; and (b) <i>Does not process the data for any of the person’s own purposes.</i> ”
Kosovo ²⁰	Data Controller: A natural or legal person that “alone or jointly with others, <i>determines purposes and means of personal data processing.</i> ”	Data Processor: A natural or legal person that “processes personal data for and <i>on behalf of</i> 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 <i>has control over or authorizes</i> the processing of any personal data, but <i>does not include a data processor.</i> ”	Data Processor: A person “who processes the personal data solely <i>on behalf of</i> the data user, and <i>does not process the personal data for any of his own purposes.</i> ”
Mexico ²²	Data Controller: An individual or private legal entity “ <i>that decides on the processing of</i> personal data.”	Data Processor: The individual or legal entity that “alone or jointly with others, processes personal data <i>on behalf of</i> the data controller.”
Philippines ²³	Personal Information Controller: A person or organization “ <i>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.</i> ”	Personal Information Processor: A natural or juridical person “to whom a personal information controller may <i>outsource</i> 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, <i>determines how Personal Data may be processed and determines the purpose(s)</i> 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 <i>on behalf of another organisation</i> 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/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.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%3A%3A2016%3A119%3ATOC>.
- ¹⁸ Act on the Protection of Personal Data No. 80 (2020), §§ 6(6)-(7), <https://dat.cdn.f0/media/opcxh1q/act-on-the-protection-of-personal-data-data-protection-act-act-no-80-on-the-7-june-2020.pdf?s=LA6lqXBchs1Ryn1Kp9h3KSPuFog>.
- 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/si9175g71u?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/>.