10 March 2022

BSA COMMENTS ON DRAFT LAW ON THE PROTECTION OF CONSUMER RIGHTS

Respectfully to: The Ministry of Industry and Trade

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide our comments to the Ministry of Industry and Trade (**MOIT**) on the draft Law on the Protection of Consumer Rights (**LPCR 2022**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow.

BSA commends the Government of Viet Nam for soliciting stakeholder input on LPCR 2022. We understand that LPCR 2022 is intended to supersede the existing Law on the Protection of Consumer's Rights, which was introduced in 2010. In so doing, the draft LPCR 2022 proposes new obligations for "online intermediary platforms" and "large online intermediary platforms", as well as provisions relating to the protection of personal information of consumers.

BSA recognizes that enacting sound policies and regulations to protect consumers is critical in the age of electronic commerce, so that consumers are effectively protected in the digital environment. Properly tailored, such policies can help grow a vibrant and innovative domestic digital economy, while also engendering greater trust in the use of technologies to facilitate the adoption of secure and effective software-enabled services. As such, it is important to ensure that the LPCR 2022 does not impose unreasonable or overly onerous requirements on software-enabled products and services, and especially those designed to support enterprise customers. The data protection obligations in the LPCR 2022 should also be consistent with Viet Nam's draft Personal Data Protection Decree (**PDPD**),[2] and interoperable with international data protection laws. Otherwise, it would impede the ability of Vietnamese businesses to effectively participate in the flourishing Vietnamese digital economy.

Summary of BSA's Recommendations

BSA recommends the following:

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] BSA notes that the Government of Viet Nam has recently promulgated Resolution No. 27/NQ-CP approving the Dossier of the draft PDPD, and that the Minister of Public Security is now tasked with reporting and consulting the Standing Committee of the National Assembly on the promulgation of the PDPD.

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

- Adjust the overly broad and unclear definitions in the LPCR 2022 to expressly exclude companies which provide services designed for enterprise customers,[3] as opposed to individual consumers, from the scope of the law;
- Distinguish between entities that decide how and why to collect personal information (**data controllers**) and those that simply process collected personal information on behalf of another company (**data processors**) and exclude data processors from specific obligations in the LPCR 2022;[4] and
- Remove Article 9 of the LPCR 2022 on consent requirement to avoid regulatory confusion and conflict with the draft PDPD.

Adjust definitions and exclude enterprise service providers

The LPCR 2022 sets out definitions for "business organization",[5] "online intermediary platform",[6] and "large online intermediary platform".[7] These definitions are expansive and impose obligations on entities which do not interact with individual consumers, such as enterprise service providers. Consequently, BSA recommends that the definitions in the LPCR 2022 be adjusted to exclude enterprise service providers from the law's scope.

Enterprise or business-to-business (**B2B**) services enable the operations of a wide range of organizations around the world, including small and medium enterprises and large companies, local and central governments, hospitals, schools, and universities, and non-profit organizations. Unlike consumer-focused services, which provide services directly to individual end-users, enterprise services are intended for organizations of all sizes and across all industries to help them operate safely and efficiently, improve productivity, enhance product and service development, and increase opportunities for them to innovate and grow. As a result, enterprise services providers work closely with the enterprise customers using their services but typically do not interact with the individual customers or end-users served by those businesses.

The LPCR 2022 imposes various new obligations on businesses, such as the requirements to obtain prior consent from consumers to use their personal data and to update or remove personal data of consumers upon request. However, many enterprise service providers are not well-placed to take on such obligations because they have limited access to their enterprise customers' data, including individual consumer identities or contact details. For example, an enterprise service provider's access to, and knowledge of such data is frequently limited by privacy and security controls built into their products and services and enforced by contractual terms between the provider and its enterprise customers. Furthermore, it is the enterprise customer (not the enterprise service provider) that typically holds the relationship with the individual end-user. To subject enterprise service providers to these obligations would not only be technically and practically infeasible, but it could also place them in breach of their contractual and other legal obligations.

For instance, under Article 21 as drafted, obligations are stipulated to provide technical solutions to prevent services from harassment of consumers. Where an enterprise service provider is used by their enterprise customers to reach their individual end-users, such an enterprise service provider is

---

[3] How Enterprise Software Empowers Businesses in a Data-Driven Economy, January 2021, https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf and **appended to this submission.**

[4] The Global Standard: Distinguishing between Controllers and Processors in Privacy Legislation, March 2020, https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf and **appended to this submission.**

[5] LPCR 2022, Article 3.2. Business organization or individual means an organization or individual that performs one, several or all stages of the investment process, from production to consumption of products or provision of services in the market in order to profitable purposes, including: a) Foreign traders and traders according to the provisions of the Commercial Law; b) Individuals conducting commercial activities independently and regularly, without having to register for business

[6] LPCR 2022, Article 3.11. Online intermediary platforms are information systems established and operated by organizations and individuals to provide an environment in cyberspace for other organizations and individuals to transact with consumers.

[7] LPCR 2022, Article 3.12. A large online intermediary platform is a platform that affects a sufficiently large number of consumers to use online services on the platform according to the Government's regulations.

not in a position to intervene in the enterprise customer's actions in relation to that customer's end-user. Obligations should not be imposed on the enterprise service provider in such scenarios.

Moreover, imposing consumer-facing obligations upon enterprise service providers does not further consumer privacy. For instance, if an enterprise service provider is required to obtain individual end-users' consent, it will often be the case that the consent was already obtained by the data controller to process their data. Requiring the enterprise service provider to obtain the same consent for the same processing is not only duplicative, but it may force the enterprise service provider to contact individual end-users who are not familiar with the enterprise service provider. This could be confusing to the individual end-user and could undermine individual end-users' privacy because the data controller may need to disclose individual end-users' contact information to the enterprise service provider (or authorize the provider to access data it otherwise would not access) to enable the latter's outreach to the consumer.

The above concerns stem from the overly broad definitions of "business organization", "online intermediary platform", and "large online intermediary platform". For example, the definition of "business organization" captures *all* business entities involved in the supply-chain leading up to a good or service being placed in the hands of a consumer. This would capture cloud service providers (**CSPs**), which offer cloud-based platforms, infrastructure, or storage services for businesses, but which have no control over how their business customers transact or interact with the consumer. Similarly, CSPs can be said to provide an "environment in cyberspace" for sellers to transact with consumers, per the definition of "online intermediary platforms", but have no control over how sellers organize their relationships with consumers.

Consequently, BSA recommends that the LPCR 2022 should only apply to companies providing consumer-facing services, which deal directly with individual end-users and their personal information, and not to enterprise service providers. This can be achieved by amending the overly broad definitions of "business organization", "online intermediary platform", and "large online intermediary platform" (e.g., by stating that these definitions do not apply to an entity that provides services primarily designed for and used by enterprise/business customers.

Distinguish data controllers from data processors, and exempt data processors from specific obligations

The LPCR 2022 presently does not distinguish between a data controller and a data processor. BSA recommends introducing this distinction, as a clear allocation of accountability between data controllers and data processors is essential for establishing and enforcing privacy-related obligations.

By distinguishing between data controllers and data processors, the LPCR 2022 can clearly tailor obligations to different types of companies based on those companies' roles in collecting and using an individual end-user's personal information. This distinction is vital in today's digital economy, where an individual may use a service from one consumer-facing company, but that company may rely on numerous enterprise service providers to store, analyze, and process the data in connection with that service.

We have significant concerns that by placing consumer facing obligations on data processors that have no direct relationship with individual end-users, the LPCR may undermine consumer privacy. These concerns are particularly pertinent to obligations surrounding **consent, notification, and responding to consumer rights requests.** [8]

- *Consent and Notification*. Consent and notification obligations are among the main consumer-facing obligations that are appropriately placed on data controllers, not data processors. Individual end-users of services typically interact with the controllers providing the services —

[8] LPCR 2022, Article 9 (Notice when collecting information of individual consumers), Article 10 (Use of personal information of consumers), and Article 12 (Check, update, correct, transfer or destroy personal information of consumers).

and may rightly expect the controllers to ask for their consent to process their personal information for certain purposes, and to provide appropriate notice as to how the controllers will be processing their personal information. However, to require data processors also to obtain consent and to notify individual end-users for such purposes not only results in duplicative notices and consent requests from multiple companies for the same processing activities, but it also risks confusing individual end-users and leading to "click-fatigue", where individual end-users are inundated with repeated notifications and requests, eroding the effectiveness of the notifications and requests as a means to inform individual end-users of relevant matters and to confirm their wishes and expectations.

- *Responding to Consumer Rights Requests*. Consumer-facing companies are also best positioned to respond to consumer rights requests, without creating potential privacy and security concerns that can arise when these obligations are placed on data processors. This is because responding to consumer rights requests to cease using or disclosing personal information often requires authenticating the identity of the individual end-user making the request and understanding whether the information requested should be provided. Such decisions should be made by data controllers, which directly interact with individual end-users, decide when and why to collect personal information, and respond to consumer rights requests. Moreover, data controllers are in a better position to decide if there is a reason to deny individual end-users' requests. These obligations are ill-suited to data processors that often are not privy to information about the nature of the data they are processing or the purposes for which such processing is being conducted. In addition, as we stated earlier, data processors may be contractually prohibited from accessing data they store or otherwise process for data controllers and may design their processing activities to minimize the amount of personal information they need to access — all of which better protects the privacy of that data. Requiring data processors to respond to individual end-user requests will therefore create data security and consumer privacy risks by requiring processors to access personal information, including data necessary to identify individuals, that they would not otherwise need to access.

As such, BSA recommends <u>exempting</u> data processors from the following obligations:

- **Providing notice to the individual consumers of their consumer-facing enterprise customers and obtaining their consent to collect or use their personal information;[9]**
- **Notifying the individual consumers of their consumer-facing enterprise customers when there are changes to the purpose and scope stipulated in the original notification/request for consent;[10] and**
- **Responding to requests from the individual consumers of their consumer-facing enterprise customers to check, update, correct, transfer, or destroy their personal information.[11]**

For greater clarity, the above obligations should apply **only** to the consumer facing enterprise customer, i.e., the controller and not to the enterprise service provider, i.e., the processor.

Remove Article 9 on consent requirement

Under Article 9, the LPCR 2022 recognizes 'consent' as the only basis for collection and processing of consumers' personal information. However, the latest draft of the PDPD proposed limited exceptions for processing without consent.[12] As such, by recognizing 'consent' as the only basis for processing personal information, the LPCR 2022 is in conflict with the draft PDPD. The conflict of laws will make

[9] LPCR 2022, Articles 9 and 10.

[10] LPCR 2022. Article 10.

[11] LPCR 2022, Article 12.

[12] PDPD, Article 10.

it confusing for businesses to navigate the personal data protection landscape in Viet Nam and may lead to inadvertent non-compliance with their data protection obligations. Further, because the LPCR 2022 and the PDPD are overseen by different Ministries, the personal information protection landscape in Viet Nam may become fragmented as a result of inconsistent enforcement, thus compounding the regulatory confusion.

This regulatory confusion can be avoided if provisions pertaining to the bases for personal information processing are contained *only* in personal data protection legislation, such as the PDPD, as opposed to appearing in *both* the PDPD and other legislation like the LPCR 2022. Consequently, BSA recommends that Article 9 be removed from the LPCR 2022 to avoid regulatory confusion and conflict with the draft PDPD.

Conclusion

We thank MOIT for the opportunity to participate in consultations on the LPCR 2022 and appreciate your consideration of our above comments. We hope that our concerns and recommendations will assist in the development of a targeted framework for consumer protection. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Manager, Policy – APAC

How Enterprise Software Empowers Businesses in a Data-Driven Economy

B2B software enables business customers to do what they do best—faster, smarter, and more efficiently.

Enterprise Software Supports Businesses' Operations

Enterprise software—or business-to-business (B2B) software—**enables** the operations of other companies. It helps organizations of all sizes and across all industries operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

The enterprise software industry supports a wide range of 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 software solutions** to support their business clients' data-processing needs, enterprise software companies enable other organizations to service their own customers in turn.

Enterprise software optimizes the use of digital technology to support and improve business operations, empowering other companies to focus on what they do best, such as R&D and product design.

In Europe, almost **80 percent of large companies** and **35 percent of SMEs** use information-sharing software.[1]

Enterprise Software Helps Businesses Benefit From Digital Transformation

Organizations in every sector of the economy increasingly rely on cutting-edge software to **run, facilitate, improve, and optimize their operations** every single day. Governments, public administrations, schools, and hospitals are also increasingly adopting these tools. Enterprise software underpins human resources and payroll operations; billing and financial transactions; research and development; product design; workforce collaboration, communication, and messaging; customer relations; and logistics and supply-chain management, among many other business services.

38 percent of small businesses in the **United States** cited increased sales and revenue as a benefit associated with using digital tools.[2]

Australian businesses are using more cloud than ever—**42 percent of businesses** across 2017–2018, up from 31 percent in 2015–2016.[3]

In times of crisis, such as the global outbreak of COVID-19, enterprise software tools help coordinate public health safety responses, maintain essential services, and support economic continuity.

ENTERPRISE (B2B) SOFTWARE PROVIDES CLIENT SOLUTIONS THAT:

Operate and Optimize Business Services
(including responsibly handling and moving information globally)

Protect and Secure Data and Business Information
(including providing strong, accountable privacy and security safeguards)

Innovate and Expand Beyond Existing Capabilities
(by using cognitive solutions such as analytics and artificial intelligence to better address customers' needs)

[1] EU DESI Index 2020, https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

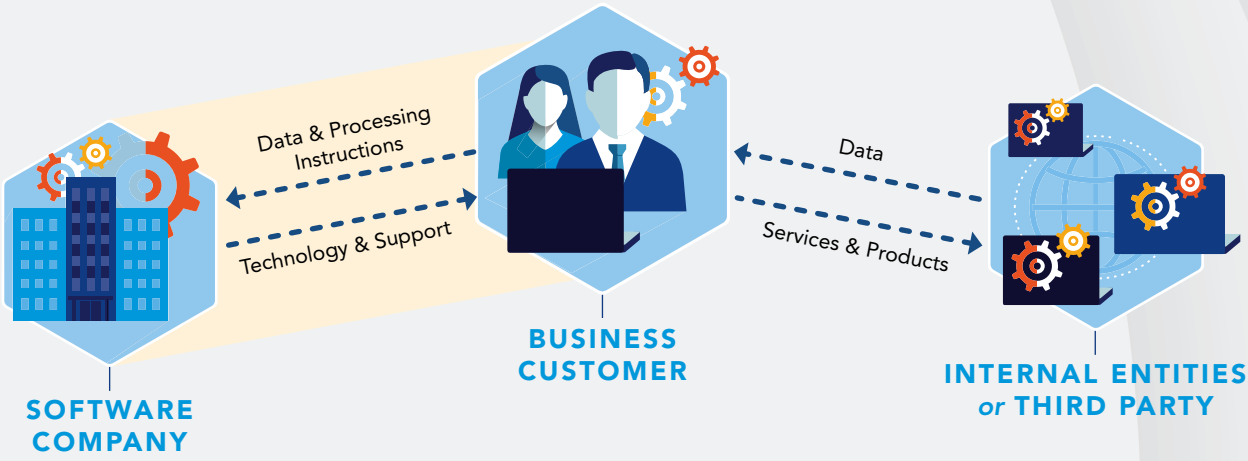
[2] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html.

[3] Characteristics of Australian Business, https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2017-18.

Enterprise Software Is Built on Transparency and Trust

Enterprise software companies and their business customers negotiate their relationship in contracts and licensing agreements to ensure they best address their clients' individual needs. **Enterprise software companies monetize their technologies and not the data of their customers.**

Enterprise software services, such as cloud computing, are used primarily for business-to-business purposes and are not consumer facing. **The business customers control their data and direct how it will be used.** Enterprise software companies do not have unfettered access to the data stored in their cloud infrastructure or service. Access and use of such data is reserved for the benefit and sole purpose of their customers.



Enterprise software companies operate under strong existing legislative requirements of data handling. Across the world, legal obligations often include accountability measures and technical safeguards that ensure enterprise software companies provide robust assurances of trust for their customers. Enterprise software companies also develop innovative, tailored, or customizable solutions for clients that are highly regulated, for example, in the health, financial, automotive, aeronautic, and telecom sectors and the semiconductor industry.[4]

For instance, machine learning solutions can use data gathered across countries to create fraud detection systems in the financial sector.

Enterprise software helps reduce legal and operational risks for business customers who can be confident they are using tried and tested software products, with appropriate remedies and support, without having to develop their own software in-house. Enterprise software companies also often provide tools to facilitate their customers' compliance, for instance on privacy, consumer protection, cybersecurity, anti-money laundering, or energy efficiency.

[4] See Cross-Border Data Flows: Enabling Local Economies and Driving E-Commerce, https://www.globaldataalliance.org/downloads/WTOEventSummary20200702.pdf.

How to Create a Successful, Responsible, Software-Enabled Economy

STRONG PRIVACY PROTECTIONS

Privacy is essential to building trust. Software-enabled business operations increasingly rely on data—and, in some cases, personal data—to function. As a result, data protection frameworks that create a user-centric approach to privacy must ensure the use of personal data is clear, transparent, and consistent with customers' expectations. Privacy laws should create robust obligations for all companies and organizations that handle individuals' personal data. This would ensure companies act responsibly while being able to pursue legitimate business interests.

CYBERSECURITY

Software innovation continues to connect people across the world. These online connections create efficiencies and spur economic growth, but they also create vulnerabilities that bad actors can exploit if the proper security measures are not in place. Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected ecosystem. One important tool is the ability to use the strongest available encryption technology when appropriate.

CROSS-BORDER DATA FLOWS

Cross-border data flows are necessary for companies to operate globally; leverage their resources and footprint across locations; innovate; and provide services to their customers, across sectors and geographies. For enterprise software companies and their business customers, the ability to transfer, and process, data globally is pivotal in ensuring the quality, reliability, security, personalization, and efficiency of service.

RISK-BASED AND TECHNOLOGY-NEUTRAL APPROACH

Software technologies evolve every day, pushing the boundaries of the benefits that technology can bring to organizations and people. Given the fast-paced nature of this industry and its adoption by customers, laws and regulations should strive to provide legal certainty, be outcome-based, and adopt a risk-based and technology-neutral approach, building on legal frameworks that already apply. Any new policy should set clear compliance goals and enable companies to adapt their practices and safeguards to the best-suited approach given their business model, the nature of their activity, their position in the value chain when contracted by others, and their risk profile vis-à-vis the established objective.

INTERNATIONAL CONVERGENCE

The value of the data-driven economy is in the ability of companies to operate across borders, reach new markets, and service customers regardless of location. Building on each region's own legal and cultural legacy, convergence of rules on privacy, cybersecurity, or data governance and compatibility of mechanisms play a critical role in growing cross-border business that increasingly rely on enterprise software around the world.

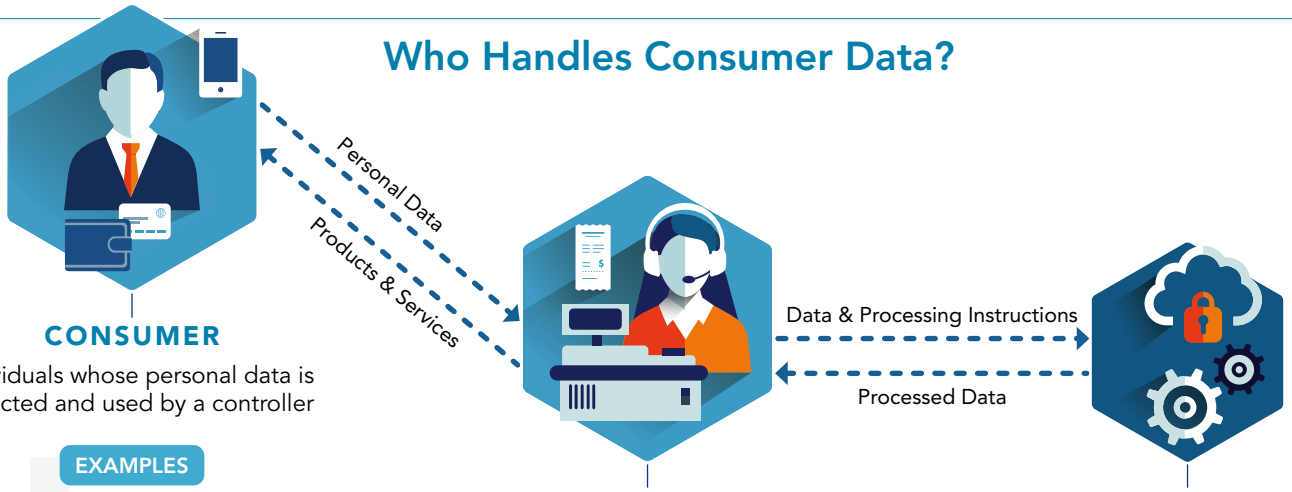
The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data on *behalf of* another company, which act as **processors** of that data

This fundamental distinction is critical to a host of global privacy laws, including the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?



CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Say no,** and opt out of broad types of use, not just sale
- **Access** information about them
- **Correct** that information
- **Delete** that information
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests for access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

Companies that decide how and why to collect consumer data.	Companies that process consumer data at the direction of others.
GDPR: Controllers Determine the "purposes and means" of processing.	**GDPR: Processors** Handle personal data "on behalf of" a controller.
CCPA: Businesses Determine the "purposes and means" of processing.	**CCPA: Service Providers** Handle personal information "on behalf of" businesses.

This distinction is crucial to a host of privacy laws beyond the GDPR and CCPA. In addition, leading international privacy standards, including ISO 27701, and voluntary frameworks that ensure data can be transferred across national borders, such as the APEC Cross Border Privacy Rules, also distinguish between controllers and processors.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

- Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like the GDPR and CCPA require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.