6 December 2021

BSA COMMENTS ON THE AUSTRALIAN PRIVACY LEGISLATION AMENDMENT (ENHANCING ONLINE PRIVACY AND OTHER MEASURES) BILL 2021

Submitted Electronically to the Attorney-General's Department

BSA | The Software Alliance (**BSA**) [1] welcomes the opportunity to provide comments to the Attorney-General's Department (**AGD**) on the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (**Bill**)[2] and the associated Explanatory Paper.[3]

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. Many of BSA's member companies are enterprise solutions providers that create the software-enabled 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, cybersecurity solutions, and collaboration software.

BSA members have made significant investments in Australia, and we are proud that many Australian organisations and consumers continue to rely on our members' products and services to support Australia's economy. Consequently, BSA has a significant interest in the Bill, and previously provided comments to the AGD on the Review of the Privacy Act 1988 and the associated Australian Privacy Principles (**APP**).[4]

It is our understanding that the Bill will enable the creation of a binding Online Privacy code (**OP code**) that applies to organisations that provide "social media services" and "data brokerage services", as well as other "large online platforms" operating in Australia (collectively, **OP organisations**).

BSA appreciates the Australian government's continuous efforts to enhance privacy protections in the online space. However, we have concerns with the overly broad scope of the OP code and the proposed

[1] BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, 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] Exposure Draft, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, October 2021, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf.

[3] Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, October 2021, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf.

[4] BSA Comments on the Review of the Australian Privacy Act 1988, November 2020, https://www.bsa.org/files/policy-filings/11272020ausprivacyactrev.pdf.

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

application of its obligations to companies without sufficiently distinguishing between those 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**). BSA therefore provides the following key recommendations to the Bill:

- Expressly exclude from the scope of the OP code companies which provide services designed for enterprise customers as opposed to individual consumers.

- Adjust the overly broad definition of "organisations providing social media services" such that its application is limited to online services and platforms which interact directly with individual end-users and enable or encourage such end-users to post content for consumption by the public. Specifically, this definition should be narrowed to exclude services used for online business interactions and other business purposes, in line with the existing definition of social media service under the Online Safety Act.[5]

- Adjust the overly broad definition of "organisations providing data brokerage services" such that it focuses on organisations that collect and sell personal information of end-users with whom they do not have a direct relationship.

- Exempt data processors from requirements to 1) provide notice to individuals about collecting personal information; 2) seek consent for collecting, using, and disclosing personal information; and 3) act on requests to cease using or disclosing personal information, as data processors do not have a direct relationship with individual end-users — the relationship remains with the data controllers.

- In the interests of transparency and clarity in rulemaking, public consultations should be undertaken under specific circumstances, such as when the Minister makes any specification under section 6W (7) of the Bill.

Exclude Enterprise Services

The Explanatory Paper states that the Bill seeks to address "the particular privacy challenges posed by social media and other online platforms that collect a high volume of personal information or trade in personal information".[6] From the legislative intent of the Bill and the proposed requirements of the OP code, it appears that the OP code is expected to apply primarily to consumer-facing services that directly interact with, or collect personal information from, individual end-users.[7] Consequently, BSA recommends that services primarily designed for enterprise customers and which do not intend to target individual end-users should be expressly excluded from the scope of the OP code.

Enterprise or business-to-business (**B2B**) services enable the operations of a wide range of organisations around the world, including small and medium enterprises and large companies, local and central governments, hospitals, schools, and universities, and non-profit organisations. Unlike consumer-focused services, which are provided directly to individual end-users, enterprise services are intended for organisations 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

[5] Online Safety Act 2021, https://www.legislation.gov.au/Details/C2021A00076.

[6] Explanatory Paper *op. cit*., p.6.

[7] Ibid., p.8.

and grow.[8] 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 OP code would set out how OP organisations must comply with several obligations under the APPs, in addition to creating new obligations such as the requirement to cease to use or disclose personal information upon request. However, many enterprise service providers, including enterprise focused cloud 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 enterprise products 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 the OP code would not only be technically and practically unfeasible, but it could also place them in breach of their contractual and other legal obligations.

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 authorise the provider to access data it otherwise would not access) to enable the latter's outreach to the consumer.

For these reasons, the OP code should apply only to companies providing consumer-facing services, which deal directly with individual end-users and their personal information, and not to enterprise service providers.

Therefore, BSA recommends adding a new subsection to Section 6W of the Bill stating that an organisation is not an OP organisation if it provides services primarily designed for and used by enterprise customers. For example, if a service is used by another organisation to manage or operate the organisation's services, it would be an enterprise service and the enterprise service providing the service should not be deemed an OP organisation.[9]

Adjust Definition of "organisations providing social media services"

The OP code will apply to "organisations providing social media services". The Explanatory Paper elaborates that these are organisations that "provide an electronic service with the sole or primary purpose of enabling online social interaction between two or more end-users, allows interactions between end-users, and allows end-users to post material on the service".[10]

[8] How Enterprise Software Empowers Businesses in a Data-Driven Economy, January 2021, https://www.bsa.org/policy-filings/how-enterprise-software-empowers-businesses-in-a-data-driven-economy and appended to this submission.

[9] Similarly, in the context of determining whether an organisation meets the thresholds to be considered a "large online platform" and in line with ensuring that the OP code only applies to consumer-facing service providers and not enterprise service providers, the "end users" to be taken into account in applying those thresholds should be those individual end users that have a direct relationship with the organisation in question.

[10] Explanatory Paper *op. cit*., p.7.

This definition is overly broad, as it may capture companies which provide communication services between end-users for business purposes, such as communicating with collaborators or customers, and which do not disseminate content to the public in a manner that is intended to amplify its reach.
We encourage the Department to narrow this definition by making clear that communication services used for business purposes are not services that "enable online social interaction" for purposes of the OP code. Indeed, the nature of business-to-business communication services is to enable business interactions, not social ones. Nor do business-to-business communication tools, including videoconferencing and collaboration tools used for business purposes, raise the same types of concerns that may arise from social media services. For example, disseminating user-generated content to the public is a common feature of many social media services, as it enables individuals to directly interact and communicate with other persons in the end-user's network or even the public-at-large. However, communication services for business purposes generally do not allow or provide for such public dissemination, nor do business-to-business services amplify content in the same manner as social media services.

Further, where such communication services are licensed to enterprise customers, it is the enterprise customer that decides how the communications services will be used, including how personal information from users will be collected and processed. The enterprise service provider offering the communication services will have little to no visibility of the personal information or content generated by the individual end-users and is generally limited by contract in how the provider can access, handle, and use that information.

We recommend narrowing this definition to exclude services used for online business interactions and other business purposes, in line with the existing definition of social media service under the Online Safety Act.[11] In particular, the definition in the Online Safety Act included notes making clear that the Act does not cover services that enable "online business interactions" or the sharing of material for "business purposes". The definition of organisations providing social media services under the Bill should be aligned with the definition of social media services under the Online Safety Act to ensure consistency across regulations. This would also help to ensure that B2B interactions are not inadvertently captured by the Bill's definition.

BSA therefore recommends adjusting the definition of "organisations providing social media services", as set out in Section 6W subsection (1) of the Exposure Draft, such that its application is limited to online services and platforms that interact directly with individual end-users and enable or encourage such end-users to post content <u>for consumption by the public</u>.

BSA also recommends incorporating a note or an express exception, similar to the one found in section 13 of the Online Safety Act 2021, stating that: "*Online social interaction does not include (for example) online business interaction or business purposes.*"

Adjust Definition of "organisations providing data brokerage services"

A data brokerage service is defined as an organisation that "*collects personal information about an individual for the sole or primary purpose of disclosing that information (or information derived from that information) in the course of or in connection with providing a service (a data brokerage service).*"

Such a broad definition could potentially be read to capture any data controller that relies on data processors to process information on their behalf. As a result, it could inadvertently capture the wide range of companies that disclose information to the vendors they rely on to provide data storage services, email services, or many other services provide at the direction of the company and in line with its instructions. For example, a data controller could be a school relying on the services of an email service provider (the data processor) to send emails to its students. Under the current definition, the school could be viewed as

[11] Online Safety Act, Section 13.

falling under the definition of a "data brokerage service" because it collects information to provide that information to the email service provider. That result is not consistent with the policy intention stated in the Explanatory Paper, which is clear that the definition is intended to capture organisations whose "business model is based on trading in personal information collected online."[12]

To better reflect the intention of this definition, **BSA recommends that the definition could be narrowed to focus on organisations that collect and sell personal information of end-users with whom they do not have a direct relationship.**

Exempt Data Processors from Specific Obligations

BSA recognises that while the Bill does not draw a distinction between data controllers and processors, this issue is presently being considered under the Australian government's wider Privacy Act Review.[13] Nevertheless, it bears reiterating that a clear allocation of accountability between data controllers and data processors is essential for establishing and enforcing a rigorous and efficient privacy regime.[14]

By distinguishing between data controllers and data processors, a privacy law 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. That 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, analyse, and process the data in connection with that service.

We have significant concerns that by placing consumer-facing obligations on data processors that often have no direct relationship with individual end-users, the OP code would risk undermining consumer privacy. These concerns are particularly pertinent to the obligations surrounding **consent, notification** and **responding to consumer rights requests**.

- *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 — 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

[12] Explanatory Paper *op cit.*, p. 8.

[13] Discussion Paper, Review of the Privacy Act 1988, October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review---discussion-paper.pdf

[14] 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.

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 exempting data processors from the following obligations:

- **Providing notice to individuals about collecting personal information;**[15]
- **Seeking consent to collect, use, and disclose personal information;**[16] **and**
- **Acting on requests to cease using or disclosing personal information.**[17]

Transparency and Clarity in Rulemaking

BSA recommends that, for transparency and due process, a good-faith public consultation of an appropriate duration should be conducted prior to:

- the Minister making any specification under section 6W(7) of the Bill (specifying conditions for an organisation to be considered a social media organisation, or specifying organisations or classes of organisations as social media organisations, data brokers, or large online platforms);
- the Commissioner registering any OP code under Part IIIB, Division 2A, Subdivision B of the Bill; and
- the Commissioner making any public interest determinations or temporary public interest determinations under Part VI of the Bill.

Conclusion

We thank the AGD for the opportunity to comment on the Bill and appreciate the AGD's kind consideration of our above comments. We hope that our concerns and recommendations will assist in the development of a rigorous and targeted OP code, which strikes a balance between enhancing online privacy protections without unduly impeding innovation within the digital economy.

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

[15] In line with APP 5.

[16] In line with APPs 3 and 6.

[17] New requirement in the OP code.

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.

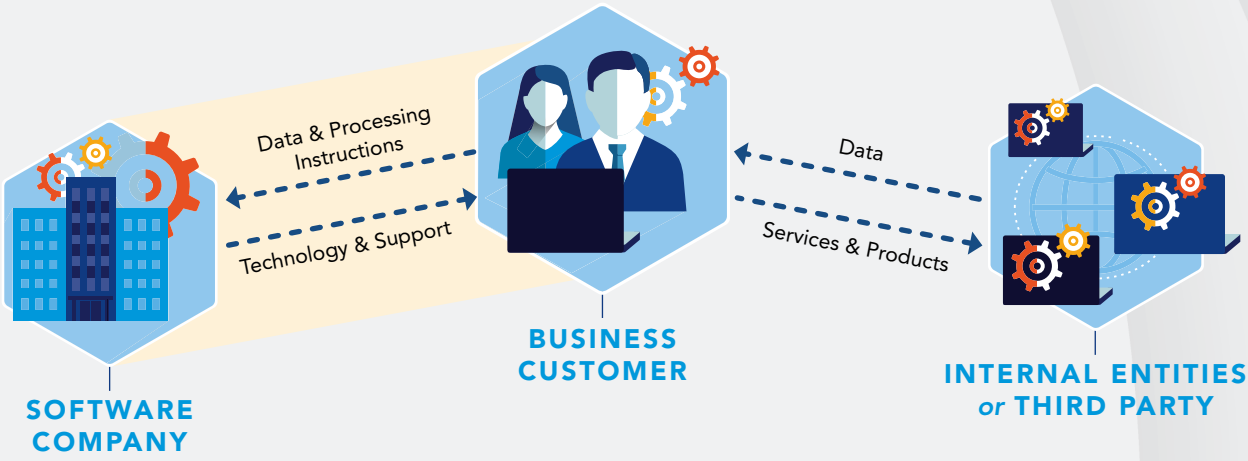
[2] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html.

[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.

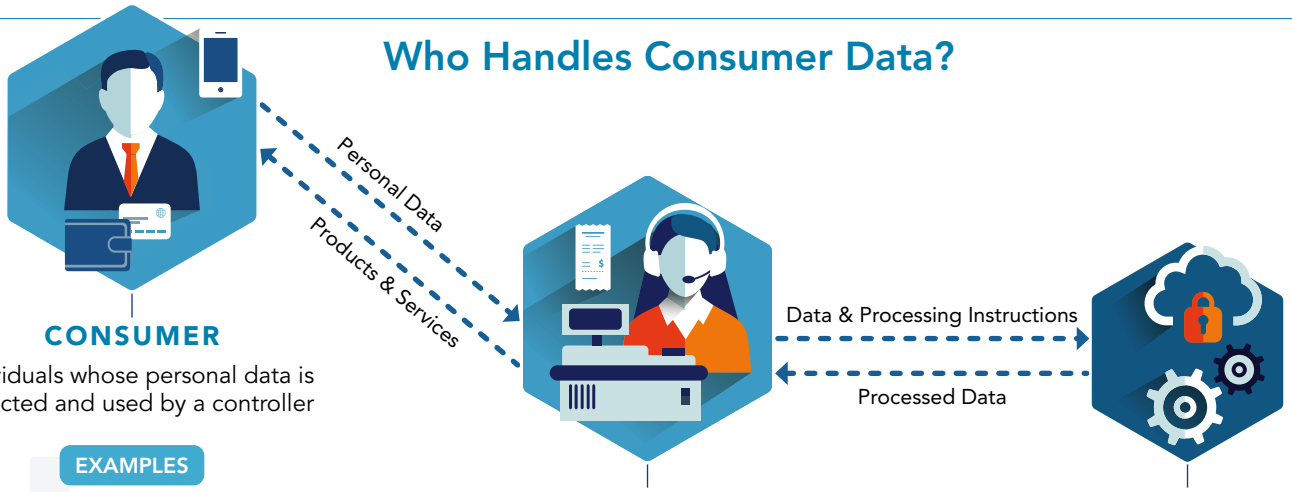
The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

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.