The Difference Between Controllers and Processors and Why It Matters for Federal Data Privacy Legislation

As Congress develops privacy legislation, it is important to consider the different roles data controllers and data processors play in the ecosystem and to tailor responsibilities accordingly.

Many privacy laws around the world — including the European Union's General Data Protection Regulation, the California Consumer Protection Act, and federal statutes governing the privacy and security of financial and health information — use these concepts, although the terminology may differ.

BSA, whose members act as both controllers and processors of data, supports maintaining this distinction in federal privacy legislation. Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

What's the Difference Between Controllers and Processors?

Controllers: The people or organizations, who either alone or with someone else, make the decisions about personal data processing. These decisions may include determining which data is processed, which third parties will have access, and when the data will be deleted.

Processors: The people or organizations who process personal data at the direction of controllers.

Control and direction, rather than possession, of personal data is the determining factor in the controller/processor relationship. The organization in charge of deciding why (purpose) and how (means) personal data is processed is the controller.

What Does This Distinction Mean in Practice?

The two examples on the next page illustrate the different roles of controllers and processors, with controllers deciding the purpose and means of handling personal information and processors performing functions at the direction of the controller.

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

EXAMPLE ONE

An organization contracts with a printing company to create invitations to an event. The organization 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 organization then sends out the invitations.

The organization is the controller of the personal data processed in connection with the invitations. The organization decides the purposes for which the personal data is processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the personal data using the invitees' address details). The printing company is the processor handling the personal data only on the organization's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing.

EXAMPLE TWO

A hotel chain that wants to make booking easier will often contract a service provider to develop a chatbot tool to assist customers. The chatbot can provide a variety of services to customers, including checking availability, booking rooms, and placing a room service order. The hotel dictates to the chatbot service provider the purpose and means for processing customers' personal data, as well as what data the hotel chain determined it needs (the customer's name, address, email address, etc.) to secure the room for the customer. The chatbot will then communicate with the hotel to reserve the room and send confirmation to the customer.

The hotel chain is the controller of the customer's personal data because it decided the purposes for which the personal data is processed (to book the room) and the means of processing (the chatbot forwarding the customer's information to the hotel). The chatbot service provider is the processor collecting, transmitting, and storing the customer's personal data only at the hotel chain's direction. The service provider does not use the personal data for its own purposes, but it does have an obligation to take reasonable security measures to protect the data.

Why Is This Distinction Important?

Role-dependent Responsibilities Improve Protections. A processor often does not have the right to know what information is in the data being processed. This restriction protects personal privacy by limiting who has the right to view personal information. Some important consumer rights — such as the right to access or correct personal data, or to object to processing — requires the company to know what is in the data. The data controller, therefore, is the party that should respond to those requests. If the obligation were on the processor, the processor may need to gain access to the consumer's personal data to respond, and in most cases the consumer would have no idea who the processor is or its relationship with the controller. As a result, having a processor respond to individuals instead of the controller would likely confuse consumers and could inadvertently undermine, not increase, privacy protection by giving processors access to personal data they would not otherwise have or need.

Both controllers and processors have important obligations that must be met to ensure consumers' privacy and security. For instance, data processors and controllers should both have an obligation to take security measures reasonably designed to protect the security and confidentiality of data. However, responsibilities must accurately reflect today's reality; a distinction for controllers and processors ensures that consumers' personal data is protected and clarifies the different roles for companies in complex business arrangements.

By incorporating a distinction for controllers and processors in federal privacy legislation, Congress would provide clear rules of the road for companies to understand their obligations in this complex data ecosystem while at the same time ensuring that there are no gaps in protection for consumers.