



Entrust's Response to Government Requests for Customer Data

Customers may be concerned with the ability of US law enforcement to reach personal data through mechanisms such as Foreign Intelligence Surveillance Act (FISA) Section 702 and other intelligence gathering activities under Executive Order (EO) 12333, or law enforcement orders under the Electronic Communications Privacy Act (ECPA), which allow for records requests to electronic communications service providers through a court order.

On June 12, 2026, Section 702 of FISA expired. While existing collection directives under Section 702 remain in place through March 2027, Entrust is not subject to any such directive. The US Department of Commerce published a [white paper](#) regarding concerns about the impact of US intelligence gathering on privacy in September 2020. We encourage customers to read this white paper.

Entrust does not provide public communications platforms or telecommunications services of the type typically subject to such authorities.

Taking into account the categories of data processed, the nature of our services, and publicly available information regarding the use of U.S. intelligence authorities or ECPA, we assess the likelihood of such requests as low.

Notwithstanding this assessment, Entrust maintains defined processes and procedures to address any legally binding request for customer personal data, including requests from U.S. intelligence authorities or under the Electronic Communications Privacy Act (ECPA).

☑ We will notify an affected customer of any legally binding and valid request for its data or any direct access to customer data by a law enforcement or other government agency unless we are explicitly prohibited from doing so by law.

↔ Where possible, we will refer the requesting government agency to the affected customer.

Where permitted by law, Entrust will, where appropriate, direct the requesting government authority to the relevant Customer. Depending on the specific service and context, Entrust may have access to customer data; however, such data belongs to the customer, and in the ordinary course government authorities seeking access to such data should address their request directly to that Customer.

⚡ We do not disclose customer data to government agencies unless compelled by law and we will challenge unlawful requests.

We will review each government request for customer data and will only comply if and to the extent we determine the request is legally binding and valid.

We will require government agencies to follow the required legal process under applicable laws, such as issuing their request via a subpoena, court order, or search warrant. We will attempt to challenge government requests for customer data when we believe them to be invalid or unlawful.

✓ **If we are required to disclose customer data to government agencies, we will ensure the transfer is necessary and proportionate and provides the minimum amount of information possible while still complying with the order, based on a reasonable interpretation of the government request.**

⦿ **If prohibited by law from notifying the affected customer, we will try to get that legal restriction waived.**

If we receive a government request for data, and we are prohibited by law from notifying the affected customer, we will request the confidentiality requirement be waived to enable Entrust to notify the appropriate data protection authorities.

In addition to these steps to protect data from unlawful government demands, Entrust implements a combination of contractual, technical, and organizational safeguards designed to protect customer data and to minimize risks of data disclosure while providing services effectively and efficiently. These measures may include, as appropriate, the use of encryption or other security controls, access restrictions, and data minimization practices, depending on the nature of the services and the customer's configuration.