Navigating Government Access to Private Data in the EU

By IAPP Westin Fellow Luke Fischer and
University of Grenoble Alpes Professor of Law Theodore Christakis

In recent years government access to private data has become a challenge for enterprises doing business in multiple jurisdictions. Compliance is increasingly complex, as numerous judicial, legislative, regulatory, national and multilateral decisions have created distinct requirements for companies when data is requested by public authorities. This complexity is compounded by jurisprudence and regulatory enforcement, which have found enough fault in the existing privacy and data protection safeguards for government access to privately held data to put a stop to cross-border data transfers.

This infographic aims to highlight some important instruments related to law enforcement and government access to private data, particularly in the EU. It is important to keep in mind this is a nonexhaustive list, and there are many national and sectoral laws and regional judicial decisions regarding government access to data that could subject companies to requirements not contained in this infographic.

JUDICIAL

→ CJEU La Quadrature du Net decision, 2020

In 2020, the Court of Justice of the European Union decided national legislation that compels electronic service providers to maintain and transmit traffic and location data to law enforcement agencies for national security purposes violates **EU law**. Notably, the court found data retention for criminal investigations is only permitted in a targeted way or in some exceptional circumstances, but it allowed general and undiscriminated access to data if there is a "serious threat" to national or public security — while requiring any measure to be "strictly proportionate" to its intended purpose.

→ CJEU 'Schrems II' decision, 2020

In the 2020 "Schrems II" ruling, the CJEU invalidated the EU-U.S. Privacy Shield for failing to provide adequate privacy protections for EU personal data. The CJEU held that any data transfer mechanism must ensure a level of protection equivalent to what is guaranteed under EU law, considering the recipient country's legal system and surveillance practices. The ruling affirmed the importance of necessary and proportionate limits on how public authorities access privately held personal data and the importance of effective and binding redress. EU and U.S. negotiators subsequently concluded the **EU-U.S. Data Privacy Framework**.

LEGISLATIVE

→ EU e-evidence package

The EU **electronic evidence package** includes a regulation to harmonize internal EU rules on law enforcement access to data, as well as a directive that would impose compliance requirements for service providers receiving production and preservation requests from public authorities. The package allows law enforcement in one EU member state to access data held by a private entity in another jurisdiction without a government intermediary. This **legal framework** aims to facilitate **cross-border data transfers** for the purposes of law enforcement investigations or prosecutions, while ensuring compliance with privacy and data protection rules.

→ ePrivacy Directive

The **ePrivacy Directive**, formally known as Directive 2002/58/EC, is **EU legislation** that complements the General Data Protection Regulation by specifically addressing the protection of privacy in the electronic communications sector. The directive establishes rules and requirements concerning issues such as cookies, unsolicited marketing communications and security of communications networks.

→ Law Enforcement Directive

The **Law Enforcement Directive**, known as Directive (EU) 2016/680, is EU legislation that establishes data protection principles, rights and obligations, like those under the GDPR but applicable to the **law enforcement context** and law enforcement authorities' processing of personal data.

REGULATORY

→ Recommendations 01/2020 on supplementary measures for international personal data transfers from Europe

In June 2021, the European Data protection Board adopted **Recommendations 01/2020** on measures that supplement transfer tools to ensure compliance with EU levels of protection of personal data. The recommendations outline procedures that businesses must follow to determine if supplementary measures are required to transfer personal data outside the European Economic Area to align with the protection level guaranteed by the GDPR. The **recommendations** compel businesses that rely on standard contractual clauses, binding corporate rules or other "appropriate safeguards" while transferring data across borders to conduct transfer impact assessments and implement supplementary technical measures when necessary.

→ EU adequacy decisions

Adequacy decisions are legal determinations made by the European Commission that recognize a non-EU country or territory as providing an adequate **level of data protection**, comparable to that of the EU under the GDPR. These decisions facilitate the free flow of personal data between the EU and the designated jurisdictions without the need for additional safeguards. In January 2024, following an examination of 11 countries' and territories' rules on government access, the Commission released a report finding that pro-GDPR adequacy decisions do not need to be modified for these third-party jurisdictions.

→ EU Essential Guarantees, November 2020

In November 2020, the EDPB adopted **Recommendations 02/2020** on the European Essential Guarantees for surveillance measures. The recommendations are an **updated version** of a document outlining permissible reasons for third countries' national security or law enforcement authorities to interfere with the fundamental rights to privacy and data protection through surveillance methods when transferring personal data. The EEGs also assist exporting states in determining whether third-country jurisdictions provide adequate protection levels that align with what is guaranteed in the EU.

US AUTHORITIES

→ US CLOUD Act

The **U.S. Clarifying Lawful Overseas Use of Data Act** establishes a **legal framework** for U.S. law enforcement to access electronic data stored by U.S.-based service providers, regardless of where the data is located. The CLOUD Act also allows for bilateral agreements with other countries to facilitate **cross-border data access** for criminal investigations. Since the CLOUD Act's enactment, the U.S. has entered into bilateral agreements with the **U.K.**, **Australia** and Canada, which eliminate domestic legal barriers so law enforcement and national security agencies may access data directly from public authorities in the other jurisdiction.

→ US FISA, Executive Order 12333, Executive Order 14086

Executive Order 12333 serves as the primary framework governing the activities of the U.S. intelligence community, outlining the roles, responsibilities and authorities of various **intelligence agencies**. The **order** allows for the surveillance and interception of foreign communications, as well as the incidental collection of U.S. citizens' information, subject to certain restrictions and oversight mechanisms.

Executive Order 14086 focuses on safeguarding critical infrastructure and ensuring data protection in both public and private sectors. It calls for **collaboration** between the government, industry and international partners to build resilience against cyber threats and maintain privacy standards.

INTERNATIONAL/MULTILATERAL

→ EDPB reports on third countries

The EDPB conducted legal analyses and published two reports detailing the data protection legislation and fundamental rights related to government access to data in certain third-party countries. The **first report** includes findings on China, India and Russia, and the **second report** analyzes the legal implications in Mexico and Turkey.

→ OECD Declaration on Government Access

The Organisation for Economic Co-operation and Development Declaration on Government Access to Private Sector Data for Public Interest Purposes is a set of principles designed to guide governments seeking access to private sector data for public interest purposes, such as fighting crime or protecting national security. The **declaration** emphasizes the need for transparent, accountable and proportionate measures while balancing privacy and data protection rights.

→ G7 Action Plan for Promoting Data Free Flow with Trust

The **G7 Action Plan** for Promoting **Data Free Flow with Trust** is an initiative that emphasizes the need for open and interoperable **digital markets**, and for the development of international rules and best practices to address challenges such as cross-border data flows, data localization and cybersecurity.

→ GPA Resolution on Government Access to Data, Privacy and the Rule of Law, 2021

The **Global Privacy Assembly Resolution on Government Access to Data, Privacy and the Rule of Law** calls for greater transparency, oversight and proportionality in government access to personal data. It emphasizes the need for a strong legal basis and upholding human rights, particularly the rights to privacy and data protection, while maintaining the rule of law.

→ UN Cybercrime Convention

United Nations member states have been negotiating a treaty to combat cybercrime since May 2021, attempting to establish the first **binding U.N. agreement** in the cyber sector. The treaty would serve as a global framework to enable international coordination for preventing, investigating and prosecuting cybercrimes. As of January 2023, member states are continuing to negotiate the terms of the treaty, but the final scope will have important implications regarding the powers public authorities are given to access personal data.

→ Covention 108+ Council of Europe

Convention 108+ is the amended version of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which served as the first binding international instrument to promote the cross-border transfer of personal data while safeguarding against vulnerabilities that accompany data flow. Notably, **Convention 108+** eliminates the exemption for the data collection and processing for national security and defense purposes that existed within the **original version**. It also includes oversight mechanisms for when data is used in the national security and defense context, requiring national security regulations to be checked article by article against the convention for consistency.

→ Budapest Convention on Cybercrime, 2001, and Second Additional Protocol on Cross-border access to electronic evidence, 2021

The Budapest Convention on Cybercrime, also known as the Council of Europe Convention on Cybercrime, is an **international treaty** that seeks to harmonize national laws, enhance international cooperation, and establish investigative and enforcement measures to combat cybercrime.

The Second Additional Protocol to the Budapest Convention on Cybercrime is a **supplementary agreement** intended to modernize and facilitate cross-border access to electronic evidence by law enforcement authorities through measures like direct requests to service providers and expedited preservation requests.

→ EU-US negotiations for agreement on law enforcement access to data

The European Commission and the U.S. Department of Justice entered **formal negotiations** in September 2019 to establish an agreement that enables law enforcement agents to access **electronic evidence** in criminal investigations. A consensus has not yet been reached, as the parties diverge on the potential scope and structure of the agreement. The EU desires an independent, EU-wide holistic agreement that would prevent fragmented applicability across member states, while the U.S. favors a framework-style agreement that would then be applied individually by member states through bilateral agreements, satisfying CLOUD Act obligations.

Published March 2024.

iapp.org