CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE GENERAL REGIME ARCHITECTURE

REF: 20-111 | September 24, 2020

All regimes for cross-border access to electronic evidence naturally follow a similar architecture, in order to reconcile high substantive and procedural guarantees with efficiency. A corresponding set of basic regime components was identified by a dedicated Contact Group[1] of the Internet & Jurisdiction Policy Network in 2018-19. The present document lists and provides definitions for these components, as a companion to the **Operational Approaches**[2] released by this Group in April 2019, which documented the degree of convergence among diverse actors on possible standards for each component. These two documents provide all actors with a common grid of analysis in the context of ongoing debates around cross-border access to electronic evidence regimes.

Regime Scope

Data Covered

Definition of the types of user data the regime intends to enable access to. Each category will determine specific procedural safeguards. The most frequent categories are: subscriber information, traffic data, and content data, albeit with some variability regarding what they precisely entail in each regime, as well as variability among providers.

Types of Crimes covered

Identification of the criminal offenses for which the regime procedures can be used. This can entail, for instance, thresholds regarding the minimum sanction incurred.

Providers Covered

Identification, if any, of the required degree of connection of the provider to the issuing State (e.g.: "providing services"), and corresponding factors.

Requesting State

Judicial/Independent Validation

Type of judicial/independent validation that would be required for each request or order from the Requesting State. Some regimes, however, may only envisage general oversight of the process rather than order-by-order validation.

Standard of Proof

Threshold of factual elements that have to be provided to justify relevance of the data requested to the case.

Necessity and Proportionality

Explicit mention that request/orders must respect necessity and proportionality principles.

---

[1] Data & Jurisdiction Contact Group 2018-2019

[2] Data & Jurisdiction Program Operational Approaches

Authorized Authorities

Criteria, if any in the regime, for what administrative levels with competence to investigate[3] under local laws are allowed to initiate, issue or transmit a request or an order.

Providers

Clarification of Requests/Orders

Definition of the conditions under which a service provider can request additional information from the issuing authority, regarding imprecise, incomplete or insufficiently documented request/orders.

Challenge of Requests/Orders

Conditions, if any, under which a service provider can object to or refuse to execute a request/order.

Conflicts of Law

Specific mechanisms (including comity analysis) to address situations where a service provider can be caught between competing and conflicting legal obligations.

Response Time

Expected response time by the provider to a properly submitted request/order.

Users

Conditions of User Notification and Secrecy of Requests/Orders

Under what modalities authorities and/or service providers should inform the targeted user to ensure the capacity of recourse and conditions under which such information can potentially be delayed.

Access to Legal and Administrative Remedies

Procedures and grounds under which users can challenge the disclosure and/or use of their data.

Other States

With Connection to the Provider

Modalities, if any, of information to a country where the provider is incorporated, has a relevant subsidiary or its legal representation, for any request/order, and/or on a periodic basis.

With Connection to the Suspect or Victim

Modalities, if any, of information to a country where the suspect or victim is a citizen, permanent resident or was present on the occasion of the investigated crime.

---

[3] Includes, inter alia, the valid legal basis, substantial connection to the crime and legitimate interest to the data sought.