Dissecting EU E-Evidence

what, who, when & how

30. Dezember 2023, 37C3 Hamburg

Bildquelle: unsplash.com

Agenda

- What is E-Evidence about?
- Categories of Data
- Who is addressed by the regulation?
- When will it enter into force?

- How does an electronic production order work?
- Protections/Problems identified so far

- Legal Challenges
- What can still be done?

What is E-Evidence about?

Regulation EU 2023/1543 (EPOC & EPOC-PR)
Directive EU 2023/1544 (Designation of Representative)

- Regulation regarding the production of electronic evidence in criminal matters

- Data concerned is in principle available through MLATs already:
  “This Regulation should cover the data categories of subscriber data, traffic data and content data. Such categorisation is in line with the law of many Member States and Union law, such as Directive 2002/58/EC and the case law of the Court of Justice, as well as international law, in particular the Budapest Convention.”

- Process:
  Data will be provided to LEA directly from the service providers based on the national law of the issuing state, irrespective of the seat of the service provider. Legality of an enquiry is conceptually only checked against the procedures established in the issuing state.

Categories of Data

- **Subscriber Data:**
  Can be requested for any criminal offence

- **Traffic Data** (except for data requested for the sole purpose of identifying the user)
  Content Data:
  Criminal proceedings only for offences that carry at least a three-year maximum custodial sentence

- **Exception** (“application for offences which carry a maximum custodial sentence of less than three years”):

  - cyber-related offences where evidence will typically be available exclusively in electronic form,(…) even those which might not be considered serious in and of themselves but which could cause extensive or considerable damage, in particular offences with low individual impact but high volume and overall damage.

  - terrorism related offences

  - offences concerning sexual abuse and sexual exploitation of children

Who is addressed by the regulation (I)?

- **Providers of electronic communication services**

  ”Electronic communication services are defined in Directive (EU) 2018/1972 of the European Parliament and of the Council and include inter-personal communications services such as voice-over-IP, instant messaging and email services.”

- **Internet Infrastructure Providers**

  “Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registries and registrars and privacy and proxy service providers, or regional internet registries for IP addresses, are of particular relevance when it comes to the identification of actors behind malicious or compromised websites. They hold data that could make the identification of an individual or entity behind a website used in a criminal activity, or the victim of a criminal activity, possible.”

Who is addressed by the regulation (II)?

- **Information society service providers**

  This Regulation should also be applicable to information society service providers within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council (16) that do not qualify as electronic communications service providers **but offer their users the ability to communicate with each other or offer their users services that can be used to store or otherwise process data on their behalf.**

Definition from EU 2015/1535, Article 1:

'service' means any Information Society Service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:
(i) 'at a distance' means that the service is provided without the parties being simultaneously present;
(ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

Broadening the field of service providers

- Telecommunication service providers are used to deliver data to (national) LEA, same goes for OTT service providers.

- Under e-evidence, all service providers/platforms where
  - communication is possible between users,
  - users can upload content which is stored and/or processed
  are subject to the regulation. No further clarification is provided.

- There is no exemption provided for i.e. associations, clubs, cloud services, IoT, of-site video storage, gaming services, etc.

- There are no size caps or similar exemptions provided in the regulation

When will it enter into force?

- Technical Definitions & Implementation Act to be finished by **Oct 2024**
- Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by **18 February 2026** (AKA “going live”)
- Service providers that offer services in the Union on 18 February 2026 have the obligation to designate at least one designated establishment or to appoint at least one legal representative by **18 August 2026** (AKA “end of transition period”)
- **Without prejudice to data protection safeguards, such designated establishment or legal representative could be shared between several service providers, in particular by service providers that are small or medium-sized enterprises**
- Statistics on usage to be collected from 18. August 2026

How does an electronic production order work?

On reception of an EPOC by the **issuing authority (IA)**,
service providers (SP) are obliged to respond or face enforcement through the **enforcing authority (EA)** in its home state.

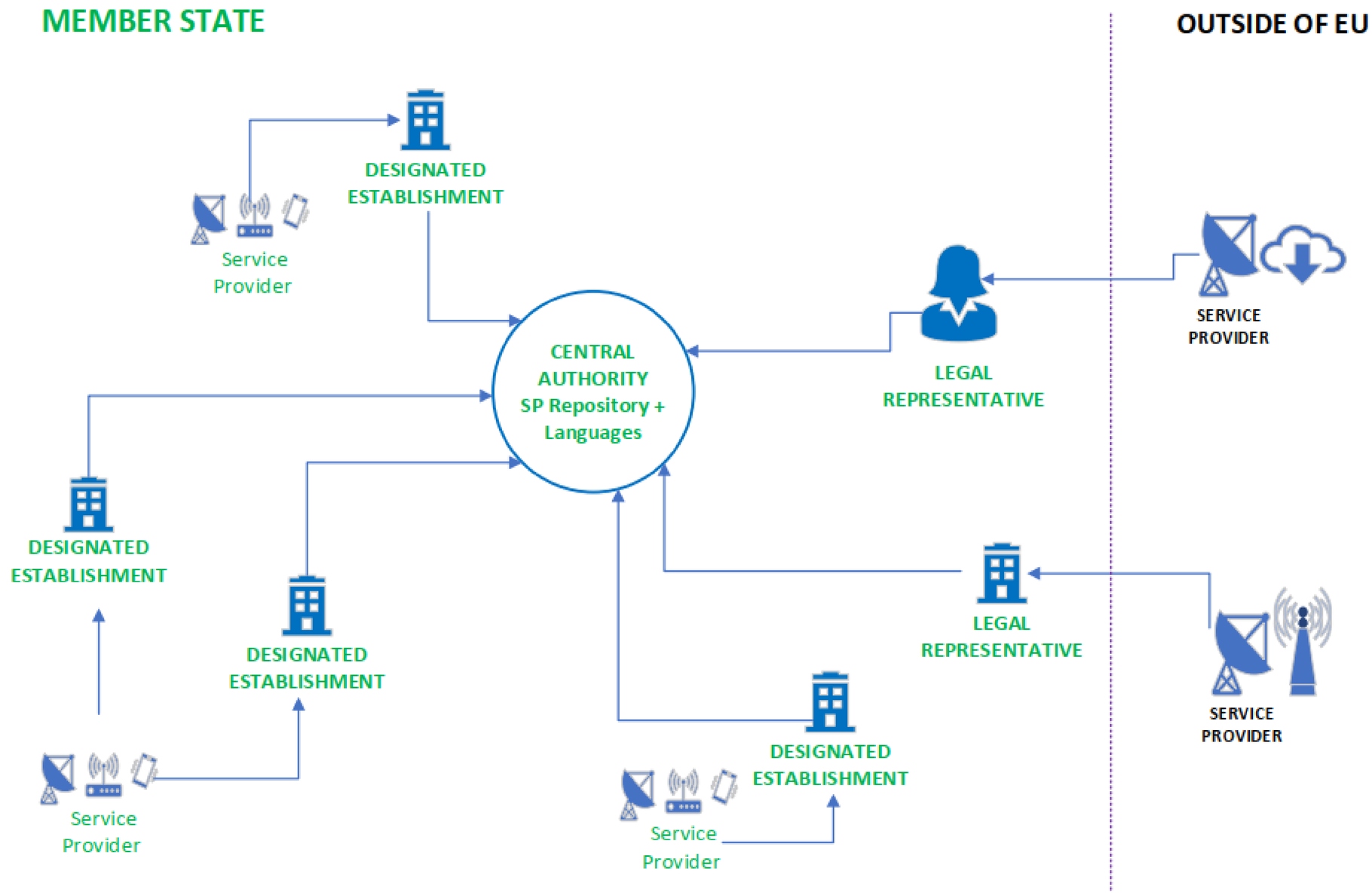
- **Production of the requested data**
  within **10 days** and in **emergency cases within 8 hours**

- **European Preservation Order**
  preservation for at least 60 days or until the data is produced or declaration that it is no longer necessary

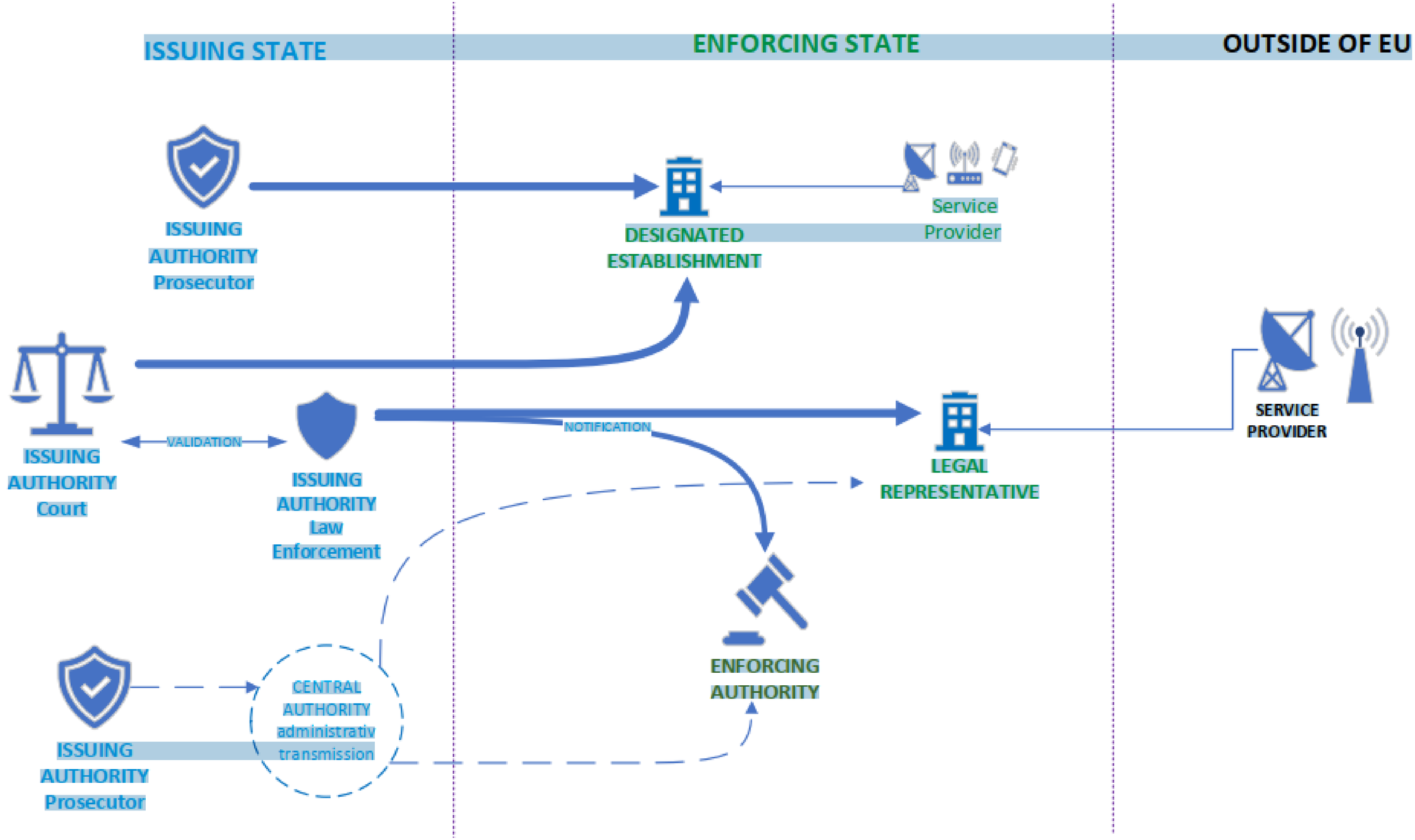
- **Confidentiality**
  no information to the person whose data is sought

- **In Principle**
  Provisions on enforcement and (pecuniary) sanctions, but also cost reimbursement
  (However, only if provided for in local law)

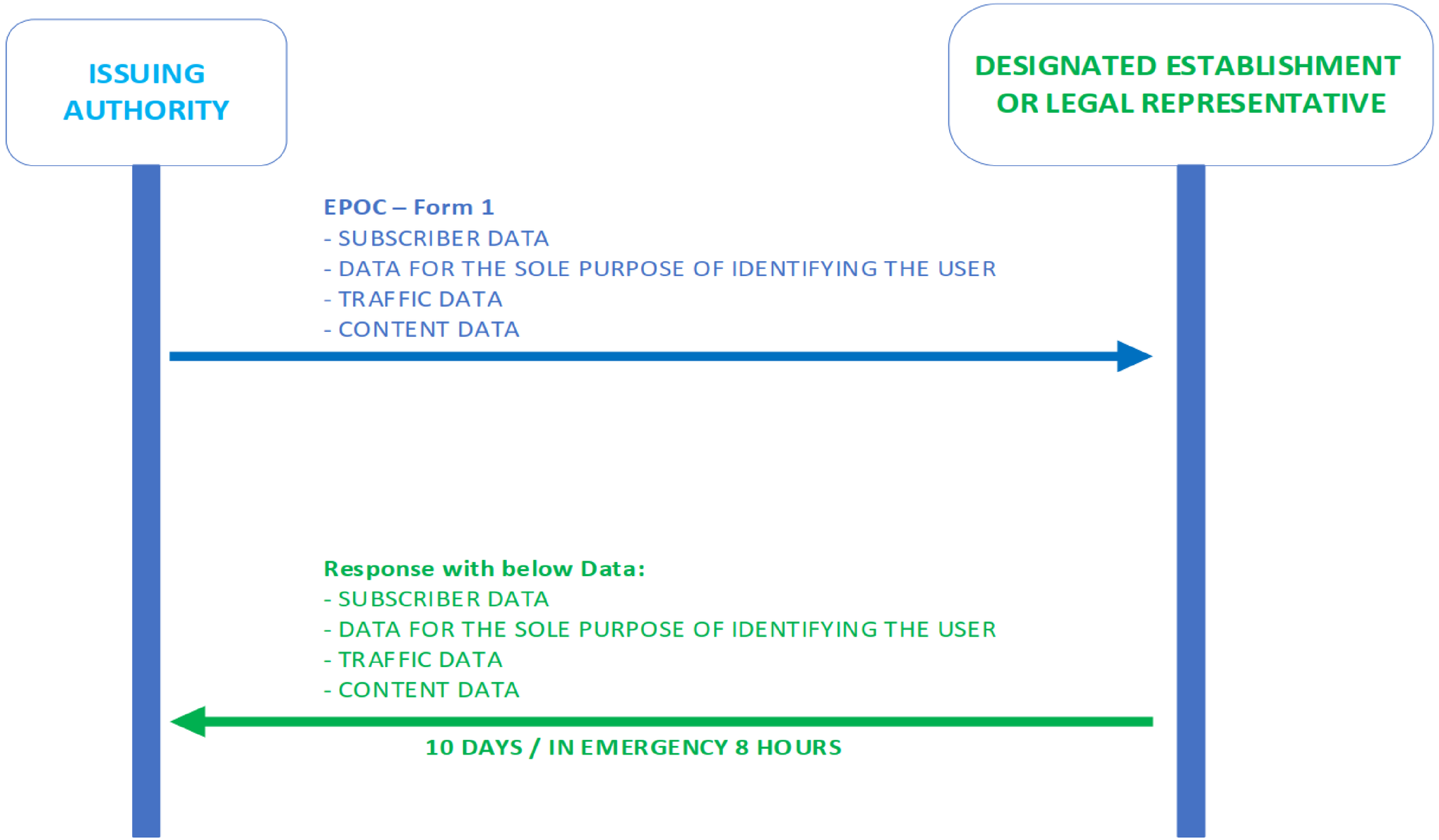
Central Authority - Directory of Service Providers



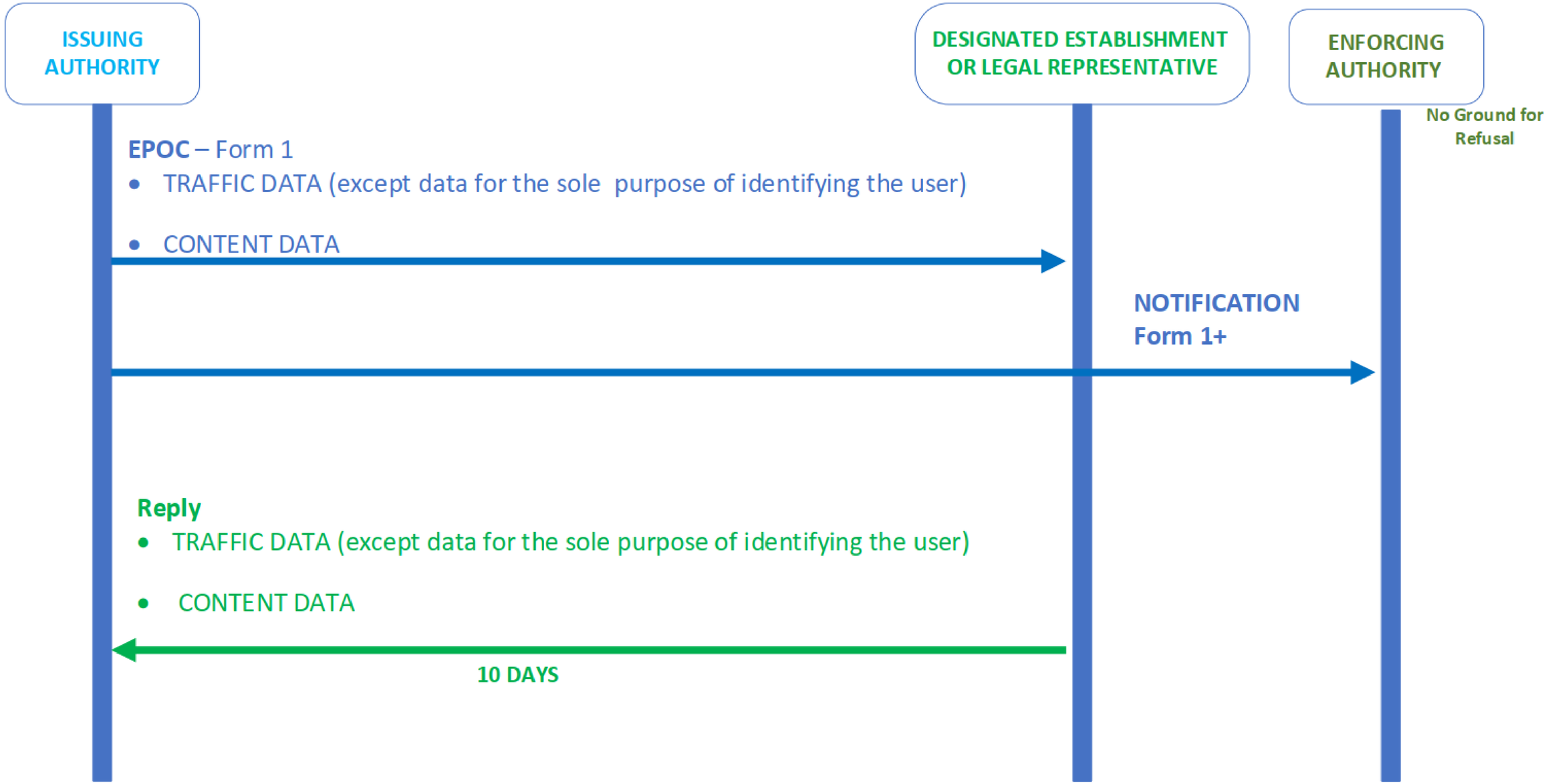
EPOC – possible regulation players



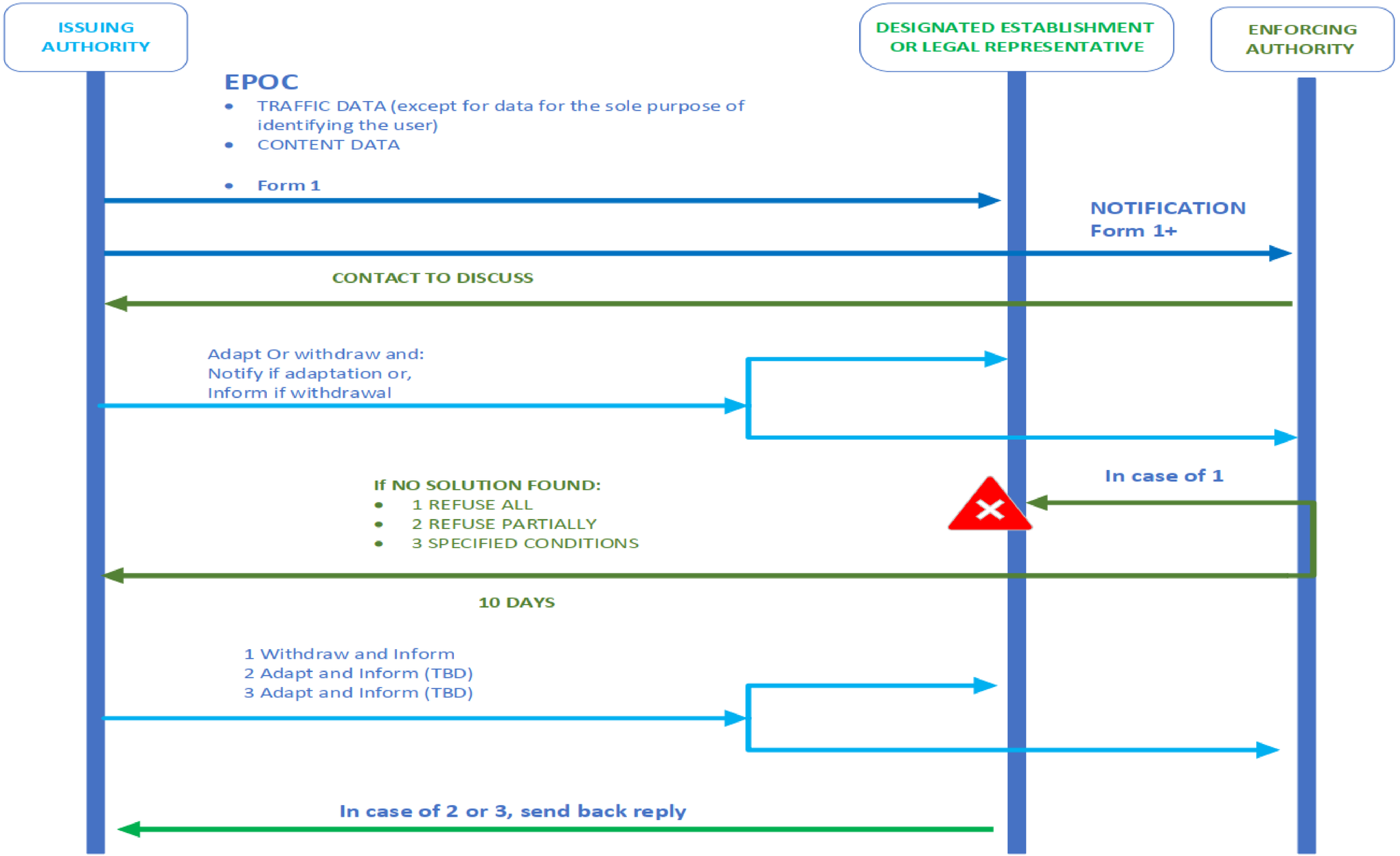
EPOC – workflow national case (no notification)



EPOC – workflow international case (notification)



EPOC – workflow international case (notification)



Protection of the individual

Grounds for refusal raised by SP or EA

(a) the data requested are protected by immunities or privileges granted under the law of the enforcing State, or the data requested are covered by rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media

(b) the execution of the order would, entail a manifest breach of a relevant fundamental right as set out in Article 6 of the treaty of the EU or in the EU Charter of human rights

(c) the execution of the order would be contrary to the principle of ‘ne bis in idem’*

(d) the conduct for which the order has been issued does not constitute an offence under the law of the enforcing State

* '**not twice in the same** [thing]', is a legal doctrine to the effect that no legal action can be instituted twice for the same cause of action

Further Protections

Additional Grounds for Refusal from considerations

(73) The procedure for enforcement should allow the addressee to invoke grounds against enforcement in case

- that the order concerned has not been issued or validated by a competent authority
- the order does not concern data stored by or on behalf of the service provider at the time of receipt of the relevant certificate

(64) It should be possible for the EA to refuse an order in exceptional (AKA political) situations

- If the EA determines whether, having regard to the personal situation of the person concerned, as well as to the nature of the offence, and the factual context that forms the basis of the order, and in the light of the information provided, there are substantial grounds for believing that there is a risk of a breach of a person's right to a fair trial on account of systemic or generalized "deficiencies concerning the independence of the issuing State's judiciary"

Problems for Service Providers

- 8h response time almost inpossible to meet for small companies, no size based exemption provided for in the regulation even so most service providers will never/almost never receive a request
- Exemption of prosecution is limited to „good faith“, i.e. if protections are already known a user might engage in legal action vs. service provider
- Significant penalties for not meeting requests (GDPR style up to 4% of global turnover)
- Service providers are required to answer to enquries not possible under the law of the seat of the service provider (risk of LEA proxy-requests)
- Possible „conflict of law“ scenarios are provided for, but only available for „3rd party“ countries outside of EU.

Effectiveness of Protections

The organizational setup of an SP makes a material difference in the disclosure of data. In effect, the seat of the designated contact point of the SP solely determines the protections considered for the disclosure of data.

Variant A:
A crime is committed in the issuing country, presumably by a user located in the SPs enforcing country. The user is a lawyer, this fact is already known to the SP.

The EPOC and notification will be addressed to the SPs as well as the EA in the users home country. After SP raises an objection, the EA will have to agree (the user is a registered lawyer). No data will be disclosed.

Variant B:
A crime is committed in the issuing country, presumably by a user of located in a country different than the SPs enforcing country. Again, the user is a lawyer, this fact is already known to the SP.

The EA will not recognize any protection as user is not a registered lawyer in EA's country (Art. 10 (5) states "under the law of the enforcing state"). Same goes for no criminality or similar concerns, even so the "criminality" of the case will under no circumstances ever concern EA's country. Objections raised by SP will not be upheld.

All data will be disclosed and - depending on country - stored even in cases of the dismissal of the investigation.

Envisioned court cases

- The non-involvement of a users home country vs. the involvement of the country of SPs registered contact will most certainly become the source of lengthy court cases and burden the EU courts for quite some time.
- Assuming a SP would register in ALL EU countries and route all cases pertaining to users home country, none of theses cases would ever occur. All (most) national immunities as well as "no criminality" would be observed.
- For the EU courts, a comparative analysis of legal proceedings in the member states is typically elemental to its findings.
- It seems unlikely that the difference in treatment will be upheld if challenged

Habeas corpus?

In cybercrime and "hacked" account scenarios, a user might be faced with a criminal investigation in the issuing state even if

- user never contracted with an entity outside of his home state
- never left his home state
- never committed a punishable offence in his home state

What can still be done?

- **Governing procedures as well as the design of the central system are determined in 2024**
  - Influence on how notifications are treated (extend of checks, treatment of spill-over)
  - Responsibility for enforcement of protections (who is responsible to raise objections?)
  - No disclosure if request is prohibited by local law (SP can NOT raise this objection!)
  - Automatic verification of authorization required (verifyable Digital Signature)
  - End2End Encryption of Messages/Released Data

- Lobby your Ministries as **affected Entities** to adopt acceptable, national rules & systems

- Possible association/federation of non-profit affected entities as designated establishments to uphold registration requirements an potentially register in all jurisdictions for optimized protections

Klaus Landefeld
Stellv. Vorstandsvorsitzender
Infrastruktur und Netze

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

fon: +49 (0)221/700048-0
fax: +49 (0)221/700048-111
klaus.landefeld@eco.de
www.eco.de

X (ehemals Twitter): @eco_de