Improving criminal justice in cyberspace

Proposals for

- **a Regulation on European Production Orders and Preservation Orders and**
- **a Directive on the appointment of legal representatives**

Electronic evidence and its relevance

- Electronic evidence: data stored in electronic form, such as information to identify a person or communications content
- Often stored by service providers that are established or store data in another country
- Today, more than half of all criminal investigations involve a cross-border request to obtain electronic evidence

Current procedures and why we need change

- Currently cross-border requests are processed through:
  - **Mutual Legal Assistance,**
  - **European Investigation Order or**
  - **Voluntary cooperation**
- Not fit for today's volume of requests: too slow and burdensome or lack transparency and accountability
- Lack of connection with the receiving State

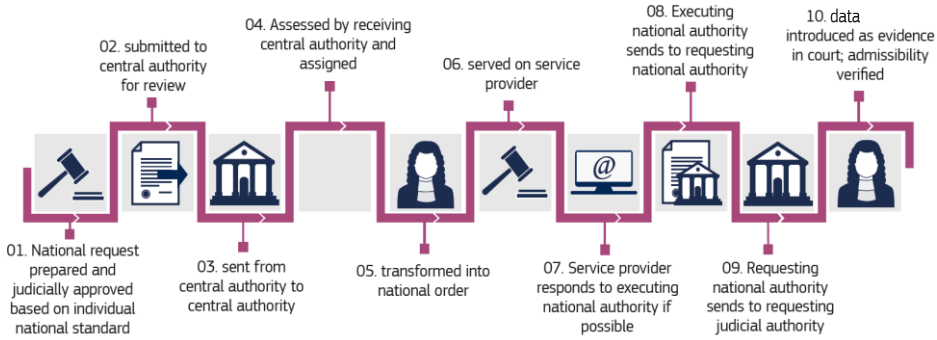
The proposals in a nutshell

- The Regulation: new form of judicial cooperation → mandatory cross-border orders for the preservation and production of e-evidence **directly** send to the service providers active in the Internal Market; irrespective of the location of their offices, their infrastructure or the data
- The Directive → to ensure a level playing field, all service providers offering services in the Union need to designate a legal representative
- The proposals build on existing principles of mutual recognition

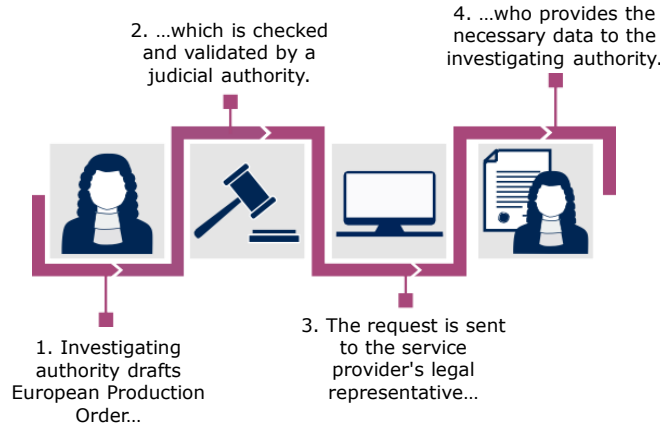
What benefits do the proposals bring?

- More efficient procedures
- Harmonised rules, legal certainty, transparency, accountability
- Strong protection of fundamental rights
- Setting an example internationally

Current MLA procedure



Future European Production Order



Which service providers are covered

- Material scope: providers of services that are used for communications purposes, the storage of data and internet infrastructure services
- Geographical scope: providers that are offering services in the European Union → enabling the use of services in one or more Member States and having a substantial connection to the European Union

Which types of data

- Subscriber data
- Access data
- Transactional data
- Content data

- All categories of data may be personal data, but they have a different level of interference with fundamental rights

- Appropriate conditions and safeguards apply

Safeguards, conditions and remedies

- All criminal law safeguards and data protection rules apply
- Prior approval by judicial authority required
- Transactional, content data: only for crimes with > 3 year penalty, cybercrimes and terrorism.
- Comity clause to address conflicting obligations under the rules of other countries, including judicial review
- Exceptions that allow for refusal
- Effective remedies for targets

Summary

- *"We need to equip law enforcement authorities with 21st century methods, just as criminals use 21st century methods for crime"* - updating tools while preserving strong protection mechanisms
- Setting an international example and protecting our acquis also vis-à-vis third states