INTRODUCTION: THE E-EVIDENCE PACKAGE IN A NUTSHELL

Brendan Newitt, De Roos& Pen, Amsterdam
newitt@deroosenpen.nl
+31652361174

1648: THE TREATY OF WESTPHALIA

Peace in Europe through state sovereignty

- **This treaty marks the end of the Spanish-Dutch Eighty Years' War, and the Thirty Years' War within the Holy Roman Empire of the German Nation.**
- **This treaty also marks the start of state sovereignty as the guiding principle of the international legal order**

1927: PCIJ VERDICT IN SS LOTUS CASE

State sovereignty in the international legal order clarified by the Permanent Court of International Justice:

- **Jurisdiction of a sovereign state may be split into three parts:**

- legislative jurisdiction

- adjudicative jurisdiction

- enforcement jurisdiction (including use of investigatory powers)

- **A state may try whomever it wants (in absentia if needed), a state may legislate whatever it wants, but enforcement may only take place inside of its own territory, unless there is a treaty basis or ad-hoc consent of the state where the enforcement (including use of investigatory powers) is to take place**

THE EIO CURRENTLY USED FOR PRODUCTION ORDERS WITHIN THE EU

ORIGINAL IMAGE SOURCE: EUROPEAN COMMISSION FACTSHEET E-EVIDENCE

THE EUROPEAN PRODUCTION ORDER UNDER THE E-EVIDENCE PACKAGE

ORIGINAL IMAGE SOURCE: EUROPEAN COMMISSION FACTSHEET E-EVIDENCE (AMENDED SLIGHTLY BY PRESENTER)

E-EVIDENCE PACKAGE CONSISTS OF:

- **Directive EU 2023/1544 (laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings)**

- final transposition date: 18 February 2026

- **Regulation EU 2023/1543 (on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings)**

– application from 18 august 2026

- **Package based on article 82 TFEU (arguably insufficient treaty base)**

REGULATION INTRODUCES:

(EU 2023/1543):

- **European Production Order (through EPOC certificate)**
- **European Preservation Order (through EPOC-PR certificate)**
- **Which can be directly addresses to an Internet Service Provider (ISP) for:**

- Subscriber data (who)

- Traffic data (how, when and where)

- Content data (what)

- **EPOC for content data and traffic data (unless traffic data is only for identification purposes) can only be sent for crimes that are punishable by > 3 years in the issuing state and specific listed crimes**
- **EPOC for traffic data (unless traffic data is only for identification purposes) and content data order require notification of ‘enforcing state’ (unless both the crime and the data subject are in the issuing state)**

DIRECTIVE LAYS DOWN RULES:

(EU 2023/1544):

- **Member states must ensure that any ISP established or offering services in the EU must appoint at least one addressee for receiving (and complying with) EPOC's and EPOC PR's**
- **Member States must be able to enforce infringements with penalties**
- **Member States must appoint a central authority to make sure the Directive is applied consistently.**

LIMITED GROUNDS FOR NON COMPLIANCE BY ISP:

- **ISP may advance limited impediments to compliance with EPOC:**

- Data requested are protected by immunities, privileges or journalistic freedom in enforcing state

- EPOC is incomplete or contains manifest errors

- It is de facto impossible to comply (outside of fault of ISP), e.g. data subject is not a customer of the ISP or data has already been lawfully deleted

- **Issuing state can acquiesce to ‘refusal’, provide further information regarding an incomplete or erroneous EPOC, or request enforcement from enforcing state.**

GROUNDS FOR REFUSAL BY ‘ENFORCEMENT AUTHORITY’:

- If notified, the enforcing state has 10 days to invoke grounds for refusal:

- Data requested are protected by immunities, privileges or journalistic freedom in enforcing state

- Substantial grounds to believe that the execution of the EPOC would entail a manifest breach of fundamental rights

- Ne bis in idem

- Absence of double criminality (if not one of the 32 listed offences)

- The same grounds for refusal may be invoked by the enforcing State after being requested to enforce the EPOC when an ISP refuses to comply.

- Culpable failure of ISP to comply with EPOC after enforcement decision, may result in fine of up to 2% of annual worldwide turnover of the ISP.

CONFLICT OF LAWS AND ‘EFFECTIVE REMEDIES’:

E-evidence package is light on explicit remedies and due process:

- **If an ISP considers that complying with a EPOC would conflict with an obligation under the law of a third country (such as privacy regulations in the State where the data is actually stored) a reasoned objection must be assessed by a court in the *issuing state***
- **The person whose data it concerns shall have right to exercise ‘effective remedies’ before a court in the *issuing state* in accordance with its national law and shall include the possibility of challenging the legality, necessity and proportionality**
- **Not fully clear to what extent domestic remedies in enforcing states will be provided (and allowed by the CJEU)**
- **To what extent does article 13 ECHR require a true domestic remedy for privacy breaches through an EPOC?**