EUROJUST

Practical tips related to requesting e-evidence from ISPs

- *"E-evidence in any form is relevant in around **85%** of total (criminal) investigations.*
- *In almost **two thirds** (65%) of the investigations where e-evidence is relevant, a request to service providers **across borders** (based in another jurisdiction) is needed."*

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT *Accompanying the e-evidence legislative package SWD(2018) 188 final, 17.4.2018*

"A better mechanism for cross-border communication and the exchange of information for the purpose of investigation, prevention and protection is clearly needed, but also to ensure that any ensuing MLA request conforms to all the relevant legal requirements of the requested country. In this context, differentiation between data requests that need to follow the MLA process (e.g. content data) and requests that typically do not need to follow the MLA process, because effective alternatives exist (e.g. the possibility of directly requesting non-content data from US-based Electronic Service Providers) may be relevant."

Common challenges in combating cybercrime as identified by Eurojust and Europol, June 2019

Regional (and national) resources

- Explanatory Report of the CoE Budapest Cybercrime Convention
- Reports of the CoE Cybercrime Convention Committee (T-CY)
  - Such as, but not limited to:
    - Criminal justice access to data in the cloud: cooperation with "foreign" service providers
    - Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY
- UNODC Practical Guide for Requesting Electronic Evidence Across Borders
- EuroMed Digital Evidence Manual: Practical Guide for Requesting Electronic Evidence from Service Providers
- CLOUD Act related resources (including the White Paper) on U.S. DoJ's dedicated webpage

Resources developed by ISPs

- Dedicated LEA pages/guidelines/portals/FAQs
- Model request templates
- Terms of Services (policy violations, notification obligations etc)

“Cooperation with the private sector is vital in combating cybercrime.”

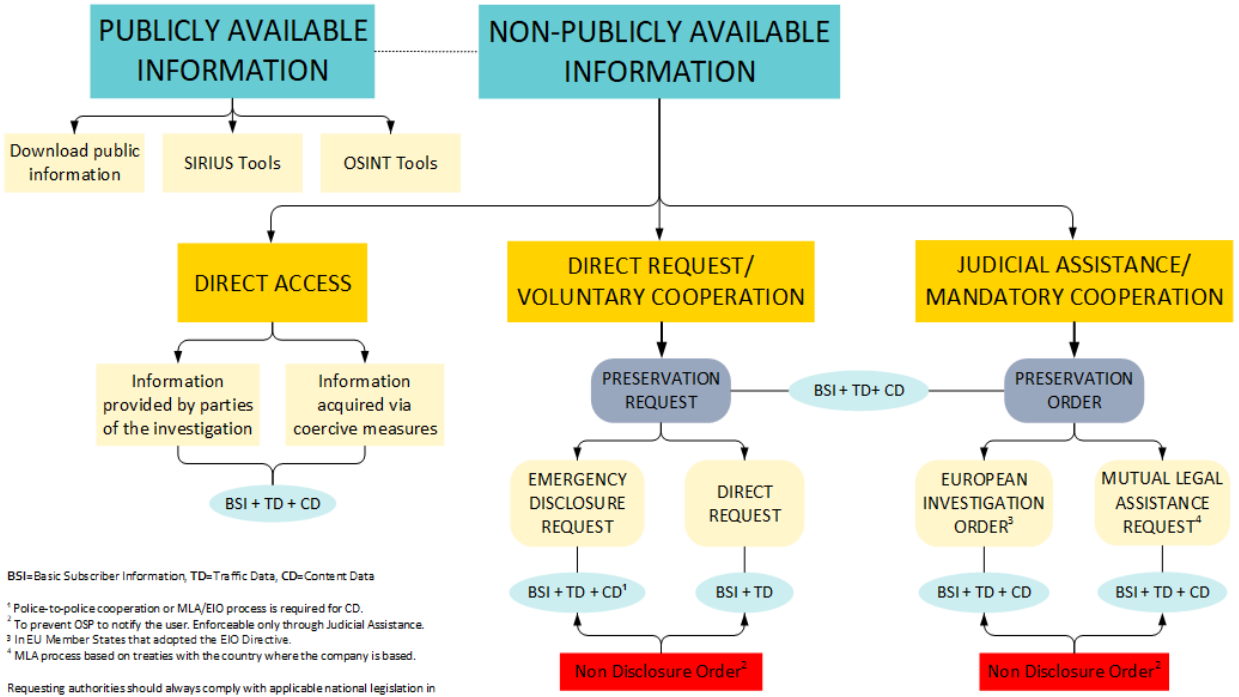
Common challenges in combating cybercrime as identified by Eurojust and Europol, June 2019



http://www.eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx

SIRIUS
CROSS-BORDER ACCESS
TO ELECTRONIC EVIDENCE

RETRIEVAL OF CROSS-BORDER INFORMATION

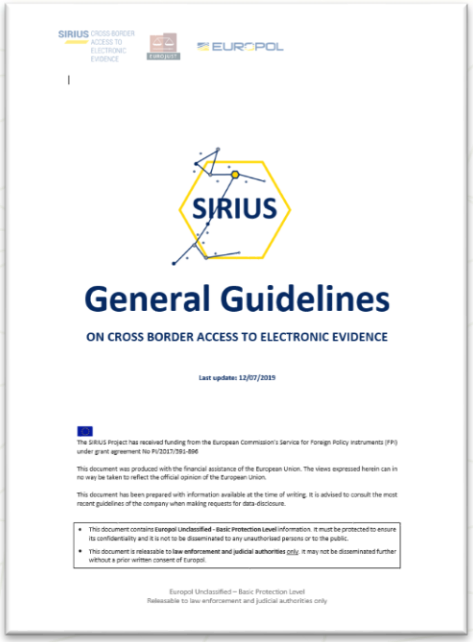


BSI=Basic Subscriber Information, TD=Traffic Data, CD=Content Data

[1] Police-to-police cooperation or MLA/EIO process is required for CD.
[2] To prevent OSP to notify the user. Enforceable only through Judicial Assistance.
[3] In EU Member States that adopted the EIO Directive.
[4] MLA process based on treaties with the country where the company is based.

Requesting authorities should always comply with applicable national legislation in regards to access to electronic evidence.

GENERAL GUIDELINE ON E-EVIDENCE



SPECIFIC GUIDELINES: ONLINE SERVICE PROVIDERS



Practical tips

- Request for preservation of data in order to ensure its availability (no data retention policies in place in many jurisdictions)
- If applicable, define emergency situation for expedited preservation (and possible production)
- Define request:
  - account ID/valid identifier(s)
  - nature of the investigation and broader context
  - legal basis
  - type of data and time period affected in connection to the relevance to the offence (target oriented requests vs bulk data requests)
- Ensure proper handling of confidentiality risks and check the user notification policy

Challenges

Challenges related to the addressee/communication means:

- addressed to the wrong legal entity/data controller
- addressed via wrong communication channels
- addressed without relevant identifiers (reference numbers, non-disclosure requests)

Challenges

Challenges related to the existence of data:

- requested data (account/user) never existed
- requested data for invalid identifier(s)
- requested data does not exist any more as deleted either by the users themselves or due to normal course of business of the ISP
- requested type of data is not collected nor retained by the ISP
- request for data disclosure is served after the expiration of the preservation period

Challenges

Challenges related to the substance of the request:

- request does not provide compliance check with the legislation of the requesting country/domicile of the ISP and/or policy of the ISP
- request does not provide any (vs proportional?) context regarding the investigation
- request is '*overly broad*' – type of information and time period is not narrowed down in connection to the offence
- request goes beyond of what is provided within the frame of voluntary cooperation

Robert Laid

Judicial Cooperation Advisor

rlaid@eurojust.europa.eu

+31 70 412 5617

www.eurojust.europa.eu

Follow Eurojust on Twitter and LinkedIn @ *Eurojust*