**1.**

* **often (in many cases)**

**2.**

* online encryption
  + **e-mail (PGP/GPG)**
  + **HTTPS**
  + **TOR**
  + **SSH Tunneling**
  + **E-data stored in the cloud**
  + **e-communications (through applications such as Skype, WhatsApp, Facebook, etc.)**
* offline encryption
  + **encrypting digital devices (mobile phone/tablet/computer)**
  + **encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)**
  + **others. WINDOWS BITLOCKER, PGP DESKTOP, WINZIP, WINRAR**

Please provide other relevant information: Nowadays, more and more suspects are using encryption in order to hide their criminal activity. When confronted with perpetrators that made use of e-communications we have no means of deepening the investigation

If you have different experiences in cross-border cases, please specify:

**3.**

* **no**

Please specify: We do not have specific legislation for encryption. No person in possession of devices/e-data is legally obliged to make them available to law enforcement.

**4.**

* **no**

Please specify: Same as previous.

**5.**

* **no**

**6.**

Please specify: obtaining the decryption key- If the internet traffic is encrypted (chats, https pages), during the intercepting we cannot obtain relevant evidence regarding the criminal activity.

**7.**

Please specify: We do not have appropriate tools for decrypting encrypted e-evidence/devices.

We can use technical solutions and communicate with private companies or law enforcement agencies.

**8.**

* **no**

Please specify: We would prefer to have specific legislation for encryption.

**9.**

* **technical**
* **legal/legislative**

Describe in more detail the issues identified above: Law enforcement professionals need more training regarding how to seize encrypted evidence and how to decrypt it.

**10.**

* **dedicated new legislation**
* **practical (e. g. development of practical tools for police and judicial authorities)**
* **improve exchange of information and best practices between police and judicial authorities**
* **create conditions for improving technical expertise at EU level**
* **improve the (legislative) conditions of communication with service providers, including through the establishment of a legislative framework**.

Please give examples: Europol can provide standards regarding the improvement of technical expertise at EU level

**11.**

* Creating EU legislative tools in this field could provide law enforcement with means of decrypting data that might constitute e-evidence for criminal matters.
* Given the diversity of the technical means used to encrypt data, the application of encryption in an increasing number of fields under the attention of law enforcement agencies, the development of a database of tools and methods, accessible to technical experts throughout the EU would be useful.
* Criminalization of the act of not disclosing the encryption keys, as well as mandatory key encryption disclosure for service providers, including social service providers as Skype, Whatsapp, etc.