In general, the Czech Republic is skeptical about a new rushed legislation at EU level, although we can see advantages of such approach. Discussions during the negotiation of E-privacy Regulation have shown that it will not be easy to reach an agreement within reasonable time framework.

Furthermore, analysis of recent judgments is in process at national level with the aim to identify the necessity of amendments to our current legislation. Therefore, if such gaps are identified, we have to draft an amendment to our legislation anyway.

Therefore, we are rather in favor of the first approach.

However, we also support further discussion at EU level (COPEN meetings, FOP or other format) and are curious about experience of the member states with targeted data retention and other aspects mentioned by Court. As mentioned by Spain at the last COPEN meeting, other possible solutions which would be in line with the CJEU´s judgements should also be explored.

As regards the questions raised by the COM:

Q 3(a)

With regards to the retention of data for national security purposes, we would strongly support regulation at national level. We are of the opinion that data retention for national security purposes, which is an area of sole responsibility of the Member States, should be regulated at national level.

Q 3(b)

[redacted]

As for the persons, it is still not clear to us, how to define it, especially in a non-discriminatory manner.

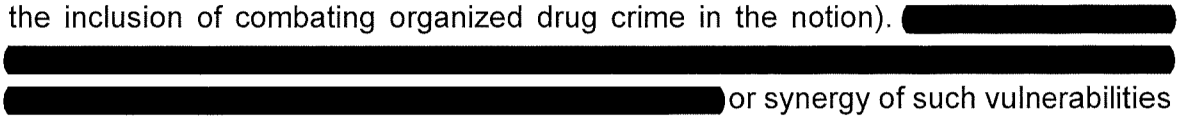
As mentioned during the last COPEN meeting, at least two member states prepared legislation defining such criteria; we are eager to learn more from their experience.

We do not see the necessity to continue in the „data matrix" discussion.

In the CZ only private actors acting under the Act on Telecommunications are obliged to retain data (as opposed to service providers acting under the Act on certain services provided to the information society). According to the Czech law, the data

retention period is set for six months, even though according to the law enforcement authorities the optimal retention period would be one year. However, this period applies only to the data retained under the Telecommunications act. According to Section 88a of the Criminal Procedure Code, the retained data can be used only for investigations of a crime with a minimum sentence of three years and exhaustive list of crimes which are usually committed with the use of mobile or internet (such as stalking) as well as for intentional crimes which must be prosecuted on the basis of valid international agreements. It is obligatory to inform the data subject (if known) about the fact that the data was retained when the proceedings are finalized, although there are some exceptions to this rule.

As far as serious threats to public security are concerned, CZ notes that the Court of Justice sometimes considers public security to be an overarching category of internal and national security fields. Frequently, functioning of institutions, essential public services, survival of the population, risk of serious disturbance to foreign relations or to peaceful coexistence of nations, risk to military interests are deemed relevant. Indeed, the extent of the notion of "public security" may significantly depend on the legal instrument and the context (see judgement C-145/39, para 45 in particular as to the inclusion of combating organized drug crime in the notion).



or synergy of such vulnerabilities and harmful events (such as the "Lisa case"). Therefore, CZ believes that precise, or even exhaustive future-proof list of serious threats to such broad and partially flexible category of public interests is impossible to establish. Finally yet importantly, many (but not all) security threats materialize as criminal offences, therefore combating such security threat in many cases corresponds to, specialized crime prevention phase. In such cases, obviously, successful prevention may often be much more important than successful criminal prosecution.

That being said, CZ believes that examples of serious threats to public security include:

- unconventional military threats ("green men", paramilitary groups or militias) and attacks
- support to extremist and non-democratic political parties and groupings and their activities
- extortion, corruption and influence over political and other high state representatives (e.g. justices dealing with systemically important case, such as contested elections)

- economical pressure, suspension of energy or material supplies, influence or ownership over key infrastructure
- fomenting public disturbances and unrest, radicalization, election disturbances and sabotages
- massive propaganda to diminish effective functioning of public institutions
- cyber-attacks against essential public services

Q 3 (c)

The retention period depends on the type of data. It would be also useful to discuss this question with the private companies.

[redacted]

According to the law, the so-called expedited preservation of stored data is used e.g. to secure the content of a server that was managed as an attacking C2 server. [redacted] With traffic and location data, law enforcement authorities can therefore exclude innocent people who were not involved in the crime and greatly narrow the range of suspects.

According to the Budapest Convention, the Police of the Czech Republic has established a contact point for so-called emergency cases where the lives and health of persons are endangered. Without information about traffic and location data, it would not be possible to react at all within this contact point.

Q 3 (d)

[redacted]

According to the Czech law, the regulation on data retention stipulates the exact data that must be retained. Czech law enforcement would like to extend the list of retained data to cover also end-user IP addresses. [redacted]

[redacted]

However, as explained above, there is no obligation to retain data for electronic communication service providers in CZ.

[redacted]

[redacted]

Q 3 (e)

Retention of civil identity data is important to fight crime effectively. It is important to find a common understanding of this concept at EU level. We understand as civil identity data user data, i.e. the identification of a contract user connected to the Internet, without the need to use operational and location data for identification. Civil identity data, however, on the contrary to subscriber data, do not in general include data on payments.