3. The policy approaches in more detail

Policy approach 1: no EU initiative

The Commission would refrain from any regulatory or non-regulatory initiative on data retention. It would be for Member States to address the consequences of the judgments at national level, in line with the Charter of Fundamental Rights and the CJEU case law, in order to take into account national specificities. The Commission would nevertheless be ready to support Member States in this process, e.g., by facilitating exchanges and organising expert meetings, including with other relevant stakeholders.

Question:

1. Do Member States see merits or drawbacks in maintaining a national approach to data retention legislative measures?

Policy approach 2: Non-regulatory initiative on data retention

This would consist of a Commission recommendation or a guidance document (Communication). This approach would follow the same structure as in point 3 below i.e., covering the various scenarios relating to all purposes and data categories or a combination thereof. The objective would be to assist Member States in bringing their laws into conformity with the rulings.

An advantage of this approach over legislation is that it could be carried out in less time than it takes to draft, negotiate and implement legislation and provides a margin of flexibility for Member States to apply the guidance to bring their laws in line with the rulings without prejudging a possible legislative proposal in the near future. A recommendation is, however, not legally binding or enforceable.

Question:

2. Do Member States consider this a viable way forward?

Policy approach 3: regulatory initiative on data retention

In the following section, five different avenues to translate the CJEU jurisprudence into EU rules on data retention are set out below. A possible EU legislative initiative could be either comprehensive, i.e. covering the retention of all (meta)data categories (traffic and location data, IP addresses) and of civil identity data and for all purposes(national security, serious crime/serious public security threats, general crime/public security threats), or limited to specific data categories and/or specific purposes. A framework could thus include all five sub-points below or a combination thereof. The five possible approaches outlined below in points 3(a) to 3(e) reflect the structure and logic of the La Quadrature du Net a.o. ruling. In considering these points, Member States may also wish to consider the following question:

Question:

3. Could Member States consider a 'mixed' approach of both national and EU measures? If so, what aspects should be regulated at which level (EU or national)?

<u>Approach 3(a): generalised retention of traffic and location data for national security purposes</u>

This approach could entail legislation harmonising obligations on electronic communication service providers, which include Over-The-Top (OTT) communications services, to retain traffic and location data in a generalised and indiscriminate manner based on a decision from independent national authorities, following a risk assessment taking into account specific national circumstances. It would not regulate the way in which state authorities themselves process these data for national security purposes, which the Court recognises as being outside the scope of the e-Privacy Directive, or how Member States approach their risk-assessments. Rather, the focus would be on the involvement of the providers in processing electronic communications metadata for national security purposes and on setting out appropriate access safeguards. For instance by articulating that:

- The threat to national security must be serious, genuine and present or foreseeable as assessed by national authorities according to Member States' individual threat/risk assessment taking into account national specificities.
- Decisions must be subject to effective (prior) review, either by a court or by an independent administrative body whose decision is binding and free from external influence.
- Decisions must be limited in time to what is strictly necessary (but without harmonising the duration as this depends on the level of existing threats and periodic national threat assessments).
- Appropriate access safeguards other than prior review e.g. ex-post review and supervision by an appropriate national authority.
- Required technical safeguards applicable to both providers and authorities to prevent unauthorised access, abuse or misuse of data.

Questions:

4. In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

<u>Approach 3(b): targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, safeguarding national security)</u>

The CJEU held that targeted retention as a preventive measure for the purposes of combating serious crime and serious threats to public security, and equally of safeguarding national security, is possible, provided that such retention is limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary. Targeted retention may, in particular, be achieved by limiting retention to specific categories of persons or to specific geographical areas based on objective and non-discriminatory factors.

In relation to <u>categories of persons,</u> the Court indicates that targeted retention legislation based on objective evidence can be directed at persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security. The persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned.

Geographical targeting measures may include areas where the competent national authorities consider, based on objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.

Targeted retention must also be limited in time but with the possibility to extend or renew the measures if necessary. The Court stipulates that data retained under such "targeted" retention obligations may be accessed for national security purposes but not for crimes in general. Possible legislation could harmonise obligations on electronic communications service providers, which include OTT communications services, to retain traffic and location data with:

- a focus on geographical targeted retention.
- harmonising the access safeguards.
- providing a fixed retention period that may be modulated according to the sensitivity of the data or other criteria to be determined (based/justified on objective criteria).
- data irreversibly deleted after expiration of the period.
- data stored in the EU, and
- setting out the types of serious crimes covered e.g. based on penalty thresholds (a custodial sentence of a minimum or maximum of at least [X] number of years) and/or a list

The following targeting parameters may be considered:

- Geographical targeting: Taking due account of Article 21 (non-discrimination) of the Charter of Fundamental Rights and based on objective and non-discriminatory factors, providing an obligation on providers14 to retain traffic and location data for a specific and renewable period and subject to periodic risk-assessments by national authorities in a number of sensitive areas e.g., a certain radius around sensitive critical infrastructure sites, transport hubs, areas with above average crime rates or that may be a target for serious crime or are high security risk e.g. affluent neighbourhoods, places of worship, schools, cultural and sports venues, political gatherings and international summits, houses of parliament, law courts, shopping malls etc.).
- Targeting of specific categories of persons: Taking due account of Article 21 (non-discrimination) of the Charter of Fundamental Rights and based on objective evidence, the following parameters could be considered: (1) known organised crime groups; (2) individuals convicted of a serious crime; (3) individuals who have been subject to a lawful interception order; (4) individuals whom authorities have a reason to believe have a link to serious crime; (5) individuals on a watch list such as for terrorism or organised crime; (6) known associates of individuals in points (1) to (5).

Such an approach could be combined with an obligation on service providers to collect subscriber/identification data about all of their clients, both those with indefinite contracts as well as 'pay-as-you-go' SIM cards15 (related to sub-point 3(e) below) or together with an obligation to retain IP addresses and, possibly, related identifiers that facilitate identification of a user (related to sub-point 3(d) below).

Questions:

5. What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses.
6. What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?
7. Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?
8. Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?
9. Can Member States share their views of what serious threats to public security entails?

Approach 3(c): expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of national security

The CJEU held that competent authorities may issue an order, subject to effective judicial review, requiring electronic communications service providers to carry out, for a specified (renewable) period of time, the expedited retention of traffic and location data in their possession, subject to strict access safeguards. This resembles the so-called "quick freeze" or "data preservation" mechanism.

Legislation could include similar access, security and oversight conditions as for targeted retention above, including delineating serious crimes by custodial sentence or list. Obviously, such a mechanism makes sense only if some metadata are retained in the first place by service providers, e.g. for business purposes.

Questions:

10. Given that a "quick freeze" provision can apply only if there is metadata available to "freeze", can Member States share any experience relating to the normal period of availability of metadata, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?
11. Can Member States share any experience relating to the use of expedited retention in their current legislation?
12. Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?

Approach 3(d): generalised retention of IP addresses assigned to the source of an Internet connection for serious crime and serious threats to public security

IP addresses assigned to the source of a communication can be retained as they are less sensitive than other traffic and location data, and are indispensable to investigate cybercrime, such as online child sexual abuse. Strict safeguards would apply: purpose limitation, limited retention period, strict access conditions.

Possible legislation could harmonise an obligation for electronic communication service providers, which include OTTs, to retain the IP addresses of the senders. The legislation could also set out a specific and

reasonable retention period, delineate the types of serious crimes covered (e.g. based on penalty thresholds and/or a list) and the applicable procedural and substantive access safeguards, including in cross-border cases.

This approach would provide a tool for investigators to fight cybercrime and cyber-enabled crime, including cross-border. It would provide clarity for joint cross-border investigations and prosecutions. It could also provide a path to overcome the challenges posed by CGN-NAT technology (where hundreds of users may be behind one IP address), for example by obliging communication providers to retain the so-called source port number or other technical identifiers that facilitate identification of a user.

<u>Approach 3(d) and 3(e) could be combined as they are similar in sensitivity and approach.</u>

Questions:

13. Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?
14. Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?
15. What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

<u>Approach 3(e): generalised retention of civil identity data to fight crime and public security threats in general</u>

Generalised and indiscriminate retention of "civil identity data" is possible.

Possible legislation could mandate the generalised retention of civil identity data. This would extend also to OTTs.

The term "data related to civil identity" is described by the Court as data that should not make it possible to get to know the date, time, duration and addressees of the communications, nor the places where they took place, or how often this happened with specific persons within a given period. Apart from "contact details of [those] users", it is not, however, specified what this term encompasses and to what extent, if any, it is different data compared with "subscriber data". In the digital environment, the notion of civil identity should cover data identifying the subscribers.

Approach 3(d) and 3(e) could be combined as they are similar in sensitivity and approach.

Questions:

16. Is retention of 'civil identity data' effective to fight crimes?
17. What specific elements should be included in this data category?

Answers to the questions

Regarding the questions 1-4

Denmark finds it of great importance that the member states work towards finding a common way forward on data retention. In principle, the EU legislators should define the way forward on a subject as important as data retention rather than leaving the regulation to the ECJ. However, from a Danish perspective it is crucial that any potential new EU legislation does not further limit the scope for data retention, i.e. include national security. If new EU legislation will reflect the ECJ position in a limiting way, Denmark will prefer policy approach 1 (no EU initiative).

Regarding the questions 5-17

In Denmark, we are in the midst of working on a revision of our national legislation following the judgment of 6 October 2020 by the ECJ (La Quadrature du Net). We expect to submit draft legislation to parliament in October. The expected revised legislation will likely include a scheme to retain data on a general and undifferentiated basis with the purpose of safeguarding national security as well as a scheme of targeted retention with the purpose of combating serious crime. Furthermore, the revised legislation is likely to comprise regulation regarding the general and undifferentiated retention of IP-addresses.

According to the current plan, the work with the draft legislation will be introduced to the Danish government after their summer holidays. Until then Denmark cannot get into further detail regarding the coming draft bill. We hope for your understanding.

However, it can generally be noted that it has been very difficult to draft legislation within the framework of the ECJ's case law, which can also serve as an effective tool for our police and security services.