

The Hague, 04/06/18

EDOC#965006v3

Concept of Restricted Data Retention and Targeted Data Access Outcome of Data Matrix Exercise

Following the annulment of the Data Retention Directive (DRD) by the European Court of Justice (ECJ) in April 2014 due to a lack of proportionality (*Digital Rights Ireland*), and the *Tele2* ruling in December 2016 according to which also Article 15 ePrivacy Directive cannot serve as legal basis for law enforcement data retention, law enforcement and judicial authorities face enormous challenges in investigating online crime.

In September 2017 Europol's Data Protection Function (DPF) presented a concept of 'restricted data retention and targeted data access' to the Council Friends of Presidency Information Exchange and Data Protection Working Party on Data Retention (FoP DAPIX WP DR).[1] This concept builds on the criteria established by the ECJ while taking due account of law enforcement needs.

The cornerstones are that only the criteria established by the ECJ in the *Digital Rights Ireland ruling* are binding for the legislator *a priori*. The stricter conditions in *Tele2* including the criterion that "storage of data must not become the rule" do not necessarily derive from the Fundamental Rights Charter but are merely a logical consequence of Article 15 ePrivacy Directive being phrased as an *exceptional rule*.

A different legislative approach would hence be possible: Restriction of retained data categories would be required just as far as it is practically possible – without rendering the whole concept useless for fighting serious crime and terrorism ('restricted data retention'). Higher safeguards with regard to storage, access and use of the data would ensure overall proportionality ('targeted data access').

The JHA Council of 7 December 2017 acknowledged that the concept could eventually serve as basis for developing a data retention framework at EU level and encouraged Europol to facilitate preparatory works for a related data matrix in close collaboration with Member States' (MS) technical experts for further discussion in FoP DAPIX WG DR.

To that end Europol, together with the Bulgarian Presidency hosted two workshops on 20 March and 14 May bringing together specialised investigators and forensic experts from 26 MS. The Commission, the General Secretariat of the Council, the EU Counter-Terrorism Coordinator's office and Eurojust participated in an observer role. In total 65 participants joined the first workshop in March while 47 were able to continue the work in May.

All workshop participants were familiarised with the concept of 'restricted data retention and targeted data access' and, in particular, with the two involved interference levels relating to the question of retention of the data as such ('interference level 1') and the question under which conditions retained data could be accessed by law enforcement ('interference level 2').

The data matrix exercise aimed at establishing whether or not it would be possible to further narrow down the scope of data to be retained for law enforcement purposes, i.e. the main focus was on interference level 1.

[1] Council of the European Union, WK 9374/2017 REV 1, 15/09/2017.

The idea was to start from broadest possible technical standards allowing for complete visibility of which data is technically being retained and then to match the operational business needs against such most comprehensive technical standards of retained data.

This was to determine whether additional restrictions in terms of data retention would be possible without undermining efficient law enforcement operations. Furthermore, the exercise was meant to enhance visibility on the fact that law enforcement is, indeed, not advocating the general or indiscriminate retention of any available information but is making best effort to implement the criteria established by the ECJ.

The overwhelming majority of participants deemed the data matrix template developed by Europol a very good basis. The template was created based on the so called ETSI standards and the Council of Europe (CoE) Electronic Evidence Guide. It included 487 data fields broken down into seven chapters relating to telephony services, asynchronous message services, synchronous multi-media services, network access, further information on data categories, online sources of investigation and digital evidence sources.

A number of delegations, however, also expressed the view that the draft matrix template as put forward by Europol would be too technically detailed and hence difficult to apprehend even for experts with broad experience in the area of communication data related criminal investigations.

Consequently, the workshops generated different sorts of feedback ranging from

- proposals for structural adjustments of the provided data matrix template towards a more generic data matrix,
- via deleting, adding or adjusting certain data fields, columns or chapters,
- and/or filling-in the data matrix template as initially developed by Europol.

Several experts raised the issue that a filled-in data matrix would be operationally sensitive since it could enable criminals to explore forms of communication beyond the agreed focus of law enforcement.

Others informed that they would not be mandated to issue any binding opinions regarding the strict necessity of individual data fields due to diverging opinions in different governmental entities. This issue, particularly, occurred in federal States due to different practices in the respective sub-entities.

Initial figures based on filled-in data matrix templates provided by four MSs revealed that out of 487 data fields 179 fields were marked by one or more MS as not strictly necessary for the fight against serious crime and terrorism. More precisely, five data fields were marked by all four MSs, 13 fields by three MSs, 47 fields by two MSs and another 114 fields by one MS.

While this result seemed promising in the first place, the following intense debate amongst workshop participants demonstrated that the development of a commonly agreed data matrix would be challenging due to a number of reasons including

- no common ground that data retention in the digital age would only be necessary for the fight against serious crime,
- different interpretations amongst MSs on the meaning of certain fields,

- different approaches on how to reflect on information which would be available based on national legal provisions other than data retention laws,

- different applied storage practices in certain MSs.

For instance, one delegate elaborated that in his country all communication service providers store GSM and UMS location parameters in a specific format referred to as WGS84 coordinates. Consequently, he could reasonably un-tick the data fields relating to any other GSM and UMS location parameter formats in the data matrix.

Other experts, however, elaborated that in their jurisdiction this would not be the case and why GSM and UMS location parameters as such would be strictly necessary – regardless of the specific format in which they are being stored.

In conclusion, there were only very few data fields deemed unnecessary by the overwhelming majority including the value indicating the length of the antenna transmitting or receiving communication signals or an indicator for the quality of a call. Also a value recording the number of ring-tones was discussed in this context. However, several forensic experts confirmed that certain organised criminal groups are known to use a ring-tone morse-code in order to communicate amongst each other.

More broadly speaking different investigative techniques across MSs and crime areas complicated a common view on filling-in the data matrix with a view to excluding certain data categories from retention upfront.

Participants on the other hand agreed that the data matrix should in any case not serve as blueprint for the legislator. A certain data category which may today not be deemed strictly necessary for the fight against serious crime and terrorism could already tomorrow become essential, for instance, if certain technical components in communication tools change. In addition, since technology continuously evolves (e.g. 5G) new data categories may emerge as essential.

Defining technical details in a legislative text has failed in the past, for instance, regarding data retention legal frameworks which only required the service providers to retain the IP address while the meanwhile widespread deployment of CGN would also require logging the source port number and an exact time-stamp in order to be able to trace back to an individual.

The requirement for tech-neutrality of any future data retention legal framework was emphasised. A generic data matrix template focussing only on the 'who, with whom, when, where and how' was ultimately deemed more appropriate in order to define restrictions at interference level 1. One delegation presented such a more generic matrix operated in their jurisdiction as a possible inspiration for the legislator.

Furthermore, all workshop participants agreed that over-the-top (OTT) providers should be subject to data retention and that subscriber information should remain easily accessible to law enforcement considering that the relevant ECJ rulings only apply to traffic data.

Another argument which workshop participants would like to see feature more prominently in the debate is that retained data can also be used for humanitarian purposes drawing a link to Article 10 of the Police and Justice Data Protection Directive[2] referring to the protection of the vital interests of

[2] Directive (EU) 2016/680 — protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data.

the data subject or of another natural person. This could, for instance, be the case in scenarios in which personal data are being processed in order to locate missing persons but also in order to exculpate individuals which have wrongfully come on the law enforcement radar.

Online portals for the handling of communication data requests are being operated in a number of MSs. Others rely on more manual processes. The positive experience in those MSs already using online portals could potentially be used for the benefit of all MSs which may then also facilitate interoperability aspects.

The workshop participants agreed to convey the following core messages as a result of their work:

- A tech-neutral data retention framework at EU level (covering also OTT providers to be incorporated into the ETSI standards) is needed striking the right balance between law enforcement needs and fundamental rights.

- In the digital age there is no common ground that data retention would only be necessary for the fight against serious crime.

- The criteria developed by the ECJ in the Digital Rights vs Ireland and Tele2 vs. Watson rulings do not apply to subscriber information which should remain more easily accessible to law enforcement.

- Law enforcement is not advocating the general or indiscriminate retention of any available information but is making best effort to implement the criteria established by the ECJ.

- The ETSI standards already represent a filtered view on even broader data sets which are technically available. The ETSI standards have been developed as a hand-over specification for the lawful intercept of communication data.

- There is a certain possibility that information as specified in a few data fields of the ETSI based data matrix could be excluded from retention upfront without rendering the whole concept of data retention meaningless in practice. However, also such restrictions would potentially have detrimental effects on law enforcement operations.

- In the interest of tech-neutrality a detailed ETSI based data matrix cannot be legislated as it only represents a snapshot in time in terms of strict necessity of the information for law enforcement purposes. A generic data matrix could serve as inspiration for the legislator.

- The implementation of the proportionality principle is mainly achievable at interference level 2, i.e. via access restrictions to retained data.

- A proportionate data retention regime is ultimately in the interest of citizens.

The AT Presidency will continue the discussions in FoP DAPIX WP DR with a first meeting on 10 July and further meetings in September, October and November as necessary.