In light of the trialogue negotiations on the proposal for the Law Enforcement Data Protection Directive[1], EDRi, fipr and Panoptykon would like to provide comments on selected key elements the current Council text.

Introduction

The proposed legal framework for the protection of personal data consists of two legislative proposals: a proposal for a Regulation with regard to the processing of personal data and on the free movement of such data (the so-called General Data Protection Regulation), and a proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

In the present analysis, we cover the most problematic points of the Directive. For our views on the Regulation, please go to our document pool.

This document concerns the Council's general approach, analysing in particular Chapters V, VI and VII of the legal framework.

Main concerns in the current text of the Directive

- Transfers decided unilaterally by the European Commission: Recital 46 says that, even if the Commission has not followed the procedures in Article 41 of the Regulation for transfers with an adequacy decision, the Commission can nevertheless decide which country or "sector within a third country" offers an adequate level of protection. Taking into consideration the recent CJEU decision on the Safe Harbor agreement[2]

1 Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

2 Case C - 362/14 Maximillian Schrems v Data Protection Commissioner

and the strategy the Commission followed when it did not suspend the agreement despite it being known to be not “safe”, needs to be considered. The notion of the Commission again unilaterally ruling on an “adequate level of protection” needs to be addressed with extreme caution. That CJEU judgement needs to be used as a reference and we need to be sure that the levels of protection are “essentially equivalent” to those guaranteed in the EU.

- International agreements as substitutes for adequacy decisions: Recital 49 mentions the possibility of using “legally binding bilateral agreements” as alternative grounds for transferring data to third countries based on adequacy decisions. The case of Safe Harbour has brought many doubts about the adequacy of these standards related specifically to data protection unless European standards are in place and enforcement and meaningful redress mechanisms are put in place. In addition, the fifteen years it took to bring an end to the illegal Safe Harbor agreement and the seven years it took to bring an end to the illegal Data Retention Directive strongly indicate that the judgement of the European Commission cannot be relied on to protect the fundamental rights of individuals. The reference in Recital 49 to agreements concluded between Europol and Eurojust and third countries is highly problematic, as not all of the already existing agreements comply with current data protection standards, especially not in the light of the recent CJEU judgments.
- In the context of transnational – indeed global – law enforcement data sharing, there is always a risk that in some countries the data could be used to support actions by state agencies that violate human rights, such as arbitrary arrest and detention, denial of due process, or even ill-treatment and torture. Any EU regulation that could relate to such possibilities should in our view contain a general human rights clause, on the following lines:
- “All persons or entities subject to this Directive shall take all possible steps to ensure that none of the processing subject to this Directive, and in particular no transfers of data covered by this Directive, will lead to serious violations of any of the rights guaranteed by the Charter of Fundamental Rights, by any persons or entities covered by this Directive, or by any other persons or entities to whom the data may be transferred, directly or indirectly. Such steps could include, for instance, human rights audits of possible recipient countries or persons or entities in such countries.”

  (Note that the words “transfers of data covered by this Directive” include transfers by any law enforcement agencies of the Member States to the

national security of the same Member State, or of other states: see our comment on article 7a, below).

Further concerns

Title of the Directive:

- *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties* ***or the safeguarding against and the prevention of the threats to public security,*** *and the free movement of such data*

This new addition to the title brings an important extension of the scope (positive, in the context of broad exemptions that are proposed in GDPR), however it is not clear what types of activities will be covered, e.g. whether it will relate to any activities of intelligence agencies (to the extent that they can fall in the EU's legal competence). This would raise questions related to data gathered pro-actively, and/or in bulk, on people who are not linked to any criminal activity - contrary to the protection of fair trial rights in Art. 6 ECHR and Art. 47 of the Charter.

Recitals

- Recital 11: It is unclear what types of bodies/entities are covered by this recital. Potentially it could include anyone from police officers to private companies performing law enforcement tasks that have been outsourced to them: "*Any body/entity entrusted by national law to perform duties or exercise public powers for the prevention, investigation, detection or prosecution of criminal offence or the execution of criminal penalties*";

- Recital 11a: The necessity of this recital is not certain. In particular, the notion of "*coercive measures*" has no particular meaning and should be defined or removed. Later on, the reference at the end which says that there can also be "other tasks" outside the scope of Union law (read: tasks related to national security) would leave these "tasks" outside the scope of both the GDPR and the LEDPD – and indeed outside of the protection of the Charter of Fundamental Rights[3].:

"*Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of the (…) Regulation EU/XXX*."

3For a more in-depth analysis, please see "EU-US Umbrella Agreement: Detailed Analysis by Douwe Korff". http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/

- Recital 11b: Due to the extension of the scope of the dDirective, there are respective changes in recitals. It is important to clarify what "*safeguarding against and the prevention of threats to public security*" means, what types of activities it covers and whether activities of agencies or units dealing with national security issues are regulated or exempted;
- Recital 16 includes wording "*data rendered anonymous in such a way that the data subject is no longer identifiable*": There is no need for defining the process of anonymisation, which can only lead to confusion with regard to the scope of the directive; if data no longer relate to an identifiable individual, it cannot be regarded as "personal data" and it would therefore fall outside of the scope of the directive. If such a reference is retained, at the very least the following words should be added at the end: "and cannot be reidentified by anyone processing the data or to whom the data are disclosed, e.g., by linking the data to other data that would allow such reidentification."
- Recital 17: Definitions given in this recital ("*which reveal information relating to the past, current or future physical or mental health of the data subject*") differ from the one given in Chapter 1: "*which reveal information about his or her health status*". The definitions in the recital refers to situations during the entire life of the subject while the one in Chapter 1 seems to refer only to the current health status. In reality, there is no such thing as "health data" about the future physical or mental health of an individual, there is only data which has been extrapolated from health data that gives indications of possible future physical or mental health.
- Recital 25a: The expression "*specific conditions applicable in specific circumstances*" is very unclear and provides no meaningful legal certainty.

Scope (art 2)

- Regarding the wording "*activity which falls outside the scope of Union law*" in Art. 2.3a: The scope of activity that falls within the scope of EU law, when it comes to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of the threats to public security, is very narrow; it would be helpful to specify – in the recitals – what types of activity will actually be covered by this instrument. this could be done, for example, by including explicit reference to title 4 and 5, part III of the Treaty on the Functioning of the EU.
- The relationship between the Directive and specific regulations covering Europol, Eurojust, SIS, VIS and Eurodac (in as far as they regulate activities performed by national bodies) should be clarified and harmonised, to ensure that all the regulations comply with the Charter, as interpreted by the CJEU.

Definitions (art 3)
- It is not clear how the directive will apply to authorities that investigate crimes and deal with threats to public security (that fall within the scope of the directive) but are also responsible for national security (that falls outside of the scope of EU law), for example the Polish ABW (Internal Security Agency).
- The distinction between activities related to “public security” and “national security” should be clarified in the recital. Furthermore, the concept of “national security” should itself be clearly defined and clarified – as is rightly demanded also in the recent resolution of the European Parliament on surveillance issues (29 October 2015).
- A definition of biometric data is missing.
- The definition of data concerning health in recital 17 is broader than definition in article 3. Generally, the concept of “health status”, which doesn't appear in the framework decision and appears to be more of a statistical term. It brings in issues of profiling, probabilities, and so on. Quite generally, all the definitions in the General Data Protection Regulation should also be applied, identically, in the context of the LEDP Directive.

Transmission of data (art 6)
Article 6 states that the competent authority “*shall **as far as practicable** verify quality of personal data before they are transmitted or made available*”. The phrasing “shall as far as practicable verify quality of personal data” refers to the act of verifying the data, which simply means checking the quality of the data. If the quality of the data is poor, the competent authority could still fulfil this requirement by verifying that the quality is poor. It does not mean ensuring that the data are sufficiently accurate or reliable and therefore of a quality that makes transfer worthwhile. If the text stated “ensuring the quality of personal data before…” that would make the phrase “as far as practicable” acceptable since ensuring the quality of data is a much stronger requirement than verifying their quality.

Specific processing conditions (art 7a):

- 7a.1 states that certain processing of personal data which falls “outside of the scope of the Union law” (e.g, “national security” activities by security agencies) will not be covered by neither the Regulation nor by the Directive. What the article really means is the following:

Personal data collected by competent authorities for the purposes set out in Article 1(1)" ***may*** "*be processed for other purposes than those set out in Article 1(1)*" ***when*** "*such processing is authorized by … Member State law (…)*" ***and*** *if* "*the processing is carried out in an activity which falls outside the scope of Union law.”*

With this in mind, it needs to be taking into consideration that any disclosure of data is a form of processing and thus, if a controller is subject to the GDPR or the Directive, "disclosing" the data to a national security agency for purposes of “national security” is subject to the GDPR or the Directive, even if the further processing of the data by the receiving national security agency is outside union law. However, in the current wording this provision explicitly and

inappropriately excludes such processing (i.e. Processing for the purpose of such disclosures) from the Directive.

If Article 43a of the European Parliament's first reading of the GDPR relating to enforced data disclosures in third countries is adopted (), the proposed Articles 7 and 7a as currently drafted would have the diametrically opposite effect. If adopted in this form, they would create a massive loophole in the law enforcement data sharing arrangements, allowing for potentially massive "leaking" of law enforcement data from law enforcement agencies in the Member States to the latter's national security agencies – including to national agencies with notorious further international data transfer practices.

Special categories of personal data (art 8)

- The wording should be made consistent with e.g. art 21 of the Charter *(1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.)*

Examples of appropriate legal safeguards regarding the processing of specific categories of personal data are only contained in recitals; provisions on minimum safeguards should be included in the main text.

Profiling (art 9)

The overall approach on profiling is deeply objectionable:

- Only decisions based on automated processing are covered, the generation of new personal data through profiling should also be specifically addressed and not only decisions based on profiling based on a fully automated process.
- The only safeguard provided is the requirement of legal authorisation; all other safeguards (in particular on transparency, right to obtain human intervention, etc) are missing.
- The general prohibition of using sensitive data in profiling is very weak: All that it is required is to have a legal basis.

Data transfers

- Transfers on the basis of an adequacy decision (art 34): The list of requirements to assess if the country or sector ensures an adequate level of protection is acceptable, as is the fact that the Commission would be obliged to monitor the functioning of the decision. The Commission could also decide that a specific country no longer ensures adequate level of protection, which could lead to repealing, amending or suspending the decision.

However, we believe that temporary suspension should not be a possibility but a requirement, as proven by the recent Safe Harbor ruling, in which the Court ruled that the Commission should have taken steps to suspend the agreement once it recognised that it was not safe. When a specific third country no longer ensures this adequate level of data protection, the Commission should have the obligation to suspend the decision and start negotiations with this country. The big problem is that, if there is a decision stating that a country no longer ensures an adequate level of protection (i.e. out of line with the primary law of the Union), transfers would still be possible on the basis of art 35 (appropriate

safeguards) or art. 36 (derogations). This is not an adequate solution and art 34.6 should be deleted, or limited only to urgent cases.
- Transfers by way of appropriate safeguards (art. 35): the provisions say that transfers are allowed if there are appropriate safeguards in legally binding instruments or if there is an assessment that such appropriate safeguard exists. First of all, there is a problem with the term "appropriate safeguards" since there is no clear definition of this term and there are no precise examples in recital 49. As explained above, this term should be replaced by the requirement of an "essentially equivalent" level of protection, both in terms of substantive law and as concerns independent oversight and the availability of effective judicial remedies to data subjects. Furthermore, there is a problem in (b) with the adequacy of using assessments prepared by the controllers themselves. This should be subject to the appropriate level of supervision of a public authority.
- Derogations (art 36): The options to permit derogations are quite broad. E.g.: "*(d) the transfer is necessary in individual cases for the purposes set out in Article 1(1)*". Derogations should only be allowed in exceptional cases, where there is an immediate threat to public security, or the life or health of individuals.
- Furthermore, art 36.2 says that a competent authority could block the transfer if the "*fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1*". We welcome the idea but more specific provisions should be included since otherwise it remains unclear how this would work.

- Transfers to private parties (rec 49a, art 36aa): There is no legal framework for such data transfers. Strict purpose limitation, data retention and prohibition of onward transfer need to be added.

This proposal allows data to be transferred directly to private parties in third countries. Rec. 49b gives example of this situation: "*in urgent cases when criminal offences have been committed by means of electronic communication technology like social networks, or where data generated by communication technology are relevant evidence of the perpetration of a criminal offence*".

We understand that this provision opens the ability to transfer data directly to Internet companies in third countries, without any public bodies involved. While the use of such procedure can be justified in some urgent matters relating to manifest, serious crimes (requesting data related to specific personally-identifiable data such as an IP address), it should not be treated as a standard procedure and additional safeguards for data subjects should be provided, in particular the obligation to notify both the data subject and the relevant Data Protection Authority (-ies) that such a transfer occurred.

Independent supervisory authorities (art 39-47)

- Art. 41.1: When the article mentions "*or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure*" it is not clear what specific body is meant – this should be clarified;

- Art. 46: Under the Directive, supervisory authorities do not have the power to impose financial sanctions. This competence is crucial to effectively exercise the activities demanded of them by this instrument.

Final provisions

- Art. 60: There is the need to include a deadline (e.g. 3 years after the entry of the directive into force) to evaluate international agreements covering transfers of personal data to third countries or international organisations, which were concluded by Member States prior to the entry into force of the directive.
- Art. 61: The evaluation of the Directive should be made sooner than after 5 years (e.g. two or three years would be more appropriate).