University of Groningen

Law enforcement access to personal data originally collected by private parties

Jasserand, Catherine

Published in:
Computer Law & Security Review

DOI:
[10.1016/j.clsr.2017.08.002](https://doi.org/10.1016/j.clsr.2017.08.002)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2018

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Jasserand, C. (2018). Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680? *Computer Law & Security Review*, 34(1), 154-165. <https://doi.org/10.1016/j.clsr.2017.08.002>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?

Catherine Jasserand *

STeP (Security, Technology & e-Privacy) Research Group, University of Groningen, The Netherlands

ABSTRACT

Keywords:

Data protection
Directive 2016/680
Law enforcement access
Safeguards
Duty of notification
Purpose limitation
Digital Rights Ireland case
Tele2 Sverige case

Access by law enforcement authorities to personal data initially collected by private parties for commercial or operational purposes is very common, as shown by the transparency reports of new technology companies on law enforcement requests. From a data protection perspective, the scenario of law enforcement access is not necessarily well taken into account. The adoption of the new data protection framework offers the opportunity to assess whether the new 'police' Directive, which regulates the processing of personal data for law enforcement purposes, offers sufficient safeguards to individuals. To make this assessment, provisions contained in Directive 2016/680 are tested against the standards established by the ECJ in *Digital Rights Ireland* and *Tele2 Sverige* on the retention of data and their further access and use by police authorities. The analysis reveals that Directive 2016/680 does not contain the safeguards identified in the case law. The paper further assesses the role and efficiency of the principle of purpose limitation as a safeguard against repurposing in a law enforcement context. Last, solutions to overcome the shortcomings of Directive 2016/680 are examined in conclusion.

© 2017 Catherine Jasserand. Published by Elsevier Ltd. All rights reserved.

1. Introduction

Law enforcement authorities around the globe have a growing appetite for personal data held by private parties and

initially collected for a purpose different from law enforcement. Many examples can illustrate this trend: the huge amount of law enforcement requests made to high-tech companies at global level,¹ the case of the transfer of passenger name record data (air traveller data) to police authorities² or the retention

* European and Economic Law Department, STeP (Security, Technology & e-Privacy) Research Group, University of Groningen, PO Box 72, 9700 AB Groningen, The Netherlands.

E-mail address: c.a.jasserand@step-rug.nl.

¹ For the second half-year 2016, Microsoft reported more than 25,000 law enforcement requests to disclose content, subscriber data or transactional data at global level, see <https://www.microsoft.com/about/csr/transparencyhub/leerr>; compare with Apple's and Google's reports for the same period, available at respectively <https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf> and at <https://transparencyreport.google.com/user-data/overview>; see also Oleg Afonin, 'Government request reports : Google, Apple and Microsoft' on ElcomSoft blog, 16 January 2017, available at <https://blog.elcomsoft.com/2017/01/government-request-reports-google-apple-and-microsoft/> [all websites have been last accessed on 01 August 2017].

² On the Passenger Name Record, see International Civil Aviation Organization, 'Guidelines on Passenger Name Record (PNR) Data', first edition 2010, available at https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf, Section 2.1.; See also Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offence and serious crime, OJ 2016, L 119/132. <https://doi.org/10.1016/j.clsr.2017.08.002>

of telecommunications data by Internet Service Providers (personal data retention) for further use by law enforcement authorities.³

Other examples for which the number of requests for access might not be publicly known could follow. Given their characteristics, one could think of the value that some types of personal data have for law enforcement authorities. This is the case of biometric data (such as fingerprints), which has been used for many decades by police authorities to identify individuals.⁴ Private parties rely more and more on biometric data to control access to buildings, IT systems or applications. Several social media companies, e.g. Facebook, have even constituted biometric databases based on the facial images of their users. In Europe, Facebook stopped facial recognition in 2012, whereas in the USA the company is still collecting such personal data.⁵ Of course, Facebook has more personal data than its users' facial images: it might also hold names (real or alias), date of birth, addresses, phone numbers and any kind of personal information a user is willing to provide under their profile. All this personal data, including biometric data, constitutes valuable information for criminal intelligence and criminal investigation.⁶ Criminal intelligence is a form of surveillance carried out by law enforcement authorities to gather information about crime or criminal activities before their occurrence or to establish their occurrence.⁷ It differs from criminal investigation, which corresponds to a procedural stage in relation to concrete criminal activities.⁸ These two activities are covered in this paper.

From a data protection perspective, the obvious questions that arise from this scenario are which legal framework applies to the case of law enforcement access to personal data held by private parties, and whether that framework provides sufficient safeguards to data subjects. The adoption of a new data

protection framework at EU level constitutes an excellent opportunity to assess the rules applicable to the scenario at that level. Adopted in April 2016, the new data protection framework is composed of a General Data Protection Regulation (Regulation 2016/679 or GDPR)⁹ - replacing the Data Protection Directive -¹⁰ and of a Directive on the protection of personal data processed for law enforcement purposes (Directive 2016/680 or the 'police' Directive).¹¹ The 'police' Directive replaces the Council Framework Decision 2008/977/JHA adopted under the previous pillar structure.¹² Directive 2016/680 defines the rules applicable to the processing of personal data for law enforcement purposes and more specifically for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."¹³ The phrase 'law enforcement purposes' should therefore be understood, in the context of this article, as referring to the purposes regulated in Directive 2016/680. The Directive does not explicitly define the different purposes but relies on national laws. Criminal investigation purposes as well as criminal intelligence purposes can therefore fall within the scope of Directive 2016/680.

Against this background, the next section, [Section 2](#), addresses the applicability of both the GDPR and the 'police' Directive to the scenario described in this article: provisions contained in the GDPR govern the initial processing of personal data by private parties, whereas rules set out in the 'police' Directive cover the further processing of the data by law enforcement authorities. After having established that the further processing of personal data falls within the scope of Directive 2016/680, [Section 3](#) analyses the rules of that Directive to determine whether they lay down sufficient safeguards to protect individuals whose personal data is accessed by law enforcement authorities. The rules are assessed against the standards established by the European Court of Justice (ECJ) in two related judgments on the retention of personal data. *Digital Rights Ireland*¹⁴ and *Tele2 Sverige*¹⁵ are particularly

³ See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006, L 105/54.

⁴ E.g. S.A. Cole, *Suspect Identities: a History of Fingerprinting and Criminal Investigation* (Harvard Press University, 2001).

⁵ It should be noted that the collection, storage, retention and subsequent use of facial images by Facebook have been challenged in Illinois for the lack of informed consent from the individuals concerned, see recent developments <http://www.breitbart.com/tech/2017/01/03/class-action-lawsuit-filed-facebook-holding-biometric-data-potentially-violating-illinois-law/>.

⁶ See for example, <https://www.theguardian.com/technology/2014/apr/11/facebook-2000-data-requests-police>.

⁷ Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ 2006, L 386/89; See Article 2 (c) that reads as follows: "crime and criminal activities with a view to establish whether concrete criminal acts have been committed or may be committed in the future."

⁸ Council Framework Decision 2006/960/JHA, see Article 2 (b) that reads as follows: "a procedural stage within which measures are taken by competent law enforcement authorities or judicial authorities, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts."

⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016, L119/1.

¹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31.

¹¹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L.119/89.

¹² Before the entry into force of the Lisbon Treaty, the EU policy areas were divided into three pillars. The first pillar was composed of the economic communities, whereas the third one regrouped police and judicial matters in criminal matters, see e.g. Catherine Barnard & Steve Peers, *European Union Law* (Oxford University Press, 2014).

¹³ Article 1 of Directive 2016/680.

¹⁴ Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* [2014], ECLI:EU:C:2014:238.

relevant to the scenario of law enforcement access to personal data held by private parties as they both relate to the retention of data for later access and use by law enforcement and national securities authorities. [Section 3](#) discusses the two cases and extracts the relevant findings in an attempt to apply them to the provisions of Directive 2016/680. Finally, [Section 4](#) addresses the issue of the change of initial purpose and critically assesses the principle of purpose limitation as a safeguard against abuses or misuses.

2. Applicable legal instrument: the GDPR or the ‘police’ directive?

This section considers which legal instrument is applicable to the scenario of law enforcement access to personal data initially collected by private parties for a non-law enforcement purpose. It provides some background on the negotiations of the ‘police’ Directive and explains how the diverging positions of the EU institutions on the issue of law enforcement access have resulted in the adoption of complicated recitals on the topic. It concludes that both the GDPR and the ‘police’ Directive apply to the scenario.

2.1. Positions of the EU institutions: between hesitation and divergence

The GDPR and the ‘police’ Directive build a bridge between them on the issues of the further processing of personal data for a purpose falling under the scope of each other’s instrument. Recital 11 of Directive 2016/680 evokes the scenario of personal data collected for a law enforcement purpose and further processed for a non-law enforcement purpose. In that case, the further processing is covered by the GDPR. Recital 19 of the GDPR describes the other-way around scenario and provides for the applicability of Directive 2016/680 to the further processing by law enforcement authorities of personal data initially collected for a non-law enforcement purpose. However, both scenarios are worded in a complicated manner.¹⁶ It could be that the wording results from the divergent approaches defended by the EU institutions during the negotiations of the new data protection framework, and in particular of the draft ‘police’ Directive.

¹⁵ Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and others*, [2016] ECLI:EU:C:2016:970.

¹⁶ Recital 11 of Directive 2016/680 refers to “other bodies or entities entrusted by Member State law to exercise public authorities and public powers for the purpose of this Directive [i.e. Directive 2016/680]” and explains that “where such a body or entity processes personal data for purposes other than for the purposes of this Directive [i.e. Directive 2016/680], Regulation (EU) 2016/679 applies.”; whereas Recital 19 of Regulation 2016/679 specifies that “personal data processed by public authorities under this Regulation should, when used for those purposes [which are purposes of prevention, investigation, detection or prosecution of criminal penalties], be governed by a more specific Union legal act, namely Directive (EU) 2016/680.”

In January 2012, the European Commission published a proposal for a ‘police’ Directive that did not contain any reference to the scenario of law enforcement access to personal data collected by third parties. Yet, a few months before, Statewatch, a civil liberties organisation, leaked a draft version of the proposal which included an article containing procedural safeguards specific to the access by law enforcement authorities to personal data initially collected for purposes other than law enforcement.¹⁷ Those very detailed safeguards comprised: (a) the persons entitled to have access to the personal data under the condition that the data met a “reasonable ground standard”; (b) a written request referring to the legal basis on which the request was made; and (c) the adoption of “appropriate safeguards” defined by the Member States, which could include, among others, a prior judicial review of the request.¹⁸ This draft never saw the light of day and the official proposal for the ‘police’ Directive did not contain any specific provisions on that issue.

During the negotiations on the proposal for the ‘police’ Directive, the European Parliament brought the issue back on the table and proposed a new article on “law enforcement access to personal data collected for a different purpose.”¹⁹ In that amendment, the usage of the personal data initially collected for a different purpose could only be limited to “investigation” or “prosecution of criminal offences”.²⁰ However, the other institutions did not endorse the amendment. With the exception of one delegation, the Council did not support the amendment and adopted a political agreement on the proposal without such a provision.²¹ As for the European Commission, it stated that it was not able to fully endorse the amendment. It argued that there was a risk of confusion –without specifying on which topic– and of non-compliance with international agreements, such as the Passenger Name

¹⁷ See draft version of a ‘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, and the free movement of such data’ (“Police and Criminal Justice Data Protection Directive”), version 34, 29 November 2011, see Article 4, (2)(a)-(c), available at <http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf>.

¹⁸ Article 4 (2)(c) of the leaked draft version of a proposal for a “Police and Criminal Justice Data Protection Directive.”

¹⁹ European Parliament legislative resolution of 12 March 2014 on the 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, and the free movement of such data (COM(2012)0010 – C7-0024/2012- 2012/0010(COD))(Ordinary legislative procedure : first reading), Article 4a.

²⁰ *Ibid.*

²¹ See Council, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regards 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, FN 130, Austrian delegation, LIMITE doc. no 7740/15, 14 April 2015.

Record and the Terrorist Tracking Programme.²² Those arguments are very surprising and not very convincing: the Commission justified its position by referring to controversial agreements providing foreign law enforcement authorities (mainly US ones) access to EU citizens' personal data.

In fine, the adopted provisions contained in the GDPR and the 'police' Directive seem to reflect the divergence of the EU institutions on this issue.

2.2. Two sets of rules governed by two different instruments

The scenario of law enforcement access to personal data generated by private parties for a non-law enforcement purpose can be split into the 'initial purpose of collection,' subject to the GDPR, and the 'purpose of further processing,' governed by Directive 2016/680.

In the scenario under review, the *initial purpose of data collection* mostly relates to customer data collected by private parties. Provided it complies with the conditions set out in Article 2(1) GDPR, the initial purpose of collection is subject to the rules contained in the GDPR.²³ The collection of personal data is also an example of processing activities explicitly covered by the GDPR.²⁴

The *further processing* of personal data held by private parties falls within the scope of Directive 2016/680 if the data is further processed for a law enforcement purpose. As already explained, on this issue, Recital 19 GDPR builds a bridge between the GDPR and Directive 2016/680. One could still regret that the applicability of the 'police' Directive is only mentioned in a non-binding provision. Law enforcement access to and use of personal data should therefore fall in the category of data processing operations, as set out in Article 3(2) of Directive 2016/680.

A discussion can ensue on the exact meaning of the term 'access'. Access is not included in the list of processing operations given as examples in Article 3(2) of Directive 2016/680.²⁵ The term is also ambiguous: it can refer to different processing

operations ('consultation' or 'disclosure') involving different actors (private parties providing the access to the data or law enforcement getting access to them) and be thus subject to different rules. If disclosure of personal data by private parties to law enforcement authorities seems to fall within the remit of the GDPR, 'consultation' of that data by law enforcement authorities could be subject to diverging interpretations. One could argue that 'consultation' by law enforcement authorities is nothing more than 'making available' the personal data to law enforcement authorities and thus disclosure. But at the same time, 'consultation' could also be considered a processing subject to the 'police' Directive if personal data is, for instance, consulted by law enforcement authorities in the context of a criminal investigation. Approaching the term from its terminological and operational meaning might be too simplistic to determine which legal instrument applies.

Trying to understand the meaning of 'access' is not a rhetorical issue since it has been mentioned in the case law of the ECJ on data retention. However, one cannot but notice that the case law does not bring much clarity on the status and meaning of 'access'. In case C-301/06 relating to the validity of the legal basis on which the Data Retention Directive had been adopted,²⁶ the Court found that the Data Retention Directive regulated the retention of personal data but not its access or use by law enforcement authorities.²⁷ By contrast, in *Digital Rights Ireland* and more clearly in *Tele2 Sverige* – both described at length in the next section – the Court viewed the operation of law enforcement access to the retained data as an accessory to the retention of personal data and extended the application of EU law to the operation of access.²⁸ The Court justified it through the link existing between the purpose of retention of the data and its use.²⁹ As noted by Woods, the Court refused to make a distinction between retention and access to the retained data and therefore to exclude access from the scope of EU law.³⁰ It should be observed that *Digital Rights Ireland* and *Tele2 Sverige* were decided before the adoption of the new data protection framework. Under the new rules, access by law enforcement authorities for a law enforcement purpose should fall within the scope of Directive 2016/680 and be distinct from retention of data processed for a non-law enforcement purpose. In any case, in this paper, what matters is the purpose for which

²² Extracted from the leaked 'Commission position on EP amendments on 1st reading': "have or risk having the effect of prohibiting lawful access by competent law enforcement authorities to PNR [Passenger National Register], TFTP [Terrorist Finance Tracking Programme] or other relevant personal data as provided for under international agreements conclude by the Union or existing or proposed legal instrument"; TFTP is an 'Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the terrorist finance tracking program', OJ 2010, L 8/11, 13 January 2010; and council decision on the agreement, OJ 2010, L 195/5.

²³ Article 2(1) GDPR defines the scope of the Regulation as follows: "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

²⁴ Article 4(2) GDPR defines the term 'processing' and provides as examples "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (emphasis added)

²⁵ Processing is defined in identical terms in Article 3(2) of Directive 2016/680 and Article 4(2) GDPR; consultation and disclosure are both examples of processing activities.

²⁶ Case C-301/06, *Ireland v. European Parliament and Council* [2009] ECLI:EU:C:2009:68.

²⁷ Case C-301/06, para. 80; see also Article 4 of Directive 2006/24.

²⁸ *Tele2 Sverige*, para. 76.

²⁹ *Tele 2 Sverige*, para. 80: "since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services."; see also Opinion of A.G. Sautmandsgaard ØE in *Tele2 Sverige*, para. 125: "the *raison d'être* of a data retention obligation is to enable law enforcement authorities to access the data retained, and so the issue of the retention of data cannot be entirely separated from the issue of access to that data."

³⁰ Lorna Woods, 'Data retention and national law: the ECJ ruling in joined cases C-203/15 and C-698/15 *Tele2* and *Watson* (Grand Chamber)', blogpost, available at <http://eulawanalysis.blogspot.nl/2016/12/data-retention-and-national-law-ecj.html>

privately held personal data is further accessed and not whether access means ‘consultation’ by law enforcement authorities or ‘disclosure’ by private parties.

As described in this section, the GDPR applies to the initial purpose of collection, whereas the ‘police’ Directive applies to the further processing of the same data by law enforcement authorities. Although both texts acknowledge the scenario and determine the instrument applicable thereto, they do not contain specific rules applicable to the law enforcement access to personal data collected for a different purpose. Yet Opinion 03/2015 of the Article 29 Data Protection Working Party (A29WP)³¹ on the proposal for a ‘police’ Directive recommended: “any processing for a purpose different than the specific one for which the data was originally processed should always have its own legal basis including clear and specific safeguards.”³² If it is established that the further processing for a law enforcement purpose of personal data held by private parties has a legal basis,³³ one can still wonder if Directive 2016/680 contains clear and specific safeguards to ensure the protection of individuals whose personal data is accessed. This issue is addressed in the next section.

3. Existence of ‘substantive and procedural’ safeguards in directive 2016/680?

Besides facilitating the free movement of personal data in the area of law enforcement, Directive 2016/680 aims at ensuring the same level of protection of individuals’ rights through the EU.³⁴ According to Recital 26 of Directive 2016/680, safeguards are an element of fair processing that should ensure that individuals are able to exercise their rights in a law enforcement context. This section will assess whether the provisions of Directive 2016/680 provide sufficient safeguards for the protection of individuals whose personal data initially collected by private parties is accessed by law enforcement authorities. To make this assessment, the paper builds on the ‘standards’ established by the European Court of Justice in its jurisprudence on data retention, i.e. in *Digital Rights Ireland*³⁵ and *Tele2 Sverige*³⁶. The first case relates to the EU data retention framework, i.e. the Data Retention Directive (or Directive 2006/24), the second one to national data retention frameworks (the Swedish and UK frameworks) as described below.

3.1. Preliminary remarks on the use of *Digital Rights Ireland* and *Tele2 Sverige* as benchmark

The two judgments are relevant to the scenario of law enforcement access even if they relate to slightly different situations. Indeed, in *Digital Rights Ireland* and *Tele2 Sverige*, the laws at stake cover traffic data collected by telecoms operators for their own usage and retained to be accessed (and further used) by law enforcement authorities. The laws impose an obligation to retain the data. By contrast, in the scenario under consideration, personal data is collected by private parties for their own use (or at least for a non-law enforcement purpose) and is then accessed by law enforcement authorities. Private parties are under no obligation to retain personal data for law enforcement access, they simply make the data available upon request. This is an important precision since the scenario under review does not relate to mass collection or mass retention of personal data. To illustrate it, one could think of the situation where an employer collects his employees’ fingerprints to give them access to secured buildings.³⁷ A criminal offence is then committed on the work premises. The police authorities request access to the biometric data files held by the employer to compare them with the biometric data found on site. In that specific scenario, what matters are the rules applicable to law enforcement authorities to get access to that data. However, despite the differences between the scenarios, the ECJ’s rulings in *Digital Rights Ireland* and *Tele 2 Sverige* also cover the issue of law enforcement access to the retained data in addition to the issue of data retention itself. It is precisely the way the ECJ approaches the issue of access that is relevant in the context of this paper.

There is also enough evidence to believe that the findings of *Digital Rights Ireland* and *Tele2 Sverige* apply to legislative measures beyond metadata retention.³⁸ The European Parliament and the European Commission have both addressed the issue of the impact of the *Digital Rights Ireland* judgment on other EU legislation. Prior to the adoption of the ‘police’ Directive, the legal service of the European Parliament delivered an opinion on the consequences of *Digital Rights Ireland*.³⁹ Since at that time, national legislations on the processing of personal data for law enforcement authorities fell outside the scope

³¹ A29WP is an independent advisory body to the European Commission on data protection matters, see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

³² A29WP, ‘Opinion 03/2015 on the draft 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’, 1 December 2015, 3211/15/EN, WP233.

³³ Recital 19 GDPR.

³⁴ Recitals 7 and 15 of Directive 2016/680.

³⁵ *Digital Rights Ireland*.

³⁶ *Tele2 Sverige*.

³⁷ e.g. guidelines by the Irish Data Protection Commission on ‘biometrics in the workplace’, <https://www.dataprotection.ie/docs/Biometrics-in-the-workplace/m/244.htm>; position of the French data protection authority (CNIL) on the use of biometric systems to control access to working places, <https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail>.

³⁸ See also Franziska Boehm and Mark Cole, ‘Data Retention after the Judgement of the Court of Justice of the European Union’, 2014 in which the authors assess the impact of the DRI judgment on other Data Retention Measures, available at https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

³⁹ Legal Service of the European Parliament, leaked document, legal opinion “LIBE- Questions relating to the judgment of the Court of Justice of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others*- Directive 2006/24/EC on data retention- Consequences of the judgment” para. 80, 22 December 2014, available at <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf>.

of EU law,⁴⁰ it considered that the rules on law enforcement access to and use of personal data collected for a different purpose were not necessarily impacted by the judgment. However, it also acknowledged that its position would be different if and when the proposal for a ‘police’ Directive would be adopted.⁴¹ A few months later, the European Parliament asked the European Commission to assess the possible impact of *Digital Rights Ireland* on the proposed Passenger Name Record (PNR) Directive.⁴² In its answer to the European Parliament, the European Commission opined that the judgment set up a framework to assess EU legislation on “the general collection and processing for law enforcement purposes of personal data of individuals.”⁴³ The Commission acknowledged in particular that the findings of the *Digital Right Ireland* case should be taken into account in the assessment of the proposal for a PNR Directive.⁴⁴

As for *Tele2 Sverige*, the judgment assesses the impact and application of the *Digital Rights Ireland* judgment to national data retention regimes. Because of the scope of Directive 2016/680,⁴⁵ it can be strongly asserted that its findings apply to national legislation relating to the collection of personal data by third parties and to its further processing by law enforcement authorities.

3.2. The benchmark set by *Digital Rights Ireland* and *Tele2 Sverige*

The Data Retention Directive was ‘struck down’ by the ECJ in *Digital Rights Ireland*; whereas national data retention measures still in place (Sweden) or adopted after the invalidation of the Directive (UK) were declared incompatible with EU law in *Tele 2 Sverige*. These two cases have a strong connection. Following the invalidation of the Data Retention Directive, national measures on data retention still had to be compliant with EU law, and in particular, with the e-privacy Directive (or Directive 2002/28/EC) adopted before the Data Retention Directive. Article 15(1) of that Directive expressly allows Member States to adopt data retention measures under specific conditions.

⁴⁰ The only data protection framework applicable in the context of law enforcement was the Council Framework Decision 2008/977/JHA that only covered cross-border processing for law enforcement purposes, see Recital 7 and Article 1 of Council Framework Decision 2008/977/JHA.

⁴¹ Opinion of the European Parliament (2014), footnote 62 reads as follows: “it [i.e. the draft Directive] will bring important changes to the Union’s data protection law in the area of criminal law, in comparison to act currently in force, i.e. Council Framework Decision 2008/977/JHA.”

⁴² European Parliament, ‘resolution of 11 February 2015 on anti-terrorism measures’, 2015/2530 (RSP), Point 13, available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONGML+TA+P8-TA-2015-0032+0+DOC+PDF+VO//EN>.

⁴³ See European Commission’s answer to the European Parliament on the PNR proposal and the consequences of the DRI judgment, as leaked by StateWatch, available at <http://statewatch.org/news/2015/mar/eu-com-eu-pnr-letter.pdf>; the European Commission referred to ‘legislation’ in general but one understands that its reasoning focuses on EU legislation and not on national legislation.

⁴⁴ Ibid.

⁴⁵ Covering both domestic and cross-border data processing.

It is against that provision that the ECJ had to determine the compliance of the Swedish and UK measures in *Tele2 Sverige*.

In *Digital Rights Ireland*, two national jurisdictions, the High Court of Ireland and the Verfassungsgerichtshof (Austrian Constitutional Court), brought a request for preliminary rulings before the ECJ on the validity of the Data Retention Directive. The national courts contested the compatibility of the Directive with Articles 7, 8 and 11 of the Charter of Fundamental Rights.⁴⁶ In *Tele2 Sverige*, a Swedish administrative Court and a UK Court of Appeal referred preliminary questions to the ECJ on the compatibility of respectively the Swedish laws on data retention⁴⁷ and the UK DRPIA⁴⁸ with the e-privacy Directive as well as with Articles 7 and 8 of the Charter of Fundamental Rights.⁴⁹

3.2.1. Elements of the benchmark

In both cases, the ECJ had to assess whether the data retention regimes at EU or national level constituted an interference with the right to privacy (Article 7 of the Charter) and with the right to data protection (Article 8 of the Charter) and if so, whether this interference was justified in application of Article 52(1) of the Charter.

3.2.1.1. *Existence of interferences?* In each case, the Court did not find one but several interferences. First, the obligation to retain data and give law enforcement authorities access to it constitute two distinct interferences with the right to privacy.⁵⁰ Then, without although much explanation, the ECJ ruled in *Digital Rights Ireland* that the Data Retention Directive also constituted an interference with the right to data protection on

⁴⁶ *Digital Rights Ireland*, para. 23 ; the national Courts asked the ECJ to review the compatibility of the Data Retention Directive with other EU provisions (Article 41 of the Charter, Article 52, para. 3, 4 and 7 of the Charter and Article 8 of the European Convention of European Rights); at national level, proceedings against national measures implementing the Data Retention Directive were brought by the advocacy group *Digital Rights Ireland* in Ireland and by more than 11.000 applicants and the regional Government of Carinthia in Austria.

⁴⁷ *Tele2 Sverige*, para. 15 and 16, respectively the Law 2003:389 on electronic communications (*Lagen (2003:389) om elektronik kommunikation* or LEK) and Regulation 2003:396 on electronic communications (*Förordningen (2003 :396) om elektronisk kommunikation*); the Code of Judicial Procedure (*Rättegångsbalken* or RB) and Law 2012 :278 on the collection of data on electronic communications in the law enforcement authorities’ investigative activities (*Lagen (2012 :278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas undersökningsverksamhet*).

⁴⁸ Opinion AG Saugmandsgaard ØE, *Tele2 Sverige*, para. 34 and 35, the data retention regime governed by the Data Retention and Investigatory Powers Act 2014 (DRIPA), the Data Retention Regulations 2014 (SI 2014/2042) and the Retention of Communications Data Code of Practice and the rules on access to communications data as defined in the Regulatory Investigatory Act 2000 as amendment by the Regulation of Investigatory Powers Order 2015 and the Acquisition and Disclosure of Communications Data Code of Practice, ECLI:EU:C:2016:572.

⁴⁹ At national level, proceedings were brought by *Tele2 Sverige*, a Swedish telecommunications provider that stopped retaining traffic data the day after the DRI judgment was delivered, and by three individuals who challenged the new UK data retention regime adopted after the invalidation of the DRI judgment; for more details, para. 48 et seqs. and para. 55 et seqs.

⁵⁰ *Digital Rights Ireland*, para 32 et seqs.; *Tele2 Sverige*, para. 100.

the ground that “it provides for the processing of personal data.” The Court clearly missed the opportunity to explain the nature and characteristics of metadata and the reasons why metadata should be considered personal data.⁵¹ In *Tele2 Sverige*, the Court put more emphasis on the distinction between the interference based on the retention of data and the interference based on access to that retained data by law enforcement authorities.

3.2.1.2. Justifications. After having established the existence of interferences, the Court assessed whether they were justified in application of Article 52(1) of the Charter. Article 52(1) sets the conditions under which fundamental rights, such as the rights to privacy and data protection, can be limited. First, limitations must be “provided by law”. Second, they must “respect the essence of those rights.” Third, they must comply with the principle of proportionality, meaning they must “[be] necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.”⁵² The assessment of the Court in the two cases is different: in *Digital Rights Ireland*,⁵³ the Court analysed in details the different conditions under which derogations to the fundamental rights are permitted, whereas in *Tele2 Sverige*, the Court mainly focused on the proportionality of the national laws derogating to the principle of confidentiality.⁵⁴ Yet it is precisely on the last condition of Article 52(1) of the Charter, i.e. the test of proportionality that both the Data Retention Directive and the national measures failed. The Court found that the Data Retention Directive and the national measures under review were not proportionate since they went beyond to what was strictly necessary.

In *Digital Rights Ireland*, the Court held that the Directive did not “lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards” for the persons affected by the measures of data retention.⁵⁵ More specifically, concerning the law enforcement access to retained data, the Data Retention Directive did not provide any limits.⁵⁶ The Court found that the Directive failed to define an ‘objective criterion’ to limit law enforcement access⁵⁷ and also failed to provide “substantive and

procedural conditions” on access and further use of the retained data by law enforcement authorities. In particular, the Court found that the Directive did not identify who could have access to the retained data and did not set a procedural rule imposing a prior independent review of the request for access.⁵⁸

In *Tele2 Sverige*, the ECJ confirmed the conditions identified in *Digital Rights Ireland*. Concerning the objective of the national instruments, the Court held that national laws must determine the conditions of access to ensure that access is limited to what is strictly necessary but at the same time, national legislation must adopt “substantive and procedural conditions governing the access” to the retained data by law enforcement authorities.⁵⁹ On that matter, the Court reiterated the conditions set out in *Digital Rights Ireland* in relation to the Data Retention Directive. Those include the (number of) persons entitled to get access to the retained data as well as a judicial or administrative prior review of the request for access.⁶⁰ In *Tele2 Sverige*, building on the case law of the European Court of Human Rights,⁶¹ the ECJ specified that “access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning or having committed a serious crime or of being implicated in one way or another in such a crime.”⁶² Thus, a link with a serious criminal activity is necessary. The Court added an extra safeguard to allow individuals to exercise their right of remedy: the Court imposed a duty of notification on law enforcement authorities that have accessed the retained data. They have the obligation to inform individuals, according to their national laws, that their data has been accessed, as soon as this notification can no longer prejudice the investigations.⁶³ The Court thus considered that this obligation of information has to be implemented in national procedural laws.

In conclusion, on the issue of access to retained data, the Court set out ‘procedural and substantive conditions’ to frame that access. Laid down in *Digital Rights Ireland* and confirmed in *Tele2 Sverige*, EU or national measures relating to the collection of personal data and its further processing for law enforcement purposes should contain: an objective criterion to define how and when law enforcement authorities should be granted access to the data; a procedural rule on an independent prior review of the request for access, and the obligation to notify individuals whose personal data has been accessed. The next sub-section applies the findings of *Digital Rights Ireland* and *Tele2 Sverige* to determine whether Directive 2016/680 contains the conditions necessary to govern law enforcement access to personal data collected by private parties for a non-law enforcement purpose.

3.3. Application of the rulings to directive 2016/680

Preliminarily, it should be observed that *Digital Rights Ireland* was decided while Directive 2016/680 was being negotiated.

⁵¹ It is quite relevant to wonder which type of info metadata can reveal about an individual, see for instance Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, ‘Evaluating the privacy properties of telephone metadata’, Proceedings of the National Academy of Sciences of the United States of America, vol. 113, no. 20, 2013, p. 5536-5541; see also the position of the A29WP that considers metadata as personal data in ‘Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes’, where it states that: “Unlike in other countries, in Europe, metadata are personal data and should be protected”, 4.

⁵² Article 52(1) of the Charter of Fundamental Rights.

⁵³ *Digital Rights Ireland*, para. 39 seq.; the Court assessed whether the Data Retention Directive infringed the essence of the rights to privacy and data protection (it did not) and checked whether the objective of the data retention directive constituted an objective of general interest (it did as it aimed at fighting serious crime).

⁵⁴ *Tele 2 Sverige*, para. 95 seq.

⁵⁵ *Digital Rights Ireland*, para. 34.

⁵⁶ *Digital Right Ireland*, para. 60.

⁵⁷ *Digital Rights Ireland*, para. 61: “must be restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.”

⁵⁸ *Digital Rights Ireland*, para. 62.

⁵⁹ *Tele2 Sverige*, para. 118.

⁶⁰ *Digital Rights Ireland*, para. 62; *Tele2 Sverige*, para. 118.

⁶¹ In particular, ECtHR, Grand Chamber, Roman Zakharov v. Russia, application no. 47143/06, 04 December 2015.

⁶² *Tele2 Sverige*, para. 119.

⁶³ *Tele2 Sverige*, para. 121.

Therefore and for the reasons explained in the previous subsection, its findings should have been taken into account and ‘implemented’ in Directive 2016/680. One should expect to find in the Directive the conditions identified in *Digital Rights Ireland*, i.e. the number of persons allowed to access the personal data as well as a procedure of prior review of the request for law enforcement access. By contrast, *Tele2 Sverige* was decided after the adoption of Directive 2016/680. It is therefore logical that its findings, and in particular, the obligation of notification, might not be found in Directive 2016/680.

This section suggests a reading of the safeguards established in *Digital Rights Ireland* and *Tele2 Sverige* in the broader context of law enforcement access to personal data held by private parties. If the safeguards have not been established for that specific scenario, they can still apply since the findings of the judgments reach beyond data retention measures.⁶⁴

3.3.1. Objective criteria to determine law enforcement access
First, the objective of Directive 2016/680 is to lay down data protection rules when personal data is processed by law enforcement authorities for “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention and the prevention of threats to public security.”⁶⁵ This objective is a general objective of fighting crime. As such, it constitutes an objective of general interest.⁶⁶ However, the objective of fighting crime is not enough to grant access to law enforcement authorities. In *Digital Rights Ireland* and *Tele2 Sverige*, the Court considered that the objective should at least be an objective of fighting serious crime.⁶⁷ Access to retained data needs to be justified by the nature of the crime. However, in the scenario under review, personal data is not retained for future access by law enforcement authorities; it is only made available if requested. As such, in a criminal investigation context, it seems difficult to argue that law enforcement authorities should only get access to personal data relating to serious crime. However, in the context of criminal intelligence where indices that a criminal activity has occurred or will occur are not established yet, it would make sense to limit the access to personal data that is linked to serious crime, to prevent the mass surveillance of individuals. Thus concerning the objective criterion of the conditions of access, a distinction between criminal investigation and criminal intelligence is necessary in relation to the nature of the criminal activity at stake. Yet Directive 2016/680 does not establish such a distinction.

Moreover, what is missing from Directive 2016/680 is the identification of individuals authorised to have access to the personal data collected for a different purpose (staff of law enforcement authorities) and the categories of personal data that should be accessible (personal data from suspects, criminals, witnesses, etc). On this issue, the leaked version of the draft ‘police’ Directive of 2011 contained a specific provision. Article 4(2)(a) proposed restraining the access to cases where “reasonable grounds give reason to consider that the processing

of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.”⁶⁸

3.3.2. Oversight mechanism: prior review of the request for access?

In *Digital Rights Ireland*, the ECJ ruled that law enforcement access to retained data should be subject to a prior review, either by a Court or by an independent administrative body. The procedure should be part of national criminal procedural law.⁶⁹ The ECJ leaves some leeway to Member States in the implementation of the review mechanism. The question is whether Directive 2016/680 contains a procedural safeguard that ensures prior review of the request for access to personal data.

Article 28 of Directive 2016/680 provides for an oversight mechanism. It requires the ‘prior consultation’ of the national data protection authority (DPA) in two cases:⁷⁰ when a data protection impact assessment has been performed and no risk-mitigating measure has been adopted (Article 28(1)(a)) or when a specific processing “involves a high risk to the rights and freedoms of individuals” (Article 28(1)(b)).⁷¹ It could be argued, with a far-stretched interpretation of Article 28(1)(b), that law enforcement access to personal data collected by private parties for a non-law enforcement purpose falls within the category of “high-risk processing”. However, not all access to personal data for a law enforcement purpose would qualify as ‘high risk processing’. If the notion is undefined,⁷² Recital 52 of Directive 2016/680 provides some guidance to assess the level of risk of a processing. The purpose of the processing is one of the factors, besides the nature, scope and context of the processing. Determining whether a subsequent processing of personal data for a law enforcement purpose constitutes a ‘high risk’ processing requires a case-by-case analysis. Therefore, it could be that the further processing of personal data would constitute a ‘high risk’ processing in a context of criminal intelligence because of the risk of mass surveillance; whereas the same processing performed in a criminal investigation context would not.

In the end, it is still questionable whether the procedure of ‘prior consultation’ of a national DPA set out in Article 28

⁶⁸ Article 4(2)(a) of the leaked draft version of the proposal for a ‘police Directive’.

⁶⁹ *Digital Rights Ireland*, para. 62, as complemented by *Tele2 Sverige*, para. 120. The prior review is initiated “following a reasoned request of those authorities submitted within the procedures for the prevention, detection or prosecution of crime.”

⁷⁰ Besides the two cases requiring prior consultation of the DPA, Member States have the possibility to establish a list of processing operations that are subject to prior consultation. One could imagine that the case of law enforcement access to personal data generated by third parties could be included in such a list; however this option is left to the discretion of Member States, see Article 28(3).

⁷¹ Article 28(1)(b) of Directive 2016/680.

⁷² Recital 52 of Directive 2016/680 only specifies that high risk is “a particular risk of prejudice to the rights and freedoms of data subjects.”; by comparison in the context of the GDPR, Article 35(3) of the Regulation provides some guidance on what ‘high risk processing’ might include: systematic profiling, large-scale processing of sensitive data or systematic and large-scale monitoring of publicly accessible areas.

⁶⁴ See sub-section 3.1 of this article.

⁶⁵ Article 1(1) of Directive 2016/680.

⁶⁶ *Digital Rights Ireland*, para. 41 et seqs.

⁶⁷ *Digital Rights Ireland*, para 42–43; *Tele2 Sverige*, para. 102.

of Directive 2016/680 amounts to the procedure of ‘prior review’ by an independent authority, as required by the ECJ case law. If DPAs are independent authorities,⁷³ it cannot be claimed that a ‘prior consultation’ is equivalent to a ‘prior review’. Directive 2016/680 indeed lacks clarity on the exact power given to data protection authorities through the prior consultation. Article 47(3) of Directive 2016/680, on the powers of national supervisory authorities, refers to their ‘advisory power’ in respect of the procedure of prior consultation. Likewise, if it is justified to require a prior judicial or administrative review of a request for access to personal data collected for a different purpose, it might be disproportionate to require the review of each request by a national DPA.

In conclusion, Article 28 of Directive 2016/680 does not seem to be a sufficient procedural safeguard. First, it is not guaranteed that all data protection authorities across the EU would have the same reading of Article 28 of Directive 2016/680. Then, the provision only requires an advice (prior consultation) and not a decision (prior review) before the further processing for a law enforcement purpose can be executed. Finally, the prior consultation of DPAs is limited to ‘high risk processing’.

3.3.3. *The right to information as a duty of notification?*

The right to be informed about the collection of one’s own personal data is a very important right since it triggers the application of the other data subjects’ rights: the right to access the personal data collected; to rectify it if it is inaccurate; to have it erased under specific conditions, as well as to be informed of the right to legal remedies. In a law enforcement context, it is logical that those rights are not as broad as in a non-law enforcement context. For instance, the necessity of a criminal investigation may validly justify restrictions to those rights. However, following *Tele2 Sverige*, individuals whose personal data has been accessed by law enforcement authorities should be notified as soon as possible and in any event as soon as the notification no longer prejudices the ongoing investigations.⁷⁴

Article 13 of Directive 2016/680 sets out the right to information, which is defined as “information to be made available or to be given to the data subject.” This provision lists all the pieces of information to be “made available or given” to an individual. However, it does not specify that the information be actively provided to the data subject. The wording of Article 13 seems to indicate that the right to information is a right of confirmation that collection of personal data has been carried out. The right to information, as set out in Article 13 of Directive 2016/680, constitutes an improvement in comparison with Article 16 of the Council Framework Decision 2008/977/JHA. This latter only provides for a right ‘to be informed’ in accordance with ‘national law.’ Yet, Article 13 of Directive 2016/680 does not establish a duty of notification. Nowhere is it mentioned in the Directive that data subjects should receive communication about the collection of their data as soon as the purpose for which their data has been collected is not at stake anymore.

By comparison principle 2.2 of the Council of Europe’s Recommendation on the use of personal data in the police sector (Recommendation R(87) 15) provides that the individual should be “informed that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.”⁷⁵

The absence of notification is even more problematic in a case where personal data has been collected by private parties under the GDPR regime and is accessed for further use by law enforcement authorities. The individuals concerned are not able to exercise their rights properly if they are not informed, at some point, that their data has been accessed. In *Tele2 Sverige*, the ECJ required that law enforcement authorities “notify the persons affected, under the applicable national procedures.”⁷⁶ The Court added that the notification is “necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.”⁷⁷ However, one could dispute the legal basis on which the ECJ imposes a duty of notification on law enforcement authorities for the further processing of the retained data. The Court based its reasoning on Article 15(2) of the e-privacy Directive ‘read together’ with Article 22 of the Data Protection Directive.⁷⁸ Yet the Data Protection Directive does not apply to the processing of data for law enforcement purposes. Those processing operations are excluded from the scope of EU law except when they are exchanged between Member States. Cross-border data processing for law enforcement purposes falls within the scope of Council Framework Decision 2008/977/JHA.⁷⁹ However, thanks to a clever artifice, the ECJ held that both the retention of data by telecoms operators and its access by law enforcement authorities fell within the scope of the e-privacy Directive. To reinforce its position, the Court added that the only reason that the data was retained was to provide law enforcement authorities access to it.⁸⁰ As mentioned in [Section 2](#), the reasoning of the ECJ on this specific issue is disputable. With the adoption of the new data protection framework, the scenario of access by law enforcement authorities to retained personal data should be considered as a processing for a law enforcement purpose and fall within the scope of Directive 2016/680.⁸¹ However, beyond the possible discussion on the scope of the e-privacy Directive and the inclusion of law enforcement access, one should focus on the interpretation of the right to information given by the ECJ. In a scenario of law enforcement access to personal data generated in a different context, the right to information ought to be interpreted as a duty of notification. Yet as drafted, article 13 of Directive 2016/680 does not lay down such an obligation.

After the analysis of the ECJ case law on data retention and its possible impact on the safeguards contained in the ‘police’ Directive, the article will assess whether the principle of purpose

⁷³ Following both the GDPR and Directive 2016/680, DPAs are required to be independent authorities; on their independence, see among others, Orla Lynskey (2016), ‘the Europeanisation of Data Protection Law’, Cambridge Yearbook of European Legal Studies, 1–35.

⁷⁴ *Tele2 Sverige*, para. 121.

⁷⁵ However, law enforcement authorities have criticized this principle because they consider it difficult to put into practice.

⁷⁶ *Tele2 Sverige*, para. 121.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

⁷⁹ Recital 6 of Council Framework Decision 2008/977/JHA.

⁸⁰ *Tele2 Sverige*, para. 79.

⁸¹ See Recital 19 GDPR making a bridge between the GDPR and the Directive in case of further use by law enforcement authorities of personal data collected under the GDPR.

limitation, as defined in Directive 2016/680, plays its role of safeguard in the context of law enforcement access.

4. Safeguards against abuses: the principle of purpose limitation?

In the scenario at stake as well as in the scenario of data retention of personal data, the main issue from a data protection perspective is the change of initial purpose: personal data collected for a specific purpose is then reprocessed for a different purpose. As stated by the A29WP in its opinion on purpose limitation (Opinion 03/2013), the principle of purpose limitation is “a cornerstone of data protection.”⁸² It constitutes a safeguard against the misuse or abuse of personal data and guides the lawful use of personal data collected for a different purpose.

In a situation where law enforcement authorities get access to personal data generated by private parties, the purpose of the further processing of personal data (law enforcement purpose) has no link with the initial purpose of data collection (commercial or operational purpose). As such, the purpose of the further processing should be deemed incompatible with the initial purpose of processing. Yet, Article 4(2) of Directive 2016/680 allows the repurposing of personal data collected by other parties for a different purpose under the conditions of legality and proportionality. The question that arises is whether this provision offers sufficient guarantees to protect individuals whose personal data is collected under the regime of the GDPR and subsequently used under the regime of the ‘police’ Directive.

4.1. Notion of purpose limitation

Described in identical terms in the GDPR and the ‘police’ Directive, the principle of purpose limitation entails that personal data is “collected for specified, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes.”⁸³ This wording originates from Article 6(1)(b) of the Data Protection Directive. As analysed by the A29WP, the principle of purpose limitation is composed of a principle of purpose specification (‘specified, explicit and legitimate purposes’) and a principle of compatible use (‘not processed in a manner incompatible’).⁸⁴ Since the focus of this paper is on the further processing of personal data and not on its initial processing, it is assumed that the purpose of initial processing satisfies the criteria of purpose specification. For the same reason, the terms ‘purpose limitation’ and ‘principle of compatible use’ are used interchangeably in this section.

4.2. Application of the principle: test of compatibility versus derogation

The interpretation given to the principle of purpose limitation is different in a non-law enforcement context from that

in a law enforcement context. When the GDPR applies, the compatibility of a further processing with the initial processing is assessed in application of a test of compatibility based on five factors as described in Article 6(4) GDPR. Those include the link between the initial processing and the further processing; the context of data collection; the nature of personal data (such as sensitive data); the impact of the further processing on data subjects, and the existence of appropriate safeguards to compensate for the change of purpose(s).⁸⁵ The factor of “context of processing” should in particular be understood as “reasonable expectations of data subjects based on their relationship with the controller as to their further use.”⁸⁶ These factors apply if the further processing is not based on the data subject’s consent for the further processing or on national or EU law allowing the further processing.⁸⁷

By contrast, in a law enforcement context, the compatibility of a further processing is not assessed in application of a test of compatibility. Instead, Article 4(2) of Directive 2016/680 provides for a derogation from the principle of purpose limitation: the further processing of personal data for a purpose different than the initial purpose of collection is allowed if it complies with the principles of legality (i.e. based on “Union or Member State law”) and proportionality (“processing necessary and proportionate to that other purpose”).⁸⁸

Article 4(2) of Directive 2016/680 raises at least two issues: the first one relates to the initial processing of personal data and the second one to the compatibility of the further processing of personal data for a law enforcement purpose with the initial purpose of its collection in a non-law enforcement context.

First, from the wording of Article 4(2) of Directive 2016/680, it is not clear which type of ‘initial purpose’ is referred to.

⁸⁵ Article 6(4) GDPR reads as follows: “Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.”

⁸⁶ Recital 50 GDPR.

⁸⁷ Article 6(4) GDPR.

⁸⁸ Article 4(2) of Directive 2016/680 reads as follows: “Processing by the same or another controller for any of the purposes set out in Article 1(1) other than for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.” Article 4(2) GDPR needs to be read together with Recital 29 of Directive 2016/680.

⁸² A29WP, ‘Opinion 03/2013 on purpose limitation’, WP 203, 2 April 2013, 4.

⁸³ Article 5(1)(b) GDPR and Article 4(1)(b) of Directive 2016/680.

⁸⁴ A29WP, Opinion 03/2013.

The first sentence of Article 4(2) provides that “the processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted. . .” Should the phrase “other than that for which” be understood as referring to any purpose other than those of Directive 2016/680, i.e. any non-law enforcement purpose? Alternatively, should it be understood as referring to any initial purpose covered by Directive 2016/680 but different from the purpose of further use? In that case, the initial and further purposes are of the same nature, i.e. they fall within the broad category of law enforcement, but they are different. For instance, one could think of personal data collected in the context of a specific criminal investigation and further used in a non-related investigation. In the end, the wording of Article 4(2) of Directive 2016/680 remains ambiguous⁸⁹ and allows for a broad interpretation that encompasses any initial purpose of processing within or outside the scope of Directive 2016/680.

Next, in application of Article 4(2) of Directive 2016/680, the further processing is authorised provided it is based on a national or EU law and it is necessary and proportionate to the purpose of law enforcement. Yet, that article establishes no link between the purpose of the initial processing and the purpose of the further processing. Does it mean that the further purpose is incompatible per se with the initial purpose of processing? It is at least not possible to draw that conclusion from the wording of Directive 2016/680. As a matter of comparison, under the GDPR, unrelated purposes of processing are not considered incompatible per se. For instance, Article 5(1)(b) of the GDPR clearly establishes that the further processing for a scientific, historical or statistical purpose is not incompatible with the initial purpose of processing, as long as it is accompanied with appropriate safeguards.⁹⁰ However, in a law enforcement context, Directive 2016/680 does not contain a similar provision. Article 4(2) of Directive 2016/680 does not even refer to the notion of compatibility between the initial and the further purposes of processing. Instead, it authorises the subsequent processing under specific conditions. The provision seems to establish a derogation from the principle of ‘purpose limitation’ described in Article 4(1)(b) of Directive 2016/680. Yet, the approach followed in Directive 2016/680 is different from the one that the A29WP advocated in Opinion 03/2013. In that Opinion, the A29WP reviewed several mixed scenarios involving an initial collection of personal data for a non-law enforcement purpose followed by a re-use of that data for a law enforcement purpose. These specific scenarios relate to the Data Retention Directive, PNR scheme, EURODAC database and use of smart metering data for the purpose of detecting tax fraud.⁹¹ In the analysis of the different examples, the A29WP did not state that the further processing was *prima facie* incompatible with the original purpose of processing. Instead, it performed a test of compatibility, weighing the further processing for a law enforcement purpose against the initial purpose of collection using

various factors. The A29WP based its whole reasoning on the initial purpose of collection. If that purpose fell within the scope of the Data Protection Directive, the further processing –whatever its nature– had to be assessed following the test of compatibility the A29WP had defined.

What is problematic in the approach of the principle of purpose limitation set out in Directive 2016/680 is the absence of test of compatibility, which is replaced instead by a derogation based on the principles of legality and proportionality. Yet, as rightly observed by the European Data Protection Supervisor in respect of the further use for a law enforcement purpose of large-scale databases initially constituted for administrative purposes: “a database regarded as proportionate when used for a specific purpose can become disproportionate when the use is expanded to other purposes afterwards.”⁹² To acknowledge this situation, some authors have even re-defined the principle of purpose limitation as a principle of ‘purpose deviation’ that reflects the absence of links between the initial and the further purposes of processing.⁹³ It is therefore the role of the ECJ to interpret the principles of necessity and proportionality in a way that will ensure the protection of data subjects. To do so, the Court ought to take into account the initial purpose of processing in its interpretation of the principle of proportionality as provided under Article 4(2) of Directive 2016/680.

5. Conclusions

The scenario of law enforcement access to personal data initially collected for a different purpose raises complex issues. If it is established that the further processing of that data for a law enforcement purpose falls within the scope of Directive 2016/680, no specific rules taking into account that scenario have been adopted. However, in light of two ECJ’s rulings, *Digital Rights Ireland* and *Tele2 Sverige*, on partially similar scenarios, the assessment of the rules contained in Directive 2016/680 reveals that the Directive lacks essential provisions to ensure the protection of individuals’ right to data protection. In particular, the Directive fails to provide objective criteria to delimit the law enforcement access to personal data generated for a different purpose and a specific procedural rule on the prior review of the request for access. As for the right to be informed, it should be interpreted, in that context, as a right to be notified, at a certain point, that data have been accessed by law enforcement authorities. The article also points out that

⁸⁹ Recital 29 of Directive 2016/680 does not bring further clarification as it relates to “personal data [that] are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it had been collected. . .”

⁹⁰ Appropriate safeguards as defined in Article 89(1) of the GDPR.

⁹¹ A29WP, Opinion 03/2013, Annex 4, examples 17 to 20, 67–69.

⁹² See EDPS (2011) Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Region-Communication on migration, 7 July 2011, para. 17; EDPS (2016) Opinion 07/2016 on the First Reform Package on the Common European Asylum System (Eurodac, EASO and Dublin regulations), para. 17.

⁹³ e.g. Els de Busser and Gert Vermeulen, “Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy” in EU and International Crime Control. Topical issues ((GofS)-Governance and Security Research Paper Series, Vol.4) (Maklu-Uitgevers nv, 2010), 102.

the absence of specific rules is also detrimental to the principle of purpose limitation, which does not link the initial purpose of processing with the purpose of further processing.

To overcome these shortcomings, several solutions could be envisaged. First, since the Directive has recently been adopted, a revision of the Directive to incorporate rules specific to the scenario is simply not a practical option.

As a solution, one could consider the opportunity provided by the ongoing revision of the e-privacy Directive to add specific rules, based on the findings of *Digital Rights Ireland* and *Tele2 Sverige*, to cover the scenario of law enforcement access to personal data generated by private parties. This option would however be limited to the further use of personal data originally processed by telecommunications providers only. Therefore, this option would be quite restrictive.

The second option would be in the hands of the European Data Protection Board, which could issue an opinion on the data protection rules applicable to the scenario, including the implications of *Tele2 Sverige* on the interpretation of Directive 2016/680. The main drawback of this option lies in its non-binding nature.

Ultimately, and this last option would offer more legal certainty, after the implementation of Directive 2016/680 in national legislations, national courts could send preliminary questions to the ECJ on the interpretation of the key provisions of Directive 2016/680 (and in particular on the right to be informed, the procedure of prior review by DPAs and on the derogation to the principle of purpose limitation). This option might not be fast. In addition, one might need, in the end, the resilience and activism of another Schrems to start tailor-made proceedings at national level and pave the way to the ECJ.

Acknowledgment

The author would like to thank Prof. Jeanne Mifsud Bonnici and Prof. Laurence Gormley for their valuable comments on an earlier draft of this article, Christina Angelopoulos for her kind suggestions as well as the anonymous reviewers; any error or omission is however the sole responsibility of the author.