Subsequent Use of GDPR Data for a Law Enforcement Purpose
Jasserand, Catherine

Published in:
European Data Protection Law Review

DOI:
10.21552/edpl/2018/2/6

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):

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.
Subsequent Use of GDPR Data for a Law Enforcement Purpose: 

The Forgotten Principle of Purpose Limitation?

Catherine Jasserand*

This article questions the role of the principle of purpose limitation in a situation where personal data are collected under the General Data Protection Regulation (GDPR) and further processed under the regime of the 'police and criminal justice' Directive. It reviews the rules set out in both instruments, concerning the principle of purpose limitation and the further processing of personal data for a different purpose. The analysis of the rules under Directive 2016/680 reveals some ambiguity: are the rules applicable to the subsequent use of any personal data (including those collected under the GDPR)? Or are the rules limited to the subsequent use of 'police or criminal justice' data? Building on the ambiguous wording of Article 4(2) of the Directive, the article addresses the two hypotheses and analyses their consequences. It concludes with the uncertainty of the applicable rules and the likelihood of diverging interpretations at the national level.

1. Introduction

Examples of cases where law enforcement authorities request access to personal data initially collected by third parties for a different purpose are numerous. Many of them relate to the legal obligation of private parties to retain and disclose personal data to law enforcement authorities, such as in the fields of air transport,1 banking2 or telecommunications3. In these cases, personal data are retained for further use by law enforcement authorities to fight fraud, terrorism and serious criminal offences. Besides these cases, there are situations where private parties collect personal data for their own uses (such as commercial or operational purposes) but are under no specific obligation to retain them for law enforcement purposes. One could think of the vast amount of personal data that social media collect and hold. Some of these data are very valuable to law enforcement authorities (ie photographs or voice recordings). Although social media are not obliged to retain these data, they can be requested to grant law enforcement authorities access to the data. As shown by the transparency reports published by the largest tech companies (eg Facebook, Google, Microsoft), the number of law enforcement requests for access to content and user accounts is rapidly growing.4 No figure is, however, available on the types of content requested

DOI: 10.21552/edpl/2018/2/6

* Catherine Jasserand, PhD researcher, Transboundary Legal Studies Department, SteP (Security, Technology & e-Privacy) Research Group, Law Faculty, University of Groningen. For correspondence: <c.a.jasserand@step-rug.nl>. The author wishes to thank Prof Jeanne Mifsud Bonnici for her valuable comments and Pim Geelhoed for fruitful discussions on law enforcement issues, as well as the peer reviewers for their suggestions and careful reading. The views expressed in this article are solely those of the author. All remaining errors are the author’s sole responsibility.

2 Obligations imposed on banks to retain financial data for anti-money laundering purposes.
4 See Aliya Ram, ‘Tech Companies Endure Near-Doubling of Requests for Personal Data’ Financial Times (30 August 2017) <https://www.ft.com/content/b734882e-8cb0-11e7-9084>
and the purposes of use. It is also almost impossible to know the exact volume of personal data collected and held by social media. Concerning photographs alone, in 2012, more than 300 million photos were uploaded to Facebook every day. Yet, as shown by the research undergone by Facebook on the uploaded images, photographs portraying individuals are very useful for facial recognition. In a different field, one could also think of biometric data (such as fingerprints, palm prints and facial images) that an employer or a school holds about their employees or students to give them access to premises, canteens or library facilities. These data are particularly valuable for identification purposes. It is, thus, not hard to imagine that law enforcement authorities could ask private parties to hand over biometric data initially collected for a purpose other than law enforcement and re-use them in the context of a criminal investigation.

Due to the availability of data and technological means to process them, the repurposing of data – in the sense of re-use for a different purpose – is a growing phenomenon. When personal data are repurposed to be used in a different context, that repurposing might challenge the principle of purpose limitation. Following that principle, personal data collected for a specific purpose should be used for compatible purposes or further processed under a different legal basis. The situation becomes complicated when personal data have been collected in a particular context (such as commercial) and are further processed in a different one (such as law enforcement). But when rules on data protection are split between two instruments, like in the new EU data protection framework, the situation becomes even more complicated. The new framework is composed of a general instrument – the General Data Protection Regulation (GDPR) – and of a specific instrument applicable to data processing in the field of law enforcement – Directive 2016/680 (Police and Criminal Justice Directive). The GDPR replaces Directive 95/46/EC (Data Protection Directive), while Directive 2016/680 replaces the Council Framework Decision 2008/977/JHA. How do the instruments interact with each other when personal data collected under the GDPR are further processed under the rules of the new Directive? And what is the role of the principle of purpose limitation in such a scenario?

By investigating the rules applicable to the further processing of GDPR data in a law enforcement context, the article attempts to delineate the scope and role of the principle of purpose limitation when data processing is carried out across the two instruments. The paper only covers the subsequent use of GDPR data by law enforcement authorities under the new Directive. It does not tackle the issue of disclosure (which can entail the transfer) of personal data
by private parties to law enforcement authorities. According to Recital 11 of Directive 2016/680, this disclosure should be covered by the rules of the GDPR. Following Purtova’s analysis, the disclosure of personal data by private parties to law enforcement authorities is subject to the GDPR and might benefit from the exceptions of Article 23 GDPR. This article analyses, instead, the rules applicable to the re-use of GDPR data once the data have been accessed by or transferred to law enforcement authorities.

Following this introduction, Section II sketches the background on the principle of purpose limitation and addresses the relationship between the GDPR and Directive 2016/680. Against this background, Section III compares the regime of the principle of purpose limitation in both instruments. It focuses on Article 4(2) of Directive 2016/680 providing the conditions applicable to further processing and questions the scope of the initial processing. Highlighting the textual ambiguity of Article 4(2), Section IV suggests a reading of the provision to encompass further processing of GDPR data; whereas Section V assesses the consequences of excluding such processing from the scope of Article 4(2).

II. Background

This section briefly describes the roots of the principle of purpose limitation and addresses the relationship between the GDPR and Directive 2016/680.

1. Origin of the Principle of Purpose Limitation

The roots of the principle are to be found in early international instruments on privacy, and in particular in the OECD guidelines on privacy and in the Council of Europe’s Convention on the processing of personal data (Convention 108). From the origin, the principle was split into two principles, a purpose specification principle and a use limitation principle. In the law enforcement sector, the Council of Europe’s Recommendation on the use of personal data in the police sector [Recommendation R(87)15] also contains a provision on purpose limitation.

Building on Convention 108, both the Data Protection Directive (Directive 95/46/EC) and the Council Framework Decision (Decision 2008/977/JHA) contain specific provisions on purpose limitation, although phrased slightly differently. In both texts, the principle of purpose limitation entails that the purposes of data collection are ‘specified, explicit and legitimate’ and that data should not be further processed in a way ‘incompatible with’ the original purposes of collection.

As acknowledged by the European Commission in its study on the implementation of the Data Protection Directive, the broad wording of the principle of purpose limitation has led to diverging interpretations in Member States. These differences concern the scope of exceptions, the meaning of compatible


[15] It should be observed that art 23 GDPR sets out exceptions applicable to data subjects’ rights and the corresponding data protection principles; one could question whether any data subject’s rights derive from the principle of purpose limitation, and thus whether art 23 GDPR could be invoked.


[18] Respectively para 9 (purpose specification principle) and para 10 (use limitation principle) of the OECD Guidelines on Privacy.

[19] Council of Europe Recommendation R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector [1987], Principle 2.1 (purpose limitation) to be read together with Principle 4 (use limitation).

[20] art 6(1)(b) Directive 95/46/EC and art 3 Council Framework Decision 2008/977/JHA; art 3(1) of the Decision provides that ‘personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected.’ The condition ‘same purpose’ is not to be found in Directive 95/46/EC.

uses, and the requirement (as well as type) of safeguards applicable to data subjects.\textsuperscript{22}

The rationale of the principle in a law enforcement context is not to be found in Directive 2016/680. Instead, it is described in the Europol Regulation (Regulation 2016/674) on law enforcement cooperation.\textsuperscript{23}

The principle of purpose limitation is defined by its characteristics, which are to contribute to transparency, legal certainty and predictability.\textsuperscript{24} According to some authors, the principle of purpose limitation is the result of the right to self-determination, ie to control how own personal data are processed and used.\textsuperscript{25} However, this approach and understanding of the principle are hard to support in a law enforcement context. In the context of a criminal investigation, it is indeed difficult to argue that an individual whose personal data have been collected for a commercial purpose should control the way the police further use his or her data. Instead, it could be argued that an individual whose data are further processed for a law enforcement purpose should be made aware, or be notified, about this processing after the investigation is over or as soon as the investigation cannot be prejudiced anymore.\textsuperscript{26} Awareness or notification is, however, different from control.

Last, the principle of purpose limitation – in particular, its specification component – is an element of the fundamental right to the protection of personal data.\textsuperscript{27} The Court of Justice of the European Union (CJEU) has recently acknowledged that ‘the protection against unlawful access and processing’ is a part of the ‘essence’ of the fundamental right to data protection.\textsuperscript{28} As such, any limitation to the principle of purpose limitation should comply with the conditions formulated in Article 52(1) of the Charter of Fundamental Rights (the Charter). This claim will be further explained in the article.

2. Relationship between the GDPR and Directive 2016/680

As argued elsewhere,\textsuperscript{29} the GDPR and Directive 2016/680 build a bridge towards each other. Recital 19 GDPR delineates the material scope of the Regulation. It excludes from its scope the processing of personal data by ‘public authorities’ for a law enforcement purpose, as defined in Article 1(1) of the Directive. Those processing operations fall instead within the scope of Directive 2016/680.\textsuperscript{30} Likewise, Recital 11 of the Directive expressly excludes from its scope processing activities by entities or bodies entrusted for law enforcement purposes when those processing activities are not carried out for a law enforcement purpose but for a purpose that would fall under the GDPR.\textsuperscript{31}

Besides the two recitals on the material scope of each instrument, the GDPR and Directive 2016/680 are pretty silent on their relationship. As adopted, the texts are far less ambitious than the European Parliament’s resolutions on the legislative proposals.\textsuperscript{32} More specifically, the resolution on the proposal for a new Directive included an article on law enforcement access to personal data initially collected


\textsuperscript{24} recital 26 Europol Regulation.


\textsuperscript{26} As discussed later in the article.

\textsuperscript{27} art 8 Charter.

\textsuperscript{28} Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union (2017)


\textsuperscript{30} See art 2(2) GDPR and recital 19 GDPR.


ECLI:EU:C:2017:592, para 150; also as cited and analysed by Coudert in Fanny Coudert, ‘The Europol Regulation and Purpose Limitation, From the ‘silo-based approach’ to . . . what exactly?’ (2017) 3(3) EDPL 313-324.
for a non-law enforcement purpose. In that case, not only did the further processing need a legal basis but it also had to comply with strict conditions (such as identification of individuals allowed to access the data, adoption of safeguards and specific format for the request). In addition, the provision limited the re-use of the data to the ‘investigation’ or ‘prosecution of criminal offences’. Subsequent use of personal data for crime prevention was, thus, not envisaged.

There is not much discussion concerning the applicability of the new Directive rules to the law enforcement use of personal data collected by private parties. If carried out by a competent authority, for one of the purposes of Directive 2016/680, the subsequent use of GDPR data falls within the scope of the Directive. What is more crucial is to determine the rules applicable to the further processing of GDPR data under the regime of Directive 2016/680. To address this issue, next section assesses the principle of purpose limitation as designed in Directive 2016/680.

III. Regime of Purpose Limitation under Directive 2016/680

This section describes the principle of purpose limitation in Directive 2016/680 and compares it with the regime established under the GDPR. It also discusses the nature and content of Article 4(2) of the new Directive, which provides the conditions of further processing of personal data collected for a different purpose.

1. Comparison with the GDPR Regime

As noted in Section II, the principle of purpose limitation is sub-divided into a principle of purpose specification and a principle of compatible use. According to Article 4(1) of Directive 2016/680, personal data are ‘collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.’ The principle is worded in identical terms in Article 5(1) GDPR. However, as explained below, the principle is interpreted differently.

The purpose specification principle focuses on the initial purpose of collection. As observed by the Article 29 Working Party (A29WP), ‘law enforcement, per se, shall not be considered as one specified, explicit and legitimate purpose.’ Each purpose needs to comply with the three criteria of specificity, explicitness, and legitimacy. In the scenarios under review in this paper, the original purpose of data collection is not a law enforcement purpose. It can be a commercial, an administrative or an operational purpose, and in general, any non-law enforcement purpose falling within the scope of the GDPR. Only the purpose of the subsequent use is a law enforcement purpose covered by Directive 2016/680.

The second principle, compatible use, entails that personal data collected for a specific purpose are used following that purpose. They should not be further processed in a way incompatible with the initial purpose of processing. What does this principle mean in the context of Directive 2016/680? First, it would be wrong to conclude that unrelated purposes are necessarily incompatible. For example, under the GDPR, the subsequent use of personal data for research or archive purposes is not considered incompatible with the original purpose of collection. Second, two law enforcement purposes are not necessarily compatible because they belong to the same field. It is, therefore, necessary to assess the compatibility between the purposes to determine their

---

33 art 4a Resolution of 12 March 2014, P7_TA(2014)0219, entitled ‘access to data initially processed for purposes other than those referred to in article (1)’. 
34 ibid art 4a(1a)-(4f).
35 ibid art 4a(2).
36 As defined in art 37 Directive 2016/680.
37 As described in art 1(1) Directive 2016/680, ie for ‘the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding of threats to public security.’
39 A29WP is an independent advisory body to the European Commission on data protection matters, see <http://ec.europa.eu/newsroom/just/itm-detail.cfm?item_id=500833> accessed 10 April 2018; it will be replaced by the European Data Protection Board (art 68 et seq GDPR).
40 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’ (2015) WP233, 6.
41 In other instruments, such as in the OECD Privacy Guidelines (n 16), the principle is described as ‘one limitation’.
42 art 5(1b) GDPR.
43 See EDPS, ‘Opinion on the Data Protection Reform Package’ (12 March 2012); para 334 states: ‘it should be clear that within the law enforcement context different purposes can be incompatible.’
compatibility. Before the adoption of the new data protection framework, in cases where personal data were first collected for a non-law enforcement purpose and further used for a law enforcement purpose, the A29WP recommended the application of several factors to assess their compatibility. Those factors have been incorporated in the GDPR but are absent from Directive 2016/680. Last, ‘irrespective of the compatibility of purposes,’ Article 6(4) GDPR provides two legal grounds for the further processing: the data subject’s consent and a national or EU law, which is ‘necessary and proportionate’ to protect specific interests identified in Article 23 GDPR. The provision does not state that Article 23 GDPR constitutes a legal ground to process data for incompatible purposes but only that a law, which is ‘necessary and proportionate’, to safeguard the interests referred to in Article 23(1) constitutes such a legal basis.

The approach followed by Directive 2016/680 is different. Article 4(2) of Directive 2016/680 only sets out the conditions under which further processing for a purpose other than the original purpose of collection is allowed. In particular, it provides that:

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.

The scope of the initial processing and the conditions of the further processing are addressed in the next subsections.

2. Scope of the Initial Processing

The wording of Article 4(2) in respect to the context of the initial processing is ambiguous. The provision only mentions the initial purpose of processing as a purpose ‘other than for which the personal data are collected.’ Article 4(2) does not state whether the initial purpose falls within or outside the scope of Directive 2016/680. The provision does not even make a link between the principle of purpose limitation (defined in Article 4(1) of the Directive) and the conditions applicable to the further processing. One understands that the two are linked through Recital 29 of the Directive. The recital describes together the principle of purpose limitation and the conditions applicable to further processing for a different purpose. Based on that recital, one could claim that Article 4(2) only applies to the further processing of personal data initially collected for a law enforcement purpose. However, because a recital is a non-binding provision, one could also argue that Article 4(2) can apply to the further processing of personal data collected outside the scope of Directive 2016/680.

This ambiguity is problematic because it has consequences for the status of the subsequent use of GDPR data for a law enforcement purpose. If Article 4(2) of Directive 2016/680 does not apply to the further processing of GDPR data, there is an uncertainty on the qualification of this subsequent processing operation. Should it be considered as initial processing under Directive 2016/680? During the negotiations on the draft Police and Criminal Justice Directive, the European Commission opined that such processing should be considered as ‘initial processing’ of ‘police or criminal justice’ data instead of further processing. The European Commission believed that ‘the further processing across the two legal instruments would create problems,’ thus ‘there was no specific articles [in the draft Directive] to be used for that.’ As a consequence, following this interpre-
tation, the further processing of GDPR data would neither be subject to the principle of purpose limitation, as defined in Article 4(1) of the Directive, nor be subject to the conditions applicable to further processing set out in Article 4(2) of the Directive. The situation does not seem, however, to be that simple. No recital or provision in both the GDPR and Directive 2016/680 confirms the European Commission’s views.⁵¹ Both texts are actually silent on that matter. Because of the ambiguous wording of Article 4(2) of Directive 2016/680, it could be argued that both hypotheses can be envisaged.

The conditions under which Article 4(2) allows further processing are analysed next.

3. Article 4(2) of Directive 2016/680, as Derogation from the Principle of Purpose Limitation?

Article 4(2) of the Directive allows the further processing under the conditions of legality [Article 4(2)(a)] as well as necessity and proportionality [Article 4(2)(b)]. However, these conditions are not linked, implicitly or explicitly, to any compatibility requirement. The term is absent from the provision. By comparison, Article 3(2) of the Council Framework Decision 2008/977/JHA, now replaced by Directive 2016/680, only applies to purposes ‘not incompatible’ with the purpose of collection.⁵² Thus, it seems that Article 3(2) of the Framework Decision was drafted as an interpretation of the principle of purpose limitation as it only authorises further processing ‘not incompatible.’

Concerning Article 4(2) of Directive 2016/680, it should be mentioned that during the negotiations on the draft Police and Criminal Justice Directive, Member States were split on its scope: some wanted to define specific rules applicable to the further processing for compatible purposes; others rules applicable to incompatible purposes.⁵³ In the end, the adopted text refers to neither. The definition of ‘compatible purposes’ is thus left at the national level.⁵⁴ As a consequence, in the absence of compatibility requirement, it can be deduced that Article 4(2) of Directive 2016/680 applies ‘irrespective of the compatibility between the purposes.’ As such, the provision constitutes an exception to the principle of purpose limitation and differs from Article 3(2) of the Framework Decision.

Next, if Article 4(2) of Directive 2016/680 is construed as a derogation from the principle of purpose limitation, it is argued that it should be interpreted in accordance with the Charter of Fundamental Rights [Article 52(1) of the Charter] and the European Convention on Human Rights [Article 8(2) ECHR].⁵⁵

a. Lower Standard of Protection?

As specified in the GDPR, restrictions on data subjects’ rights and on the corresponding data protection principles should apply in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁵⁶ One could add that the requirements have to be understood as interpreted by the CJEU and the European Court of Human Rights (ECtHR).

Directive 2016/680 does not contain a similar provision. It only provides, in Recital 46, that ‘any restrictions of the rights of the data subject’ must be in accordance with both the Charter and the ECHR. Thus, restrictions on data protection principles are

---

⁵¹ One could add that statements made by the European Commission, as well as by other EU institutions, during the negotiation process of a legislative instrument have no legal binding value in the absence of reference to these statements in the instrument itself, see Case C-292/89 R v Immigration Appeal Tribunal ex parte Gasdorf Devidier ps Antonissen [1991] ECR-I-745, para18.

⁵² Article 3(2) Framework Decision reads as follows: ‘Further processing for another purpose shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data were collected…’; this requirement of ‘non-incompatibility’ can also be found in Principle 5 of the Council of Europe’s Recommendation R(87)15.

⁵³ See discussions among Member States, and in particular the position of Sweden opposed to limit the rules on the further processing to compatible purposes whereas the Czech Republic supported rules applicable to purposes ‘not incompatible’ with the initial purpose of processing; respectively ins 151 and 152 of Delegations Document on the draft proposal Directive, Council of the European Union, 10335/15, 29 June 2015.

⁵⁴ Even if this is not expressly mentioned in Directive 2016/680; by comparison, see recital 6 Council Framework Decision that explicitly specifies ‘the Framework Decision should leave it to Member States to determine more precisely at national level which other purposes are to be considered incompatible with the purposes for which the personal data were originally collected.’

⁵⁵ Article 52(1) of the Charter is a general limitation clause; whereas article 8(2) ECHR is a specific limitation clause applying only to interferences with the right to privacy.

⁵⁶ Recital 73 GDPR read together with art 23 GDPR; as previously observed, one could still wonder whether any data subject’s rights can be derived from the principle of purpose limitation (see n 15).
not expressly subject to the same requirements. It is argued here that, as worded, Directive 2016/680 provides for a lower standard of protection than the GDPR. However, since the principle of purpose limitation is a component of the fundamental right to data protection, derogation from that principle should, in any event, be interpreted according to the case law of the CJEU and the ECtHR.

b. Interpretation of the Derogation

The right to the protection of personal data, enshrined in Article 8 of the Charter, expressly refers to the principle of purpose limitation as one of its constitutive elements. Article 8, paragraph 2, specifies that personal data ‘must be processed fairly for specified purposes’.

Following Article 52(1) of the Charter, restrictions on fundamental rights should comply with the following conditions: be ‘provided by law’, respect the essence of the rights’ at stake, be ‘subject to the principle of proportionality’ and ‘necessary and genuinely meet the objectives of general interest’ or ‘the need to protect the rights and freedoms of others.’

As analysed by Lynskey, the requirements of legality, proportionality, and necessity set out in Article 52(1) can be rooted in the case law of the ECtHR, whereas the requirement of ‘respect for the essence of the right’ is new. Thus the legality, necessity and proportionality requirements, provided by Article 4(2) of Directive 2016/680 should be understood as interpreted by both the ECtHR and the CJEU.

i. Legality, Necessity, and Proportionality

First, concerning the legality principle, formulated as ‘in accordance with the law’, Directive 2016/680 indicates that the principle should be understood as interpreted by the two Courts. The Directive is, however, silent on the interpretation of the principles of necessity and proportionality, which are worded in general terms in Article 4(2) of Directive 2016/680. By comparison, the GDPR makes more explicit references to the case law of the ECtHR when it describes the principles as ‘necessary and proportionate in a democratic society’. This wording refers in particular to the requirement of necessity set out in Article 8(2) ECHR, where any interference with the right to privacy has to be ‘necessary in a democratic society’. Article 8 ECHR pertains to the right to privacy, which encompasses the right to the protection of personal data as interpreted by the ECtHR. As such the case law of the ECtHR - as far as it relates to the protection of personal data as part of the right to privacy - is also relevant to the interpretation of the right to the protection of personal data.

ii. Essence of the Right

Second, on the requirement of ‘respect of the essence of the right’, very little case law is available on what constitutes the ‘essence’ of the fundamental right to data protection. Only in Schrems did the Court find a violation of the essence of the right to privacy (but not of the right to data protection). In more recent decisions, Digital Rights Ireland and Telia Sverige, the Court checked whether the Data Retention Directive and national data retention measures violated the essence of the right to data protection. Based on the existence of data security provisions, the Court concluded there was no violation of the essence of the right to data protection. This reasoning prompted some authors to argue that

[t]he Court is therefore perhaps suggesting that the essence of the right to data protection is not an ob-

58 Brkan explains however that the requirement of essence can find its origin in several Member States’ Constitutions, see Maja Brkan, ‘In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy’ (2017) 2017-01 Maastricht Faculty of Law Working Paper, 5-10.
60 art 6(4) GDPR.
62 eg S and Marper v United Kingdom Apps nos 30562/04 and 30566/04 (ECHR, 4 December 2008), para 103 where the ECtHR states: ‘[t]he protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by article 8 of the Convention.’
63 On the relationship between the right to privacy and the right to the protection of personal data, see Lynskey (n 57) ch 4, 89-130.
64 See also Brkan (n 58) 13.
65 Case-C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:550, para 94, where the Court found that ‘permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.’
66 Digital Rights Ireland (n 3) para 40.
...of that right (such as privacy protection or individual control over personal data) but rather it is the means of achieving data protection that constitutes the essence of the right.67

Interestingly in Opinion 01/2015 on the proposed agreement between the EU and Canada on passenger name record (PNR) data,68 the Court seemed to admit that the proposed agreement does not violate the essence of the right to data protection because it contains 'rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect against unlawful access and processing.'69 Thus, the Court seems to include the principle of purpose limitation (or at least its objective) within the scope of ‘the essence’ of the right to data protection.

As a consequence, the test of legality, necessity, and proportionality, set out in Article 4(2) of Directive 2016/680 should be interpreted according to the case law of the Courts on respectively Article 52(1) of the Charter and Article 8(2) ECHR. The characteristics of the different tests are illustrated in the next section with case law. Since Article 4(2) of Directive 2016/680 is understood as an exception to the principle of purpose limitation, measures allowing the subsequent use of personal data should also be assessed in respect of their impact on the ‘essence of the fundamental right’ to data protection.

Building on the ambiguous wording of Article 4(2) of Directive 2016/680, Section IV suggests a reading of the provision that would encompass the further processing of GDPR data.

IV. Further Processing of GDPR Data Falling within the Scope of Article 4(2) of Directive 2016/680

As explained in the introduction, the article discusses the role of the principle of purpose limitation when GDPR data are re-used for one of the purposes of Directive 2016/680. When the processing activities are carried out across the two instruments, no specific role seems to have been assigned to the principle of purpose limitation. For illustration purposes, one could refer to the examples provided in the introduction on the further processing of personal data: the case of law enforcement access and further use of biometric data held by social networks, employers or schools for administration purposes.

Based on other authors’ analysis,70 this section suggests a different approach to the principle of purpose limitation focusing on the subsequent use of personal data. Article 4(2) of Directive 2016/680 seems to follow this approach as it regulates the conditions of further processing, irrespective of the compatibility between the purposes. Thus, the article proposes a reading of Article 4(2) that would apply to personal data initially collected for a purpose within or outside the scope of the Directive. To control how law enforcement authorities further use GDPR data, the article suggests tying the principle of purpose limitation to the accountability obligation of law enforcement authorities (i.e., Article 19 of Directive 2016/680).

1. Focus on the Regulation of Data Use instead of Data Collection?

It could be argued that the principle of purpose limitation has not been forgotten, but its application in the specific scenario of reprocessing GDPR data for a law enforcement purpose is left to the discretion of Member States. This interpretation would, however, not be consistent with the fundamental nature of the principle. Thus, it seems difficult to bypass the principle. But since the new technological environment did not exist at the time the principle was first adopted, some authors have questioned its applicability as initially conceived.

In the context of big data, Morel and Prins have shown the inadequacy of the principle with the mass-collection of personal data and propose instead a test based on legitimate interests.71 If the principle of purpose limitation is not adapted to big data,72 it is, how-

---

67 Lynsey in 57: ch 5, 171.
68 Opinion 1/15 (n 28)
69 ibid, para 150.
70 In the context of big data and big data analytics.
ever, questionable if it could be replaced by a test based on the legitimate interests of data controllers, as suggested by the authors. More interesting in the context of this paper are the arguments brought forward by Coudert on the application of the principle of purpose limitation in the field of law enforcement cooperation. In a well-argued article, Coudert analysis the provisions on purpose limitation in the new Europol Regulation. According to Coudert, the Europol Regulation moves towards a different approach to the principle of purpose limitation in the context of big data analytics in the criminal field. In her view, the traditional approach of the principle that she describes as a ‘silo based’ approach – referring to the separation of data in distinct databases – is replaced by ‘the regulation of legitimate data uses’. However, as she explains, the Europol Regulation falls short on the practical implementation of this new approach. To control the use of personal data by data controllers and restrict further processing, Coudert suggests relying on privacy by design obligations and on the oversight by national data protection authorities.

In the current article, the context of processing does not focus on big data analytics but on the subsequent use of GDPR data in the context of criminal investigations or criminal surveillance. The interpretation suggested by other scholars might, thus, not be entirely suitable. Instead, the paper focuses on the breadth of Article 4(2) of Directive 2016/680. The next subsection suggests a reading of the provision that would apply to any initial processing. As such, the further processing of GDPR data would be subject to Article 4(2) of Directive 2016/680.

2. Interpretation of Article 4(2) to Encompass Subsequent Uses of GDPR Data

Based on the findings of the previous section, the article attempts to provide an interpretation of the legality, necessity and proportionality of the subsequent use of GDPR data for a law enforcement purpose. Since Article 4(2) of Directive 2016/680 is interpreted as a derogation from the principle of purpose limitation, the article also discuss whether and how the ‘essence of the right’ should be added as an extra criterion.

a. ‘In Accordance with the Law’

The first condition ‘in accordance with the law’ sets up the legality requirement. Extensively interpreted by the ECtHR, the term ‘law’ is broadly understood and does not need to result from a legislative procedure. The law needs, however, to be clear, accessible and foreseeable. The legality requirement does not call for many remarks. On the foreseeability aspect one could, however, observe that the ECtHR has introduced nuances taking into account the context of the interference. In a general context, a foreseeable law is a law, which is ‘formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.’ A law is for instance sufficiently precise if it describes its scope; provides safeguards to ensure the security, confidentiality, and safety of the data; and details how the data are stored, retained and further used. Those examples originate from case law on the retention and storage of biometric and DNA data for criminal purposes. In the context of police-led surveillance (such as interceptions of communic-
sions) or secret surveillance in the interest of national security, the ECtHR has established a different standard. Foreseeability in those contexts ‘cannot mean that an individual should be enabled to foresee precisely what checks will be made.’ Instead, the law should be clear enough to give an ‘appropriate indication’ as to the ‘circumstances’ and ‘conditions’ under which surveillance measures are allowed.

In the case of subsequent use of GDPR data for law enforcement purposes, the legality requirement could imply the existence of a national criminal procedural law that would detail the conditions under which personal data can be requested, accessed and further used. If the data are necessary for surveillance purposes, the national law would have to provide an ‘adequate indication’ as to the ‘circumstances’ and ‘conditions’ under which surveillance measures are allowed. According to the ECtHR, the law must contain specific safeguards, which include ‘procedure to be followed for examining, using and storing the obtained data.’

On its side, the CJEU interprets the legality requirement by reference and analogy to the case law of the ECtHR on Article 8 ECHR. As a consequence, a national or EU legislation must ‘lay down clear and precise rules’ on the ‘scope’ and ‘application’ of the measure and provide ‘minimum safeguards’ to prevent abuses, such as ‘unlawful access and use’ of data in the cases of data retention. The same conditions apply irrespective of the field, whether it falls within the scope of law enforcement or not.

In conclusion, under Article 4(2)(a) of Directive 2016/680, a legality test should be performed. That would imply checking if a specific national law (eg a national criminal procedural law) allowing law enforcement authorities (eg police authorities) to further process personal data held by third parties contain the elements described by the courts.

The two other requirements, proportionality and necessity, are more subjective than the legality requirement. They are dealt with separately, but as pointed out by the European Data Protection Supervisor (EDPS), they overlap and could be carried out concurrently or even in the reverse order. However, the order followed here is the one provided by Article 4(2) of Directive 2016/680. It is fair to say that due to the order if the measure has not passed the ‘test of necessity’, the principle of proportionality should not be assessed.

b. ‘Necessary to that Other Purpose’

The ECtHR and the CJEU have issued slightly different tests of necessity. According to the ECtHR, ‘necessity’ refers to a measure that ‘is necessary in a democratic society.’ In the context of the protection of personal data, this means that a measure answers ‘a pressing social need’ to meet the necessity requirement. Member States benefit from a margin of appreciation to determine the existence of a ‘pressing social need’. The protection of national security constitutes, for instance, a pressing social need. As analysed by the A29WP, the test of ‘pressing social need’ is defined by the ‘context’ of the measure and ‘evidence’ of the necessity of such a measure for society. As a consequence, the ECtHR only applies a test of strict necessity if the circumstances of the interference require it. In the context of ‘secret surveillance’, the Court ruled in particular that interference had to meet the criteria of ‘strict necessity’.

---

84 eg Malone (n 79).
85 eg Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).
86 eg Malone (n 79) para 67 as cited for example in Leander (n 85) para 51 and Amann v Switzerland App no 27798/95 (ECtHR, 16 February 2000), para 56.
87 Weber and Saravia v Germany App no 54934/00 (ECtHR, 29 June 2006), para 95.
88 eg Digital Rights Ireland (n 1) para 54; joined Cases C-203/15 and C-698/13 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, para 109.
89 EDPS, ‘Assessing the necessity of measures that limit the fundamental right to protection: A toolkit’ (11 April 2017).
90 ibid, 5.
91 See Handside v UK App no 5493/72 (ECtHR, 7 December 1976), para 48 where the Court described ‘necessity’ in the following terms ‘whilst the adjective “necessary”...is not synonymous with “indispensable”... “the words absolutely necessary” and “strictly necessary”...neither has it the flexibility of such expressions as “admissible”, “ordinary”, “useful”, “reasonable”...or “desirable.”
93 This margin depends on the ‘nature of the legitimate aim pursued’ and on the ‘nature of interference at stake’, see Connor v the United Kingdom App no 66746/01 (ECtHR, 27 May 2004), para 82.
94 Leander (n 85) para 39.
95 A29WP, ‘Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector’ (2014) WP211.
96 Szabo and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), para 73.
As for the CJEU, the Court has developed a test of ‘strict necessity’ in its case law on Articles 7 and 8 of the Charter of Fundamental Rights. The test of necessity applies even in the context of law enforcement or in relation to surveillance measures. According to the EDPS, the requirement of ‘strict necessity’ flows from the important role the processing of personal data entails for a series of fundamental rights, including freedom of expression. Even if specific rules are adopted in the field of law enforcement, for instance, Directive 2016/680, this does not justify a different assessment of necessity.

One could get inspiration from the toolkit developed by the EDPS on the test of necessity to guide the EU institutions before the adoption of new legislative measures. Based on the case law of the CJEU and the ECtHR, the test of necessity requires a ‘factual’ analysis, the identification of the fundamental rights impaired, the objective of the measure and the ‘less intrusive’ option to achieve the same goal. Transposed to a measure allowing the subsequent use of GDPR for a law enforcement purpose, the test of necessity would require going through the four steps. First, the factual assessment of the further processing could determine whether the processing is strictly necessary to the law enforcement purpose. That would imply identifying the purpose, such as criminal investigation or criminal surveillance (and whether targeted or not). Different factors could be taken into account such as the individuals impacted by the further processing (suspects, witnesses, victims or citizens); the type of data processed (sensitive data or personal data); the kinds of processing operations as well as the persons who have access to the processed data. An assessment of impacts on data subjects’ rights should also be carried out, and in particular how individuals will be able to exercise their right to remedy. Finally, it might be essential to consider the initial context of processing, especially when data are further used for criminal surveillance.

c. ‘Proportionate to that Other Purpose’

As observed by some authors, it might be difficult to distinguish the test of necessity from the test of proportionality. Advocate General Maduro wrote in Huber that ‘the concept of necessity...is well established as part of the proportionality test.’ In a narrow sense, however, the test of proportionality refers to ‘proportionality stricto sensu’. According to the CJEU, proportionate measures are ‘appropriate’ in relation to their objectives and ‘do not go beyond what is necessary’. The analysis of what constitutes a measure that ‘would go beyond what is necessary’ is very factual. For example, the CJEU has relied on the existence of ‘specific guarantees’ to ensure that the processing of sensitive data (such as fingerprints) was ‘effectively protected from misuse and abuse.’

Concerning the subsequent use of GDPR data for a law enforcement purpose, the proportionality of the measure might be assessed taking into account existing safeguards (such as limited storage of data in an identifiable form, description of uses, procedures to preserve the confidentiality, security, and integrity of the data).

d. Missing Criterion: Respect of the Essence of the Fundamental Right to Data Protection?

As explained, the requirement of ‘respect of the essence of the right’ is a condition imposed by Article 52(1) of the Charter on the limitations to fundamental rights. Yet, if as argued in the previous section, Article 4(2) of Directive 2016/680 is construed as an exception to the principle of purpose limitation, its application should comply with the requirements of the Charter and the ECtHR as respectively interpreted by the CJEU and the ECtHR. On the constitutive elements of the ‘essence of the right’ to data protection, few details are available. However, as mentioned in the previous section, in Opinion 1/15, the CJEU established the ‘protection] against unlawful access and processing’ as an element of the essence of the right.
The criterion of ‘essence of the right’ is absent from Article 4(2) of Directive 2016/680. If it is accepted that the provision should be interpreted in compliance with Article 52(1) of the Charter, the essence criterion should also be assessed.

3. Accountability of Law Enforcement Authorities as Additional Safeguard?

Last, as already suggested, a different approach to the principle of purpose limitation should be supported by additional safeguards. Article 19 of Directive 2016/680 sets out the accountability of law enforcement authorities to enable them to demonstrate compliance with their data protection obligations. As worded, the principle of accountability relates to the obligation that law enforcement authorities have to comply with their data protection obligations.

Even if the provision is vague, it ties the obligation of accountability to the implementation of appropriate technical and organisational measures, such as the obligation of ‘data protection by design’. That could include the adoption of policies describing the legality, necessity and proportionality assessment of the subsequent use of GDPR data and the impacts on data subjects.

In the next section, the hypothesis following which the subsequent use of GDPR data falls outside the scope of Article 4(2) of Directive 2016/680 is addressed.

V. Shortcomings: Consequences of Subsequent Uses of GDPR Data outside the Scope of Article 4(2) of Directive 2016/680

In that section, Article 4(2) of Directive 2016/680 is considered as applying exclusively to the further processing of personal data initially collected for one of the purposes of Directive 2016/680.

This interpretation, favoured by the European Commission, will most likely prevail among Member States. As a matter of illustration, several Member States have already decided to clear up the ambiguity in their draft implementing laws. For example, both the UK and the Dutch draft laws specify the nature of the initial purpose of collection. In the United Kingdom, Section 34 of the Data Protection Bill defines the principle of purpose limitation and restricts the rules on the further processing to personal data ‘collected for a law enforcement purpose.’

The Dutch draft law suggests a similar implementation of Article 4(2) of the Directive since the rules on the further processing will only apply to ‘police’ data (‘politiegegevens’).

1. Subsequent Use of GDPR Data as ‘Initial Processing’ under the Directive?

Following the analysis made in the previous sections, the subsequent use of GDPR data falls within the remit of Directive 2016/680 but is not expressly included into the scope of Article 4(2) of the Directive. In case Article 4(2) exclusively applies to the further processing of personal data initially collected in a law enforcement context, does it mean that the further processing of GDPR data is considered as initial processing of ‘police’ data under the Directive? If so, what are the consequences?

First of all, such an interpretation does not seem to be in line with the positions defended by the EDPS and the Az9WP on various occasions. They both reiterated the importance of the principle of purpose limitation in scenarios where personal data were accessed and further used by law enforcement authorities for a purpose unrelated to the initial purpose of collection. In particular, they have issued opinions in the context of the PNR Directive, the repurposing of Eurodac data for law enforcement purposes, and during the negotiations of the new data protection framework. For instance, concerning the proposal for a PNR Directive, the EDPS criticized the lack of objective criteria to limit the access to and the sub-

106 Coudert (n 28).
108 See the position of the European Commission (n 49); it also seems consistent with recital 29 of the Directive (n 48).
sequent use of the PNR data by law enforcement authorities. The EDPS found that the purposes for which the data could be re-used had not been precisely identified. Similar critics were formulated about the recast of the Eurodac database, originally constituted to manage asylum applications among Member States. In 2012 already, the EDPS found that the extension of the scope of the database for law enforcement purposes was ‘difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law.’ The EDPS also opined that ‘the assessment as to the necessity and proportionality of the creation of the Eurodac would have been completely different if law enforcement access was envisaged from the outset.’

Second, this qualification has consequences on the determination of the applicable regime. As explained in the previous section, further processing of ‘police’ data for a different law enforcement purpose is subject to the conditions of legality, necessity and proportionality set out in Article 4(2) of the Directive. The question that arises is whether the rules imposed on the initial processing are similar to the ones applicable to the further processing, ie whether the initial processing under Directive 2016/680 is also subject to conditions of legality, necessity, and proportionality. The rules applicable to initial processing under the Directive are therefore assessed.

According to Article 8 of Directive 2016/680, a processing operation is lawful if it is ‘necessary for the performance of a task carried out by a competent authority’ for one of the purposes of the Directive and ‘is based on Union or State law.’ An initial processing operation is, thus, also subject to a legality requirement. This requirement is understood as interpreted by the ECtHR and the CJEU, ie the law must be clear, accessible and foreseeable.

Article 8 also provides for a condition of necessity. However, that condition is different from the test of necessity under Article 4(2) of Directive 2016/680. As observed by the EDPS, the condition of ‘necessity’ can be a requirement for the ‘lawfulness of the processing’ as well as a condition applicable to the restrictions on fundamental rights. However, the two concepts of necessity are distinct. As explained in the previous section, the condition of necessity referred to in Article 4(2) of Directive 2016/680 should be interpreted as a condition of strict necessity. This results from the case law of the CJEU on the application of Article 52(1) of the Charter on interferences with the right to data protection. Therefore on the necessity requirement, initial processing does not seem to be subjected to the same test as further processing.

An initial processing operation must also comply with the criteria set out in Article 4(1) of the Directive, ie the data protection principles applicable to any processing. Among the different principles, the one described in Article 4(1)(c) is of particular interest. It relates to the principle of data minimisation in the context of law enforcement. As such, it requires the processing of personal data ‘not to be excessive in relation to [their] purposes.’ It could be argued that the provision only provides a mild obligation of proportionality since the criterion used to determine the amount of data collected (‘not excessive’) is less precise than the requirement of proportionality imposed by the courts (‘not beyond what is necessary’). As such, the obligation of proportionality applicable to the initial processing [Article 4(1) of the Directive] is not identical to the one applicable to the further processing [Article 4(2) of the Directive].

In conclusion, the conditions of necessity and proportionality to which an initial processing operation would be subject are not comparable to the conditions set out in Article 4(2) of the Directive, as interpreted in this article. Likewise, an initial processing operation is not subject to the requirement of ‘respect of essence of the right.’ Last, one might wonder if considering a subsequent use of GDPR data as initial processing of ‘police’ data would not impair the fundamental right to data protection since the principle of purpose limitation is one of its constitutive elements.
2. Consequences on Data Subjects’ Rights

Finally, there is a critical shortcoming linked to the regulation of data processing through two distinct instruments. Data subjects whose personal data are first collected for a GDPR purpose have specific rights attached to that processing operation. However, if their data are further used in a law enforcement context, they do not benefit from the same safeguards. In particular, they are not informed that their data have been further processed for law enforcement purposes. The nature of law enforcement activities obviously requires some adjustments in respect of data subjects’ rights to protect on-going investigation for example. However, the current right to information set out in Article 13 of Directive 2016/680 only imposes an obligation to make specific information available to individuals. It does not, expressly, provide for an obligation to notify individuals about the processing of their personal data. Yet, according to the CJEU’s case law, individuals whose personal data have been accessed by law enforcement authorities should be notified once the investigations are over or can no longer be jeopardised. The purpose of the notification is to allow individuals to exercise their right to remedy.

One could claim that a national law that would inform individuals about the possible access to and further use of their personal data by law enforcement authorities would not be sufficient in light of the CJEU’s case law. Transparency about a possible processing operation is not the same as notification of an actual processing operation. As argued elsewhere, it might be necessary to interpret Article 13 of Directive 2016/680 as obliging Member States to adopt national laws to notify individuals about the access to and subsequent use of their personal data by law enforcement authorities. On this specific issue, the Council of Europe seems to follow this approach in its ‘practical guide on the use of personal data in the police sector’. The report emphasizes that even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Last, the absence of obligation of notification is even less understandable in a situation where the further processing relates to individuals who are not suspects but who can be witnesses or victims in the context of a criminal investigation and even more in the absence of any suspects in the case of criminal surveillance.

VI. Conclusions

As demonstrated in this article and surprisingly, the principle of purpose limitation does not seem to play any role in the reprocessing of GDPR data for one of the purposes of Directive 2016/680. Still, the principle of purpose limitation is a constitutive element of the fundamental right to data protection.

First of all, if the GDPR and Directive 2016/680 define in identical terms the principle of purpose limitation, they do not provide similar rules concerning its application. In particular, Directive 2016/680 does not provide any guidance on the notion of ‘compatibility’, leaving the issue up to Member States. Instead, Directive 2016/680 provides, in Article 4(2), rules applicable to further processing. In the absence of precision, these rules seem to apply irrespective of the compatibility between the initial and secondary purposes of processing. As such, Article 4(2) of Directive 2016/680 can be construed as an exception to the principle of purpose limitation.

Second, the scope of the exception is not clearly defined. From the wording of Article 4(2) of Directive 2016/680, it is unclear whether it covers the further processing of personal data initially collected for a law enforcement purpose or the further processing of personal data initially collected for any purpose (which would include GDPR data).

Building on this textual ambiguity, the article has suggested two diverging paths: the application of Article 4(2) of Directive 2016/680 to the subsequent use of GDPR data or its exclusive application to ‘police and criminal justice’ data. In the first hypothesis, the

---

120 Arts 12-20 GDPR.
121 Tele2 Sverige in B88.
122 Tele2 Sverige in B88 para 121.
123 Such as national data retention law on communications data.
124 See also Jasserie and (n 29).
126 Ibid, 6.
principle of purpose limitation might play a role, which needs, however, to be redefined. In the second hypothesis, where the subsequent use of GDPR data most likely qualifies as initial processing under Directive 2016/680, the principle of purpose limitation does not play any role. That is problematic. First, Directive 2016/680 is a ‘minimum harmonisation’ Directive, leaving non-harmonised areas of Directive 2016/680 to the discretion of Member States. One could argue that the rules applicable to the further processing of GDPR data by law enforcement authorities are domestic issues. Second, like the United Kingdom and the Netherlands, Member States will most likely exclude the subsequent use of GDPR data for a law enforcement purpose from the scope of the provision implementing Article 4(2) of Directive 2016/680.

Ultimately, and contrary to the European Commission’s views, not providing a specific legal basis for the further processing of GDPR data in a law enforcement context does not avoid ‘creating problems’. The issue is thus left in the hands of Member States and their national courts until it gets challenged before the CJEU.