The right of access under the Police Directive

Dimitrova, Diana; de Hert, Paul

Published in:
Privacy technologies and policy

DOI:
10.1007/978-3-030-02547-2_7

Publication date:
2018

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

The Right of Access Under the Police Directive: Small Steps Forward

Diana Dimitrova[1(✉)] and Paul De Hert[2]

[1] FIZ Karlsruhe, Karlsruhe, Germany
Diana.dimitrova@fiz-Karlsruhe.de
[2] Vrije Universiteit Brussel, Brussels, Belgium
Paul.De.Hert@vub.be

Abstract. The present article sets out to examine the right of access under Directive 2016/680, which regulates the processing of personal data by EU Member States' law enforcement authorities. The article analyses in detail the provisions on the right of access. More precisely, it looks at whether the right provides for sufficient transparency towards the data subject and whether its scope allows for a harmonized data protection across the law enforcement sector in the EU. The article concludes that while the provisions on the right of access make a significant step towards more transparency, they also suffer from deficiencies. Also, the limited scope of the Directive takes away from the harmonization attempts.

Keywords: Right of access · Data protection · Law enforcement
Directive 2016/680

1 Introduction

The right of access to one's personal data plays an important role in allowing data subjects to exercise control over the processing of their data [1]. Its significance is evidenced by its explicit inclusion as a constitutive element of the fundamental right to data protection in Article 8 (2) Charter of Fundamental Rights of the European Union (CFREU) [2] and by its presence in every instrument on data protection in Europe, e.g. Article 12 (a) Directive 95/46/EC [3], Article 15 General Data Protection Regulation (GDPR) [4], as well as Council of Europe instruments [5].

Despite the lack of a comprehensive data protection framework in the law-enforcement sector in the EU until the entry into force of Directive 2016/680 [6], the right of access to one's own data has been provided for in different Area of Freedom Security and Justice (AFSJ) instruments, e.g. Article 17 2008 Framework Decision [7], which is about to be replaced by Directive 2016/680.[1] The said Directive is supposed to improve the protection of data subjects' personal data in the law enforcement sector,

[1] Article 59 Directive 2016/680.

M. Medina et al. (Eds.): APF 2018, LNCS 11079, pp. 111–130, 2018.
https://doi.org/10.1007/978-3-030-02547-2_7

not least because it expands the scope of application of the 2008 Framework Decision.[2] Thus, it will be applicable not only to the exchange of personal data between the competent Member State law-enforcement authorities but to the entire cycle of processing of personal data by them. As a result, data subjects may exercise their rights, e.g. the right of access, as regards all law enforcement data processing operations, subject to the limitations provided for in Directive 2016/680.

Further, by replacing the 2008 Framework Decision, Directive 2016/680 would be applicable to the already existing AFSJ instruments, to which the 2008 Framework Decision used to apply, such as SIS II Council Decision [8],[3] PNR [9],[4] and the instruments regulating the Member State law enforcement authorities' access to VIS [10][5] and to EURODAC [11].[6] These instruments themselves, except the EU PNR Directive, contain substantive and procedural rules on the rights of data subjects, e.g. the right of access. These more specific provisions leave Member States a certain margin of appreciation, e.g. as to the procedures for allowing data subjects to exercise their rights and as to the limitations to these rights.[7] Thus, at the time of the entry into force of Directive 2016/680 the patchwork of provisions on the right of access in the law-enforcement sector remains.

This situation gives rise, amongst others, to two questions. First, would the right of access in Directive 2016/680 allow data subjects to exercise their right of access in the law enforcement sector effectively? Second, does Directive 2016/680 bring about a harmonized and consistent application of the right of access in the law enforcement sector?

To answer these questions, the following Sect. 2 will examine the legal sources of the right of access in Europe, while Sect. 3 will examine the significance of that right. Section 4 will introduce the scope of the right of access under Directive 2016/680, followed by Sect. 5 on the information which the controller has to provide under that provision. Section 6 will examine the limitations of the right of access under Directive 2016/680. Next, Sect. 7 will focus on the procedural issues related to the exercise of the right of access. Last but not least, Sect. 8 will discuss in how far the right of access under Directive 2016/680 harmonizes the provisions on that right across the law-enforcement authorities in Europe.

2 Legal Sources of the Right of Access

In Europe, the right of access is one of the subjective rights granted to data subjects in several legal instruments. As mentioned above, the right is enshrined in Article 8 CFREU. It is further to be found in Article 8 (b) of Council of Europe Convention 108,

[2] Compare Article 2 Directive 2016/680 and Article 1 2008 Framework Decision.

[3] Recital 21 Council Decision SIS II.

[4] Article 13 (1) EU PNR Directive.

[5] Recital 9 VIS Council Decision.

[6] Recital 39 EURODAC Regulation.

[7] E.g. Article 58 Council Decision SIS II.

pursuant to which any person shall have the right to "obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form." [12][8] The provision on the right of access as enshrined in Article 12 (a) Directive 95/46/EC is similar. In addition to the requirements in Convention 108, it requires the controller to provide the requesting data subject a minimum set of detailed information about the processing of the data subject's personal data. Article 15 GDPR will replace Article 12 (a) Directive 95/46/EC and expand its scope. Article 15 GDPR applies in the framework of data processing by private and public actors which are not law enforcement or security authorities. It would require data controllers to confirm to the data subject whether they process personal data relating to him and provide him information concerning the processing of his data. The obligatory information pieces are more as compared to Directive 95/46/EC, e.g. as to the envisaged storage period, sources of the data and safeguards used for international transfers. In addition, the data subject has the right to one copy of his data free of charge.

As to the ECHR, Article 8 ECHR on the right to private and family life does not explicitly provide for a subjective right of access to one's data as such. However, in its case-law the ECtHR has tackled the topic of access to one's personal data as an essential part of one's enjoyment of his private and family life, e.g. obtaining details about one's past [13],[9] or as part of ensuring the legal processing of one's data, e.g. by the law enforcement authorities [14].[10] Also, it has assessed under Article 13 ECHR on effective remedies whether on a procedural level access to one's data or at least opportunities for independent supervision and review were provided for [15, 16].[11]

As to the police sector, the right of access to one's data has been enshrined since 1987 in Principle 6.2 of the Council of Europe Committee of Ministers Recommendation Nr. R (87) 15. It provides for the right of every data subject to have access to a police file, which is understood to mean a police file containing data concerning the particular data subject, at regular intervals and without excessive delay, in accordance with domestic law [5].

Following the recent legislative developments concerning data protection in the police sector, the right of access "at reasonable intervals, without constraint and without excessive delay or expense" in Article 17 2008 Framework Decision will be replaced by Article 14 Directive 2016/680. Its provisions and implications will be analyzed in Sect. 5.

---

[8] Article 8 (b) Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981.

[9] ECtHR, *Gaskin v the United Kingdom*, Application no. 10454/83, 07. 07. 1989. *In casu*, obtaining information about claimed abuse while in foster care.

[10] ECtHR, *Khelili v Switzerland*, Application no 16188/07, 18 October 2011 (discussed below).

[11] ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, 6.06.2006; ECtHR, *Amann v Switzerland*, Application no. 27798/95, 16 February 2000.

3 Four Main Purposes of the Right of Access

As mentioned in the introduction, the right of access is a tool which enables data subjects to exercise control over their data. This broad purpose could be broken down into four more concrete purposes. These are: (1) transparency, (2) supervision of legality of the personal data processing and an enabler of the exercise of the other data protection rights, (3) monitoring the execution of the corrective measures, and (4) raising awareness about practices that impact a large number of data subjects, thus triggering changes. The purposes were derived from case-law and academic literature and complied in the present section.

First, in *Rijkeboer*, the Advocate General (AG) argued that the purpose of the right of access is to give data subjects **transparency** by ensuring that they are aware of the information stored on them [17].[12] One could add that by enhancing transparency, the right of access contributes to the achievement of informational balance between the data subject and the controllers, which is especially important in the law-enforcement sector where the nature of the work involves more secrecy than other sectors.

Second, the knowledge of the personal information stored and the related details allows the data subject to "**supervise**" whether the processing of his data is **lawful and react to illegalities in the processing.** Thus, the right of access is "a means for a data subject to oversee and enforce observance of the law," especially the principles of data protection, *in casu* those enshrined in Article 6 Directive 95/46/EC such as fairness and lawfulness, purpose limitation, data accuracy, data minimization and limited storage period.[13]

In that respect it is argued that the right of access is a **pre-requisite and enabler for the exercise of the remaining informational rights**, "the gatekeeper enabling data subjects to take further action." [14, 18].[14] For the data subject to exercise the other rights – to rectification, erasure, restriction of processing, objection, the right not to be subject to automated individual decision-making such as profiling, and under the GDPR also data portability[15] – he first has to be aware that a certain controller is processing his data and obtain further information related to that processing. Although the data controller is obliged to provide the said information under his information obligations,[16] the two rights are not the same or mutually exclusive. The right of access

[12] CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E. E. Rijkeboer*, 7.05.2009 (Hereinafter "*Rijkeboer*"), Opinion of the Advocate General Ruiz-Jarabo Colomer, 22.12.2008, par. 33 and 34. In *Rijkeboer*, the applicant requested the College van burgemeester en wethouders van Rotterdam to inform him of the recipients to which it had transferred data relating to him, especially his address, in the two years preceding the request. The College provided the requested information only as regards the disclosure of the data one year prior to the request, the rest was automatically deleted.

[13] Ibid.

[14] See also Joined cases C 141/12 and C 372/12, *YS v Minister voor Immigratie, Inte- gratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M* (Hereinafter "*YS*"), 17.07.2014, par. 44.

[15] Chapter III GDPR and Directive 2016/680.

[16] Art 10 and 11 Directive 95/46/EC, Articles 13 and 14 GDPR, Article 13 Directive 2016/680.

allows the data subject to inquire at any time the controller about the current and past stand of the processing of his data, i.e. the right of access *a fortiori* refers also to the past [17].[17]

Third, the right of access allows the supervision of the legality of the processing not only until the moment of the first access request. It further allows the data subject to **monitor whether a certain illegality has been effectively redressed and when.** A case in point is the ECtHR case of *Khelili*. The Geneva police had found business cards in the possession of the applicant, Khelili, whose content could suggest that she was a prostitute. Thus, she was entered in the police system as a "prostitute." She objected, claiming she was not a prostitute. She demanded the police to change her profession to "tailor." The police acknowledged that since they could not find evidence that the applicant was indeed a prostitute, the profession should be corrected. After subsequently requesting from the Geneva police information about her file several times, the applicant learned from police officials that "prostitute" seemed to have been corrected in the police information system, but not in the criminal record of the applicant, who had been later detained and sentenced on probation for small crimes. *Khelili* shows the importance of having a framework for (directly) accessing one's data in all files held by the police in order to detect illegalities and ensure their timely rectification. This is especially important in the police sector due to the potential consequences on the data subjects [14].[18]

Advocate General Kokott reminds in the *Nowak* case which concerns access to exam scripts, however, that exercising the rights of rectification, erasure or blocking is not the sole aim of the right of access. Rather data subjects in principle have a "legitimate interest in finding out what information about them is processed by the controller," when at all information is processed, i.e. it refers more broadly to transparency [20].[19] This confirms the plurality of the role of the right of access in protecting our private lives and right to data protection.

Fourth, the disclosure of different illegalities related to the processing of one's data could have a wider impact, i.e. **trigger political, judicial and policy-making action** by raising awareness about the processing operations which affect the public at large. An example is the case of Max Schrems's access to his Facebook data which lead to more Facebook users claiming access to their data and to judicial proceedings and legislative changes such as striking down the Safe Harbour and replacing it with the Privacy Shield [18].

---

[17] CJEU, C-533/07, *Rijkeboer,* par. 54.

[18] ECtHR, *Khelili v Switzerland*, Application no. 16188/07, 18 October 2011. The Court held in favour of the applicant, because "prostitute" was not deleted for a long time, the Swiss authorities gave contradictory statements as to whether the term "prostitute" was deleted, the police could not prove the accuracy of the data and that it had been rectified/deleted (a requirement under Swiss law), par. 68–71.

[19] CJEU, C-434/16, *Peter Nowak v Data Protection Commissioner*, Opinion of Advocate General Kokott, 20.07.2017, par. 38–39. The case concerns the request for access to one's exam scripts and the comments made by the examiners. The main question was whether exam scripts qualify as personal data.

4 Scope of the Right of Access in Directive 2016/680

The right of access is enshrined in Article 14 Directive 2016/680. Briefly said, it grants data subjects the right to be informed whether a controller processes data concerning them and receive certain details about the data and the data processing operations. Articles 12 and 17 regulate the modalities of the exercise, while Articles 15 regulates the limitations to the right, i.e. the cases in which the controller may restrict the right, the conditions that need to be fulfilled and the procedures which need to be followed in that case.

The right of access is to be exercised by the data subject against *the controller*. Only officials working in the field of law-enforcement when they carry out law-enforcement tasks on behalf of the competent EU Member State authorities may qualify as controllers under Directive 2016/680.[20] This means that theoretically if a data subject evokes his right of access against a controller from the private sector, e.g. Facebook Ireland, to check whether it disclosed his data such as exchange of messages to the Irish police authority, then the data subjects may not evoke Article 14 Directive 2016/680 against Facebook Ireland. In that scenario Facebook Ireland would still be acting within the scope of the GDPR since it is not a law enforcement authority itself [21], whereas the actions of the Irish police would fall within Directive 2016/680. Further, Directive 2016/680 does not apply to EU institutions, agencies and bodies which process personal data for law-enforcement purposes, e.g. EUROPOL,[21] or to processing which does not fall within the scope of EU law.[22]

5 The Controller Has to Provide Six Categories of Information to the Data Subject

When the data subject evokes the right of access under Directive 2016/680 and the controller decides to grant him that right, the controller shall first **confirm** to the data subject whether he is processing personal data concerning the data subject. If this is the case, he should further **grant him access to the said data** and **communicate** to the data subject **six categories of information** concerning the data processing.[23] By contrast, under Article 17 (1) (a) 2008 Framework Decision the data subject was entitled only to **three categories** (Table 1).[24]

[20] Article 2 (1) Directive 2016/680.

[21] Article 2 (3) (b) Directive 2016/680.

[22] Article 2 (3) (a) Directive 2016/680.

[23] Article 14 Directive 2016/680.

[24] Article 17 (1) (a) 2008 Framework Decision.

Table 1. Comparison between the 2008 Framework Decision and Directive 2016/680

Information to the data subject under the right of access	2008 Framework Decision	Directive 2016/680
Confirmation that data are being processed by the controller		√
Purposes of processing		√
+ Legal basis for the processing		√
Categories of personal data		√
(Categories of) recipients	√	√
Envisaged storage period/criteria for the storage		√
Rights to rectification, erasure or restriction of processing		√
Right to lodge a complaint with the supervisory authority		√
+ Contact details of the supervisory authority		√
Personal data undergoing processing	√	√
+ Information about the origin of the data		√
Confirmation that data have been transmitted/disclosed	√	

Thus, one sees that the information concerning the processing which the controller needs to provide under Directive 2016/680 is broader than the details to which the data subject was entitled under the 2008 Framework Decision.

Below is a detailed discussion of the information to be provided to data subjects under Directive 2016/680.

5.1 The Purposes of and Legal Basis for the Processing (Art. 14 (a))

The provision of this information is essential for the data subject who needs to understand clearly why his data is being processed and most importantly - whether it has a legal basis. On that point Directive 2016/680 goes one step further from Article 15 GDPR which does not require the provision of information on the legal basis. The addition of this requirement in Directive 2016/680 could be due to the fact that Directive 2016/680, unlike the GDPR, does not contain a list of grounds for legitimacy of data processing, e.g. consent or contractual obligations.[25] Article 8 Directive 2016/680 only requires the data processing be *based on Union or Member State law*

[25] Article 6 GDPR.

and that it be *necessary for the performance of a task related to the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, carried out by the competent authority*.[26] Thus, pointing to the specific law underlying the processing is an indispensable piece of information for the monitoring of the legality of the processing.

The legal basis of the processing is not the same as the purpose of the processing, although the legal basis must specify the objective and purposes of the processing as well as the personal data to be processed.[27] Communicating the purposes of the processing in addition to the legal basis enables the examination of whether the purpose is legitimate and whether the other principles, namely data accuracy, minimization and storage, are complied with, as they are tested against the purpose. On that note, one should not forget that the original controller himself *or another controller* may conditionally process the data for another purpose, different from the one for which the data were collected.[28] This implies that also the change of purpose of and legal basis for the processing by the controller contacted should be communicated to the data subject. This is important, since change of purpose does not have to be communicated to the data subject under the controller's information obligations.[29] Thus, the only way for a data subject to stay aware of the (new) purposes of the processing of his data is by exercising his right of access "at reasonable intervals."[30]

However, the wording of Article 14 Directive 2016/680 suggests that the controller is obliged to communicate information only about the processing he is engaged in, not processing of the same data which is carried out by other controllers, e.g. for a different purpose. Thus, to have a clear overview of the full cycle of the processing of his data and the legality thereof, the data subject might need to file separate requests to the different controllers, of which he may gain knowledge through the information on the recipients of the data (see point 3 below).

5.2 The Categories of Personal Data, the Personal Data Which Is Processed and the Origin of the Data (Art.14 (b) and (g))

The essence of this provision is to allow the data subject to have an overview of the personal information which the controller processes, verify and possibly contest its accuracy and monitor other aspects of legality of the of the data, e.g. data minimization, and exercise his rights as a data subject.[31] While the GDPR grants data subjects the right to obtain a copy of their data,[32] this is not explicitly granted in Article 14 Directive 2016/680. Pursuant to the wording of Article 14 Directive 2016/680 and

---

[26] Article 8 (1) Directive 2016/680 j Article 1 (1) Directive 2016/680 (emphasis added).

[27] Article 8 (2) Directive 2016/680.

[28] Article 4 (2) Directive 2016/680. The provision is similar to the requirements in Article 8.

[29] Article 13 Directive 2016/680. See by contrast Article 13 (3) GDPR.

[30] Recital 43 Directive 2016/680. Note that the possibility to exercise the right "at reasonable intervals" is not mentioned in the text of Article 14 itself.

[31] Recital 43 Directive 2016/680.

[32] Article 15 (3) GDPR.

Recital 43 Directive 2016/680 it seems sufficient that the controller provide a "full summary … in an intelligible form" listing each piece of personal data. The summary could be provided also in the form of a copy of the data which are processed (see footnote 31). As the CJEU argued in the *YS* case, the form in which the personal data are provided to the data subject is immaterial as long as the data is presented in such a way as to allow the data subject to understand which personal data of his are being processed and monitor the legality of their processing.[33]

Where the data controller possesses information about the origin of the data, e.g. another law enforcement authority, this information could be precious to the data subject since it would reveal the details about the information held on them by other controllers. However, if the data originated from natural persons, their identity *should not* be disclosed, in particular if the sources are to remain confidential (see footnote 31). This could be attributed to the fact that the right of access should not cause harms to others, e.g. vulnerable witnesses. It is not surprising that the right of access may be restricted in order to "protect the rights and freedoms of others."[34] In addition, as Advocate General Sharpston argued in her *YS* Opinion, the right of access to one's personal data does not cover the right of access to the personal data of others.[35]

5.3 Recipients or Categories of Recipients, Especially in Third Countries (Art. 14 (c))

If the data controller further discloses the personal data to recipients, then he should include this in the response to the access request. This allows the data subject to control whether his data was treated with due confidentiality [22]. However, there are two caveats about this provision. In the first place, the controller may restrict the information only to "categories of recipients," thus not providing a full list of recipients. The article does not provide further guidance as to when the controller may choose to provide only the categories of recipients, e.g. does it depend on the effort involved in providing the complete information, or a conflict with a confidentiality requirement, etc.

In the second place, Directive 2016/680 excludes from the definition of recipients those public authorities which receive data in the framework of a particular inquiry in the general interest in accordance with Union or Member State law, e.g. tax and customs authorities.[36] This exception is quite broad and it is not clear why information

---

[33] Joined cases C 141/12 and C 372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M* (Hereinafter "*YS*"), 17.07.2014, par. 57–58. See also Advocate General Sharpston's Opinion of 12.12.2013, par. 77–78. The case concerned the application of Third Country Nationals to review the legal reasoning of the Dutch authorities' decision on their application for residence permits. The Court ruled that the analysis or the minutes are not personal data and do not fall within the scope of the right of access under Directive 95/46/EC and thus disclosing the whole legal analysis, i.e. providing a copy thereof, was not necessary, whereas a summary only of the personal data contained in the applicants' files was enough.

[34] Article 15 (1) (e) Directive 2016/680.

[35] Advocate General Sharpston's Opinion of 12.12.2013, par. 77, op. cit.

[36] Article 3 (10) and Recital 22 Directive 2016/680.

on the transmission of the data to any of these authorities shall be excluded from the information to be provided to the data subject.

Shortly put, Article 14 (c) Directive 2016/680 unfortunately does not oblige the data controller to provide complete information as to who has received the data of the data subject.

5.4 Envisaged Storage Period (Article 14 (d))

The controller should inform the data subject of the envisaged storage period. If this is not possible, the controller should at least indicate the criteria according to which the storage period will be determined. However, one should be aware that the purpose(s) of the processing might change. If at the time of the access request the future change of purpose is already certain and it is known that it would lead to a longer storage period, then for the sake of transparency the controller had better communicate the exact storage period or the criteria for determining it. However, if this is not the case but the purpose changes later, the data subject might not be aware of the new storage period and as explained above, the data controller is not obliged to inform the data subject of the purpose change.

5.5 Existence of Other Rights (Article 14 (e))

The controller should clearly indicate to the data subject that he may request the rectification, erasure or restriction of processing of his data. Such requests could follow after the data subject has examined the data undergoing processing and detected irregularities, e.g. the data is incorrect (such as wrong spelling of his name) or that data not concerning the applicant are wrongly attributed to him and have to be deleted.

Directive 2016/680, unlike the GDPR, does not grant data subjects the right to object to the processing of their data and it is questioned why data subjects are deprived of this right. Thus, also the data controller cannot inform the data subject of his non-existing right to object.

Another missing point is the obligation of the controller to disclose the existence of automated decision-making such as profiling, the algorithmic logic of the processing and the potential consequences for the data subject.[37] Nowadays the law-enforcement authorities are using more and more profiling techniques which could impact data subjects, even if this software does not itself take the final decision, e.g. PNR profiling which assesses the risk of each passenger.[38] While disclosing the exact logic of the algorithms might sometimes endanger the work of the law-enforcement authorities, it is not clear why the data subject may not be made aware of the mere existence of such automated decision-making. This might be needed in cases when even if the data is correct, the software might still wrongly process the data, e.g. a technical failure in the matching of biometric data when someone's fingerprints are matched against the

[37] Compare Article 15 (1) (h) GDPR.

[38] Article 6 EU PNR Directive.

database of available fingerprints, e.g. of convicts. Not being aware of such automated decisions could prevent the data subject from challenging the conclusions.

5.6 Lodging a Complaint with the Supervisory Authority (Article 14 (f))

This provision concerns the general right of data subjects to submit a complaint to the supervisory authority of their choice when they consider that the processing of their data infringes the provisions of Directive 2016/680.[39] Thus, the purpose of the provision is to inform the data subject of that right and provide them with the contact details of the supervisory authority, i.e. to facilitate the exercise of that right. This is compatible with the obligation of the controller in Article 17 (2) to inform the data subject that, in case the controller refuses to grant him access to his data, the data subject may exercise his right of access indirectly, via the supervisory authority.

6 The Right of Access Is Not Absolute

As already indicated above, the data subject's right of access to his data is not absolute. The data controller may wholly or partially restrict it if **four conditions** are met. First, the limitation must be based on a legislative measure adopted by the Member States. Second, the restriction may apply only for as long as it constitutes a necessary and proportionate measure. Third, due respect has to be taken of the fundamental rights and legitimate interests of the data subject.[40] In that regard, any limitation should be compatible with the CFREU and the ECHR.[41]

Fourth, the restriction should pursue at least one of the legitimate purposes provided in Article 15 (1) Directive 2016/680, namely:

(a) avoid obstructing official or legal inquiries, investigations or procedures;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security; (d) national security; (e) the rights and freedoms of others. However, as the AG in the *YS* case noted, the rights and freedoms of others do "not encompass the rights and freedoms of the authority processing personal data."[42]

These grounds for exemption are the same as the ones that applied under the 2008 Framework Decision [23].[43] Further, the Member States may adopt legislative

[39] Article 52 Directive 2016/680.

[40] Article 15 (1) Directive 2016/680.

[41] Recital 46 Directive 2016/680 and CJEU, C-465/00, 138/01, 139/01 *Öster- reichischer Rundfunk*, 20.05.2003. In that case the CJEU ruled that if a limitation on the data protection rights of individuals is not compatible with the fundamental rights, e.g. to privacy as enshrined in the ECHR and by extension nowadays in the CFREU, then the limitations cannot be deemed to be compatible with provisions of secondary law, e.g. Directive 2016/680.

[42] Opinion of Advocate General Sharpston in the *YS* case, op. cit., par. 93 (4).

[43] Art. 17 (2) 2008 Framework Decision.

measures about the categories of processing which may be subject to exemption.[44] The grounds are phrased quite broadly and thus the controller would have a wide margin of appreciation making use of these exceptions. As some have noted, the restrictions on the right of access might end up easily curtailing the effectiveness of the right of access of the concerned individuals [24].

It is still to be seen how broadly the Member States would phrase the exemptions when implementing Directive 2016/680. For example, the German implementing law requires that when the recipients of the data are intelligence, military counter intelligence, constitutional protection authorities and other authorities involved in national security, then information about these recipients could be given to the data subject only if the concerned recipient gives its agreement [25].[45] This restriction is beyond the control of the data controller and leaves the recipients a wide margin of appreciation.

Further, the German legislator allows the controller to restrict the right of access also when data are stored only due to legal requirements or they are used only for purposes of data security or data protection audits, when granting the right of access would pose disproportionate effort and all measures have been taken to prevent their processing for other purposes.[46] The right of access could be denied also if the data subject does not provide enough information which allows the controller to find his personal data without disproportionate effort.[47] Thus, new grounds for denial of access have been added by the German legislator. It is questionable whether they are in line with Directive 2016/680.

If the controller restricts wholly or partly the right of access of a certain data subject, he should inform the data subject of the complete refusal or the restriction of access, including the reasons for the decision. This information is to be communicated to the data subject "in writing" and "without undue delay." If disclosing such information would undermine one of the legitimate grounds for the restriction, then the controller may omit it. However, he has to inform the data subject of his right to lodge a complaint with a supervisory authority and to seek a judicial remedy.[48] While it is clear that the controller has to inform the data subject about the refusal to grant access in whole, the wording of the provision does not make it clear whether in case of a partial refusal the controller may inform the data subject at least about which part of his request has been refused or he should omit both this information and the reasons for the partial refusal. Reading this provision in light of the purpose of the right of access, as a matter of principle the controller should inform the data subject also if he partially restricts the right of access.

In any case, it is positive that the controller is to be accountable about his decision by documenting the factual or legal reasons for the refusal and making them available to the supervisory authorities.[49]

---

[44] Article 15 (2) Directive 2016/680.

[45] § 57 (5) German implementing law.

[46] Ibid, § 57 (2).

[47] Ibid, § 57 (3).

[48] Article 15 (3) Directive 2016/680.

[49] Article 15 (4) Directive 2016/680.

7 Directive 2016/680 Imposes Procedural Requirements

The controller, the supervisory authorities, as well as data subjects will have to follow the procedures established by Directive 2016/680, as discussed in the present Section.

7.1 Direct Access Becomes the Rule, Indirect - The Exception

Article 14 Directive 2016/680 is phrased in a way which suggests that the data subject may in all cases **directly** contact the data controller to request access to his own data [26]. The benefit of this direct contact is evident from the *Khelili* case discussed in Sect. 3. However, in the cases in which the controller decides not to grant him full or any access to his data, then the data subject may turn to the competent supervisory authority.[50] It is the controller who should make the data subject aware of this possibility.[51] When the data subject turns to the supervisory authority, the latter should carry out the necessary checks, e.g. check which data concerning the data subject are processed, whether the processing is lawful, whether the data are correct, etc. The supervisory authority should inform the data subject "at least" that the necessary verifications and/or review have been carried out and that the data subject may apply for a judicial remedy.[52] This means that further information may also be provided. Whether and which additional information may be further provided should be assessed on a case-by-case basis in accordance with the principles of proportionality and necessity. For example, an innocent person's name might be entered in a police database because of a spelling mistake. When the supervisory authority establishes and corrects this mistake, it seems unproblematic to communicate to the data subject the fact that there was a spelling mistake which was corrected. In that scenario the data subject still exercises his right of access, but only **indirectly**. Similarly, the ECtHR reached several times the conclusion that if direct access cannot be granted to the data subject, due to the need to balance different interests, then at least the decision of the controller should be reviewed by an independent authority.[53]

However, it is questionable whether indirect access fulfills the main purposes of the right of access, e.g. whether the supervisory authority is always in a position to detect irregularities, ensure they are rectified and if not, then the question arises how a data subject can pursue his case in court if he does not have access to his data and might not know whether the supervisory authority rectified the illegalities. Another problem is that the information which the supervisory authority may disclose will have to be "approved" by the law enforcement and possibly other authorities. This challenges the requirement that supervisory authorities be independent.[54] As the EDPS noted with regards to the Proposal for a EUROJUST Regulation, for an independent supervisory

[50] Article 17 (1) Directive 2016/680; also §57 (7) and §59 German Implementing Law.

[51] Article 17 (2) Directive 2016/680.

[52] Article 17 (3) Directive 2016/680.

[53] ECtHR, *Amann* and *Gaskin,* op. cit.

[54] Article 42 Directive 2016/680.

authority which is subject to court oversight, the decision should be taken independently, after consultation with the controller [36].

Granting data subjects the right of **direct** access, unless a restriction applies, represents a departure from current practice. For example, the right of access under the 2008 Framework Decision, SIS II and VIS may be exercised through the national supervisory authority which may decide what and how information is to be communicated to the data subject.[55] Other instruments, e.g. the EU PNR Directive and EURODAC Regulation simply refer the 2008 Framework Decision for the exercise of data subjects' rights, i.e. they allow for indirect access.[56] Now certain Member States might need to align their procedures with Directive 2016/680. As a result, access under the other instruments might also become direct, which might harmonize the access procedures under the different instruments. However, it is yet to be seen whether the procedures will be amended and whether instruments such as SIS II and VIS will be amended accordingly.

7.2 The Controller Should Communicate with the Data Subject Intelligibly and in a Timely Fashion

The controller should communicate in "clear and plain language," using "concise, intelligible and easily accessible form."[57] This is supposed to help data subjects actually comprehend the data processing and how they are affected by it. The controller should also facilitate the exercise of the rights, e.g. of access, and provide it free of charge if the request is not excessive or manifestly ill-founded. Otherwise he could charge a fee or even refuse the request, bearing the responsibility for proving that the request was excessive or ill-founded.[58]

Pursuant to Article 12 (5), the data controller may take measures to make sure that the applicant is the concerned data subject in case he has doubts about his identity.

Articles 12 and 14 Directive 2016/680 do not impose hard limits on the data controller to respond to a request by the data subject, unlike some AFSJ instruments.[59] He only has to inform the data subject of the follow-up to his request "without undue delay."[60] For example, in the case of *Haralambie* the ECtHR ruled that granting access to the requested data only six years after the request was submitted was not compatible with Article 8 ECHR [27].[61] Similarly, in the *Yonchev* case the ECtHR held that the

---

[55] Article 58 (1) and (2) Council Decision SIS II; 14 (1) and (2) VIS Council Decision; Article 17 (1) (a) 2008 Framework Decision.

[56] Article 13 (1) EU PNR Directive and 33 (1) EURODAC Regulation.

[57] Article 12 (1) Directive 2016/680.

[58] Article 12 (2) and (4) Directive 2016/680.

[59] E.g. Article 14 (6) VIS Council Decision and Article 58 (6) Council Decision SIS II. How are they different.

[60] Article 12 (3) Directive 2016/680.

[61] ECtHR, *Haralambie v Romania*, application no. 21737/03, 27.10.2009. The applicant wanted to know whether the security services had a file on him from the time during the Communist regime. A file indeed existed, but the applicant was allowed to see it only 6 years after he filed the request.

fact that the applicant was refused with finality access to his file only 5 years after the application for access was unduly long [28].[62]

8 Challenges Still Remain

The right of access under Directive 2016/680 is already a step forward towards more law enforcement accountability and transparency. Nevertheless, one should take into account the broader picture of law-enforcement use of personal data in the EU, including in the framework of EUROPOL, EUROJUST, SIS II, VIS and EURODAC, where different procedures on the right of access apply. This causes frictions, which take away from the effectiveness of the right of access.

8.1 Data Protection in the Law-Enforcement Sector in the EU Remains Fragmented

The first problem is the variety of law enforcement authorities processing personal data, the different information systems they operate with and thus the applicability of several legal instruments on data protection. Which authorities – national and European - process the personal data of a specific individual might not be known to the concerned data subject.

For example, a national authority may disclose the data which it holds on a data subject on one or several national information systems upon his request under Directive 2016/680. It is not clear whether the contacted authority also has an obligation to disclose information about data stored on the data subject on the EU-wide SIS II or whether the data subject has to file a separate request for access under the SIS II Council Decision. This is likely to depend on whether the contacted national authority is also a controller for SIS II or whether one will interpret the notion of "controller" broadly to mean that, e.g. any police authority if contacted has to provide access concerning all files held by the different police authorities in the particular Member State. Still in the case of SIS II, the decision on disclosure of SIS II data would be influenced by the Member State which entered the alert if the alert was not entered by the authority to which the data subject filed his request.[63] In case of denial of access in such cross-border cases effective cooperation between national supervisory authorities will be needed. It is also not clear whether in deciding if a restriction on the right of access applies in the case of SIS II only the grounds for exemption in Article 58 (4) Council Decision SIS II apply or also the ones in Article 15 Directive 2016/680.

EUROPOL and EUROJUST add another level of complexity. As EU agencies, they fall outside the scope of Directive 2016/680. Thus, if a national authority has

[62] ECtHR, *Yonchev v. Bulgaria*, application no. 12504/09, 7.12.2017, par. 61. The applicant requested access to the results of his psychological assessment as an applicant for a police mission abroad. It was refused on grounds of confidentiality. It turned out that the documents were not confidential, the decision was taken by a body which was not entitled to take such decisions and the procedure had taken too long.

[63] Article 58 (3) Council Decision SIS II.

forwarded data to EUROPOL, it is assumed that it will notify the data subject of this disclosure, pursuant to Article 14 (c) Directive 2016/680. However, EUROPOL might hold further data on the same data subject, obtained from other sources. To obtain access to all the data held on him by EUROPOL the data subject has to trigger the procedure prescribed by the EUROPOL Regulation, which provides for indirect access only via the national authority of the respective Member State, following a lengthy and complex procedure [29].[64]

Last but not least, the Commission has been promoting the concept of interoperability between the different AFSJ databases. This could lead to, amongst others, quicker and easier law enforcement access to data, e.g. on VIS and EURODAC, as well as new databases, e.g. the Multiple Identity Detector (MID) and the Common Identity Repository (CIR) [30, 31].[65]

The two interoperability proposals refer to the data subjects' rights as enshrined in the GDPR and Regulation 45/2001 on data protection by the EU institutions, bodies and agencies [32].[66] No references are made to Directive 2016/680.[67] This is peculiar since, for example, a law-enforcement authority such as SIRENE in the framework of SIS II, which could fall under Directive 2016/680, could qualify as a data controller in the context of MID.[68] However, for the definition of controllers the proposals refer only to the GDPR, although the processing of data in SIS II in the law enforcement context is subject to Directive 2016/680 [33].[69] It is not clear whether excluding the application of Directive 2016/680 is a mistake or not. The result is that if the proposal is not modified accordingly, then interoperability will lead to additional fragmentation and complication in the exercise of the right of access.

8.2 The Blurred Lines Between Law Enforcement and National Security Challenge the National Security Exemption in Directive 2016/680

Another problem are the blurred lines between law enforcement and national security authorities. The latter do not fall within the scope of Directive 2016/680.[70] For example, the PNR Directive, whose purpose is the fight against terrorism and serious crime,[71] poses challenges. The reason is that the PNR Directive leaves freedom to each Member State to establish or designate the authority which is responsible for fighting terrorism and serious crime and which will process PNR data, called Passenger Information Unit (PIU).[72] In some Member States the PIU is part of the national

[64] Article 36 EUROPOL Regulation.

[65] EU Interoperability Proposal 1 and 2, 2017.

[66] Regulation (EC) No 45/2001.

[67] Article 47 Proposals COM (2017) 794 final, Brussels 12.12.2017 and COM (2017) 793 final, 12.12.2017 op. cit.

[68] Article 29 (2) COM (2017) 794 final, Brussels, 12.12.2017, op. cit.

[69] See also Article 64 SIS II Proposal 2016.

[70] Recital 14 Directive 2016/680.

[71] Article 1 (2) EU PNR Directive.

[72] Article 4 (1) EU PNR Directive.

security agency [34, 35]. Normally national security falls outside the scope of Union law and by extension Directive 2016/680.[73] However, Directive 2016/680 and the procedures on the right of access in it are applicable to the PNR. Thus, when PIUs handle access requests, they have to follow the procedure established in Articles 12, 14, 15 and 17 Directive 2016/680.[74] The increasing role that security/intelligence authorities play in law-enforcement matters demonstrates that the separation between them in terms of the applicability of Directive 2016/680 is difficult to explain and may be detrimental for the consistent enforcement of the right of data subjects.

9 Conclusion

The discussion above demonstrates that the right of access to one's data under Directive 2016/680 is expected to improve the transparency and accountability of the law-enforcement sector and to trigger amendments to the currently existing procedures on right of access under the AFSJ instruments in force. In how far the new procedures for its exercise will be harmonized on national level and how broadly the exemptions of the right of access will be framed is still to be seen after the Member States adopt the necessary implementing laws. However, as the discussion evidenced, deficiencies can already be identified in terms of the transparency it seeks to ensure and consistency across the law enforcement authorities' data protection obligation on EU and Member State level. The problems can be summarized as follows:

1. The right does not include essential information such as on profiling measures and the recipients of the data;
2. The fact that the right is to be exercised against controller in a world of many interconnected controllers might make it difficult for the data subject to obtain a thorough overview of his data;
3. The different controllers are subject to different legal frameworks and procedures which causes fragmentation.

An ideal solution would be the harmonization of the substantive and procedural provisions on the right of access in all instruments. However, the fragmentation reflects the evolution of Member State police cooperation and EUROPOL as special areas, which might make harmonization politically challenging.

References

1. The Schengen Information System: A Guide for exercising the right of access. SIS II Supervision Coordination Group, p. 8, October 2015
2. Charter of Fundamental Rights of the European Union, O.J. C 364, 2000/C364/01, 18 December 2000

[73] Article 2 (3) Directive 2016/680.

[74] Article 13 EU PNR Directive j Article 59 Directive 2016/680.

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, O.J. L 251, 23 November 1995
4. 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), O.J. L 119, 4 May 2016
5. Principle 6 Recommendation No. R (87) 15, Council of Europe, Committees of Ministers to Member States regulating the use of personal data in the police sector, 17 September 1987
6. 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, O.J. L 119/89-131
7. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L. 350/60-71, 30 December 2008
8. Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, ("Council Decision SIS II"), 7 August 2007
9. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, p. 132–149 ("EU PNR Directive"), 4 May 2016
10. Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, pp. 129–136 ("VIS Council Decision"), 13 August 2008
11. Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, O. J. L 180/1-30, ("EURODAC Regulation"), 29 June 2013
12. Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981
13. ECtHR, Gaskin v the United Kingdom, Application no. 10454/83, 07 July 1989
14. ECtHR, Khelili v Switzerland, Application no. 16188/07, 18 October 2011
15. ECtHR, Segerstedt-Wiberg and Others v. Sweden, Application no. 62332/00, 6 June 2006
16. ECtHR, Amann v Switterland, Application no. 27798/95, 16 February 2000
17. CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v M.E. E. Rijkeboer, 7.05.2009, Opinion of the Advocate General Ruiz-Jarabo Colomer, par. 33 and 34, 22 December 2008

18. L'Hoiry, X., Norris, C.: Introduction – the right of access to personal data in a changing european legislative framework. In: Norris, C., de Hert, P., L'Hoiry, X., Galetta, A. (eds.) The Unaccountable State of Surveillance. LGTS, vol. 34, pp. 1–8. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-47573-8_1
19. C 141/12 and C 372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M, 17 July 2014
20. CJEU, C-434/16, Peter Nowak v Data Protection Commissioner, Opinion of Advocate General Kokott, 20 July 2017
21. Bäcker, M.: Art. 23 Beschränkungen. In: Jürgen Kühling, J., Buchner, B. (eds.) Datenschutz-Grundverordnung: Kommentar, p. 486, par. 14, C.H.Beck (2017)
22. Galetta, A., de Hert, P.: A European perspective on data protection and the right of access. In: Norris, C., de Hert, P., L'Hoiry, X., Galetta, A. (eds.) The Unaccountable State of Surveillance. LGTS, vol. 34, pp. 21–43. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-47573-8_3
23. CJEU, C-465/00, 138/01, 139/01 Österreichischer Rundfunk, 20 May 2003
24. De Hert, P., Papakonstantinou, V.: The new police and criminal justice data protection directive: a first analysis. New J. Eur. Crim. Law **7**(1), 12 (2016)
25. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Bundesgesetz- blatt Jahrgang 2017 Teil I Nr. 44, Bonn, ("German Implementing Law"), 05 July 2017
26. Computers, Privacy and Data Protection (CPDP) 2017 Conference. https://www.youtube.com/watch?v=g7YYlrxQe20
27. ECtHR, Haralambie v Romania, application no. 21737/03, 27 October 2009
28. ECtHR, Yonchev v. Bulgaria, application no. 12504/09, 7 December 2017
29. Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, O.J. L. 135/53-114, ("EUROPOL Regulation"), 25 May 2016
30. Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM (2017) 794 final, Brussels ("EU Interoperability Proposal 1"), 12 December 2017
31. Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, COM (2017) 793 final, ("EU Interoperability Proposal 2"), 12 December 2017
32. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ.L. 8/1-22, ("Regulation 45/2001"), 12 January 2001
33. Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EUCOM (2016) 883 final, Brussels ("SIS II Proposal 2016"), 21 December 2016

34. The European Parliament adopted the Passenger Name Record (PNR) Directive for the Passengers with EU Air Carriers. The Republic of Bulgaria, Commission for Personal Data Protection, 19 April 2016. https://www.cpdp.bg/en/index.php?p=news_view&aid=954
35. Article 11 (a) Law on the State Agency "National Security" of the Republic of Bulgaria, Official Journal 109, 20 December 2007. Latest amendment: 19 January 2018
36. European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO'), Brussels, p. 18, par. 91, 5 March 2014

Legislative Compliance Assessment: Framework, Model and GDPR Instantiation

Sushant Agarwal(✉), Simon Steyskal(✉), Franjo Antunovic(✉), and Sabrina Kirrane(✉)

Vienna University of Economics and Business, Vienna, Austria
{sushant.agarwal, simon.steyskal, franjo.antunovic, sabrina.kirrane}@wu.ac.at

Abstract. Legislative compliance assessment tools are commonly used by companies to help them to understand their legal obligations. One of the primary limitations of existing tools is that they tend to consider each regulation in isolation. In this paper, we propose a flexible and modular compliance assessment framework that can support multiple legislations. Additionally, we describe our extension of the Open Digital Rights Language (ODRL) so that it can be used not only to represent digital rights but also legislative obligations, and discuss how the proposed model is used to develop a flexible compliance system, where changes to the obligations are automatically reflected in the compliance assessment tool. Finally, we demonstrate the effectiveness of the proposed approach through the development of a General Data Protection Regulatory model and compliance assessment tool.

Keywords: Compliance · GDPR · ODRL

1 Introduction

The interpretation of legal texts can be challenging, especially for people with non-legal backgrounds, as they often contain domain-specific definitions, cross-references and ambiguities [29]. Also, generally speaking legislations cannot be considered in isolation, for instance European Union (EU) regulations often contain opening clauses that permit Member States to introduce more restrictive local legislation. Additionally, depending on the legislative domain additional legislations may also need to be consulted. For example, when it comes to data protection in the EU, in addition to the General Data Protection Regulation (GDPR) [4], the upcoming e-privacy regulation (for e-communication sector) [5] or the Payment services (PSD 2) directive (for payments sector) [3] may also need to be consulted. As such, ensuring compliance with regulations can be a daunting task for many companies, who could potentially face hefty fines and reputation damage if not done properly. Consequently, companies often rely on legislative compliance assessment tools to provide guidance with respect to their legal obligations [8].

Over the years, several theoretical frameworks that support the modelling of legislation have been proposed [7, 10, 14, 22, 23, 25, 32], however only some of which were validated via the development of legal support systems [7, 10, 23, 25, 32]. One of

M. Medina et al. (Eds.): APF 2018, LNCS 11079, pp. 131–149, 2018.
https://doi.org/10.1007/978-3-030-02547-2_8

the major drawbacks of such approaches is the fact that some do not consider concepts like soft-obligations (i.e. obligations that serve as recommendations rather than being mandatory) [22, 25] or exceptions (i.e. scenarios where the obligations are not applicable) [10, 29]. Additionally generally speaking the models are only loosely coupled with the actual legislation text, making it difficult to verify the effectiveness of such systems. More recently, a number of compliance assessment tools have been developed [18, 26, 28]. However, these systems are either composed of a handful of questions that are used to evaluate legal obligations [18] or do not filter out questions that are not applicable for the company completing the assessment [26, 28]. One of the primary drawbacks of existing compliance assessment tools is the fact that they do not currently consider related regulations.

In order to address this gap, we propose a generic legislative compliance assessment framework, that has been designed to support multiple legislations. Additionally, we extend the Open Digital Rights Language (ODRL) [34] (which is primarily used for rights expression) so that it can be used to express legislative obligations. Both of which are necessary first steps towards a context dependent compliance system that can easily be adapted for different regulatory domains.

The contributions of the paper are as follows: (i) we devise a flexible and modular compliance assessment framework, which is designed to support multiple legislations; (ii) we propose a legislative ODRL profile that can be used to model obligations specified in different legislations; and (iii) we develop a dynamic compliance system that can easily be adapted to work with different legislations. The proposed framework is instantiated in the form of a GDPR compliance assessment tool, which is subsequently compared with alternative approaches.

The remainder of the paper is structured as follows: Sect. 2 presents different approaches that can be used to model data protection legislations, along with compliance assessment tools for the GDPR. Section 3 details our framework that decouples the legislative obligations from the compliance assessment tool. Section 4 introduces our legislative model and illustrates how it can be used to model the GDPR. Section 5 describes the compliance tool. In Sect. 6 we compare and contrast our proposal with alternative solutions. Finally, Sect. 7 concludes the paper and presents directions for future work.

2 Related Work

Although the modelling of legal text has been a field of study for many years, in this section we discuss those that focus on the modelling of data protection related legislations, and present three different tools that have been developed to help companies to comply with the GDPR.

Barth et al. [7] present a theoretical model for the representation of privacy expectations that is based on a contextual integrity framework [27]. The approach is validated via the modelling of the Health Insurance Portability and Accountability Act