EJLT European Journal of Law and Technology

Legal consistency after the General Data Protection Regulation and the Police Directive

Bart van der Sloot[1]

Abstract

The General Data Protection Regulation (GDPR) and the Police Directive (PD) have replaced the Data Protection Directive 1995 and the Framework Decision 2008 in the European Union (EU). Both the EU and the Member States' legislative corpus needs to be in full compliance with these new rules, also taking into account the jurisprudential standards developed by the European Court of Justice and the European Court of Human Rights with respect to the fundamental rights to privacy and data protection. This article suggests that although the GDPR and the PD bring legal consistency in the field of data protection throughout the EU and even globally, it might have a negative effect on the legal inconsistency vis-à-vis other fields of law.

1. Introduction

The General Data Protection Regulation (GDPR),[2] replacing[3] the Data Protection Directive (DPD) from 1995,[4] has come into effect in May 2018.[5] The newly adopted Police Directive (PD) [6] specifies the data protection rules for the police and other law enforcement authorities, and repeals[7] the Framework Decision (FD) of 2008 as of May 2018.[8] Obviously, many European Union (EU) documents, national laws and international agreements are affected by the new data protection framework. Both the GDPR and the PD contain provisions on the reforms that need to be taken by the EU and the Member States (MSs) and the effect both texts have on existing legal instruments. The GDPR clarifies its relationship[9] with the e-Privacy Directive[10] and with previously concluded agreements,[11] and, more importantly, contains two substantive provisions on the legislative reforms that need to be initiated.

First, it specifies that by May 2020, a review and evaluation should be held, in which the application and functioning of the GDPR shall be assessed, in particular in relation to the rules on the transfer of data to third countries and the rules on cooperation and consistency.[12] Second, it specifies that the Commission shall 'if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.'[13]

The Police Directive, which has the Member States as its main addressee,[14] is perhaps even more explicit on the reforms that need to be initiated. Still, it specifies that the specific provisions

for the protection of personal data in Union legal acts that came into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the treaties within the scope of the Directive, shall remain unaffected.[15] In addition, it makes clear that international agreements involving the transfer of personal data to third countries or international organisations, which were concluded by Member States prior to 6 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.[16]

There are two provisions on the specific legislative reforms that follow from the adoption of the PD. First, by May 2020, there should be a review and evaluation of the PD. Again, this review should have special attention for the rules on the transfer of personal data to third countries or international organisations outside the EU.[17] Second, 'Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018. When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.'[18]

Consequently, there is a need to bring both the EU legislative corpus and that of the Member States in conformity with the GDPR and the PD. What is important to point out is that both instruments mention in particular the rules on the transfer of data to third countries. Obviously, this focus has been spiralled by the recent European Court of Justice (ECJ) decision[19] on the safe harbour[20] and the subsequent developments.[21] Because both privacy and data protection are contained in the EU's Charter of Fundamental Rights (Charter)[22], and because the ECJ oversees the respect for these fundamental rights, the question whether the EU's and Member State's legislative corpus are in conformity with the data protection rules and principles depends ultimately on the ECJ's interpretation of the GDPR and the PD, and of the fundamental rights contained in the Charter. The ECJ assesses the principles of proportionality and necessity and determines whether certain provisions or legislative documents might undermine the essence of the right to privacy and data protection. It can ultimately invalidate Directives and Regulations.

In addition, the Charter specifies that it 'contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'[23] Consequently, not only the Schrems decision, but also cases like the Tele2,[24] Digital Rights Ireland[25] and Google Spain[26] should be taken into account when bringing the laws and instruments into conformity with the data protection rules and principles. In addition, Member States also have to adhere to the decisions of the European Court of Human Rights on matters concerning Article 8 of the European Convention on Human Rights (ECHR),[27] containing the right to privacy. All members of the EU are also members of the Council of Europe's ECHR.[28] Like the ECJ, the ECtHR has been very outspoken on the processing of personal data, inter alia in its recent Zakharov[29] and the Szábo & Vissy cases.[30]

This means that there is a very complex web of rules, standards and jurisprudential principles that both the EU and the Member States have to take into account when bringing their legislative corpus into conformity with the data protection rules and principles. Not for nothing, the European Parliament (EP) requested by means of a Pilot Project in the EU budget the creation of an independent expert group to carry out a fundamental rights review of any existing EU

legislation, instrument or agreement with third parties that involves the collection, retention, storage or transfer of personal data. The Pilot Project would establish and support an independent expert group responsible for reviewing the compliance of EU data collection instruments and mechanisms with the EU Charter of Fundamental Rights, with particular attention being paid to the application of the proportionality principle and to an assessment of relevant safeguards for the fundamental rights to privacy and the protection of personal data. The four general tasks for the expert group are:

(1) Cataloguing existing EU legislation (and any related national transposition laws), law-enforcement instruments and cooperation, and third-party agreements involving the collection, retention, storage or transfer of personal data;

(2) A legal analysis and fundamental rights review in the light of the most recent EU case law in the field of privacy and the protection of personal data;

(3) Analysing and assessing compound effects of existing EU data collection programmes, with a view to identifying potential fundamental rights loopholes and interference with those rights;

(4) Drawing up specific policy recommendations for each element identified and reviewed.[31]

In a similar vein, the European Commission's (EC) DG JUST (Directorate-General Justice and Consumers) has commissioned[32] a research project in which it called for:

(1) The creation of a catalogue of existing EU legislation (and any relevant related national transposition laws), law-enforcement instruments and cooperation, and third-party agreements, including those with third countries and international organisations, involving the processing (including collection, retention, storage or transfer) of personal data.

(2) A fundamental rights review of EU data collection instruments, in which the legislation catalogued will be reviewed against the requirements of the fundamental rights ensured by the Charter of Fundamental Rights of the European Union (CFR) and the European Convention on Human Rights (ECHR), in particular against the requirements of the case law on Articles 7 and 8 of the CFR of the Court of Justice of the European Union and the case law on Article 8 of the ECHR of the European Court of Human Rights.

(3) The review foreseen in Article 62(6) of the Police Directive, for which the existing EU acts on data protection for police and criminal justice authorities should be examined and compared with the provisions of the Police Directive.

(4) Drawing up specific recommendations for revising the legislative corpus.[33]

Such reviews seem necessary, but at the same time, a full and comprehensive revision of the entire legislative corpus may be virtually impossible. This article will not discuss what the new rules and principles in the GDPR and the PD are; these include, but are not limited to, the requirement to perform a Data Protection Impact Assessment (DPIA), appoint a Data Protection Officer (DPO) and tightened rules on the validity of consent.[34] Rather, it starts by stressing that one of the main goals of the GDPR and the PD is to increase consistency in the data protection laws of EU Member States (section 2). Subsequently, the scope and applicability of these standards will be discussed (section 3). Given the wide applicability of the GDPR and the PD, many legislative instruments may be affected; so many that consistency between data protection rules and other fields of law that incorporate an element of data processing seems hard to achieve (section 4). The question is what kind of consistency the EU achieves through the adoption of the GDPR and the PD; although it may have a harmonising effect in one particular field of law, it may

result in inconsistency between the data protection framework and other fields of law (section 5). The article concludes with some final observations (section 6).

2. Legal consistency: one of the main objectives of the GDPR and the PD

There has been a trend of harmonisation of data protection rules on a European level. The two resolutions of the Council of Europe from 1973 and 1974 were quite literally one-pagers and the Council of Europe merely recommended member states of the CoE to adopt rules to protect the principles contained in the Resolutions.[35] It was at their discretion to implement sanctions or rules regarding liability. Only in the Convention of 1981 was it explicitly provided that '[e]ach Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.'[36] The explanatory report to the Convention stressed that this could either be done through civil, administrative, or criminal sanctions.[37] Moreover, the Convention explicitly provided a number of rules regarding the application and enforcement of the rule on transborder data flows;[38] it stimulated, *inter alia*, the cooperation between states and the national Data Protection Authorities to assist each other by providing full and detailed information of their laws and of data processing within their borders[39] and it specified that states and DPAs should assist citizens living abroad, on the territory of another state.[40] Finally, the Convention installed a Consultative Committee, [41] which could advise the Committee of Ministers (CoM) on revising the Convention.[42]

The adoption of an EU-wide Directive in 1995[43] was aimed at bringing uniformity in the national legislations of the different countries,[44] in order to provide an equal level of protection,[45] but also to facilitate the transfer of personal data in Europe.[46] This uniformity was further promoted by providing further and more detailed rules for cross-border data processing.[47] For example, personal data may only be transferred to third countries if they have an adequate level of data protection, similar to that of the European Union.[48] The Article 29 Working Party (WP29) was installed, consisting of the representatives of all national DPAs, and with a broad mandate to give opinions on almost every aspect of the Directive – on how it should be interpreted, implemented, and amended, etc.[49] The Directive also specifies that the Commission shall be assisted by a Committee composed of the representatives of the Member States when adopting measures pursuant to the Directive.[50]

The explicit goal of the GDPR is to further harmonisation. It stresses that although the DPD sought to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between MSs,[51] technological developments and globalisation allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.[52] Those developments require a strong and more coherent data protection framework in the EU, backed by strong enforcement, according to the GDPR.[53] The reason to adopt the GDPR, replacing the DPD, is to prevent legal uncertainty.

'The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal

data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC. In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. '[54]

In short, there are three problems with legal consistency the GDPR and PD address.

- First, the lack of harmonisation of rules on MSs level. There were major differences in how MSs had implemented the rules of the DPD and FD in their national legislation. This both undermined the protection of rights of natural persons and the transfer of personal data across the EU, as data processing organisations still had to comply with other rules in, say, Germany than in the Bulgaria. Although MS are still at the discretion to adopt special rules for processing sensitive personal data and for fields in which data protection clashes with other legal principles,[55] such as the freedom of expression,[56] this problem is addressed by adopting a regulation instead of a directive for the general data protection framework and a directive instead of a framework decision for the data protection principles in the law enforcement sector.
- Second, the enforcement of the data protection rules was invested with national data protection authorities. As a result, there were differences in how the rules were applied and violations sanctioned. Consequently, international companies established themselves in countries where the regulatory burden was low and the enforcement of the rules was weak. This problem is tackled by the fact that the GDPR and PD place more emphasis on enforcing the rules by the EU itself, that there are more possibilities for cooperation for the various national enforcement bodies and that a so called one-stop-shop mechanism has been introduced.
- Third, the problem was that companies located outside the EU, in particular in the United States of America, lingered in respecting the data protection principles vis-à-vis EU data subjects. In addition, foreign law enforcement agencies often required EU based companies, with an establishment outside the EU, to provide access to the personal data in their possession, when this was deemed necessary for the protection of national security or public order. The new EU data protection framework addresses this issue by enlarging the territorial scope, among others including non-EU based companies that profile EU citizens or use personal data to offer goods or services to EU citizens and by specifying that any 'judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State'.[57]

3. The scope of personal data principles

Member States and the EU must bring their legislative corpus in conformity with the GDPR and PD. To understand which instruments will be affected, it is necessary to briefly point out the width of

the scope and applicability of these instruments. The EU data protection framework applies when (1) personal data, (2) are processed, (3) the EU has competence and (4) no exception is applicable.

First, the scope of 'personal data' has grown substantially over time in Europe. It includes both information about both an identified and an identifiable person and both direct and indirect identifiable information. The GPDR contains a non-exhaustive list of potential identifiers, such as 'a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'[58] The WP29 has clarified: 'Ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light. So, the question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case.'[59] As is acknowledged by the WP29 and is increasingly emphasised by scholars, the broadened scope of personal data brings with it that potentially all data could be personal data. Data which at one moment in time may contain no information about specific persons whatsoever, may in the future, through the use of advanced techniques, be used to identify or single out a person.[60] Moreover, data that may not directly identify a person can increasingly be linked to other data points, inter alia by interconnecting and harvesting databases, and can be used to create profiles.[61] Consequently, two or more non-identifying datasets may become identifying datasets if integrated.[62] It should also be stressed that both in the case law of both the ECJ and of the ECtHR, meta-data and aggregated data have occasionally also been provided protection under the right to privacy and data protection.[63] That is why many scholars have argued that in fact, all data are or can become personal data;[64] in addition, the EU has now proposed a regulation which will address the transfer of 'non-personal data'.[65]

Second, the data protection rules in the GDPR and the PD apply when personal data are processed. Processing is described inclusively as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[66] Consequently, even deleting personal data is considered processing. The GDPR applies to the processing of personal data when this is done 'wholly or partly by automated means'. It also applies to the processing, other than by automated means, of personal data which form part of a filing system or are intended to form part of a filing system.[67] A filing system is described as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.[68] Consequently, only a small number of offline activities involving personal data, such as handwritten notes, will not fall under the GDPR. The Regulation emphasises the technology neutrality of its application: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'[69]

Third, the territorial scope is broadened. Inter alia, the GDPR specifies that the data protection principles not only apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not, but also to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or the monitoring of their behaviour as

far as their behaviour takes place within the Union.[70] This means that most internet companies offering services to EU citizens and/or profiling them for advertising purposes, also those located in the United States of America (USA) and elsewhere, will need to comply with the principles set out by the GDPR. The broad applicability of the data protection principles outside the EU was also confirmed by the ECJ in Google Spain and Weltimo.[71] In addition, there are new rules on transborder dataflows in both the GDPR and the PD. These will need to be taken into account when revising and updating legal instruments and international agreements that may involve transferring personal data from EU soil to countries outside the EU. The recent Schrems case has obviously had a big impact on this doctrine. The ECJ invalidated the safe harbour agreement for a number of reasons.[72] Although a successor to the safe harbour agreement has been adopted, the Privacy Shield, it is clear that this will be challenged before court.[73] Obviously, the same principles that the Court has developed for transfer of data to the USA apply to the dataflows to other countries. European instruments that require or facilitate transborder dataflows should be re-evaluated on the relevant points as set out in the case law, in addition to those contained in the GDPR and the PD. Because many companies and countries cooperate with the EU and EU Member States, and because data processing is often an integral part of that, many companies and countries will need to abide by the EU data protection standards. This has been called the 'Brussels effect'.[74]

Fourth and finally, although the applicability of the GDPR and the PD is very wide, there are exemptions. Still, these exemptions are marginal. Two are of importance. First, when the processing of personal data takes place in the context of national security or common foreign and security policy of the Union.[75] Also, when data processing is necessary for the public interest, certain parts of the data protection framework may be limited, though the majority of the provisions still have to be respected.[76] Second, processing personal data for purely personal reasons by natural persons is exempted from the GDPR.[77]

4. The potential impact on the EU's and MS's legislative corpus

Given the broad scope of the data protection framework, perhaps not all, but quite a substantial part of the information being processed may fall under the scope of the data protection framework. As there is a trend towards data-driven decision making and policy making, most likely, in a decade or so, almost all activities will involve data processing one way or the other.[78] Consequently, repositories containing data should be assessed on the question of whether they contain personally identifiable information. If an EU document or a national law, for example, requires that a 'register' should be installed, there is a very high chance that this register will contain personal data. This may regard a name, home address or social security number, but it may be enough that there are indirect personal data registered. Essentially the same may be said about words such as 'document', 'file' or 'record'.

Of course, whether a register, document or file contains, in fact, personal data needs to be assessed on a case by case basis. But what is clear is that if the EU and the MSs want to bring their legislative corpus into full compliance with the EU data protection rules, they should at least analyse the legal instrument containing words such as 'file', 'document' and 'register', on the point of whether the new data protection framework has an impact on it and whether amendments to the law should be proposed.[79]

Therefore, the task of cataloguing existing EU legislation involving the processing of personal data will concern thousands of legislative acts. To support this point, Table 1 reports the results of an initial search in the EUR-lex database,[80] limited to three search terms 'document', 'file' and 'register' - the figures are further limited to EU Regulations, Directives and Decision.

Obviously, not all files, documents and registers will contain personal data and 'document', 'register' and 'file' may also be used in those texts as a verb and not as a noun. Moreover, there are doubles in these numbers, as one directive might for example contain both a reference to a register and a file.

On the other hand, these are not all types of instruments that will be relevant, because international agreements, treaties and other legal texts should be included as well. Moreover, there are other search terms that might be relevant. The exact number of relevant instruments is not important at this stage. What is important is that the number of instruments that might be relevant, that might be affected by the GDPR, the PD and/or the case law of the ECJ and the ECtHR, seems to be quite big.

	Register	Document	File
Regulation	7784 instruments	9927 instruments	2274 instruments
Directive	692 instruments	1293 instruments	643 instruments
Decision	3992 instruments	13466 instruments	2172 instruments

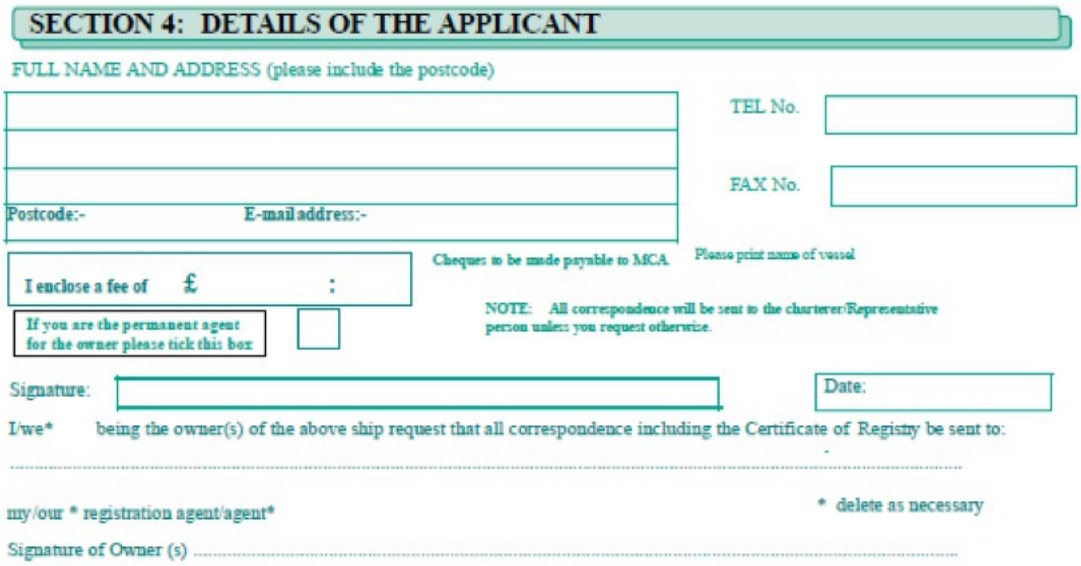
Table 1 Implicit references to the processing of personal data[81]

To provide an example, the first three hits when searched in Eurlex for 'register' are:[82]

- Regulation (EC) No 789/2004 of the European Parliament and of the Council of 21 April 2004 on the transfer of cargo and passenger ships between registers within the Community and repealing Council Regulation (EEC) No 613/91.
- Regulation (EC) No 166/2006 of the European Parliament and of the Council of 18 January 2006 concerning the establishment of a European Pollutant Release and Transfer Register and amending Council Directives 91/689/EEC and 96/61/EC.
- Regulation (EU) 2016/1627 of the European Parliament and of the Council of 14 September 2016 on a multiannual recovery plan for bluefin tuna in the eastern Atlantic and the Mediterranean, and repealing Council Regulation (EC) No 302/2009.

Neither of these documents refers to 'personal data' or to the DPD. But they all do seem to involve or require the processing of personal data to some extent.

The first regulation facilitates the transfer of personal data within EU member states. Its goal 'is to eliminate technical barriers to the transfer of cargo and passenger ships flying the flag of a Member State between the registers of the Member States while, at the same time, ensuring a high level of ship safety and environmental protection, in accordance with International Conventions.'[83] This means that if someone has a boat registered in the United Kingdom (UK) and wants to register it in France, both countries should in principle facilitate the transfer of the boat from one register to another. Such registers will contain personal data.



SECTION 4: DETAILS OF THE APPLICANT

FULL NAME AND ADDRESS (please include the postcode)

TEL No.

FAX No.

Postcode:- E-mail address:-

I enclose a fee of £ :

Cheques to be made payable to MCA

Please print name of vessel

If you are the permanent agent for the owner please tick this box

NOTE: All correspondence will be sent to the charterer/Representative person unless you request otherwise.

Signature:

Date:

I/we* being the owner(s) of the above ship request that all correspondence including the Certificate of Registry be sent to:

my/our * registration agent/agent*

* delete as necessary

Signature of Owner (s)

Figure 1 Part of the application form for registering a ship in Britain

The second regulation introduces the European Pollutant Emission Register (PRTR), which is a publicly accessible electronic database. Article 4 specifies among others: 'The Commission shall publish the European PRTR, presenting the data in both aggregated and non-aggregated forms, so that releases and transfers can be searched for andidentified by: (a) facility, including the facility's parent company where applicable, andits geographical location, including the river basin; (b) activity; (c) occurrence at Member State orCommunity level; (d) pollutant or waste, as appropriate; (e) each environmental medium (air, water, land) into which the pollutant is released; (f) off-site transfers of waste and their destination, as appropriate; (g) off-site transfers of pollutants in waste water; (h) diffuse sources; (i) facility owner or operator.' The owner of the facility or the operator may be a natural person, in which case it qualifies as personal data. Also, if the company is, for example, a one-man firm working as an independent contractor, the business will often be named after the owner, for example Beppe Grillo Limited Company. This would also qualify as personal data. Finally, in certain cases, 'the name and address of the recoverer or the disposer of the waste and the actual recovery or disposal site' should be reported.[84]

Finally, the third Regulation, inter alia, requires the keeping of fishing log books. It holds that fishing logbooks must specify at least dates and ports of departure, dates and ports of arrival, the vessel's name, register number, ICCAT number, international radio call sign, the fishing gear used, operations at sea with one line (minimum) per day of trip, the means of weight measure, and also the 'Master's name and address' and the 'Master's signature'.[85] This would again qualify as personal data.

This small sample shows that many EU documents referring to 'register' will require or have an impact on the processing of personal data. This does not mean that these documents need to be revised in full, but it does mean that if the EU wants to bring its entire legislative corpus into full compliance with the new data protection standards, it has to assess each and every document and analyse, first, whether indeed 'personal data' are indeed processed and second, assess whether the data protection rules and principles are upheld and whether the new rules in the GDPR or the PD, such as the obligation to do a DPIA or install a DPO or whether the tightened rules on the legitimacy of the data subject's consent have been respected. Essentially the same counts for the legislative corpus of the EU Member States, which means that a full review of 28 legal systems must be brought about. Instruments impacting the GDPR and/or the PD, such as potentially the new e-Privacy Regulation (EPR),[86] need to be identified as well as the potential changes they

bring about with regard to the data protection framework. In addition, the judgments of the ECJ and the ECtHR having an impact on the interpretation of the DPD, FD, GDPR and PD should be identified and analysed.

Direct references	Reference to "95/46"	Reference to "2008/977"	Reference to "2016/679"	Reference to "2016/680"	Reference to "personal data"
ECJ[87]	220 cases	4 cases	10 cases	6 cases	545 cases
ECtHR[88]	96 cases	2 cases	4 cases	0 cases	1065 cases

Table 2: Direct reference in case law to primary data protection instruments and 'personal data' [89]

Indirect reference	Reference to "document"	Reference to "file"	Reference to "information"	Reference to "record"	Reference to "register"
ECJ	13963 cases	8222 cases	18436 cases	4319 cases	11638 cases
ECtHR	8135 cases	6732 cases	8055 cases	3680 cases	1507 cases

Table 3: Indirect reference through the words 'document, 'file', information', 'record' and 'register' [90]

Both on EU and MSs level, the documents, instruments and laws that require or affect the processing of personal data, either directly or indirectly, such as by requiring files, registers, documents or other items containing personal data, should be identified, and it should be analysed to what extent the new rules of the GDPR and the PD, potentially complemented by the standards as described in the recent judgements of the ECJ and the ECtHR, require a revision of the documents, instruments or laws at EU or MSs level.

Although both the GDPR and the PD contain provisions on the mapping of legal instruments affected by the new data protection framework, and although both the EP and the EC have started initiatives to bring those instruments into conformity with the new standards, it may be almost impossible to achieve harmonisation on this point. Rather, it seems that given the fact that there is a trend to work with data both in the private and the public sector and because the concepts of personal data and processing are so wide, in time, almost every instrument that requires or regulates the processing of data, whether directly referring to the processing of personal data or indirectly, by referring to a register, file or document, may need to be revised and updated. This means that although the GDPR and the PD may have a positive effect on the harmonisation of the data protection provisions both on MSs level, EU level and even on a global level, it may have a negative effect on the consistency vis-à-vis other sectors of law.[91]

5. Legal consistency

Legal consistency is regarded as a prerequisite for legal certainty, which is deemed one of the pillars of the Rule of Law.[92] Without consistency, citizens and organisations alike do not know which rules apply to them and remain in the dark on how conflicts between rules must be resolved.[93] Hence, inconsistent laws or an inconsistent application of the law is deemed unjust

vis-a-vis the subjects of the law.[94] 'Inconsistency is one of the most frequent manifestations of unfairness that a person is likely to meet.'[95] As such, the goal of the EU in the field of data protection must be understood in a broader strategy to enhance legal consistency and harmonisation on an EU and MSs level.[96]

The aim of legal consistency is also embedded in the Treaty on the Functioning of the European Union (TFEU). Article 3 provides the domains in which the EU has exclusive competence and specifies that the EU 'shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.'[97] And Article 7 explicitly contains the general principle of legal consistency: 'The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.' Consistency of policies and laws is emphasised in 11 other articles in the TFEU[98] and a whole title is devoted to the subject of enhanced cooperation.

Still, there is no standard definition of or common approach to what legal consistency means or how it can be achieved. For example, consistency and coherence are often seen as twin-concepts. 'In the literal sense, though, consistency does not necessarily denote coherence and vice versa. In EU law, consistency is often defined as 'the absence of contradictions, whereas coherence refers to positive connections'. While recognising that EU policies shall be both consistent and coherent, [consistency can be referred to] as an all-encompassing principle rather than a precondition to coherence.'[99]

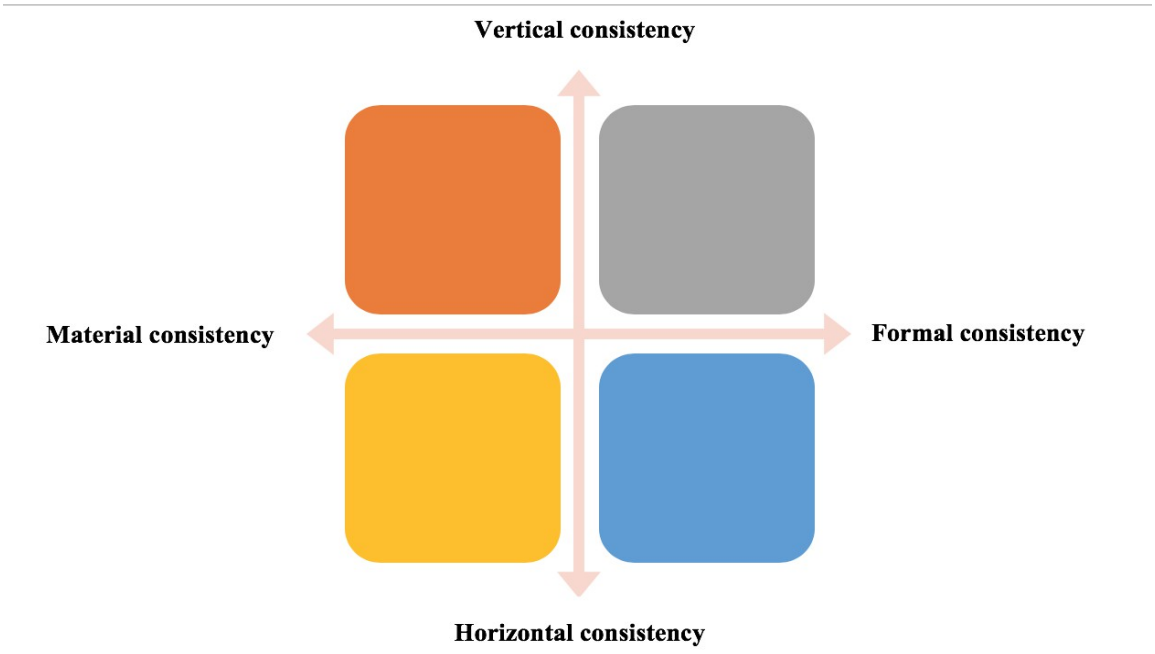
Among others, Lon Fuller describes consistency as one of the eight ground rules for good law-making, but also stresses that it 'is rather obvious that avoiding inadvertent contradictions in the law may demand a good deal of painstaking care on the part of the legislator. What is not so obvious is that there can be difficulty in knowing when a contradiction exists, or how in abstract terms one should define a contradiction. It is generally assumed that the problem is simply one of logic. A contradiction is something that violates the law of identity by which A cannot be not-A. This formal principle, however, if it has any value at all, has none whatever in dealing with contradictory laws.'[100]

The push for legal consistency may even come into conflict with the so-called 'subsidiarity principle' on EU. 'The principle of subsidiarity is defined in Article 5 of the Treaty on European Union. It aims to ensure that decisions are taken as closely as possible to the citizen and that constant checks are made to verify that action at EU level is justified in light of the possibilities available at national, regional or local level. Specifically, it is the principle whereby the EU does not take action (except in the areas that fall within its exclusive competence), unless it is more effective than action taken at national, regional or local level. It is closely bound up with the principle of proportionality, which requires that any action by the EU should not go beyond what is necessary to achieve the objectives of the Treaties.'[101]

Consequently, uniformity and consistency seem to come at the price of flexibility and openness. As the law can never fully foresee all potential aspects affected by a law nor specify in detail how general rules should be applied to specific circumstances, the law necessarily contains an element of openness and flexibility. The law maker sets the general standards, the court interprets how such general rules apply to specific instances. The push towards harmonisation and legal consistency can mean that the essential benefit of having open standards and norms in laws is lost. In addition, national democracy can be curtailed by such an EU agenda.

More importantly, legal consistency is not a flat and one sided concept, it is complex and multifaceted. In the EU context, at least two aspects should be distinguished:

- First, there is formal consistency and material consistency.
    - Material consistency is consistency on content of rules. This can be achieved if the EU adopts concrete standards that should be respected by all MSs. An example may be: 'Each MS may import no more than 20 kilo of Ivory per year'.
    - Formal consistency can be achieved by having open norms, allowing for exceptions. A formulation could be as follows: 'MSs should endeavor to promote a clean and healthy living environment, while keeping in mind the country's economic well-being.' MSs can then adopt their own interpretation of such a norm or keep a broad and open ended formulation in their national law.
- Second, there is vertical and horizontal consistency.
    - Vertical consistency exists when, in one field of law, there is consistency between the local and national level and the EU legislative level. The EU might invest in harmonising all MSs laws on a particular aspect or legal domain, such as consumer law, car safety or access to telephony. It may, however, leave open the relationship of such legal instruments vis-à-vis other sectors of law. A typical example may be found in the Directive on the Re-Use of Public Sector Information, which 'leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Unionand national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC.'[102]
    - Horizontal consistency exists when there is consistency between fields of law at one level of regulation, for example MSs level, or EU regulatory level, such as between data protection and other fields of law. Here, the EU or MSs can invest in stipulating in detail how various laws and legal principles relate to each other and should be interpreted in practice. Traditionally, such is done more often at MSs level than on EU level, but there is no reason why this should be the case per sé.



6. Conclusion

If the division between material and formal and between vertical and horizontal consistency is adopted as the lens through which to judge the approach taken by the EU when adopting the GDPR and the PD, it seems that it is moving towards both material and vertical consistency, while is seems willing to sacrifice formal and in particular horizontal consistency. A few observations to support this claim:

- A clear historical line can be discerned in the European data protection instruments away from open norms and towards laws that specify in detail which rights and obligations data subjects and data controllers have. In plain numbers, the two Resolutions from 1973 and 1974 contained 8 and 10 articles respectively. The Convention (1981) contained 27 provisions, the Directive (1995) 34 and the proposed Regulation (2016) 99. While the two Resolutions were literally one-pagers, the proposed Regulation consists of almost 100 pages.
- The initial Resolutions of the Council of Europe were code of conduct like documents, containing duties of care for data controllers, merely recommending the Member States of the CoE to adopt rules to protect the principles contained in the Resolutions. It was at their liberty to implement sanctions or rules regarding liability. The subsequent Convention already brought more vertical consistency and the Directive from 1995 aimed specifically at bringing uniformity in the national laws of the various MSs. A Regulation is the type of instrument that leaves the least room for MSs to interpret their own rules and interpretation of the provisions contained in the instrument, among others, because a Regulation has direct effect. Although under the GDPR, Member States are at liberty to adopt national rules on the processing of sensitive data and special regimes for the processing of personal data for reasons of public interest, even these special regimes need to incorporate the rules of the GDPR in almost every aspect.[103]
- The enforcement of the rules has moved more and more to a European level. The two Resolutions of the Council of Europe left it at the discretion of MSs to implement sanctions or rules regarding liability. Only in the Convention of 1981 was it explicitly provided that: 'Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.'[104] Moreover, the Convention explicitly provided a number of rules regarding the application and enforcement of the rule on transborder data flows,[105] the cooperation between states and the national Data Protection Authorities.[106] With the EU Directive, cooperation between MSs was brought a step further and partial powers were transferred to EU organs. The Working Party was installed and the European Commission was granted a role, both with regard to adopting adequacy decisions[107] and with reviewing the application of the DPD on national level.[108] With the Regulation, the enforcement of the rules is brought on a EU level even more, among others by replacing the WP29 with the EDPB, which has more powers and tasks, by granting a bigger role for the European Commission and by laying down a one stop shop mechanism.
- A final example is the legal basis for the EU instruments. The legal basis of the Data Protection Directive was the regulation of the internal market, namely Article 100a of the Treaty Establishing the European Community, which specified that measures shall be

adopted for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishing and functioning of the internal market. For the GDPR, the legal basis is no longer found in the regulation of the internal market, but in the protection of the right to data protection, as specified in Article 16 of the Treaty on the Functioning of the European Union. Consequently, in the EU, data protection is now protected on the highest level; it is seen as a fundamental right as contained in the Charter of Fundamental rights and the EU has an explicit mandate to regulate the field of data protection established by the Treaty, which is unique compared to other fundamental rights. The GDPR and the PD must be seen as an implementation of the fundamental right to data protection, as laid down in the Charter and the Treaty. This limits the margin of appreciation of MSs to an even further extent, giving the ECJ ultimate power to decide over the validity of both MSs and EU legislation in the field of data protection.

In conclusion, it is clear that European data protection rules have focused more and more on material consistency. Although the GDPR and the PD still primarily consist of open norms and broad exceptions, it is incomparable to the level of openness of the earlier instruments. In particular, the EU has endeavored to achieve vertical consistency in the field of data protection. As this article has shown, this comes at the cost not only of various other legal values, but also of what may be called horizontal consistency, or the existence of uniformity between the rules in the different fields of law. The EU has provided no further guidelines or principles on how such a horizontal consistency could be achieved. Although the European Commission and the Parliament have initiated projects that should map the various instruments potentially affected by the GDPR and the PD, it is clear that it will be almost impossible to check every legal instrument on EU and MS level that might require the processing of personal data on the question of whether the GDPR or the PD apply and if so, whether all provisions contained therein have been respected.

---

[1] Senior Researcher, Tilburg Institute for Law, Technology, and Society, Tilburg University, Netherlands

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[3] Article 94 GDPR.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050.

[5] Article 99 GDPR.

[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

[7] Article 59 PD.

[8] Council Framework Decision 2008/977/JHA of 27November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60–71.

[9] Article 95 GDPR.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of

personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[11] Article 96 GDPR.

[12] Article 97 GDPR.

[13] Article 98 GDPR.

[14] Article 65 PD.

[15] Article 60 PD.

[16] Article 61 PD.

[17] Article 62 PD.

[18] Article 63 PD.

[19] ECJ, Maximillian Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015.

[20] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), Official Journal L 215 , 25/08/2000 P. 0007 – 0047.

[21] E.g. Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Brussels, 12.7.2016 C(2016) 4176 final

[22] Article 7 & 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01). <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[23] Article 52 Charter.

[24] ECJ, Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis, Joined Cases C-203/15 and C-698/15, 21December 2016.

[25] ECJ, Digital Rights Ireland and Seitlinger and others, Joined cases C-293/12 and C-594/12, 8 April 2014

[26] ECJ, Google Spain vAgenciaEspañoladeProtecciónde Datos,MarioCostejaGonzález,C-131/12,13May2014.

[27] Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950.

[28] See also: Article 53 sub 3 EU Charter. 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.'

[29] ECtHR, Zakharov v. Russia, Application No. 47143/06, 04 December 2015.

[30] ECtHR, Szábo and Vissy v. Hungary, application no. 37138/14, 12 January 2016.

[31] <http://ec.europa.eu/budget/library/biblio/documents/2017/DB2017_WD04_en.pdf>.

[32] <https://etendering.ted.europa.eu/cft/cft-display.html?cftId=1831>.

[33] <http://ec.europa.eu/budget/library/biblio/documents/2017/DB2017_WD04_en.pdf>.

[34] For a first overview, see e.g. C. Hoofnagle, B. van der Sloot & F. Zuideveen Borgesius, 'The European Union General Data Protection Regulation', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3254511

[35] Council of Europe, Committee of Ministers, Resolution (73) 22 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies). Council of Europe. Committee of Ministers, Resolution (74) 29 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the public sector. (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

[36] Article 10 Convention (1981).

[37] Article 11 Convention (1981).

[38] Article 12 Convention (1981).

[39] Article 13 Convention (1981).

[40] Article 14 Convention (1981).

[41] Article 18 Convention (1981).

[42] Article 19 and 21 Convention (1981).

[43] U. U. Wuermeling, 'Harmonisation of European Union Privacy Law', 14 J. Marshall Journal Computer & Information Law 411, 1996.

[44] See among others: B. Niblett, 'Data Protection Act 1984', London, Oyez Longman, 1984.

[45] Article 1 DPD.

[46] See for the tension between e-commerce and data protection among others: H. W. K. Kaspersen, 'Data Protection and e-commerce', in: A. R. Lodder & H. W. K., 'eDirectives: guide to European Union Law on E-Commerce', Kluwer Law International, The Hague, 2002.

[47] See further: R. Laperrière, 'Crossing the Borders of Privacy: Transborder Flows of Personal Data from Canada', Ottawa, Ontario, Communications and Public Affairs, Department of Justice Canada, 1991.

[48] Article 25 DPD.

[49] W. J. Maxwel, 'Data Privacy: the European Commission pushes for total harmonization', February, 2012 <https://www.hldataprotection.com/uploads/file/translation_data_Privacy_article_Feb_2012.pdf>.

[50] Article 31 DPD.

[51] Recital 3 GDPR.

[52] Recital 6 GDPR.

[53] Recital 7 GDPR.

[54] Recital 9-10 GDPR.

[55] L. Shields, 'Consistency and privacy: do these legal principles mandate gamete donor anonymity?', Health Law Review, 12(1), 2003.

[56] See chapter: CHAPTER IX Provisions relating to specific processing situations GDPR.

[57] Article 48 GDPR.

[58] Article 4 sub a GDPR. See also: ECJ, Worten—Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), Case C-342/12, 30 May 2013

[59] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 13.

[60] D. Skillicorn, 'Knowledge Discovery for Counterterrorism and Law Enforcement', Boca Raton, CRC Press cop., 2009. D. T. Larose, 'Data Mining Methods and Models', Hoboken, Wiley cop., 2006. M. Hildebrandt & S. Gutwirth (eds), 'Profiling the European Citizen Cross-Disciplinary Perspectives', Dordrecht, Springer cop., 2008. C. Westphal, 'Data Mining for Intelligence, Fraud & Criminal Detection', Boca Raton, CRC Press cop., 2009. K. Guzik, 'Discrimination by Design: Data Mining in the United States's "War on Terrorism"', Surveillance & Society 7, 2009. P. Kuhn, 'Sex discrimination in labor markets: The role of statistical evidence', The American Economic Review 77, 1987. M. LaCour-Little, 'Discrimination in mortgage lending: A critical review of the literature', Journal of Real Estate Literature 7, 1999. G. D. Squires, 'Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas', Journal of Urban Affairs 25, 2003.

[61]Arguably, the Breyer case has limited the scope of personal data somewhat. ECJ, Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, 19October 2016.

[62] See among others: M. R. Koot, 'Measuring and Predicting Anonymity', Amsterdam, Informatics Institute cop., 2012.

[63] See among others: ECtHR, Malone v. United Kingdom, application no. 8691/79, 02 August 1984. ECtHR, P.G. and J.H. v. United Kingdom, application no. 44787/98, 25 September 2001. ECJ, Digital Rights Ireland v. Ireland, C-293/12

AND C-594-12, 8April 2014.

[64] See inter alia: B. van der Sloot, 'Privacy as virtue', Intersentia, Cambridge, 2017.

[65] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, Brussels, 13.9.2017 COM(2017) 495 final , 2017/0228 (COD).

[66] Article 4 sub (2) GDPR.

[67] Artice 2 para. 1 GDPR.

[68] Article 4 sub (6) GDPR.

[69] Recital 15 GDPR.

[70] Article 3 GDPR.

[71] ECJ, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, 1October 2015.

[72] ECJ, Schrems v. Data Protection Commissioner, C-362/14.

[73] See also earlier case about PNR: ECJ, Parliament v. Council (PNR), C-317 and 318/04, 30 May 2006.

[74] A. Bradford, 'The Brussels Effect', Northwestern University Law Review, Vol. 107, No. 1, 2012.

[75] Article 2 para. 2 (a) and (b) GDPR. Recital 16 GDPR.

[76] Article 23 and 85-91 GDPR.

[77] Article 2 para 2 (c) GDPR. See however also:

[78] See inter alia: V. Mayer-Schönberger & K. Cukier, 'Big data: a revolution that will transform how we live, work, and think', Boston, Houghton Mifflin Harcourt, 2013.

[79] See for example: Directive 2014/66/EU of the European Parliament and of the Council of 15 May 2014 on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer may be a case in point. It specifies in the recitals that "The collection and transmission of files and data should be carried out in compliance with the relevant data protection and security rules."

[80] < http://eur-lex.europa.eu/advanced-search-form.html>.

[81] Search executed from a local computer on 20-03-2018.

[82] Search executed from a local computer on 20-03-2018.

[83] Article 1 Regulation (EC) No 789/2004.

[84] Article 5 Regulation (EC) No 166/2006.

[85] Annex II Regulation (EU) 2016/1627.

[86] <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>.

[87] <http://eur-lex.europa.eu/advanced-search-form.html?locale=en>. Use has been made of EURLEX, limiting the search results to 'EU court case'. This includes opinions by the AG.

[88] HUDOC was used for this purpose, limiting the search results to the cases being 'judgments'.

[89] Search executed from a local computer on 20-03-2018.

[90] Search executed from a local computer on 20-03-2018.

[91] See also Mark Van Hoecke & J. Dhont, 'Obstacles and opportunities for the harmonisation of law in Europe', <https://www.researchgate.net/publication/292353945_Obstacles_and_opportunities_for_the_harmonisation_of_law_in_Europe>.

[92] T. Ayhan, 'The Principle of Legal Certainty in EU Case Law', Review of Public Administration, Volume 4 No 3, 2010.

[93] See for an original approach: L. Anderlini, L. Felli & A. Riboni, 'Legal Efficiency and Consistency', Working Papers 2016-22, Center for Research in Economics and Statistics.

[94] J. E. Coons, 'Consistency', 75 Calironian Law Review 59, 1987.

[95] K. Steyn, 'Consistency - A Principle of Public Law', 2 Jud. Rev. 22, 1997.

[96] H. Ahmetaj, 'Legal certainty and legitimate expectation in the EU law', Interdisplinary Journal of Research and Development, Vol (I), No.2, 2014.

[97] Article 3 para. 2 TFEU.

[98] Article 121, 127, 146, 148, 181, 196, 212, 214, 219, 256 and 329 TFEU.

[99] E. Herlin-Karnell & T. Konstadinides, 'The Rise and Expressions of Consistency in EU Law: Legal and Strategic Implications for European Integration', Cambridge Yearbook of European Legal Studies (2012-2013).

[100] L. L. Fuller, 'The Morality of the Law', Yale University Press, 1964, p. 65.

[101] <https://eur-lex.europa.eu/summary/glossary/subsidiarity.html>.

[102] Article 1 para 4 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

[103] See, inter alia, Chapter IX Provisions relating to specific processing situations of the GDPR.

[104] Article 10 Convention.

[105] Article 12 Convention.

[106] Article 13 Convention.

[107] Article 25 DPD.

[108] Article 33 DPD.