



PROCEED WITH CAUTION:

Flexibilities in the General Data Protection Regulation

ARTICLES IN THE GDPR CONTAINING FLEXIBILITIES ALLOWING FOR DIVERGENCIES IN IMPLEMENTATION

General Note on divergencies:

One of the main reasons for adopting the main Data Protection Directive (DPD) in 1995 was that the different data protection laws in the Member States (MSs) (and the absence of such laws in some of them) hampered the Single Market. The aim of the 1995 DPD was to create a largely harmonised data protection system throughout the EU (and the EEA). However, reviews of the laws that EU MSs adopted to implement the Directive showed that it had, in many respects, failed to achieve harmonisation: there were still many, often major, differences between the laws in the MSs. As was noted in a review of the situation for the Commission as long ago as 2002:¹

- in almost all respects there were still “a large number of significant differences” between the laws of the Member States;
- the Directive “appeared to almost invite the application of multiple laws (laws from several EU Member States) concurrently to the European activities of non-EU-based controllers”, and was unclear as to when the national laws of the Member states apply to activities of such controllers over the Internet.

These divergences could – and were – used by some MSs to lower the bar for the protection of citizens’ data to unacceptable levels. In addition, the laws in some MSs failed to adequately transpose the Directive (a full one-third of the UK Data Protection Act was held by the Commission to fall short of the Directive, as did the rules on the status of data protection authorities in Germany, for example). The spirit of the GDPR is completely the opposite, as it aims at creating a level playing field for the single market and harmonising data protection for every EU citizen and -person at a high level, as required by the Charter.

The main reasons for replacing the Directive with a Regulation, the General Data Protection Regulation (GDPR), was that a Regulation is not “transposed” into national law in the MSs by means of national implementing legislation. Instead, it applies directly in the MSs. This, it was assumed, would avoid the divergences in national legal data protection regimes in the different MSs. For those cases where different interpretations by different DPAs might still threaten harmonisation,

1

important “cooperation”, “mutual assistance” and “consistency” mechanisms were included in the Regulation. If properly used, those will lead to central determinations overruling any such divergent interpretations.

However, as the attached overview shows, the GDPR still contains a large number of provisions that allow the MSs to set the rules in many important contexts, i.e., that effectively still allow for divergences between the data protection rules in the MSs. In some respects, this need not necessarily be seriously problematic. For instance, the Regulation stipulates, in Article 9(2)(b), that sensitive data may be processed if the “processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law”. The relevant employment and social security laws in the different MSs are likely to differ in the specifics of such requirements, e.g., as to whether trade union membership or race or disability may or must be recorded in certain forms. This should not cause too many problems as these matters apply almost solely within one state, and most employers and employees may be expected to be familiar with their own laws and forms in these respects. Even then, a certain convergence can be expected, in that the Regulation adds to the above that the relevant national requirements must be laid down in “Union law or Member State law or a collective agreement pursuant to Member State law”; and that these legal instruments must “provid[e] for adequate safeguards for the fundamental rights and the interests of the data subject”. The latter means that compliance of the relevant instruments with these conditions can now be checked by the courts, and ultimately the CJEU.

But other provisions allowing for divergences are much more problematic. Some are so broad as to give states almost complete freedom to evade the normal requirements of the Regulation in large areas. Others are particularly problematic in the online environment and threaten the functioning of the Digital Single Market – one of the top priorities of the Commission and many MSs.

In the chart below these problematic “flexibility” clauses are indicated by **red** “traffic lights”.

Other provisions that could, but perhaps will not necessarily lead to problems, are indicated by **yellow** “traffic lights”. And provisions that allow for different national applications of the law (or for the adoption of national laws that regulate certain matters at the discretion of the MS concerned), but that appear to cause few or only minor problems are indicated by **green** “traffic lights”, as further explained in the [Legend](#).

The reasoning behind the classifications are given in the text in the final column.

ARTICLES IN THE GDPR ALLOWING FOR DIVERGENCIES

LEGENDA: THE MEANING OF “TRAFFIC LIGHT” INDICATORS NEXT TO THE ARTICLES:





The provision poses no serious problems, in particular not in relation to the online environment and the Single Digital market




The provision poses problems that are either moderately serious or potentially serious problems in a narrow range of circumstances



The provision poses really serious problems, especially in relation to the online environment and the Digital Single Market

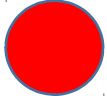
CHAPTER 1: GENERAL PROVISIONS			ANALYSIS
<p>Article 4(7)</p> 	<p>Generally: Recital 10</p>	<p>Definition of “controller”; designation by law</p>	<p>In the private sector, the determination of a controller is to be made on an assessment of the facts: the controller is the person or entity “which alone or jointly with others determines the purposes and means of the processing of personal data”. This is unchanged from the Directive. While there are some issues with this definition (e.g., What if the entity that determines the purposes of the processing leaves the means to someone else? And how to divide responsibilities if there are more than one “joint” controller: see the analysis of Article 24, below). overall these have not caused many problems.</p> <p>The Regulation adds (again, in line with the Directive) that “where the purposes and means of processing are determined by Union law or Member State law” - i.e., in effect, in the public sector - “the controller or the specific criteria for his nomination may be designated by Union law or by Member State law.” This means that, for instance, a Minister can be designated as the controller of all the processing by any of the departments within his or her ministry; or conversely that one particular department can be designated as the controller for specific operations closely linked to that department. This too has not been too much of a problem.</p>
<p>Article 4(9)</p> 	<p>Recital 31</p>	<p>Definition of “recipient” excludes certain authorities</p>	<p>The definition (again taken from the Directive) includes a potentially dangerous carve-out for public authorities: “public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of these data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.” This could be read as meaning that disclosures of data to such authorities in relation to such an inquiry do not constitute a disclosure. That would be dangerous in that it would</p>



mean that no data protection restrictions apply to them at all. This was never tested under the Directive. **Such a problematic interpretation in the GDPR should be opposed.**



CHAPTER 2: PRINCIPLES			ANALYSIS
<p>Article 6(1) (c) & (e) read with Articles 6(2) & (3)</p> 	<p>Recital 10</p>	<p>Further rules on data processing in certain contexts</p>	<p>Article 6(2) authorises member states to lay down “more specific” rules on the processing of personal data covered by Article 6(1)(c) or (e), i.e., on processing which is “necessary for compliance with a legal obligation” <u>or</u> “necessary for the performance of a task carried out in the public interest” <u>or</u> “[necessary] in the exercise of official authority vested in the controller”. These three categories give rise to different analyses (in a different order from the above):</p> <ol style="list-style-type: none"> 1. <u>Processing “in the exercise of public authority”</u> will by its nature (almost?) always be done by a public body; and it is in principle not problematic to allow MSs to draft those rules (typically, in the form of a law governing the work of the public body in question) – especially since the Regulation adds that the relevant rules must be set out in a law and must “meet an objective of public interest” and be proportionate to that interest. In other words, the legality, legitimate aim and proportionality of these rules can be challenged and checked under EU law. These rules will also operate essentially only at a domestic level and will therefore have limited impact of the online transnational environment (leaving aside the problem of laws authorising national authorities to “exercise [their] authority” by online means in another country – an issue that relates mainly to law enforcement and national security agencies, that should be addressed under the LEDP Directive and other relevant instruments, rather than the GDPR). 1. The reference to <u>processing which is “necessary for compliance</u>



with a legal obligation” is not problematic if it relates to typical, normal duties imposed on controllers in Western democracies, such as duties of record-keeping imposed on employers (cf. Art 9(2)(b)). These rules will again operate essentially at a domestic level and be known to the controllers and data subjects, with little impact on online transnational activities. However, **the lack of specificity of the “legal obligations” is worrying**: it suggests that MSs can simply create any legal obligation to process personal data (e.g., to disclose personal data to a public authority) they wish. Here, the stipulation that the relevant legal obligations must be set out in law and serve “an objective of public interest” and be proportionate and necessary to that interest are insufficient. At the least, MSs should be required to publicise all the relevant legal rules in a comprehensive and accessible form, and inform the Commission and the new European Data Protection Board of them, so that their compliance with these requirements can be assessed (and such assessments should be carried out).


2. “Tasks carried out in the public interest” are not only performed by public bodies acting under a legislative mandate. For instance, banks can reasonably argue that their monitoring of transactions to detect fraud is not just in their own interests and the interests of their clients, but also in the public interest; retailers can claim that trying to spot shop lifters also does that. These are activities that are less necessarily limited to purely-domestic operations (banks monitor for fraudulent use of their payment cards abroad too). It is useful that the Regulation now demands that such processing be based on law (i.e., cannot be allowed merely on a “voluntary” basis unregulated by law). However, in this context it is not sufficient that the Regulation merely says the relevant legal rules must “meet an objective of public interest” and be proportionate to the relevant interest. That **should be spelled out in more detail** - both to achieve the required legal certainty for data



			<p>subjects and because otherwise this will lead to seriously divergent rules in the online digital environment, and cause problems for the Digital Single Market. At the very least, this “flexibility” should be accompanied by “applicable law” rules clarifying which of the national rules should follow in such regards, in relation to cross-border anti-crime etc. activities.</p>
<p>Article 6(4)</p> 	Recital 50	Further processing for “incompatible” purposes	<p>This new article relates to processing for secondary purposes that are “incompatible” with the original (primary) purpose for which the data were collected, including processing for the special purposes listed in Article 21(1): national security; defence; public security; crime prevention etc.; “other important objectives of general public interests” including economic or financial interests of the state; court proceedings and civil claims; professional ethics; and “a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority”; and “the protection of the data subject or the rights and freedoms of others”.</p> <p>Article 6(4) usefully lists a number of matters to be taken into account in determining whether the “incompatible” processing can be allowed or not. However, it suffers from three defects: 1. It suggests that the assessment of the compatibility or incompatibility of the processing is one that can essentially be left to the controller; 2. The matters to be taken into account, while useful as broad rules-of-thumb, are much too vague to make the application of this provision foreseeable for data subjects (which is contrary to the rule of law); and 3. The rules and matters to be taken into account will inevitably be differently applied in different MSs - which, in any cross-border or online context, will cause serious problems.</p> <p>It should be made clear, perhaps by the EDPB, that the assessments of the controllers on “compatibility” is subject to review by the relevant DPA - and especially, that in relation to any cross-border activities, the</p>

			<p>views of the DPA in question will in turn be subject to the cooperation-, mutual assistance- and consistency mechanisms. Indeed, for important or regular types of “incompatible” processing, the EDPB should issue much more specific guidance and rules. This is especially important in relation to “incompatible” processing for ill-defined concepts such as “national security”, “other important [but unspecified] objectives of general public interests” and “the protection of the data subject or the rights and freedoms of others”.</p> <p>Without close EU-level supervision over and guidance in relation to the application of this sweeping provision, it can lead to serious abuses by public authorities and breaches of privacy and data protection; and would undermine the operation of the Digital Single Market.</p>
<p>Article 8(1)</p> 		Age of consent for InfoSoc services	<p>The provision authorises the MSs to set the age of children's consent to the signing up to information society services anywhere between 13 and 16. This means that online and transnationally operating information society service providers will have to comply with different rules across the EU, depending on where an underage user of their services is based – which (together with the other divergencies noted in this overview) undermines the Digital Single Market for such services.</p>
<p>Article 9(2) (a)</p> 		Prohibition on processing of sensitive data even with consent	<p>This provision allows MSs to prohibit, in certain contexts, the processing of so-called “sensitive data” (or some categories of sensitive data), even with the consent of the data subject. This is currently done in some MSs that, for instance, prohibit employers from asking for certain sensitive data from their employees: they are not allowed to collect and use such information even with the consent of the data subjects. As long as this exception is applied only in such clearly-defined areas, in typically purely-domestic contexts, it will not be problematic.</p>

<p>Article 9(2) (b)</p> 	<p>Recital 52</p>	<p>Processing of sensitive data under employment etc. law</p>	<p>This provisions allows MSs to require the (collection and further) processing of sensitive data under employment-, social security- or social protection law. This reflects current differences: for instance, some MSs require the recording of religion in such contexts, while others expressly prohibit it. As long as this divergence only applies in such typically solely domestic-legal contexts, they will not be too problematic (except perhaps for multinational companies with employees in several MSs). However, there should be restrictions on the use of such sensitive data, especially by private entities or (public- or private sector) employers for purposes not directly related to the operation of the relevant employment-, social security- or social protection law. To some extent, this can be read into the rules but further guidance on this would be useful.</p>
<p>Article 9(2) (d)</p>  <p>See also Article 91</p>	<p>Recital 51</p>	<p>Processing of sensitive data by not-for-profit/trade union/religious bodies</p>	<p>This provision allows not-for-profit (NfP) bodies, trade union-related and religious bodies to process sensitive personal data on their members and “regular contacts” for “legitimate purposes”. The provision requires “appropriate safeguards” but does not spell these out – which means that the rules on processing by such entities are likely to remain different in different MSs. This is again not too problematic if applied to entities that operate in purely domestic contexts. However, increasingly NfP entities and trade union-related and indeed religious bodies operate transnationally, especially also online. This then raises serious problems of compliance with different laws in the different MSs. In fact, there can be problems in relation to the question of how an organisation that is regarded as NfP or trade union-related, or indeed religious in one MS, but not in another MS, should operate under these rules. Again, this can only be resolved by “applicable law” rules on cross-border/online activities by such entities.</p>
<p>Article 9(2) (g)</p>	<p>Recitals 52 – 56</p>	<p>Processing of sensitive data for</p>	<p>The provision allows MSs to adopt laws authorising processing sensitive data for reasons of “substantial public interest”</p>



		<p>“substantial” public interest</p>	<p>(without consent or any other legal basis). This broad undefined concept will be understood differently from one country to another – as is indeed clear from Recital (56), which seems to legitimise the UK practice of political parties compiling regional and wider databases on the political allegiances of all households, without the consent of the data subjects; something that would be regarded as in manifest breach of data protection in other countries. That particular oddity may be confined to the one country and essentially domestic activities. However, there is nothing in the provision to prevent MSs from using it to allow the collection of sensitive data in cross-border/online contexts, by public- and/or private entities, for reasons that other MSs may not agree with.</p>
<p>Articles 9(2)(h), 9(2)(i) and 9(4)</p> 	<p>Recitals 52 – 54</p>	<p>Processing of sensitive data for health purposes</p>	<p>Article 9(2)(h) allows for MSs to provide for specific rules allowing the processing of data for very broadly-formulated health care and health-related purposes without consent, not only on the basis of a Union or MS law, but also “pursuant to contract with a health professional”. Although the article adds that this must be “subject to the conditions and safeguards referred to in paragraph 4”, these in fact only require the data to be “processed by or under the responsibility of a professional subject to the obligation of professional secrecy” or “by another person also subject to an obligation of secrecy”. The details are to be spelled out in national law or in “rules established by national competent bodies”. This is extremely vague and certain to lead to different rules in the MSs (for example in Poland the government has already implemented a central health register, which is likely to affect national rules regarding data integration and access to data). Given that not just health care but also secondary uses of health data, by public and private bodies, are becoming increasingly transnational (and certainly pan-European), this could seriously affect the Digital Single Market in health care and health data-related goods and</p>


			<p>services. If under (still missing) “applicable law” rules, the law of only one relevant entity would be the applicable law to pan-EU collecting and further processing of such data for such purposes, this could lead to the circumvention of safeguards in MSs that are strict in relation to such matters, by entities in other MSs that are more lax in their Regulation of the use of health data. This appears to be expressly confirmed in Recital (53) which stipulates that stricter rules in one MS on the use of genetic data, biometric data or data concerning health “should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.” That is somewhat obscure but is surely highly contentious.</p>
<p>Articles 9(2) (j) & 89</p> 	<p>Recitals 53 – 54</p>	<p>Processing of sensitive data for archiving purposes and, historic and scientific research</p>	<p>Member states can authorise the processing of sensitive data without consent for archiving purposes done in the public interest, or for historic and scientific research, subject to the requirements of Article 89(1). The latter, however, mainly only reiterates the (in any case applicable) requirement of data minimisation and maximum pseudonymisation or (where possible) anonymisation of data held for historical/archival/scientific purposes. “Public interest” is not defined and the scope of this provision is consequently essentially left to the MSs (which in practice can be heavily affected by temporary political priorities). There are two risks here: first of all, the general risk that private- and public-sector research bodies (which are increasingly intertwined) will try to stretch the provision to allow them to do anything they want with sensitive data they can obtain, certainly also for commercial “research” purposes. The second one is the same as noted earlier: the possibility that the application of this provision will lead to circumvention of safeguards in MSs that are strict in relation to such matters, by entities in other MSs that are more lax in their Regulation of the use of sensitive data for “research” (for example the Polish government appears likely to use this flexibility to process</p>

			sensitive data for the purposes of “investigations” into past political activity of its ideological enemies). Yet again, that would be unacceptable . As noted later, Article 89(2) & (3) specifically allow for divergent – more strict/less strict – application of this special exemption in the different MSs.
Article 9(4) 	Recital 53	Member State flexibility <i>re</i> processing of genetic-, biometric- or health data	This provision stipulates that MSs “may maintain or introduce further conditions , <u>including</u> limitations, with regard to the processing of genetic data, biometric data or health data ”. It should be made clear (e.g., by the EDPB) that this wording does not allow MSs to relax the rules in the GDPR further than as expressly envisaged in the Regulation: they can impose conditions that do not amount to limitations (e.g., purely technical standards), or conditions that do amount to limitations, but not conditions that amount to relaxations of the rules. Even then, this provision is problematic in any transnational/online context . Thus, biometric checks are increasingly carried out in such contexts (e.g., in accessing a mobile phone or online bank account), and health and even genetic data may well be collected and/or further processed in such contexts. Once again, this could to some extent be resolved by “applicable law” rules - but only at the risk of strict rules in some MSs (expressly permitted by this provision) being evaded by providers of such goods or services based in MSs with less strict rules.
Article 10 		Processing of data relating to criminal convictions and offences	In principle, this is a positive provision , ensuring that when data related to criminal convictions and offences are processed, this is done under the control of an official authority, and stipulating that MS law must provide “adequate safeguards for the rights and freedoms of data subjects”. However, these safeguards, and thus the rules on when private entities can collect and exchange such data, and the extent of such processing and sharing, are still likely to differ between MSs , which could be problematic in relation to exchanges and sharing


			of crime data in the online environment, e.g., in relation to fraud- and crime detection by private entities. As the provision now stands, it remains unclear to what extent the relevant data will really be closely regulated (or not) in the Digital Single Market.
--	--	--	---


CHAPTER 3: RIGHTS OF THE DATA SUBJECT ANALYSIS
Section 2: Information and Access to Data

<p>Article 14(5) (b)</p> 	<p>Recital 62</p>	<p>Exception to right to information when data are not obtained from the data subject</p>	<p>This provision allows controllers to keep data subjects in the dark about the use of their data for “archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes” (note that the research, unlike the archiving, need not be “in the public interest”). This is subject to the conditions set out in Article 83(1) – which as already noted only require data minimisation and (consideration of) pseudonymisation or anonymization – and to a duty on the part of the controller to “take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information [about the research] publicly available”. Different MSs are likely to have different views on what measures are “appropriate” in this regard, or how such publicity is to be achieved. It will be crucial to both clarify the “applicable law” and to fully apply the cooperation-, mutual assistance- and consistency mechanisms to the application of this provision to any transnational research.</p>
<p>Article 14(5) (c)</p> 	<p>Recital 62</p>	<p>Exception to right to information when data are not obtained from the data subject</p>	<p>This provision stipulates that when the obtaining of personal data (including by compulsory or non-compulsory – disclosure of the data by a controller) is “expressly laid down” by EU law or by the law of a MS, the data subjects need not be informed of the disclosure or any details of the disclosure (such as the identity of the recipient/new controller, the purpose of the disclosure, the categories of data concerned, the further recipients of the data, or any intended transfer of the data to a third country or an international organisation, the period for which the data are to be retained by the recipient/new controller,</p>


			<p>etc.) – provided only that the EU or MS law in question “provides appropriate measures to protect the data subject's legitimate interests”.</p> <p>In a Digital Single Market in which consumers are supposed to increasingly obtain goods and services from providers in other MSs (especially online), the former will often be unaware of such statutory disclosure duties resting on the provider in another MS - and will therefore be in the dark about what may happen to their data.</p> <p>In some Mss, the law provides for excessively wide compulsory data disclosure duties (or “expressly” allows non-compulsory disclosures), in particular in relation to national security and public order (e.g. preventing tax evasion or fraud), but sometimes also for other purposes such as “research”. Under this provision, EU citizens buying goods or services online from companies in other MSs will be left in the dark about possibly extensive, and possibly excessive, disclosures of their data by those companies in other MSs to the authorities (or “researchers”) in those other states. This is both unacceptable in principle and will undermine trust in the Digital Single Market.</p>
<p>Article 14(5) (d)</p>  <p>See also Article 90</p>	<i>None</i>	<p>Exception to right to information when data are not obtained from the data subject</p>	<p>This is a very strangely-worded provision, which is not clarified in any recital. It says that the duty to inform data subjects of the fact that their data have been obtained by a controller rather than directly from them (i.e., when their data have been disclosed to the recipient by another controller), and of the details of the processing in question, does not apply “where the data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.” Presumably, what is meant is: “where the data are subject to an obligation of professional secrecy or to a statutory obligation of secrecy, imposed by Union or Member State law.” But that still means that the provision</p>

			<p>confuses, and wrongly conflates, a professional duty of confidentiality (such as exist between a doctor and a patient, or a lawyer and a client, or a priest and a penitent) and a statutory obligation of secrecy. The duty of confidentiality is widely recognised in all MSs (perhaps with some differences when it comes to exceptions to that duty). But the unspecified reference to, it would appear, any “statutory obligation of secrecy” is much less acceptable. It suggests, first of all, that it is entirely up to the MSs to create any such obligation as they deem fit. Secondly, it suggests that such obligations can – perhaps even always should – be comprehensive: if data were obtained under a statutory obligation of secrecy, then the data subject will not be informed of the obtaining of his/her data by the controller (or of the disclosing of her data by another controller that led to the obtaining by the new controller), and s/he will also not be provided with any details of the processing in question. In effect, this appears to allow the MSs to create major holes in the fabric of the Regulation whenever they want (because, without transparency about processing, the effectiveness of data protection rules is fatally weakened). (Cf. the analysis of Article 22(2)(b), <i>re</i> automated decision making and profiling, below.)</p> <p>MSs should at least be required to report in detail on how and to what extent they rely on this provision to allow for secret processing of personal data. The provision should also be read as implicitly being subject to a requirement that any such “statutory obligations of secrecy” be based on (clear and foreseeable) law, serve a legitimate purpose in a democratic society, and be necessary and proportionate to that purpose – this flows from the Charter of Fundamental Rights, even if here it is, regrettably, not spelled out.</p>
--	--	--	---

CHAPTER 3: RIGHTS OF THE DATA SUBJECT (Section 3: Rectification and Erasure)			ANALYSIS
Article 17(1) (e) & (3)(b) 	Recital 65	Right to erasure ("right to be forgotten")	<p>The provisions allow the EU and the MSs to lay down "legal obligations" requiring (certain) data to be erased in certain circumstances. In relation to the RTBF, this means that that right can also be used by data subjects to enforce adherence with such legal obligations, irrespective of other reasons to exercise the right. Interestingly, the provision contains an "applicable law" clause, in that it says that the data have to be erased if this is required by a law of a MS "to which the controller is subject". This provision is unlikely to be problematic, even though the legal obligations concerned may be different in the different MSs.</p>

CHAPTER 3: RIGHTS OF THE DATA SUBJECT (Section 4: Right to Object and Automated Individual Decision Making)			ANALYSIS
<p>Article 22(2) (b)</p> 	<p>Recitals 70, 71 & 72</p>	<p>Automated individual decision making, including profiling</p>	<p>The provision enables member states to adopt laws authorising fully-automated decisions and profiling (note: by private- and public sector controllers) that produce legal effects for the data subjects or otherwise “significantly affect” them, outside (pre-)contractual contexts and without the consent of the data subject. Such “legally authorised” decisions and profiles must be subject to “suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests”. However, different from automated decisions and profiling in (pre-)contractual contexts or with the consent of the data subject, for “legally authorised” decisions and profiles, these need not include “the right to obtain human intervention on the part of the controller, to express his or her [i.e., the data subject’s] point of view and to contest the decision” (cf. Article 22(3)). There are three serious problems with this. <u>First</u> of all, it would appear that MSs may impose a “statutory obligation of secrecy” on controllers, forbidding them from even informing data subjects that their data may or will be used in automated decision making and profiling (see the analysis of Article 14(5)(d), above), thereby effectively allowing for completely secret automated decision making and profiling – which is extremely dangerous, whatever the supposed safeguards. <u>Secondly</u>, one can only wonder what kinds of safeguards other than “human intervention” and a right of data subjects to contest a fully-automated decision can ever be effective or therefore “suitable”. <u>Third</u>, this special exception is again highly problematic in a transnational/online context: it means that data from individuals in</p>

			<p>one MS can be used for fully-automated decision making and profiling with serious repercussions for the data subjects, by public- and private-sector controllers in another MS, if this is allowed by the law of that other MS, even if this would not be allowed in the MS of the data subjects. If MSs were to adopt such legal authorisations in relation to processing in commercial contexts (be that for direct profit-making purposes or for say fraud prevention), including online commerce, that would significantly affect the Digital Single Market. For example, Poland has recently adopted the law providing for the establishment of a private entity that will use automated data processing techniques to detect and prevent tax fraud.</p>
--	--	--	---

CHAPTER 3: RIGHTS OF THE DATA SUBJECT Section 5: Restrictions			ANALYSIS
<p>Article 23</p> 	Recital 73	Restrictions on data subjects' rights	<p>The article authorises member states to restrict by law the application of data subject's rights for purposes of national security, defence, public security, the prevention or investigation of crimes, "other important objectives of general public interests", protection of judicial independence, breaches of professional ethics, protection of data subject rights, "a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority", or enforcement of civil law claims. Apart from the addition of the last issue (civil claims), the provision is largely the same as the corresponding one in the 1995 Data Protection Directive (Article 13(1)), but expands on some important conditions, i.e., by stipulating that each such legal restriction must "respect [] the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society" to safeguard the listed interests. It</p>

also usefully adds that the law in question must contain “specific provisions” setting out the purposes of the processing, the categories of data concerned, the scope of the restrictions, the rights of data subjects (limited though these may be) and the relevant safeguards “to prevent abuse or unlawful access or transfer” (Article 23(2)).

Even so, subject to these broad and in any case largely Charter-required conditions, **the application of the exemptions remain largely discretionary and almost entirely in the hands of the MSs.** The only limitation in this respect is that compliance with the conditions just mentioned is now a matter of EU law: MSs can be challenged for non-compliance with these conditions – e.g., on the basis that an exemption is too broad, or that the applicable safeguards are ineffective – and the matter can ultimately be determined by the courts, including the CJEU. However, that is not sufficient to ensure that, from the beginning (i.e., from the moment the Regulation applies), MSs will limit their exemptions accordingly. It should not be left to onerous, costly and time-consuming litigation to bring the MSs’s exemptions in line with the Rule of Law.

Moreover, under this provision **MSs can adopt domestic exemptions that directly impact on the processing of personal data in transnational and online contexts:** the provision is not limited to exemptions for the benefit of public authorities only, but **can also be used to exempt private-sector controllers (companies) from the normal requirements relating to data subject rights**, e.g., in relation to online fraud detection by banks, civil litigation, telecommunication data retention or providing commercial data on request of law enforcement agencies and other bodies (many EU countries, including UK, Spain, France and Poland have very broad provisions allowing for such disclosures). In these contexts in particular, the relevant legislative exemptions can therefore **directly affect the**

			<p>Digital Single Market. That should not be left so unclear. At the very least, MSs should again be required to inform the EDPB and the public of the way in which they use the exemptions, and much more detailed guidance should be provided on what exemptions are, and are not, acceptable, in particular in the Digital Single Market.</p> <p>In its present, excessively vague and permissive form, Article 23 constitutes one the largest loopholes in the Regulation.</p>
--	--	--	--

CHAPTER 4: CONTROLLER AND PROCESSOR
Section 1: general obligations

ANALYSIS

Article 26(1)




Recital 79 (cf. also 110)

Joint controllers

When processing is carried out by several “**joint controllers**” acting together, this provision in principle leaves it to those controllers to determine their respective roles and compliance responsibilities between them in what is called an “**arrangement between them**”. There is no requirement that this arrangement be put in writing, or be submitted to the relevant DPAs (although presumably, in any inquiry, the DPAs can ask for the details of the arrangement to be explained to them). There are only a few requirements for such an arrangement. It must “reflect the joint controllers’ respective effective roles and relationships vis-à-vis data subjects”, i.e., at least in relation to the data subjects it must reflect actual divisions of power, control and responsibility: the arrangement should not be a deceptive front hiding the real divisions of responsibility. However, it will be difficult for **data subjects** to gauge this since, under this provision, they **are only entitled to be provided with “the essence” (i.e., not the detail) of the arrangement, on request**. The only sop provided to the data subjects is that they can exercise their rights under the Regulation “in respect of and against each of the [joint] controllers.” The latter “may” moreover “designate a [presumably single] point of contact for data subjects” – but even that is not required.



This provision grants excessive freedom to joint controllers – which are increasingly common in the increasingly complex chains of companies involved in commercial activities, in particular also online – to choose “arrangements” for themselves that place their operations under the (for them) least demanding regime. If the Regulation were to really create a harmonised legal framework for data protection in the

			<p>EU, this would be a lesser danger. However, as the analyses in this paper make clear, even after the Regulation comes into force and is applied, there will still be many differences in the rules in the MSs: some will maintain or adopt weak rules or broad exemptions where others will have strong rules with few, narrow exceptions. Corporations will try to benefit from the lax rules and avoid the strict ones; and this provision gives them a means to try and do so.</p> <p>In order to counter this serious risk, the stipulation that the “arrangements” should reflect actual divisions of responsibility rather than create evasions from strict rules in some MSs, should be strongly and firmly enforced by the DPAs in the MSs, also and in particular in relation to multinational corporations, and/or corporate chains operating in the online environment, especially by means of the cooperation-, mutual assistance- and consistency mechanisms in the Regulation. If this is not done, this provision could threaten the Digital Single Market by turning it into a strict-data-protection-law-evasion device.</p>
<p>Article 28(3) (a)&(g)</p>  <p>(Cf. also Articles 29, 32(4) & 38(5))</p>	<p><i>None</i> (in particular not addressed in Recital 81)</p>	<p>Processor ordered to process contrary to instructions</p>	<p>These provisions contain exceptions to the principle that a processor must process any personal data sent to him/her by the relevant controller as instructed by the controller; that the processor may thus also not transfer or disclose the data sent to him to a third country or international organisation unless specifically instructed to do so by the controller; and that the processor must delete or return the data to the controller at the end of the contract to act as a processor. The provisions effectively state that when EU law or the law of a MS requires the processor to process the data other than as instructed by the controller, e.g., to disclose the data to a law enforcement- or national security agency in the MS, or indeed to transfer or disclose the data to a third country or international organisation; or to not erase the data at the end</p>


of the contract, the processor must do as thus instructed by the MS, irrespective of the will of the controller (or the purpose-limitation principle). The provision stipulates that the processor must (“shall”) inform the controller of the relevant legal requirement (or instruction) – but adds to this: “unless [the law of the MS where the processor is established] prohibits such information [i.e., such informing of the controller] on important grounds of public interest”, i.e., when the law allows for the issuing of so-called “gagging orders” to entities ordered to provide data.

It is, in principle, of course not surprising that the Regulation recognises that processors are subject to their local laws, in particular also as concerns rights of access to data by (and rights to demand the disclosure of data to) law enforcement- and national security agencies.

This would not be seriously problematic if, in all the EU MSs, those local laws on access to/disclosure orders in relation to (personal) data by such agencies were fully in accordance with the rule of law, the ECHR and the EU Charter of Fundamental Rights. However, **regrettably, this is not the case:** in many EU MSs the relevant laws do not meet these standards; several, in particular those of the UK (which has the largest intelligence operations in the EU linked to the USA), are being challenged in the European Court of Human Rights on precisely this ground. Moreover, the UK government believes that these laws cannot be assessed under EU law because MSs’ activities in relation to national security are outside EU law. Also, in Poland the law providing for law enforcement and intelligence agencies access to telecommunication and Internet data does not fulfil the standards set by the ECtHR and ECJ jurisprudence, and has recently been subject to the inquiry of the Venice Commission for that reason. Also, in the Netherlands, the proposed law for the Dutch intelligence services would allow generalised access to communication and does not

			<p>meet the standards of the before mentioned jurisprudence.</p> <p>In those circumstances, the <i>carte blanche</i> that paras. (a) and (g) of Article 28(3) provides fails to protect EU data subjects against the kind of “generalised access” to their data by EU MSs’ agencies that the CJEU found in relation to the US agencies to impinge on the very “essence” of the right to privacy. The fact that many EU MSs are carrying out exactly the same kinds of indiscriminate surveillance as the USA has long been the “elephant in the room” in the EU. This provision confirms this willing blindness and allows the elephant to trample over our fundamental rights without redress, indeed in secret. It is unacceptable.</p>
<p>Article 28(4)</p> 		Sub-Processors	<p>The provision refers to “legal acts” adopted by MSs that impose on sub-contractors of processors (sub-processors) the same duties as rest on the main processor, and that set out technical and organisational standards that (sub-)processors must meet. Provided that these standards are in accordance with the Regulation and other EU legal requirements (e.g., IT security rules and -standards), this provision is not problematic.</p>
<p>Article 29</p> 	<p><i>None</i> (in particular not addressed in Recital 81)</p>	Processing under the authority of the controller and processor	<p>This provision essentially repeats the stipulations in Article 28(3)(a) & (g), discussed above, with regard to “any person acting under the authority of the controller or of the processor who has access to personal data”. It effectively states that when EU law or the law of a MS requires such a person to process the data other than as instructed by the controller or the processor, e.g., to disclose the data to a law enforcement- or national security agency in the MS, or indeed to transfer or disclose the data to a third country or international organisation; or not to erase the data at the end of a processing contract, the person concerned must do as instructed by the MS, irrespective of the will of the controller or the processor (or the purpose-limitation principle). The conclusion must therefore be the same: this constitutes another</p>

			<i>carte blanche</i> that fails to protect EU data subjects against the kind of “generalised access” to their data by EU MSs’ agencies that the CJEU found in relation to the US agencies to impinge on the very “essence” of the right to privacy. It too is unacceptable.
--	--	--	--

CHAPTER 4: CONTROLLER AND PROCESSOR Section 2: data security		ANALYSIS	
Article 32(4) 	Security of processing	This provision is essentially a repetition of Article 29. However, it is notable that, in this article, it is contained within the section and first article dealing with data security (Section 2, Article 32). This can only mean that the legal duties in mind here relate in particular to IT security measures - or rather, to legally imposed duties to bypass or undermine the security of the processing in question, e.g., the compulsory installing of “back doors” into databases or communication systems. If this is indeed what the provision seeks to expressly allow to be done - indeed requires to be done - whenever that is provided for (required) under the domestic law of a MS, it again constitutes an unacceptable <i>carte blanche</i> allowing for interferences with EU data subjects’ privacy- and data protection rights, in violation of the Charter. It should also be noted that the Dutch government specifically issued a statement regarding the importance of not undermining cryptography standards and the prohibition of imposing back doors unto software or hardware. This clause could undermine this statement and would, if used by other Mss, harm the Digital Single Market.	

CHAPTER 4: CONTROLLER AND PROCESSOR.
Section 3: data protection impact
assessment and prior consultation

ANALYSIS

Article 35(10)




Recitals 92 &
93 (cf. also
84, 89 – 91,
94 & 95)

Data protection impact
assessment
(DPIA)

This provision relates to the situation in which processing is carried out in compliance with a legal obligation, in the performing of a task in the public interest, or in the exercise of public authority (see the analyses *re* Article 6(1)(c) & (e), above) and is based on EU or MS law. It says that if the relevant law regulates the specific processing operation or set of operations, and a DPIA has already been carried out for that operation or set of operations as part of a general impact assessment carried out in the context of the adoption of the relevant law, a new DPIA of any new processing operation of the same kind is not required. **This appears to be unproblematic, provided the original (general) DPIA was thorough; the new operation is indeed of precisely the same kind as was assessed in that original DPIA; and the legal rules and interpretations of the rules or technical or ethical standards in question have not changed.**

But if the provision were to be treated as giving a *carte blanche* for all kinds of vaguely similar operations by large numbers of actually quite different entities, more or less forever, it would be much more problematic and defeat the purpose of the requirement of a DPIA in cases of processing that poses real risks to the rights and interests of data subjects.

There is also the risk that broad general DPIAs of this kind in one MS could effectively allow for processing in that MS which would not be regarded as acceptable (or even lawful) in another MS. **It is therefore essential that whenever there is such a general DPIA in relation to processing operations that are, or could be, transnational**

			(e.g., in relation to “tasks in the public interest” or the “exercise of public authority” in the online environment, or that involve data sharing between public and/or private entities in more than one MS), the cooperation-, mutual assistance- and consistency mechanisms are fully used, to avoid conflicts.
Article 36(5) 	Recital 94	Prior consultation or authorisation	<p>This provision is clearly a compromise between MSs that only wanted to provide for “prior consultations” with the DPA “where a data protection impact assessment as provided for in Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk”, and MSs that in such circumstance want to require the “prior authorisation” of their DPA for such operations (as they often already do under their current laws). The provision makes “prior consultations” the main requirement, but allows the latter kinds of MSs to retain their requirement for “prior authorisations” – but only in relation to “the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.” In practice, this will mainly apply to public bodies – but as explained in the analysis of Article 6(1)(c) and (e), above, some “tasks” performed by private entities, such as fraud detection, can also be argued to be “in the public interest”.</p> <p>The provision means that when there are processing operations of the kinds covered by this provision, which are transnational in nature (such as, e.g., cross-border public health-related activities by public authorities, or cross-border anti-fraud measures by banks), some of the controllers involved may only be required to “consult” their DPA on the measures to be taken to mitigate the risks to data subjects’ rights and interests, while others would need to obtain “prior authorisation” from</p>

			<p>their DPA for the same operations.</p>
--	--	--	--

While therefore creating some formal differences in the data protection regimes in the MSs, **this would perhaps not be too problematic in practice.** It may be noted that this could be precisely one kind of scenario in which “joint controllers” could evade the more onerous requirements through their (semi-secret) “arrangements”: see the analysis of Article 26, above.

CHAPTER 4: CONTROLLER AND PROCESSOR
Section 4: data protection officer

ANALYSIS

Article 37(1) & (4)



Recital 97


Designation of the data protection officer (DPO)


Article 37(1) makes the appointment of a **DPO compulsory for public bodies, but for private bodies only in certain limited cases**, i.e., when they carry out “systematic monitoring of data subjects on a large scale” or when their “core activities” involve processing of sensitive data “on a large scale”. The latter tests (“large”, “core”, “systematic”) are already vague – and this requirement is therefore certain to be applied differently in the different MSs (unless the cooperation-, mutual assistance- and consistency mechanisms are used to avoid that).


Article 37(4) first of all makes clear that **private entities may of course also voluntarily appoint a DPO** even if they are not required to do so under Article 37(1) – and of course many already do have a DPO (or CIO).


Secondly, it says that **MSs may also extend this duty to other entities than those covered by Article 37(1)**, i.e., to private entities not carrying out “systematic monitoring of data subjects on a large scale” or processing of sensitive data “on a large scale”. This is likely to be done in countries such as Germany that have a long history of requiring a DPO in most sizeable companies.

This difference in compulsory requirements of a DPO in different MSs is unlikely to be problematic, especially since (as just noted) many companies in any case already appoint one voluntarily. But it may be noted that the “arrangements” for “joint controllers” discussed in the analysis of Article 26, above, could be used to avoid the appointment of a DPO in certain scenarios

Article 38(5) 		Secrecy and confidentiality duties of the data protection officer	This provision stipulates that secrecy and confidentiality requirements incumbent on DPOs can be determined by EU or MS law. This is basically not problematic – except perhaps with regard to exceptions to such duties, in particular in relation to compulsory disclosures of information to law enforcement- and national security agencies, as discussed in the analyses of Articles 28(3)(a)&(g), 29 and 32(4), above.
---	--	---	---

CHAPTER 5: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS			ANALYSIS
<p>Article 46(2) - general</p> 	<p>Recital 108</p>	<p>Transfers on the basis of “appropriate safeguards”</p>	<p>Article 46 deals with transfers of personal data to third countries that do not provide “adequate” protection of personal data (which now means that the protection must be “essentially equivalent” to the EU rules, as acknowledged in Recital 104). Such transfers must be subject to “appropriate safeguards” (Article 46(1)). Article 46(2) lists a number of means by which such safeguards can be provided “without requiring any specific authorisation from a supervisory authority”. For most of these, this latter stipulation is understandable, because the relevant means are otherwise subject to systems to ensure they are agreed between the DPAs and, if needs be, subject to the consistency mechanism: BCRs; standard clauses adopted by the Commission; standard clauses adopted by DPAs; and approved codes of conduct. Article 46(3) lists some further means, including “administrative [i.e., non-legally-binding] agreements between public authorities or bodies”, which are also subject to the consistency mechanism (Article 46(4)).</p> <p>However, Article 46(2) also lists two means of providing for “appropriate safeguards” that are (i) also expressly do not require “any specific authorisation from a DPA”, yet (ii) appear to be not subject to the consistency mechanism. These are discussed below because they can clearly lead to dangerous divergencies between the MSs - and indeed seem to create an option for circumvention of the - in principle - strict data transfer regime.</p>


<p>Article 46(2) (a)</p> 	<p>Recital 108</p>	<p>Transfers subject to appropriate safeguards provided for in legal instruments between public bodies</p>	<p>Article 46(2)(a) allows controllers or processors to transfer personal data to countries without adequate data protection if “appropriate safeguards” are provided for by means of “a legally binding and enforceable instrument between public authorities or bodies”. Transfers on this basis may be made “without requiring any specific authorisation from a supervisory authority”. Presumably, the “binding instruments” are between public authorities or bodies in the EU MS in question and public authorities and bodies in the third country.</p> <p>The form that the “appropriate safeguards” or indeed the “instruments” can or should take are largely left to the MSs; Recital 108 merely says that the safeguards can be “inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects”, but that is just an example. It adds that when the safeguards are provided for in “administrative arrangements that are not legally binding”, authorisation should be obtained from the competent DPA. But otherwise, the DPA apparently need not have any input in them. There is not even a requirement that the “instrument” be made public or that it meet the ECtHR “quality requirements” for “law”: that it must be detailed, precise, clear, foreseeable and published.</p> <p>This provision appears to constitute yet another <i>carte blanche</i> through which MSs can self-authorise transfers of any personal data, for any purpose, to any “public authorities or bodies”, in any country without adequate data protection - without any control by their own DPA or by any other MS DPA or the EDPB (or the Commission). All that is required is that the MS and the third country in question adopt some kind of “legally binding and enforceable instrument” covering the transfer (or, typically, kind of transfer); this need not even be a published “instrument”. This could be, for example, a trade agreement.</p>
--	--------------------	--	--

			<p>This provision drives a horse and cart through the GDPR data transfer regime. This flexibility used in data transfer schemes related to cooperation not only in criminal or national security matters (that are beyond the scope of GDPR) but also in the context of immigration or tax evasion detection.</p>
<p>Article 46(2) (f), read together with Article 42(5) and 43(1)</p> 		<p>Transfers subject to appropriate safeguards provided for in privacy certifications (privacy seals)</p>	<p>Article 46(2)(a) allows controllers or processors to transfer personal data to countries without adequate data protection if “appropriate safeguards” are provided for by means of “an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights”. Article 42(2) adds that such seals can also be obtained by controllers and processors in such third countries, to demonstrate that they offer “appropriate guarantees” to allow data to be transferred to them.</p> <p>Such “certification mechanisms” (privacy seals) can be operated by the DPA in question – and, in that case, the decision to award a seal is a decision of the DPA that is subject to the consistency mechanism. However, Articles 42(5) and 43(1) makes clear that privacy seals can also be issued by “certification bodies” that are separate from the DPA, other than that they may be accredited by the DPA – although they could also be accredited by the relevant national accreditation body without any involvement of the DPA.</p> <p>The point is that privacy seals issued by such certification bodies that are not DPAs are still stipulated in Article 46(2)(f) to be able to provide “appropriate safeguards” to allow data transfers to third countries without adequate protection, “without requiring any specific authorisation from a supervisory authority”. Moreover, since the issuing of such seals – with major effects on data transfers – by such separate bodies are not acts or decisions of the DPA in the MS concerned, they are also not subject to the consistency mechanism.</p>

This means that it will in principle be possible for certification bodies in certain MSs to effectively authorise transfers of personal data to countries without adequate protection, without any involvement of the DPA in that country in the issuing of the individual seals. However, the DPA in question can order the certification body to withdraw a certification, or not to issue it (Article 58(2)(h)) and/or order the suspension of the consequent transfer(s) (Article 58(2)(j)), which is a major safeguard.

But there remains an issue if a DPA chooses not to use this power in relation to a transfer that also affects data subjects in other MSs. In particular, there is a serious question as to whether such a non-ordering of a withdrawal of a certification (seal) and/or the non-ordering of a suspension of transfers in such cases is subject to the cooperation-, mutual assistance- and consistency mechanisms. It would appear that the first two of these can be invoked (cf. Articles 61 and 64(2)), but this is less clear as concerns the consistency mechanism which, on its face, seems to apply only to decisions of DPAs. As long as this is interpreted as including decisions not to act (i.e., in this context, not to order the withdrawal or non-issuance of a seal, or not to suspend the transfers based on a seal), that can be overcome.

This is a matter that should be addressed urgently by the new EDPB. **If the EDPB agrees to follow this line and to allow for the application of the consistency mechanism in relation to the issuing of seals as a basis for data transfers, there may not be a problem - in fact, such seals could play a very useful role. However, if it were to be held that the consistency mechanism cannot be used in relation to certifications issued by certification bodies that are not also DPAs, this provision could create another serious loophole in the supposedly strict data transfer regime.**


<p>Article 48</p> 		<p>Transfers or disclosures not authorised by Union law (the so-called “Anti-NSA Clause”)</p>	<p>This provision derives from a draft article inserted into the GDPR by the European Parliament to counter the use by third countries of orders (including secret orders, i.e. orders with a “gagging order” attached to them) requiring controllers and processors subject to their jurisdiction to surreptitiously disclose data on EU data subjects to third countries’ law enforcement- and/or national security agencies, in circumstances in which such disclosures could lead to violations of the EU data subjects’ rights – such as the secret orders issued by the US authorities in the mass surveillance operations exposed by Edward Snowden. The EP’s clause was consequently dubbed the “Anti-FISA Clause”.</p> <p>However, some important requirements contained in the EP clause are no longer included in the GDPR text agreed in the “trilogues”. In particular, the EP wanted to impose on controllers and processors subject to the Regulation a duty to inform the DPAs in the EU if they were served with such an order; and to prohibit them from making the disclosures without “prior authorisation” from the DPAs. The DPAs would also inform the other relevant domestic authorities and indeed the data subjects (unless there were good reasons not to do so). Regrettably, these requirements have been removed.</p> <p>Consequently, the provision now merely states that judicial or administrative disclosure orders issued by authorities of a third country to a controller or processor subject to the Regulation “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”.</p> <p>There are three major problems with this reduced text.</p> <p><u>First of all</u>, the UK is relying on the references to “recognition” and “enforcement” of third-country judgments and decisions to claim that</p>
--	--	---	--

this provision is about judicial cooperation – and that it therefore falls within an area of EU law from which it has been allowed to **opt out** (under Protocol 21 to the Lisbon Treaty).^{*} This is highly **dubious**, since the whole point of the provision is to counter both judicial and administrative disclosure orders (in particular those with a “gagging order” attached) issued outside of the normal Mutual Legal Assistance Treaty (MLAT) frameworks. But presumably the UK – which is the most important partner to the USA in relation to global, secret and indiscriminate data-gathering for ill-defined “intelligence” purposes – will still refuse to apply the provision.

Secondly, the reduced text appears to allow controllers and processors subject to the Regulation (which includes not just EU-based controllers but also third country-based ones offering goods and services to EU data subjects, including the “Internet Giants” Facebook, Twitter, etc., and third country-, including US-based-, “Cloud” providers and other processors, etc.) to comply with such third-country judicial or administrative orders as long as there is (any kind of) “international agreement” in place covering the disclosure, between the third country and the MS (or MSs) involved. Crucially, the “international agreement” in question clearly does not have to be an MLAT – **any kind of “international agreement” will do, even secret ones** – of which there are believed to be many.

Third, there is nothing in the text to prevent the kinds of disclosure orders covered by the provision from being accompanied by a “**gagging order**” issued by the same court or body that issued the disclosure order. More specifically, the provision does not require the disclosure of such an order, and/or such a “gagging order”, to any body in the EU MS concerned, including the DPA in that MS.

In effect, the EP, by agreeing to this text, has accepted the complete emasculation of its own “Anti-NSA Clause”: the


			<p>wording in the text agreed in December 2015 provides no serious protection against disclosures of even highly sensitive data on EU data subjects to non-EU (including US) law enforcement- and national security agencies, on the basis of orders (including secret orders) of the third-country's courts, or even of those agencies themselves. And the controllers and even the DPAs in the EU and, of course, especially EU data subjects, can be kept completely in the dark about these disclosures. Indeed, there is nothing in this provision to safeguard data on EU data subjects against "generalised [i.e., indiscriminate] access" to their data by the third-country agencies, in clear violation of the Charter as interpreted by the CJEU in the <i>Schrems</i> case.</p> <p>This provision is in manifest breach of the EU Charter of Fundamental Rights.</p>
<p>* See: http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2016-02-04/HLWS500/</p>			
<p>Article 49(1) (d), read together with (4)</p> 	<p>Recitals 111&112</p>	<p>Derogations for data transferred for important reasons of public interest</p>	<p>Article 49(1)(d) allows the transfer of personal data to third countries without adequate data protection, without the consent of the data subjects or any other basis for the transfer as listed in Article 46(1), if the transfer is "necessary for important reasons of public interest"; and para. (4) adds that the "public interest" in question must be "recognised in Union law or in the law of the Member State to which the controller is subject".</p> <p>Recital 112 lists as examples of relevant transfers: "international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order</p>


to reduce and/or eliminate doping in sport”; transfers which are “necessary to protect an interest which is essential for the data subject's or another person's vital interests”; and “transfer[s] to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts”. However, these are only examples.

Presumably, all the special public interests listed in Article 23 (analysed separately, above) also all qualify as such interests: national security, defence, public security, the prevention or investigation of crimes, “other important objectives of general public interests”, protection of judicial independence, breaches of professional ethics, protection of data subject rights, “a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority”, and even enforcement of civil law claims (the claims may be private, but the general principle of enforcement of civil claims serves a wider public interest: upholding the rule of law, also in transnational cases).


As noted in the analysis of Article 23, **some of these interests are already excessively broad and vague, which means that their application in practice is not foreseeable (which contravenes the rule of law in itself). But Article 49(1)(d) allows MSs to actually go even beyond those purposes: the “public interests” listed here are left completely undefined.** It could include, for instance, “maintaining good relations” with the third country to which the data are to be transferred, or even “boosting trade”.



It is odd that, unlike Article 44(5a), discussed below, Article 44(5) does not stipulate that the MSs relying on this provision “shall notify [the relevant provisions of their national law] to the Commission.”

			<p>As it stands, this provision is effectively yet another <i>carte blanche</i> handed to the MSs, allowing them to circumvent the otherwise seemingly strict rules on data transfers. Its application by the MSs should be most closely watched, to detect any abuses of this provision.</p>
<p>Article 49(1) (g)</p> 	Recital 111	Derogations for data from registers open to the public	<p>This provision allows the transfer of personal data to third countries without adequate data protection, without the consent of the data subjects or any other basis for the transfer as listed in Article 49(1)(b)-(f), if the data come from “a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest”, provided that “the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.” This applies, e.g., to land, buildings or company ownership registers, access to which is typically granted by law either to everyone (registers open to the public) or to certain categories of people specified in the law regulating the register, e.g., house buyers or litigants.</p> <p>In principle, this may seem unproblematic. However, the EU DPAs have made clear, in several “Article 29 Working Group” opinions,** that under EU data protection law, data released from public registers should remain subject to the purpose-limitation principle, and that the data once released can therefore not be used for any other purpose. It is notable that the provision refers to compliance with the conditions for “consultation” of the data – i.e., with the conditions for access to and obtaining of the data – but not to any conditions that may be imposed on the further use of the data.</p> <p>When data from public registers are transferred to third countries without adequate (or indeed any) data protection, the WP29’s important limitation is very likely to be ignored. In other words, the provision is</p>

			<p>likely to lead to the loss of control over the use of data that can be obtained from public registers, or registers open to certain categories of people, in the EU, contrary to the purpose-limitation principle. For instance, in the USA, data that have been made public effectively lose all privacy protection.</p>
<p>** See, e.g.: Opinion No. 3/99 of 3 May 1999 on <u>Public sector information and the protection of personal data</u> (WP20); Opinion 5/2000 of 13 July 2000 on <u>The Use of Public Directories for Reverse or Multi-criteria Searching Services (Reverse Directories)</u> (WP33); Opinion 7/2003 of 12 December 2003 on <u>The re-use of public sector information and the protection of personal data – Striking the balance</u> (WP83).</p>			
<p>Article 49(5)</p> 	<p>Recital 112</p>	<p>MSs may limit data transfers for important reasons of public interest</p>	<p>This provision is the mirror of the one contained in Article 49(1)(d), read with Article 49(4), discussed above. It allows the EU and the MSs to “set limits”, by law, to “the transfer of specific categories of personal data to a third country [without adequate (or indeed any) data protection] or an international organisation”, for the same undefined “important reasons of public interest”.</p> <p>It follows from the structure of the article that these “limits” are to be applied in cases in which the data can, in principle, be transferred to the third country in question, on the basis of the consent of the data subject or any of the other legal bases listed in Article 49(1). The nature of the “limits” is unspecified – presumably, they could amount to a complete ban on transfers of the “specific” (i.e., specified) categories of data concerned to the third country or international organisation concerned. It is therefore difficult to predict how and in what kinds of circumstances the EU or the MSs will invoke this provision.</p> <p>However, when used by one MS but not by others, the provision does raise problems in transnational contexts. Because under the Regulation – and as a fundamental principle of the Digital Single Market – data, including personal data, can be freely moved between MSs, any such</p>


			<p>restrictions on transfers imposed by the one MS can, it would appear, be easily evaded by controllers: all they have to do is send the data to another MS that does not impose the “limits”, and transfer them on from that other MS to the third country in question. In fact, if this provision were to be widely relied on by MSs to impose special national-legal restrictions on international transfers that do not apply in the other MSs, or if different MSs were to adopt different “limits”, and/or apply them to differently-defined “specific categories of personal data”, the very principle of harmonised rules for transfers of such data to third countries would be abandoned.</p> <p>This provision therefore places a “ticking bomb” under the supposedly-harmonised regime for transfers of personal data from the EU to third countries without adequate (or any) data protection: as long as it is not (or extremely sparingly) used, it may not be too problematic. But it could easily wreck the entire EU data transfer regime.</p>
--	--	--	--

CHAPTER 6: INDEPENDENT SUPERVISORY AUTHORITIES Section 1: independent status			ANALYSIS
Article 53(1) 	Recitals 117ff.	Appointment of the members of the supervisory authority	Member states can choose which body is to appoint the members of their supervisory authority (or authorities): this can be their parliament, government, head of state, or another independent body (such as a judicial council). Some such appointments, in particular appointments by the executive (government or head of state) have been problematic in the past in terms of independence. Appointment by the national parliament or by an independent body such as a judicial council is


			preferable. However, the real test of the pudding is in the eating.
Article 53(3) 	Recitals 117ff.	End of duty of the members of the supervisory authority	The reference to states' retirement law is not problematic.
Article 54 	Recitals 117ff.	Rules on the establishment of the supervisory authority	Various details of the authority are to be provided for by the MS law, with some flexibility as concerns qualifications and eligibility of members; rules and procedures for appointment; duration of term (but this must be at least four years); whether members can serve more than one term; conditions of employment; and duties of confidentiality. These are not necessarily problematic - the main issue is their competence and independence in practice, which can only be assessed in practice (although a four-year term seems too short: cf. the case-law of the ECtHR on appointment of judges).


CHAPTER 6: INDEPENDENT SUPERVISORY AUTHORITIES
Section 2: competence, tasks and powers


ANALYSIS



Article 55(2) read with Article 6(1)(c)& (e) and Article 56 	Recital 128	Competence in relation to cross-border processing to comply with a legal obligation, for a public interest task, or under official authority	Article 55(2) says that in relation to processing covered by Article 6(1)(c) or (e) (i.e., processing to comply with a legal obligation, for a public interest task, or under official authority), the DPA of the MS concerned (i.e., of the MS imposing the legal obligation, or regulating the relevant public interest task or granting the official authority) shall be competent. That would seem uncontroversial. However, the text adds that “In such cases Article 56 does not apply”. That article deals with the determination of a “lead authority” in cases of cross-border processing - which is defined in Article 4(23) as also covering “processing of personal data which takes
---	-------------	--	--

			<p>place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.” Some of the processing covered by Article 6(1)(c) or (e) can well include cross-border processing, e.g., processing of personal data by banks to detect credit card fraud, or processing of such data by “cybersecurity” agencies of MSs or private “cybersecurity” companies.</p> <p>Even more problematically, it could cover the compulsory handing over of personal data held by private companies (e.g., providers of e-communication networks or -services, or social networks, or financial institutions or travel companies) to the law enforcement- and/or national security agencies of the MS concerned under any “legal obligation”. This could easily “substantially affect[] or [be] likely to substantially affect data subjects in more than one Member State”. But since Article 56 does not apply, the DPA of the MS that imposes such “legal obligations” need not even inform the other DPAs of such handing over of data. It is unclear whether the cooperation-, mutual assistance- and consistency mechanisms apply in such cases, since they all hinge on the “lead authority” working closely with the other DPAs concerned. If there is no lead authority, how is this to be achieved? In the wake of the Snowden revelations, it has become clear that certain MSs have used vague provisions under which they have compelled telecommunication service providers to hand over communications data in bulk (e.g., the UK under S.94 of the Telecommunications Act).</p> <p>This article is dangerous. (See also the analysis of Article 61(4)(b), below)</p>
Article 58(6)	Recital 129	Granting of additional powers to the DPAs	Article 58 contains several long lists of powers that all MSs must grant to their DPAs. These are useful and important, e.g., as concerns the right of

			<p>DPA to order the withdrawal or non-issuing of a certificate (privacy seal) (Article 58(2)(h): see the analysis of Article 46(2)(f), above) and the right to initiate judicial proceedings (Article 58(5)). The article adds that MSs may grant their DPAs additional powers, as long as this does not impede the operation of the consultation-, mutual assistance- and consistency mechanisms. This would appear to be unproblematic.</p>
---	--	--	---

CHAPTER 7: CO-OPERATION AND CONSISTENCY Section 1: co-operation		ANALYSIS	
<p>Article 61(4)b)</p> 	<p><i>Not addressed in the recitals on cooperation & assistance</i> (See Recitals 133 - 135)</p>	<p>Refusal of cooperation and mutual assistance</p>	<p>This provision stipulates that a DPA in one EU MS may refuse to comply with a request for assistance from a DPA in another MS if “compliance with the request would infringe” the law of the former MS. Neither the article nor the recitals clarify when and how this provision will apply, or give any illustrations or examples. The article is problematic if read in the light of Article 55(2), analysed earlier, which stipulates that if processing is carried out to comply with a legal obligation, for a public interest task, or under official authority (by private or public bodies), the rules on “lead authority” do not apply, even if the processing affects data subjects in other MSs. In respect of that article, we noted that it is unclear whether, in such cases, the cooperation-, mutual assistance- and consistency mechanisms apply, since they all hinge on the “lead authority” working closely with the other DPAs concerned. Article 61(4)(b) makes clear that even if in principle those mechanisms do apply (although they would be hampered by the non-application of the rules on “lead authority”), any MS can still simply stop them from applying if its national law says so. This creates concerns in particular due to the unclear scope of “national security” issues that, in principle, fall outside the scope of the Regulation. Thus, if a DPA in one MS (“MS A”) feels that the rights of data subjects in that MS may be affected by, say, disclosures by private companies in another MS (“MS B”) (the data collection and the actual disclosure being nonetheless under the Regulation) to the national security agencies of MS B (or if a data subject or association complains about this), then the DPA in MS B will be prevented in cooperating in the investigation, if the law in MS B prohibits this activity (or essential</p>

			<p>elements thereof) such as the disclosure of any information relating to the relevant matter (e.g., again, national security).</p> <p>This article creates a serious loophole in the intra-EU data protection enforcement system.</p>
<p>Article 62 (3) & (4)</p> 	<p><i>Not specifically addressed</i> (cf. Recital 134)</p>	<p>Joint operations of supervisory authorities</p>	<p>Under Article 62, MSs can set up “joint investigations” and take “joint enforcement measures” in appropriate cases; and staff from all the DPAQs concerned can participate in this. Paras.; (3) and (4) stipulate that if such staff from a concerned DPA is seconded to the lead authority, they can be given and may exercise public powers (under the supervision of the host authority) insofar as the law of the host country allows and in accordance with the law of the host country.</p> <p>The express providing for secondments is a positive matter, and it is only natural that the powers that are granted are determined by the law of the host country (as long as there is no obstruction to the effective operation of the cooperation mechanism).</p>

CHAPTER 8: REMEDIES, LIABILITIES AND SANCTIONS			ANALYSIS
Article 80 	None	Representation of data subjects	<p>Although the Regulation, in this article, now expressly provides for the possibility of not-for-profit organisations representing data subjects in the making of complaints, this will only actually be the case in MSs where the law provides for this (Para. (1)). Similarly, MSs may, but are not required, to allow such organisations to lodge complaints of their own motion (para. (2)). This means collective actions and similar tests cases will become possible in some MSs but not necessarily in all MSs. This in effect creates inequalities in enforcement of data subject rights in practice.</p>
Article 83 (7) & (8) 	Recital 148	General conditions for imposing administrative fines	<p>Article 83(8) stipulates that the imposition of administrative fines must in each MS be subject to “appropriate procedural safeguards”, and that these safeguards must be “in accordance with Union and Member State law”. That is positive. It confirms the rule of law and indeed allows the EU (including ultimately the CJEU) to assess whether any such safeguards provided for in any particular MS are indeed appropriate and in accordance with the Charter.</p> <p>However, Article 83(7) stipulates that “whether and to what extent administrative fines may be imposed on public authorities and bodies” is to be determined by the law of the MS where the relevant body is established. This means that the enforcement regime for public authorities and bodies will be different in different MSs. On the other hand, even MSs that might not want to allow for the imposition of administrative fines on public authorities and -bodies are still required to provide for “effective, proportionate and dissuasive” penalties, and must inform the European Commission of the specific penalties it has adopted before the Regulation comes into full force (Article 84). Article 83(7) will probably not be problematic in practice as long as the DPAs in all MSs are</p>

			committed to real and effective enforcement (which they have not all been under the 1995 Directive).
--	--	--	--

CHAPTER 9: PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

ANALYSIS

Article 85




Recital 153



Processing of personal data and freedom of expression and information


Article 85(1) stipulates that MSs must (“shall”) reconcile the right to data protection freedom of expression (which includes the right to “[seek,] receive and impart information and ideas without interference by public authority and regardless of frontiers”, Article 11 CFR) “by law”, i.e., in their domestic law. Usefully, unlike the 1995 Directive, the Regulation requires this “reconciliation” quite generally, i.e., “including [but not limited to] processing for journalistic purposes and the purposes of academic, artistic or literary expression”. On the other hand, the second paragraph adds that “[f]or processing carried out for journalistic purposes or the purpose of academic artistic or literary expression” [only], this must include exemptions or derogations from the basic data protection principles, the rights of data subjects, the duties of controllers and processors, restrictions on transborder data flows, the supervision by DPAs “if they [i.e., such exemptions or derogations] are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.”


This provision opens up a whole series of cans of worms. The first point to be made is that the provision leaves the “reconciling” entirely to the MSs’ laws, except for the proviso that all the relevant exemptions and derogations must be “necessary” to reconcile the two rights. In practice, **the laws on privacy** (in the narrower sense than data protection, i.e., as concerns invasion of other people’s private sphere) **are still very different in the different MSs. The article perpetuates that.** Recital


			<p>153 adds (in an unusual reference to applicable law) that “Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply.” Does this mean that publications by a (say) UK-based publisher (or blogger) should benefit from relatively lax rules on privacy of “celebrities” there, even if the publication in question would be barred if published by a (say) French publisher, even though the UK publication is easily (and online directly) accessible from France? Even if the publication was in French and directed at a French audience? This brief suggestion on applicable law is insufficient for the online environment. Unless this is more specifically addressed in the successor to the e-Privacy Directive, it will make the legal environment for free speech very unclear, particularly in the online digital environment. <u>Secondly</u>, in the digital age, it is increasingly difficult to define “journalistic, academic, artistic and literary” activities. Many people publish, express themselves or post their opinions online, often to a wide audience. Although Recital 153 rightly says that “In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly”, it is still unclear to what extent this provision covers the activities of bloggers, online activists and digitally self-publishing authors and artists. In some MS, like Poland, the law still provides for a very narrow, traditional definition of “journalism” when regulating respective privileges and responsibilities. <u>Third</u>, the second paragraph gives no guidance whatsoever on the precise scope of the exemptions that might be “necessary”. In some respects – e.g., as concerns the principle that processing should be “fair and lawful”, or as concerns the requirement that “every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay” – it is difficult to see how</p>
--	--	--	---

			<p><i>any</i> exemption could ever be necessary. Depending on the actual level of political influence of national associations of journalists or publishers, MS may go as far as to provide for full derogation from the basic data protection principles, the rights of data subjects, the duties of controllers and processors, restrictions on trans-border data flows and the supervision by the DPA. Such “total derogation” was, for example, advocated by the influential Association of Polish Journalists (Stowarzyszenie Dziennikarzy Polskich).</p> <p>This provision is far too unclear. It will lead to serious conflicts of law that will hamper the free single market (including, in particular, the free Digital Single Market) in relation to published materials. At the very least, the new European Data Protection Board should issue guidelines urgently on how this provision is to be applied; and in that it should consult civil society, including freedom of expression- and digital rights groups. The continued use of the term “necessary” – which of course refers to Article 52(1) of the Charter – means that the laws adopted (or retained) by the MSs in this regard can, when they touch on privacy and data protection, be tested on that “necessity” (and on their clarity and foreseeability, etc.) in the courts, including the CJEU.</p>
<p>Article 86</p> 	Recital 154	Processing of personal data and public access to official documents	<p>Not dissimilar from the previous article, this article allows MSs to reconcile data protection, here with the principle of access to documents held by public bodies and bodies tasked with public tasks. Given that the documents in question will generally be in the hands of public bodies of the MS in question (or in the hands of companies charged with the carrying out of a public task, such as privatised prisons), the differences in this respect will not be as problematic as the ones discussed in relation to Article 85. However, it would still be better if there was greater harmonisation between the MSs in this respect. Indeed, when it comes to access to documents relating to matters or bodies that are subject to</p>

			<p>Union law, it would seem appropriate for the rules to be formally harmonised. Why should people in, say, the UK, have less access to, say, data on EU agricultural subsidies including the names of beneficiaries in their country than people in, say, Sweden (or the other way around)?</p>
<p>Article 87</p> 	<p><i>None</i></p>	<p>Processing of national identification number</p>	<p>It was already recognised in the 1995 Directive that national identification numbers and similar identifiers of general application (such as the UK national insurance number) pose risks in terms of data protection, in particular by allowing easy linking or matching of different datasets or even whole databases. Article 87 also recognises this but again leaves this effectively entirely up to the MSS: they “<i>may</i> determine the specific conditions” for the use of the numbers, provided only that they ensure that the numbers are “used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.” The Regulation gives no indication of what such “appropriate safeguards” might be; it does not even require that the conditions and safeguards are provided by law. The national rules on the use of such national IDs and general identifiers will therefore continue to be very difficult from MS to MS.</p> <p>This will become increasingly problematic because such numbers are increasingly used – and demanded – in cross-border trade, e.g., in relation to cross-border payments. This would appear to be another area in which much further harmonisation – or at least clarification of the applicable law rules – is urgently needed.</p>
<p>Article 88</p> 	<p>Recital 155</p>	<p>Processing in the employment context</p>	<p>The provision allows MSs to adopt “more specific rules” on processing of personal data in the employment context. It recognises that in many (in particular Continental-European) MSs, numerous employment-related issues are addressed in “collective agreements” between employers and trades unions (in some countries, such as NL, with state involvement), and therefore allows these data protection matters also to be resolved there. All this is sensible – except that in a context in which increasing</p>

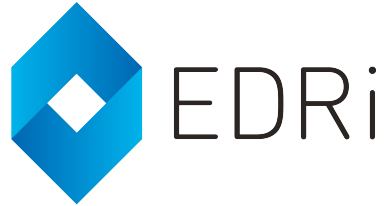
			numbers of workers work in multi-national companies, greater harmonisation may be needed in the not-too-distant future.
Article 89 	Recitals 156 - 163	Safeguards and derogations for the processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes	<p>In the analysis of Article 9(2)(j), above, we noted that that article can lead to serious abuses of sensitive data for anything labelled “archiving in the public interest” or “scientific” uses, including use of such data for commercial research. The second and third paragraphs of Article 89 seriously aggravate this, by expressly allowing MSs to adopt different – more/less strict – rules in this regard, subject only to the very vague data minimisation/pseudonymisation/anonymization requirements of Article 89(1) (with minor variations between the permitted exemptions from data subject rights regarding archiving and scientific research).</p> <p>Between them, these provisions create dangerous loopholes in the protection of personal, and especially sensitive, data.</p> <p>Presumably, the reference in Article 89(1) to the need for “appropriate safeguards” means that the actual safeguards adopted by the different MSs can be challenged in the courts including, ultimately, the CJEU. But that would be difficult, expensive and time-consuming, against very well-funded major research bodies (that have lobbied hard for “flexible” rules and exemptions such as are provided here).</p> <p>It will be crucial for the new European Data Protection Board to issue clear and strict guidance on these issues as a matter of great urgency.</p>

<p>Article 90</p>  <p>See also Article 14(5) (d)</p>	<p>Recital 164</p>	<p>Obligations of secrecy</p>	<p>Under this article, MSs may “adopt specific rules” on (in practice, limit) the powers of DPAs in relation to controllers or processors “that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy”. It is right that the Regulation recognises the need for special care as regards (highly sensitive) personal data processed in the context of typical matters of professional secrecy such as doctor-client-, priest-penitent-, or lawyer-client relationships. Given that these matters are regulated differently in the different MSs, it is also sensible to leave this, in those contexts, to the MSs.</p> <p>However, the reference to “other equivalent obligations of secrecy” is disturbing (as was also noted in our analysis of Article 14(5) (d)). Could this include duties of confidentiality imposed on companies or public bodies that are required (under secret orders) to disclose personal data they hold to national security agencies, i.e., to duties of confidentiality imposed by means of “gagging order”? To limit the powers of the DPAs in respect of such disclosures would be seriously problematic in view of the Snowden revelations.</p> <p>In that regard, it is useful that Article 90(2) stipulates that the MSs must inform the Commission (and, through this, presumably also the EDPB) of the specific rules adopted (or retained) under this article. This is especially useful in that the stipulation in Article 90(1) that the “specific rules” (exceptions) must be “necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy” means that they can be challenged in the courts, including ultimately the CJEU.</p> <p>It will again be crucial for the new European Data Protection Board to issue clear and strict guidance on these issues as a matter of great urgency.</p>
---	--------------------	-------------------------------	--

<p>Article 91</p> 	<p>Recital 165</p>	<p>Existing data protection rules of churches and religious associations</p>	<p>In our analysis of Article 9(2)(d), above, we already noted that that provision allows (<i>inter alia</i>) religious bodies to process sensitive personal data on their members and “regular contacts” for “legitimate purposes”; and that that provision requires “appropriate safeguards” but does not spell these out – which means that the rules on processing by such entities are likely to remain different in different MSs. We also already noted there that some entities may be regarded as “religious” in one MS but not in another. These differences are problematic, at least on paper, because both the mainstream churches and such other entities increasingly operate transnationally and online. They have only not been problematic in practice because processing by religious bodies has been largely left unexamined by the EU MSs’ DPAs. In some MSs (e.g., Germany), the main churches are subject to detailed data protection rules and elaborate supervisory regimes – but these are separate from the main rules and supervisory systems and do not apply to other denominations. In most other MSs, little or no attention has been given to processing of personal data by religious bodies.</p> <p>Article 91 can be seen as a first step towards bringing the data protection rules for religious bodies in line with the mainstream rules: para. (1) stipulates that “Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules</p>
--	--------------------	--	---

			<p>may continue to apply, provided that they are brought into line with this Regulation.” However, notably, no deadline is stipulated in this regard: there is no stipulation that the MSs must inform the Commission and the EDPB of the specific rules adopted, retained or amended under this article within a specified time. The second paragraph also expressly allows for the continuation of separate supervisory regimes for religious bodies - although it usefully stipulates that the relevant special supervisory authorities must meet the conditions laid down in Chapter VI of the Regulation, i.e., including the requirements as to independence, resources, appointment (if not by parliament, the government or the head of state) by “an independent body entrusted with the appointment under Member State law” (Art. 53(1)), the details of their appointment to be specified by law (Art. 54); and powerful competences of investigation, the issuing of orders, and the imposition of administrative fines of up to 4% of annual turnover (which for some religious bodies can be very substantial). This stipulation in Article 91(2) also means that any special authorities supervising religious bodies may be (and in the appropriate circumstances must be) involved in the cooperation-, mutual assistance- and consistency mechanisms.</p> <p>This article can have major implications for both mainstream and non-mainstream religious bodies. The EDBP should again <u>urgently</u> issue further guidance on its application (and the application of Article 9(2)(j)).</p>
--	--	--	---

This document was prepared by:



PROTECTING DIGITAL FREEDOM

