Council of the
European Union

Brussels, 9 October 2019
(OR. en)

12756/1/19
REV 1

JAI 1024
DAPIX 286
DATAPROTECT 226
FREMP 143
DIGIT 151

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	11292/19
Subject:	Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States

In preparation of the note setting out the Council positions and findings of the application of the GDPR, delegations will find in Annex comments made by the following Member States BE, BG, CZ, DK, DE, EE, IE, FR, HR, LV, LT, LU, NL, AT, PL, PT, RO, SI and SE.

ANNEX

TABLE OF CONTENT

BELGIUM

Following consultations with relevant stakeholders, Belgium submits the following observations concerning the application of various provisions of the GDPR.

In general, Belgium is of the opinion that, while the implementation of the GDPR is still relatively new, the Council report and the Commission evaluation and review should not be limited to those Chapters explicitly mentioned in Article 97.2 GDPR. The past two years have shown a clear interest and need for a broad discussion and more guidance on the implementation of the GDPR. The evaluation and review process should therefore be seized as an opportunity to contribute to providing greater clarity.

Concerning chapter V (TBDF)

- Article 45: adequacy decisions are an excellent instrument to the benefit of cross-border data exchanges in the private sector, reducing red tape and creating legal certainty for companies. As such they contribute to realising the goals of the single (digital) market. However, this instrument remains to date underused. Greater attention should therefore go to the conclusion of adequacy decisions with third countries;

- Article 46: the threshold of providing appropriate safeguards for those transfers which cannot benefit from adequacy decisions – i.e. the majority of transfers – is a necessary and flexible subsidiary mechanism but at the same creates discrepancies between companies. This runs counter to the harmonization objectives of the GDPR. The conclusion of SCC's in particular can prove difficult with branches unfamiliar with this instrument and therefore reluctant to sign them. Also the availability of a variety of subsidiary instruments can lead to complex situations or to them not being applied at all;

- Article 46.2 c) and d): the mixture of EU and nationally approved standard data protection clauses could lead to disparities in the EU, complex and costly operations for companies to determine the right set of SCC's. Branches in third countries are not familiar with SCC's approved by a national DPA which could complicate negotiations. Also, while standard data protection clauses have been established in an inter-controller relationship as well as for transfers between controllers and processors, in an increasingly digital market sub-processors are relied upon. Hence there is a demand to also cover the processor and sub–processor dimension;

- Article 46.2 e): there is a clear interest from various stakeholders to make use of codes of conduct but there is reluctance to engage in this process due to a lack of clear guidelines. This instrument is therefore, still difficult to implement in practice;

- Article 47: the Binding Corporate Rules approved by national DPA's create discrepancies between companies. This instrument, while a useful and necessary subsidiary mechanism, also runs counter to the harmonization objectives of the GDPR.

Concerning data processing by courts in their judicial capacity

Article 55.3: the application of provisions relating to data processing by courts remains a matter of concern. Not only are we faced with a divide between data processing within and outside of judicial activities (for which a clear definition is lacking). The judicial system also falls under the scope of both the GDPR as well as Directive 2016/680. Furthermore, there is a lack of clarity when it comes to the obligation to establish an independent mechanism. Therefore, there is a demand for clarification and guidance specifically for the judicial sector. We could also benefit from an overview of the different solutions adopted by MS.

Concerning Article 89 and specifically in relation to scientific research

- In general the application of the provisions relating to scientific research has shown that there is need for a more integrated regime, especially for European research;

- Specifically concerning Article 89.1 there appears to be contradiction between:
    - Article 9.2 j) which states that scientific research needs to be accompanied by suitable measures based on EU or national law, and
    - Article 89.1 which doesn't mention EU or national law.

BULGARIA

1. In terms of the concepts

Although the legal framework in the field of personal data protection dates from 1995 (in the Republic of Bulgaria since 2002), it seems that the figures of the controller and the processor at the moment remain as a conceptual issue. There are difficulties in distinguishing between the concepts "Controller" and "Processor" and defining their respective quality. They are manifested mainly in more complex contractual relationships. This requires frequent intervention by the supervisory authority and the involvement of its advisory function, which often goes hand in hand with requests for individual legal advice - something we consider incompatible with the supervisory role of the authority.

Although on various occasions the issue of defining the concept of 'large-scale processing' of personal data has been raised for debate, there are currently no clear criteria or at least a method to determine which processing is large-scale. This impedes both the supervisory authority in the exercise of its functions and the data controllers processing the personal data of an unlimited or significant number of data subjects. The establishment of different national legal regimes on that matter would hinder the uniform and consistent application of the General Regulation, while creating the preconditions for legal uncertainty.

2. With regard to the exercise of powers of the supervisory authority

According to Art. 33 of the Regulation, in case of a personal data breach, the controller shall notify the supervisory authority for it and at the same time, in the presence of the preconditions set in Art. 34 – and the data subjects. One of the conditions for applying the obligation to notify data subjects is to assess whether the breach of personal data is likely to result in a high risk to the rights and freedoms of individuals. The purpose of this communication to the data subjects is, depending on the nature of the infringement and the risk created, to assist them to take steps to prevent any possible negative effects. At the same time, however, Art. 77 of the Regulation, stipulates that every data subject may lodge a complaint where he or she considers that the processing of personal data concerning him or her infringes the Regulation. The practice shows that data subjects, after reporting a security breach, refer to the supervisory authority in accordance with Art. 77. In the case where the supervisory authority has taken over and exercised its powers as a result of the personal data breach notification received, difficulties arise in handling complaints on the same issue.

This means that the supervisory authority should consider a single case several times (in the order of notification and in the order of the complaint), and where the complaints are a significant number, it will seriously impede the work of the authority. The Bulgarian supervisory authority is in the current hypothesis (after notification of a security breach in the National Revenue Agency) with the affected individuals exceeding 5 million and the deadline for lodging complaints is 2 years, which implies that the total number of complaints may be significantly increased. Regardless of the end result of the actions of the supervisory authority, incl. taking into account the *ne bis in idem* legal principle, the obligation to handle complaints itself obstructs the work of the data protection authority. It should be pointed out that the hypothesis of Art. 57, para. 4 of the Regulation on the excessiveness of a request to the supervisory authority is made in terms of repetitiveness of requests arising from a single data subject and not in terms of repetition of multiple identical requests made by a large number of data subjects to the supervisory authority regarding the same case.

3. Regarding the codes of conduct

We believe that codes of conduct are an extremely useful and practically oriented voluntary accountability tool. As far as it is new to the Bulgarian practice in the field of personal data protection, our observations show that codes of conduct are widely regarded as a form of indulgence that impedes the powers of the supervisory authority. This required an outreach to raise awareness regarding the abovementioned accountability tool, including the period prior to finalizing the national legal framework and before adopting the guidelines of the European Data Protection Board on this subject. To date, the supervisory authority has addressed 14 requests for approval of codes of conduct, and has delivered 12 opinions on them.

Notwithstanding the foregoing, of the review carried out, including meetings with entities initiating codes of conduct, the following fundamental issues arise which require a uniform approach by Member States:

- Is it possible and admissible to have more than one code of conduct in a given sector;
- Is it possible and admissible for a single controller or processor to join more than one code of conduct, including codes applicable to different sectors;
- What objective criteria can be applied to define the term "sector" as far as there are controllers whose activities fall into different sectors and areas of public relations;
- What is the binding mechanism of a code of conduct to processor who is not party to it, but the controller who has assigned processing activities to him is party to the same code. Complications arise in the case where the data processor himself is a party to another code of conduct.

CZECH REPUBLIC

CZ supports the Presidency aim to develop a position of the Council in relation to GDPR. After consultations with various parts of industry and public administration, we wish to submit following initial suggestions:

General Observations

The GDPR ***contributed to the unification of personal data protection rules*** among Member States. While there indeed are opinions within the industry that the unification should go even further, CZ believes that national solutions, where allowed, such as age of online consent in Art. 8, stimulated domestic debate and led to greater national ownership of the GDPR. However, where the Regulation follows the political logic of national cultural specificities, rather than business logic of unification, it is crucial that business can determine with certainty what particular rule to apply.

The ***efforts of EDPB in providing clarifications are greatly appreciated*** despite certain cases where EDPB was needlessly prescriptive or imposed additional requirements [1] or where the necessity as an element of Art. 6 and 9 has been interpreted too strictly as a factual impossibility.

While certain observations indicate a room for improvement of the legal text, CZ is convinced that ***any possible future amendments should be considered carefully***, after taking into account practice in different Member States and after exhausting non-legislative solutions. Of course, all the observations, which are based on practice, should be treated seriously, because, due to the ***breadth of the definition of personal data***, these issues surpass specific examples and concern many areas of life.

Specific Observations

a. Private-sector controllers would, as stated above, really appreciate ***clarification of the territorial and personal scope of national adaptation legislation*** e.g. in the form of opinions[2] by European institutions on this question. Even though CZ had deliberately approached this issue in a very conservative manner and relies only on GDPR as such (e.g. recitals 25, 153, Art. 3(3) or Art. 55(2)), this issue gives rise to significant legal uncertainty in the context of the whole Union.

---

1 e.g. as regards dashcams in Guideline 3/2019 or portability requirements in former WP29 opinion.

2 probably drawing on Art. 4 of Directive 95/46.

b. The possibility of using certain modern techniques, such as ***biometric authentication, should be clarified and probably relaxed*** (in strictly justified cases, such as employees accessing strictly restricted areas). Current limitations of Art. 9(2) may lead either to security gaps or to over-reliance on hasty legislative solutions with generic safeguards, while properly made test under Art. 6(1)(f) could bring more appropriate protection.

c. A specific problem has emerged regarding processing of special categories of personal data within the context of a contract. For example, when an enterprise provides privileged services for persons with disabilities, it needs to rely on their consent with processing of their personal data concerning health. That makes the consent under Art. 9(1)(a) a condition to use a privileged service, which is open to challenge given the language of Art. 7(4) and strict position taken by WG29 Guidelines on Consent (wp259.rev01).

d. While the EDPB endeavours to include examples in its Guidelines, real cases of ***best practice could be published online*** for the benefit of other Member States (e.g. regarding conflict of interests of DPOs, professional qualifications for DPO, status of controller and processor, compliance with transparency obligations to data subjects where data has been obtained from public sources, additional identification pursuant to Art. 11 etc.); the same applies to cases of bad practice. This would improve practical implementation of the GDPR across the EU.

e. While the national lists under Art. 35(4)(5) are submitted to the EDPB, if the EDBP had the option ***to issue its own*** (even non-exhaustive) ***lists of processing operations subject to/exempted from impact assessmen***t applicable throughout the EU, it would contribute to much more uniform and consistent application of the GDPR.

f. Since the DPOs are a completely new element in most Member States, ***practical impact of DPOs and of their activities should be evaluated*** in more detail, taking into account various factors, such as whether the Member State requires certain qualifications, whether their position was uniformly specified (e.g. within public administration), what share of controllers employ DPOs, whether the designation of DPO led to better compliance or lower sanctions (if applicable) over time etc.

g. ***Outreach*** to both controllers, processors and the public ***should continue*** in many areas, in particular ***where the Regulation has brought new rules***, e.g. about the practical working of one-stop-shop and related cooperation between DPAs in cross-border cases.

h. More certainty (including coordination, clarification and less divergence in practice) regarding ***possibilities and limitations to use*** (further process) ***publicly available personal data*** (GDPR vs open data, sharing of public sector data) is essential for the success of digital single market.

DENMARK

The Danish Ministry of Justice would like to make the following contribution to the evaluation and review of the General Data Protection Regulation (GDPR):

In line with Germany's remark's at the DAPIX meeting on 3 September 2019, the Ministry of Justice would like to highlight the existence of the national margin of manoeuvre in e.g. Article 6 (2) and (3). According to recital 10 of the GDPR, the Regulation provides a margin of manoeuvre for Member States to specify its rules, including determining more precisely the conditions under which the processing of personal data is lawful.

In Denmark, we have numerous national rules concerning the legality of processing of personal data, which the GDPR gives us the possibility to maintain and introduce – precisely because this margin of manoeuvre was a result of the negotiations of the GDPR. According to Article 6 (3) these national rules may contain specific provisions on e.g. the general conditions governing the lawfulness of processing by the controller, the purpose limitation and storage periods. For example, the Danish Video Surveillance Act contains specific provisions on which types of private entities that lawfully may have video surveillance in public areas and the storage period.

GERMANY

I. Preliminary remark

Germany is pleased that the Council plans to prepare a position on the evaluation and review of the GDPR. Germany expressly approves of and supports the procedure presented by the Finnish Presidency to draw up such a Council position.

According to Article 97 (1) of the GDPR, the Commission must submit a report on the evaluation and review of the GDPR to the European Parliament and the Council by 25 May 2020. According to Article 97 (2) of the GDPR, in the context of this evaluation and review, the Commission must examine, in particular, the application and functioning of chapters V and VII. In Germany's view, this emphasis on the two chapters does not imply that the evaluation and review cannot focus on other regulatory objects of the GDPR as well.

The Council's position and the Commission's report should therefore also be able to contain certain other regulatory objects than those explicitly mentioned in Article 97 (2) GDPR.

Germany believes it is important that the Commission take into account in its evaluation the cumulative experience with the GDPR of all practitioners and stakeholders. This will help ensure that the evaluation is comprehensive. In this way, the Council position will ensure that the experience and concerns of the governments are taken into account as well. Further, the Commission should make use of the possibility explicitly provided in Article 97 (3) to request information from supervisory authorities.

However, Germany notes that in some cases, national law has not yet been fully amended in line with the GDPR. It should also be noted that the GDPR has applied only since May 2018.

Individual reviews of EU legislative proposals reveal that, in some of the Commission's drafts, references to the old Directive 95/46/EC have not yet been revised (e.g. in the Proposal for a COUNCIL REGULATION amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in order to combat VAT fraud, COM/2018/813 final). Sector-specific EU law must also be checked and brought into line with the GDPR to prevent the risk of conflicts and legal uncertainties.

II. General remarks on the application and interpretation of the GDPR

The GDPR's entry into application has further increased awareness in Germany of the issue of data protection. At the same time, despite the two-year phase for implementing and adapting to the GDPR following its entry into force, some businesses and government agencies have said they feel overwhelmed following the GDPR's entry into application. Some users have felt considerable uncertainty been very confused by what seem to be new instruments created by the GDPR (records of processing activities, data protection officers), even though they already existed under Germany's data protection law before the GDPR entered into application (e.g. directory of procedures).

Germany supports the approach already chosen by the Commission of encouraging uniform application of the GDPR by working closely with the data protection supervisory authorities, thereby seeking to further reduce uncertainty regarding the application of the GDPR. This is especially desirable with regard to the following:

- taking into account the special interests of children in the context of Article 6 (1) (f) GDPR;
- the issue of how voluntary consent can be if it is not possible to consent separately to different operations processing personal data;
- technical and organizational measures to ensure privacy by design and privacy by default (Article 25 GDPR);
- the requirements regarding security of processing (Article 32 GDPR);
- transparency and obligations to provide information pursuant to Article 12 ff. GDPR: there is no uniform practice for how information and notifications are to be transmitted in precise, transparent, understandable and easily accessible form, in clear and simple language, or whether discontinuities of media, such as reference to websites with privacy statements, are allowed;
- the right of access, for example, if data subjects do not wish to reveal the specific nature of their interaction with a government agency, then it is difficult or impossible to answer their request for information;

- in practice, the problem arises that companies are only able to provide information on data stored under the data subject's name, not under the IP address, advertising ID or device number, even if the data subject provides this information;
- the extent of the right to copies under Article 15 (3) GDPR is unclear, in particular whether the data subject may request underlying documents;
- there are no practical guides to the requirements for the erasure of data.
- pseudonymization and anonymization: criteria need to be developed for when personal data must be anonymized or pseudonymized and in which cases the pseudonymous use of certain services must be offered. Questions also arise regarding the limits to and definition of identifiability, de-anonymization, re-identification and pseudonymization. Some practitioners criticize the GDPR's lack of precise criteria, which they say leads to an uncertain legal situation;
- regarding the reporting of personal data breaches, in particular how the term "risk to the rights and freedoms of natural persons" is to be interpreted in this context.

Many businesses would also like faster and more concrete assistance from the data protection authorities. Data subjects would like more advice and faster processing of their requests. The Member States' data protection supervisory authorities should harmonize their practice of interpretation more closely (e.g. they have different lists of risky processing operations and privacy impact assessments), and uniform standards for weighing up must be found

Uncomplicated ways should be found to bring privacy-related court decisions in the individual Member States to the attention of courts and practitioners in other Member States in order to develop a uniform legal practice.

Comments from businesses and feedback during Federal Government events indicate that businesses are trying hard to implement the GDPR. They also point to stricter requirements concerning the rights of the data subject and documentation obligations (chapters III and IV of the GDPR). Small and medium-sized enterprises (SMEs) as well as associations and volunteers whose main activity is not processing personal data have called for simplifying these rules.

The Commission should examine whether experience so far with the GDPR's effectiveness has revealed any gaps which would make detailed or additional rules or clarification (possibly also additional sector-specific legislation) conceivable, in particular in the area of scoring and profiling and the use of artificial intelligence, or to enable private bodies to transfer data to law enforcement and security authorities.

III. Individual points

1. Article 6 (1) and Article 9 GDPR

The relationship and the application of the prerequisites for processing in Article 6 (1) GDPR (in particular processing on the basis of consent, for the performance of a contract and for the purpose of legitimate interests) and in Article 9 GDPR seem difficult to understand in practice. In addition, these provisions are applied differently in the Member States. Further guidance is needed for interpretation, for example to clarify the dogmatic relation of Article 6 to Article 9 GDPR, under which conditions lawfully collected data may be processed by the same processor under Article 6 (4) GDPR for a different purpose, also for special categories of data under Article 9 GDPR and according to which rules data processing may be based on a different legal provision after consent has been withdrawn.

2. Right to object to data processing by public bodies

Article 21 (1) GDPR grants data subjects a comprehensive right to object to data processing for the performance of a task carried out in the public interest (Article 6 (1) (e) GDPR). However, an exception often applies in such cases. Data subjects find this difficult to understand.

3. Specifying the requirements for data processing without consent

Legal authorization to process personal data must be sufficiently defined with regard to the conditions to be met. If such authorization, particularly in the private sector, is based on balancing legitimate interests, it is the responsibility of the processor to weigh up the different interests. This fundamental problem is already inherent in Article 6 (1) (f) GDPR. "Legitimate interests" may be interpreted very differently across Europe.

It is therefore necessary to consider issuing concrete sector-specific rules for certain data processing operations which ensure legal certainty and an appropriate balance with the fundamental rights affected.

4. Consent

Controllers should be provided with guidance for data processing based on consent and for shaping consent. This would better ensure than at present that the information necessary for informed consent is provided to the data subject in a structured way, and that the data subject can better understand the information with a reasonable amount of effort.

The Commission should quickly make use of the power granted it in Article 12 (8) GDPR to adopt delegated acts, develop procedures for providing standardized icons as referred to in Article 12 (7) GDPR and determine the information to which the icons correspond.

5. Privacy by design and by default

The effectiveness and operability of Article 25 GDPR should be further improved, for example by providing practical guides for interpreting the technical safeguards for data security and for privacy by default. Special attention should be paid to data processing involving special risks (such as artificial intelligence and platforms). Specific design requirements for such processing should be considered in order to manage the special risks effectively.

6. Limited scope of Article 30 (5) GDPR

Article 30 (5) GDPR is intended to reduce burdens on small and medium-sized enterprises, but it creates difficulties in interpretation. These difficulties mean that the provision is partly assumed to have only a very limited scope. Although Working Party 29 has already drafted a position paper on this matter, it would be useful to have written clarification in the text.

7. Reporting personal data breaches

The obligation to notify data supervisory authorities of personal data breaches and to document such breaches (Article 33 GDPR) has caused a great deal of uncertainty particularly among SMEs. The problem is that, according to Article 33 (1) GDPR, a simple risk to the rights and freedoms of natural persons is enough to trigger the obligation. By contrast, Article 34 GDPR refers to a "high risk" to the rights and freedoms of natural persons, and its paragraph 3 specifies exceptions which are not found in Article 33 GDPR.

According to media reports, by 30 April 2019 data protection supervisory authorities in Germany had received 22,756 reports of personal data breaches and those in the EU more than 89,000 such reports in accordance with Article 33 GDPR. Further research is needed, for example by sorting the reports according to topics, to determine the type and severity of personal data breaches reported.

These figures show that the threshold set in Article 33 for reporting personal data breaches is too low. Apart from that, the data protection authorities are most likely overwhelmed by the massive volume of reports. It is worth considering whether to limit the scope of Article 33 by bringing it into line with Article 34.

8. Information to be provided

Although the Data Protection Directive also required information to be provided, the obligation in Article 13 GDPR has caused concern among many micro enterprises in situations of daily, "analogue" life. In practice, the requirements of informed consent are often mixed up with the requirements arising from Article 13 GDPR.

Practical facilitation should be created for transactions in ordinary life, such as ordering merchandise in a (bricks-and-mortar) shop or presenting one's business card. Such facilitation could take the form of using standardized wording to meet the requirements of information to be provided.

9. Drafting sector-specific codes of conduct

Drafting sector-specific codes of conduct in accordance with Article 40 GDPR could be a suitable way to ensure the consistent application of the GDPR throughout the EU, in particular in areas of Member State competence such as the processing of health data.

A central list of codes of conduct currently being agreed with the supervisory authorities could help improve coordination and support for such projects. Instruments and measures to encourage the drafting of such codes of conduct should be increased and further developed.

10. Adequacy decisions pursuant to Article 45 GDPR

So far only 13 adequacy decisions have been taken, some of which are limited to certain sectors. A large number of data flows therefore has to be based on other instruments of Chapter V. This makes information-sharing among government agencies noticeably more difficult. One example is the recent adequacy decision concerning Japan: because it refers only to the business sector, it does not provide a basis for information-sharing among government agencies. The Commission must keep up its efforts to bring about additional adequacy decisions and to expand the existing ones to additional areas and sectors.

11. Difficulties in creating appropriate safeguards (Article 46 GDPR)

In accordance with Article 46 (2) (a) GDPR, Germany has drafted a standard data protection clause for concluding international treaties. This clause is intended to ensure that the requirement of appropriate safeguards is met when Germany concludes an international treaty, especially with regard to rights of the data subject which are effective, i.e. can be enforced in national law. Initial feedback during treaty negotiations shows that including such safeguards in international treaties can be difficult in practice (for example in the social security agreement with Canada). As a result, it is not always possible to agree as desired on sharing personal data, which is necessary from an expert perspective.

The GDPR needs to clarify the minimum standard needed for appropriate safeguards in the public sector. Meeting this standard must then be sufficient for data transfers to third countries. In a globalized world, the Member States are an integral part of the international community and are oriented on international cooperation. This also means that Member States must be able to work and share data with countries whose legal systems do not entirely agree with that of the EU (or even the Federal Republic). This must be taken into consideration when setting the minimum standard necessary for an appropriate level of protection.

The standard treaty clauses for data transfers to third countries developed under Directive 95/46/EC urgently need to be revised in line with the GDPR and with practical needs. We therefore ask the Commission to update the standard treaty clauses and draft additional standard text soon, for example to use when subcontractors are deployed in third countries.

12. Fines

Given the much higher limits for administrative fines, it would be desirable to define transparent criteria for the supervisory authorities to issue fines in order to ensure comparability and uniform enforcement.

ESTONIA

1. A clarification is needed on what is meant by „related security measures“ in art 10.

2. Art 27 establishes the institute of a representative of controller or processor not established in the Union. According to art 30(2) the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller. Under art 30(4) the controller's or the processor's representative, shall make the record available to the supervisory authority on request. It is not quite clear what are the supervisory authority’s options, if the representative does not fulfill these duties. Perhaps an explanation on this matter is needed.

3. Art 42: it is difficult to carry out a certification process in a small country like Estonia mainly due to high cost.

4. Art 64(3) sets out time limit (eight weeks plus six weeks) for adopting of the opinion of the European Data Protection Board. The time limit may prove insufficient due to the preparation and coordination process of the response of a member. Extension of these time limits should perhaps be considered.

5. A clarification of art 72(1) and (2) is needed in respect of „simple majority“ and „two-thirds majority“.

IRELAND

1. Ireland welcomes the Presidency's initiative and plan on preparation of a Council position on the evaluation and review of the GDPR and submits the following observations for inclusion in the Council report.

Data protection rights of children

2. While the GDPR states that "children merit specific protection with regard to their personal data", its approach to the protection of children is both fragmented and disjointed. References in various recitals (i.e. recitals 38, 58, 65, 71, 75) and Articles (i.e. 6.1(f), 8, 12, 40, 57) resemble a jigsaw puzzle but, unlike a completed jigsaw, they do not provide a coherent picture of protection for children.

3. Paragraph (f) of Article 6.1, which provides a legal basis for processing based on the 'legitimate interests' ground, contains a specific reference to the rights and freedoms of children ("… in particular where the data subject is a child"), but no indication of what that should mean in practice. The balancing exercise required under the 'legitimate interests' ground remains a matter, at least in the first instance, for the controller concerned. As the Court of Justice case law makes clear, more specific provisions in national law for the protection of children are not permitted.

4. During lengthy parliamentary debates on Ireland's Data Protection Bill, the GDPR's protection of children's personal data was criticised as fragmented and inadequate. The Ombudsman for Children and various advocacy bodies also expressed public concern about the GDPR's inadequate protection of children's personal data.

5. While the Commission's report under Article 97 may not provide an opportunity for reopening negotiations on the GDPR, the possibility of a more coherent, binding approach to the protection of children's data may yet be found in Article 40 (Codes of conduct). Paragraph 7 provides that where a draft code relates to processing activities in several Member States, the competent supervisory authority must submit the draft code to the consistency mechanism in Article 63, and the EDPB shall then provide an opinion on whether the draft code complies with the GDPR. Where it deems the draft code compliant, it must submit its opinion to the Commission and the Commission then has the possibility to decide, by way of implementing act, that such an approved code of conduct has general validity within the EU.

6. Ireland considers that such a code of conduct under Article 40 has the potential to enhance the data protection rights of children across the Union, and to ensure a more coherent approach to the processing of children's personal data. Such an outcome would be entirely in accordance with the content of recital 38.

Applicable law

7. The manner in which Article 8 provides for varying ages of consent between 13 years and 16 years has given rise to legal uncertainty concerning the applicable law within Member States. It has not only contributed to a fragmented digital market in the Union, but has resulted in a lack of transparency and legal certainty. Unlike recital 153, which, in the case of freedom of expression, specifies that the law of the controller shall apply, there is no specific 'connecting factor' in the case of Article 8. This is clearly unsatisfactory. It would be helpful if the Article 97 report could provide up-to-date information on the situation resulting from the manner in which Member States have implemented Article 8.

Safeguards, including effective judicial remedy and due process

8. Recital 148 states that "[T]he imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process." Article 58.4 provides that the exercise of the powers conferred on supervisory authority powers shall be subject to appropriate safeguards, including effective judicial remedy and due process. Article 83.8 requires appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. The Commission's recent Communication ("Data protection rules as a trust enabler in the EU and beyond – taking stock") contains a welcome recognition of the need for the data protection authorities to "gather relevant evidence, respect all procedural steps under national legislation and ensure due process in often complex files." And as the Communication acknowledges, this requires time and involves a significant amount of work, which explains why many of the investigations are ongoing.

10. When it comes to dispute resolution by the European Data Protection Board under Article 65, there is no specific reference to safeguards and due process standards. Greater clarity on the applicable safeguards and due process standards within the Board's decision-making processes, would not only improve transparency but also legal certainty.

Representatives of controllers and processors not established in the Union

11. Article 27 requires controllers and processors falling under Article 3.2 to designate a representative in the Union. Such a representative must be mandated by the controller or processor concerned to deal with the supervisory authorities and data subjects on all issues relating to processing for the purposes of ensuring compliance with the GDPR.

12. This is an important GDPR requirement, designed to ensure adequate redress for data subjects and to avoid any undue competitive advantage for controllers and processors that are not established in the Union but offer their goods or services to data subjects, or monitor their behaviour, in the Union. It would be helpful if the Article 97 report could provide up-to-date information on the current situation regarding the designation of representatives under Article 27.

FRANCE

The French authorities would like to highlight the following points for consideration which could usefully be referred to in the Council's position on the application of the GDPR:

Transfer of personal data outside the Union

- **Adequacy decisions**

The first adequacy decision adopted under the GDPR, in relation to Japan, is both an encouraging sign in terms of the Union's ability to maintain the necessary data exchange between the European Union and its external partners, and a precedent that should be used to adjust practice for subsequent decisions.

Fundamentally, adopting adequacy decisions which not only evaluate the legislation of the third country concerned but also take into account additional rules specific to transfers between the EU and these third countries is an ingenious solution, but nonetheless should not be considered as a precedent for future adequacy decisions.

The principle underlying these instruments is to recognise the existing legal framework of the third country rather than negotiate an additional framework. The binding force which practitioners recognise these additional rules as possessing will have to be closely monitored in the context of the implementation of the adequacy decision. Similarly, the existence of a precise and effective mechanism for monitoring these rules, in particular in regard to subsequent transfers of the European data transmitted, must be a *sine qua non* for the adoption of an adequacy decision, and must be regularly assessed by the European authorities.

As regards the procedure for the adoption of these decisions, the principle of sincere cooperation requires that, given the major challenges associated with data transfer in our digital economies, the relevant documents are sent to all stakeholders sufficiently in advance to allow for informed and useful discussions, so that they are fully involved in the preparation of adequacy decisions before they are finally adopted. In this respect, the role of the European Data Protection Board must, under the conditions set out in the GDPR, be fully ensured so that the EU's internal and external legislative work on data protection has the full benefit of its expertise and its independence.

- **Codes of conduct and, more generally, new accountability tools put in place by the GDPR (e.g. certification, Data Protection Officer)**

In our view, promoting these tools, which organise the transfer of data outside the EU (Article 46(2)(e) and (f)) and compliance by controllers and processors, is essential to ensure that they are developed and widely adopted, so as to contribute to the proper application of the GDPR.

For example, in July 2019, the French data protection authority (Commission nationale de l'informatique et des libertés – CNIL) issued its first approval concerning the powers of the Data Protection Officer.

- **Choice of criterion to determine the legislation applicable between Member States in the event of divergences when they have made different choices within the discretion allowed by the GDPR (criterion of the residence or establishment of the controller)**

We would point out that recital 14 of the GDPR states: *'The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.'*

For instance, the GDPR allows some discretion as regards genetic data, biometric data and data concerning health (Article 9(4)). Consequently, we are uncertain as to which law is to apply to a European or an American company. This could also result in a lead supervisory authority under the one-stop-shop mechanism deciding on another Member State's law if a case is referred to it concerning a resident of another Member State[3]. It would be helpful for the supervisory authorities to draw up guidelines on the subject.

---

[3] In France, the criterion of the person's residence has been chosen, except for processing covered by Article 85(2) of the GDPR. Article 3 of the Law on Information Technology and Freedoms: '[...] II. *The national rules adopted on the basis of the provisions of the Regulation which leave it to national law to adapt or supplement the rights and obligations provided for by the Regulation shall apply if the data subject is resident in France, including in cases where the controller is not established in France. However, where one of the processing operations referred to in Article 85(2) of the Regulation is involved, the national rules referred to in the first subparagraph of paragraph II shall be those to which the controller is subject, if the controller is established in the European Union*.'

In addition, the difficulties are not solely connected with the GDPR since in some fields, such as the implementation of health research, other specific national legal frameworks also have to be complied with. For instance, the hosting of health data collected when providing healthcare must be entrusted to an approved or certified hosting service provider, in accordance with the provisions of the French Public Health Code.

- **Processing for archiving purposes in the public interest - Article 89 of the GDPR and the issue of private archives of public interest**

Article 89(1) of the Regulation stipulates the need for appropriate safeguards for the rights and freedoms of the data subject when processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Article 89(2) deals more specifically with processing for scientific or historical research purposes or statistical purposes, while Article 89(3) only concerns processing for archiving purposes in the public interest. Article 89(4) provides that the derogations are to apply only to processing for these specific purposes.

As regards processing for archiving purposes in the public interest, Article 89(3) provides that national law may provide for derogations from the rights of the data subject (right of access, right to rectification, right to object, etc.), in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes. This derogation regime is applicable where processing is carried out owing to a legal or regulatory obligation (recital 158), regardless of whether the data controller is a public authority or a public or private organisation.

Some private archives may be considered of public interest under national law, but do not result from a legal obligation (e.g. the archives of churches, political parties, or foundations, such as the archives of the Shoah Memorial). Consequently, they are not covered by the derogation regime which applies to archives. Since the application of the derogation regime has been made conditional on the existence of a legal obligation, we wonder if this regime is not excessively strict, at the risk of excluding some actors?

- **Among the subjects listed in Article 97 of the GDPR, that of the supervisory authorities and the exercise of their powers is essential.**

Given that supervisory authorities are key players in the implementation of the provisions of the GDPR and guarantors of its effective application, we consider that any substantial developments in the report should relate to those authorities' exercise of powers and in particular the implementation of Chapter VII of the GDPR on cooperation and consistency.

In this regard, we propose that it be highlighted that while the arrangements for cooperation must necessarily be put in place gradually and be adapted as supervisory authorities' practices in this area adapt, there are two points which already require attention in this first evaluation:

- On a technical level, the information system made available to data protection authorities (the Internal Market Information System – IMI) is still not very user-friendly or well-adapted to the cooperation procedures provided for by the GDPR. A better-adapted tool should be considered in order to enable smoother exchanges and better interaction with internal monitoring tools.

- On a procedural level, national disparities which hinder cooperation for supervisory authorities should be examined and removed. In particular, national procedural rules which seek to avoid decisions of supervisory authorities being subject to the cooperation mechanism and the one-stop-shop mechanism should be removed (for example, amicable resolution procedures which result in no formal decision being taken by the authorities and the plaintiff's authority thus never being consulted within the framework of one-stop-shop procedures).
  The role of the European Data Protection Board, which acts with complete independence in exercising its prerogatives and is a driving force in the implementation and promotion of the GDPR, should also be highlighted.

The role of the European Data Protection Board, which acts with complete independence in exercising its prerogatives and is a driving force in the implementation and promotion of the GDPR, should also be highlighted.

Finally, we would like to make the following comments in response to remarks made by some Member States:

- **Child's consent (Article 8 of the GDPR)**

We wish to point out that the discretion left to Member States regarding the age of consent of minors is likely to cause implementation difficulties. Reflections and discussions on this issue should therefore continue in order to come up with imaginative solutions. Were exploratory work to take place at a later stage aimed at assessing whether the GDPR should be revised, this issue should be a priority.

- NL/DE: the derogations from the obligation to keep records of processing for SMEs should be extended (Article 30(5) of the GDPR).

We consider that the decision made during the negotiations to opt for an approach based on the risk associated with controllers, rather than their size, was justified and that further derogations are not necessary. Nevertheless, given some small organisations' need for support and simplification, some supervisory authorities (including the CNIL) have developed specific tools ('simplified' records, awareness-raising guides for micro-enterprises and SMEs and local authorities) to facilitate compliance with the GDPR.

- **Provisions on scientific research**

We note that there are many derogations relating to scientific research and that they do not always fit in easily with the text's other provisions. The very concept of research is also difficult to grasp and raises real practical difficulties. Furthermore, those difficulties are compounded in the field of health research by the fact that there are two sets of circumstances in which discretion can be exercised – those listed in Article 9(4) and those listed in Article 89. Further work on clarifying the principles of this point would certainly be useful.

- BE: What solutions have been adopted by the other Member States regarding data processing by the courts (incorporation or not of provisions into codes of procedure)?

We would point out that the Regulation allows courts to create a specific data processing system (recital 20). Where there is more than one national data protection authority (allowed by recital 117), cooperation between them should be considered (recital 119 and Article 51).

France has chosen not to amend existing law (Code of Administrative Justice, Code on the Organisation of the Judiciary, Code of Criminal Procedure) and to make the courts subject to a supervisory authority as part of its judicial functions[4]. The provisions of the GDPR and the Law on Information Technology and Freedoms[5] are applicable to the courts for processing carried out by them which does not fall within the scope of Directive (EU) 2016/80.

- PL pointed out a problem regarding the interpretation of the concept of national security, in Article 2, and the absence of a legal basis for processing when the data subject himself or herself makes the data public, in Article 6.

We consider that no particular position was taken on this subject during the negotiations and do not see any real problem with the wording of Article 2. Regarding Article 6, we do not fully comprehend the scope of Poland's observations.

---

[4] *If this were not the case, this power could have been given to, for example, the Permanent Mission for the Inspection of Administrative Courts (MIJA), which deals with administrative justice. This authority would not have had the power to impose sanctions but merely an advisory role.*

[5] *Article 48 of the Law on Information Technology and Freedoms on profiling.*

CROATIA

1) Information Member States would like to share on the use of adequacy decisions by their stakeholders and/or relevant developments in countries or territories benefiting from a Commission's adequacy decision.

The decision on the adequacy of the personal data protection level is a decision of the European Commission establishing that a third country provides a comparable level of protection of personal data to that in the European Union, through its domestic law or its international commitments. As a result, personal data can flow safely from the European Economic Area (EEA - the 28 EU Member States, as well as Norway, Liechtenstein and Iceland) to that third country, without being subject to any further safeguards or authorisations. Thus, each decision applies to all transfers of personal data from the EEA to business entities in a third country, thereby, increasing, among other things, the advantages of mutual economic cooperation between the EEA and third countries by respecting the fundamental right of each individual to protection with regard to the processing of personal data, in accordance with Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union (UFEU).

2) Information concerning the independence and resources of the Data Protection Authorities (DPAs). This includes notably their capacity to exercise their powers provided by the GDPR and to comply with their obligations in the context the cooperation and consistency mechanisms.

The Act on the implementation of the General Data Protection Regulation (Official Gazette No 42/18) entered into force in the Republic of Croatia on 25 May 2018 with regard to Chapter VI, Section 1 of the General Data Protection Regulation concerning the independent status of the supervisory authority. Article 4 of the above Act on the Implementation of the General Data Protection Regulation prescribes that Personal Data Protection Agency is the supervisory authority within the meaning of the provision of Article 51 of the General Data Protection Regulation as the independent state authority autonomous and independent in its work and responsible to the Croatian Parliament. Furthermore, Title III of the said Act prescribes provisions relating to Agency management, the conditions for the appointment and dismissal of directors and deputy directors, expert service of the Agency, etc.

An exhaustive list of investigative, corrective and advisory powers of the national supervisory authorities is provided in Article 58 of the GDPR. In addition, pursuant to paragraphs 5 and 6 of the said Article, the Act on the implementation of the General Data Protection Regulation lays down the powers of the Agency, pursuant to which it can inform the judicial authorities about the infringements of this Regulation, and, where necessary, institute judicial procedures or otherwise participate in them in order to implement the provisions of this Regulation and additional powers arising from the application of the provisions of the national Act itself.

The Act on the implementation of the General Data Protection Regulation also lays down, among other things, cooperation with supervisory authorities for data protection in other countries with regard to the actions taken by the Agency as the competent authority for personal data protection in a mutual assistance procedure pursuant to Article 61 of the General Data Protection Regulation.

With regard to the Agency resources, the Act on the Implementation of the General Data Protection Regulation lays down that the resources available to the Agency are provided under the state budget of the Republic of Croatia. In line with the aforementioned and with the aim of ensuring efficient implementation of the legislation concerning personal data protection, in 2018 the Agency was granted HRK 6,570,802.00 under the state budget. On 23 May 2018, reallocation of the funds under the 2018 state budget of the Republic of Croatia was granted, and accordingly HRK 6,790,802.00 was made available to the Agency. In the given period, the Agency applied the principles of rational distribution of the granted funds taking into account the legal limitations in expenditures and it used a total of HRK 6,975,968.50, that is, 105.13% of the planned and granted amount of the Agency budget for 2018. For comparison, in 2016 the Agency used HRK 5,333,329 from the total budget planned, and in 2017 HRK 5,939,418.

3) Information which would allow to verify the effectiveness of the coherent interpretation and application of the GDPR throughout the EU by the cooperation and consistency mechanism provided by the GDPR.

Pursuant to the provisions of Article 68 of the General Data Protection Regulation, the European Data Protection Board (EDPB) was established as a Union body with legal personality. The EDPB is composed of heads of one supervisory authority from each Member State and the European Data Protection Supervisor, or their representatives. The role of the EDPB is to promote cooperation and efficient exchange of information and best practices among the Member States' national supervisory authorities, as well as to ensure the consistent application of the GDPR. The specific tasks of the EDPB are laid down in Article 70 of the GDPR. An IT platform was established as the operational basis of cooperation for providing support to Member States in cooperation and ensuring the consistency in the application of the GDPR (IMI - Internal Market Information System), which has been functioning from day one of the full application of the Regulation.

In accordance with its tasks, the EDPB has so far issued a great number of guidelines, recommendations and examples of best practice (available on the following link: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en), as well as opinions (available on the following link: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en).

In addition, we would like to point to the fact that the EDPB submitted a report in February this year to the Civil Liberties, Justice and Home Affairs Committee - LIBE of the European Parliament on the implementation of the GDPR, which is available on the following link: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-libe-report-implementation-gdpr_en. The said report contains data on financial and human resources, as well as statistical data on the number and type of cases based on the data provided by supervisory authorities from 31 countries of the European Economic Area (EEA) by the time of the submission of the report.

LATVIA

1) Information Member States would like to share on the use of adequacy decisions by their stakeholders and/or relevant developments in countries or territories benefiting from a Commission's adequacy decision.

2) Information concerning the independence and resources of the Data Protection Authorities (DPAs). This includes notably their capacity to exercise their powers provided by the GDPR and to comply with their obligations in the context the cooperation and consistency mechanisms;

3) Information which would allow to verify the effectiveness of the coherent interpretation and application of the GDPR throughout the EU by the cooperation and consistency mechanism provided by the GDPR.

In view of the foregoing, we give the following answers.

Regarding the first question, Latvia is not aware of any troubling or worrisome developments in country's that are subject to a European Commission adequacy decision, beside from publicly available information (including ongoing court proceedings regarding US privacy shield).

Regarding the second question, Personal data processing law Article 3 part 1 states that the Data State Inspectorate (hereafter – Inspectorate) is an institution of direct administration under the supervision of the Cabinet of Ministers, Article 3 part 3 states that the Inspectorate shall be independent in the operation thereof – such legal framework ensures the independence in the decision making process of the Inspectorate in the operations of the Inspectorate.

Recent developments are positive in the regard of increase of the capacity of the Inspectorate – changes in legal acts on salary of public servants allow for the employees of the Inspectorate to receive more competitive salaries also during next years budget negotiations the Inspectorate has received a first budget increase since 2016.

Regarding the third question, Inspectorate actively participates in the work of the European Data Protection Board (main tasks of which in accordance with the GDPR Article 70 (1) is to ensure consistent application of the GDPR), both by applying the guidelines drafted, by the expert subgroups of the European Data Protection Board and also by taking into account opinions provided by the European Data Protection Board (for example opinion by the European Data Protection Board regarding Latvian proposed list of fields where data protection impact assessment is mandatory).

Cooperation between supervisory authorities has ensured a more effective review of complaints in cross border cases, both in terms of investigating a complaint and also when enforcing corrective measures. There have been several complaints by data subjects that have been resolved successfully by cooperating between Latvian and Lithuanian supervisory authorities.

So far relevant stakeholders have not indicated that the application of the GDPR by the Inspectorate would differ significantly from interpretations and approaches used by other Supervisory authorities. Where such discussions would arise the tools for ensuring consistency are in place and there is no reason to doubt the capability of the European Data Protection Board to ensure a consistent approach.

In conclusion, we would like to agree that it is only less than a year since the GDPR was applied. At this time, we are unable to highlight a specific issue for which we cannot find a solution. Greater experience in applying the GDPR will improve the quality of data protection awareness and enforcement.

LITHUANIA

Thank you for the opportunity to submit our observations concerning practical application of the General Data Protection Regulation (hereafter – Regulation) and for the information regarding the aspects related to Article 97 of the Regulation.

More than a year has passed since the Regulation came into force. It was a period of big change for many – people, business, the public sector. The application of the Regulation actually has only started gaining momentum, it is still an ongoing process within companies to adapt to its requirements; supervisory authorities have just started making use of the wider powers provided for in the Regulation; the first cases concerning decisions taken by the supervisory authorities start reaching national courts. We therefore consider that the revision of the Regulation and the evaluation of the provisions at this stage are still too early.

Below is the information specified in the document 11292/19.

1) We are not able to provide any detailed information answering the first question, because in practice there have been no situations where there would be an examination of the transfer of personal data by the controller or processor to third countries using the Commission's adequacy decision.

2) Lithuania has designated two supervisory authorities - State Data Protection Inspectorate and Inspector of Journalist Ethics (when personal data are processed for journalistic purposes and the purposes of academic, artistic or literary expression). These institutions are independent in the performance of their functions and in the decision making, and their independence is guaranteed by law.

State Data Protection Inspectorate has the human, technical and financial resources, facilities and infrastructure needed to carry out its tasks and execute its powers. Funding for this institution has increased by almost 54% since 2017.

However, the more important role of supervisory authorities and their increased workload, due, among other things, to cooperation and consistency mechanism, require more and more resources, so the need to seek for resources to strengthen their functioning remains.

3) Here are the remarks on some of the provisions of the Regulation.

1. Pursuant Article 28 (8), supervisory authority may adopt standard contractual clauses in accordance with the consistency mechanism. These standard contractual clauses must be submitted to the Board prior to approval. However, recital 81 of the preamble states that standard contractual clauses may be adopted by the supervisory authority only after approval by the European Commission. In our view, the situation where the European Commission's power to approve standard terms and conditions adopted by the supervisory authority is referred only to in the preamble and not in a specific Article, creates legal uncertainty as to the mandatory nature of such procedure. It is worth considering whether the aforementioned powers of the European Commission should not be explicitly enshrined in Article 28 (8) of the Regulation.

2. Issues of practical application of Article 60 of the Regulation arise when supervisory authority with which the complaint was lodged adopts a decision where a complaint is dismissed or rejected on the basis of the findings of the lead supervisory authority and the complainant appeals against that decision to the national court, which in turn declares the rejection unfounded. There are doubts as to whether such a judgment is binding on the lead supervisory authority in another jurisdiction.

3. On the right of access by the data subject

3.1. In practice, data controllers have questions about the period for which the data subjects must be familiar with certain personal data, e.g. information about the data recipients to whom the personal data have been disclosed (Article 15 (1), point c). Before the entry into force of the Regulation, national law provided for a period of at least one year.

3.2. There are doubts about the proportionality of the right of the data subject to obtain a copy of the personal data, as set out in Article 15 (3) of the Regulation. In our view Article 15 (3) of the Regulation could be amended to provide that a data subject should only receive a copy of their personal data if they so request. Data subjects often do not need a copy of their personal data but they receive it automatically, which increases the administrative burden on data controllers.

LUXEMBOURG

Luxembourg's observations on the experiences obtained from the application of the GDPR

The Presidency invited the delegations, in its document dated on 18th July (11292/19) and at the WP DAPIX on 3rd September, to send written observations on the experiences obtained from the application of the GDPR.

Luxembourg takes note of the Contribution from the Multistakeholder Expert Group to the stock-taking exercise of June 2019 on one year of GDPR application and of the European Commission's Communication on data protection rules as a trust-enabler in the EU and beyond – taking stock (COM(2019)374).

Luxembourg firmly believes in the necessity of a high level of protection of personal data and that the GDPR is an important instrument and milestone which contributes to the European Union's outreach both to protect this fundamental right and to foster trust-enabling innovation.

At national level, the adoption of the Act of 1 August 2018 on the organisation of the National Data Protection Commission ("CNPD") and the general data protection framework accompanied the application of GDPR. Our independent Data Protection Authority was reinforced, in line with the new competence, tasks and powers attributed by the GDPR: between 2017 and 2018, its budget has increased (+85%) and so has its staff volume (+55%). These changes were necessary to cope, in particular, with the increased number of written queries (+110%) and of claims (+125%) in 2018.

The Eurobarometer survey on GDPR released in March this year shows that 44% of respondents in Luxembourg know what the GDPR is, which is 8 points above the EU28 average. This is the fruit of a strong commitment to raise awareness on the new data protection regime, which continues at national level.

At this stage, we consider that efforts are ongoing both from private and public sectors to reach the full potential of the GDPR and that it is rather early to draw conclusions for a potential review of this instrument, including on the transfer of personal data to third countries or international organisations and on cooperation and consistency mechanisms.

THE NETHERLANDS

1. Introduction

The Netherlands supports the aim of the DAPIX working party to prepare a Council position on the evaluation of the GDPR and approves of the procedure presented by the Finnish Presidency to draw up such a Council position. The Netherlands would like to emphasize that, in our view, the evaluation to be conducted by the Commission shouldn't be limited to the two topics mentioned in Article 97 (2) of the GDPR. A broad review is necessary. A broad review not only helps to ensure that the review is comprehensive, but is, in the view of the Netherlands, also necessary in light of the ever evolving developments in information technology and information society.

Technology never stands still. While the Netherlands acknowledges that the GDPR has only been applicable for a relatively short time, we believe that in this short time span already several developments in information technology and information society have become visible that could propose a future challenge to the GDPR. We have the following developments in mind, which we will address in the next paragraphs:

- The data power of a number of large tech companies (§ 2.1);
- Big data analysis and profiling (§ 2.2);
- Profiling and price discrimination (§ 2.3);
- Blockchain applications (§ 2.4).

If the EU waits for these developments to fully materialize, before amending the GDPR to take these developments into account, the Netherlands believes there is a risk that the proverbial genie will be out of the bottle and these amendment will turn out to be too little, too late. We therefore believe it is important that we start discussing these (admittedly: complex) developments and phenomena rather sooner than later. The first evaluation of the GDPR provides a good opportunity to take stock of these potential future challenges to the GDPR, and to start the discussion about possible ways to meet these challenges.

Apart from these broader developments in information technology and society, the Netherlands believes we should take the opportunity provided by the first evaluation of the GDPR to tackle some issues related to specific GDPR-provisions:

- Consistency of other directives and regulations with the GDPR (§ 3.1)
- Article 8: age of consent (§ 3.2);
- Article 30 (5): records of processing activities and the derogation for SME's (§ 3.3);
- Article 42: certification (§ 3.4);
- Article 41: the monitoring of approved codes of conduct (§ 3.5)
- Some other instances of ambiguous language in the GDPR-text and the need for more guidance (§ 3.6);
- Practicalities (§ 3.7);
- Technicalities (§ 3.8).

These issues currently lead to a lively discussion in the Dutch parliament and in Dutch society. In our estimation the resolution of these issues will, generally speaking, be more easy than the resolution of the aforementioned issues related to developments in information technology and information society. At the same time, the solution of these problems could, in our view, do a lot for the (continued) acceptance and legitimacy of the GDPR in our society. Solving these problems can therefore be regarded as an opportunity for a 'quick win'.

The European Commission has asked the Member States to provide information on the use of adequacy findings, concerning the independence and resources of our DPA, and information which could shine a light on the effectiveness of the cooperation and consistency mechanism provided by the GDPR. These questions will be addressed in paragraph 4.

2. Developments in information technology and in the information society

2.1 The data power of a number of large tech companies

One of the biggest privacy issues, in the view of the Dutch government, concerns the enormous power of big tech companies ('big tech') and the massive amounts of personal data they collect on their customers, even if they operate fully within the boundaries set by the GDPR.

Consequently we are happy to see that the Commission made a connection between the processing of personal data and competition law in it's Commission Communication of July 29th of this year. The Dutch government welcomes that the Commission will follow and foster cooperation between competition, consumer and data protection authorities. However, we believe the Commission should take one step further and consider a modernization of European competition law to better adapt the rules to the challenges of the digital economy.

Notwithstanding any potential efforts in the area of competition law, the Netherlands believes that the GDPR should also be evaluated in light of the data power of large tech companies. Just like the Commission intends to look at the cooperation between data protection, consumer and competition authorities, the Netherlands thinks that we should evaluate all these areas of law in light of the data power of big tech. Solely focusing on one area of law will not be sufficient to tackle the problems that come with the enormous data power of big tech.

This dual approach is preferable because these areas of the law all take a different perspective. Where competition law mostly focuses on market power from a top-down perspective, data protection law takes a bottom-up approach that aims to give individuals control over their personal data. Where competition law aims to prohibit abuse of a dominant market position (potentially based on the possession of data), data protection law should facilitate that individuals have or take control over their personal data and are in the position to determine where they want to store their data and under which conditions, thereby limiting data power of big tech.

In addition, competition law and consumer law contain norms that can be interpreted based on data protection law. Exemplary for this is the recent case of the *Bundeskartellambt* in which Facebook's violation of European data protection rules was at the heart of the ruling in which Facebook was found guilty of 'exploitative abuse' of its consumers. The company abused its dominant position by combining data of all sorts of third-party sources with Facebook profiles thereby creating very detailed profiles of its users. This complementarity could also apply to consumer law norms such as 'misleading commercial practices': misinforming consumers about the use of personal data can constitute a breach of consumer law. The complementarity between these areas of law demonstrates why it is important to evaluate whether data protection provisions are sufficient. Solely focusing on competition or consumer law will not suffice because possibly opportunities will be missed.

Consequently the Netherlands believes that the European Commission should consider evaluating whether the GDPR is sufficiently equipped to provide individuals with control over their data, specifically regarding big tech companies. We have identified a number of points that could be taken into account in this evaluation:

1. First of all, we would like to evaluate whether the right to data portability in Article 20 works well enough for individuals in practice. We have received multiple signals that the scope of the Article is quite narrow. For example we see that there are certain situations in which it is problematic that this right only refers to data that 'he or she' provided. In certain cases it might be necessary to be able to transfer personal data that others provided about you, for example when it concerns a review of you or your work, especially when these reviews are aggregated into certain 'scores'. Another example is that people continue to make use of certain digital services (e.g. social media) even though they do not like the data sharing policies of the service. They might consider transferring to another service, but this would mean losing all data that they did not 'provide', as for example their connections on a social media platform, which means that these people are 'locked-in' with the particular digital service. We therefore propose to evaluate whether Article 20 (1) properly equips citizens with the ability to control their data.

2. Secondly, and also relating to the right to data portability, Article 20 (2) mentions that the right can only be invoked where transmission is 'technically feasible'. We would like to evaluate whether this wording doesn't hinder effectuation of the right in practice and whether companies are doing work on creating formats to support the effectuation of data portability.

3. Thirdly, we believe that it could be very useful to evaluate whether the tools of the Data Protection Authorities are effective enough to oversee and efficiently address the processing activities of companies that process very large amounts of data. More specifically, we need to evaluate whether it is necessary to introduce specific sanctions for when these companies breach the GDPR multiple times. A possible option could be to introduce the possibility for DPA's to station someone within the company – or even in the board of directors – for a given period of time, to internally oversee the processing activities of the company. Such a competence could be modelled after Articles 28 and 29 of Directive 2014/59/EU which deals with recovery and resolution of credit institutions and investment funds. These Articles grant authorities the ability to (temporarily) replace senior management with a temporary administrator. It would be very interesting to see whether, and under what conditions, such a competence should also be introduced for DPA's.

2.2 Big data analysis and profiling

The Netherlands believes that it is necessary to further regulate Big-data analysis, in particular profiling. Recently we have introduced new guidelines for big-data analysis by government or government agencies. The rules aim at increasing the transparency and improving the quality of algorithms and profiling(methods) and outcomes; crucially the quality measures aim to ensure the avoidance or suppression of discriminatory effects. After using the guidelines in practice, we will evaluate whether we can convert (a number of) them into legal guarantees. Ideally, the Netherlands would introduce similar legal guarantees for profiling by non-government entities. However, we foresee that such guarantees would undermine the European level-playing field. Therefore we would like the European Commission to evaluate whether European guidelines for data-analysis by non-government entities could be introduced at a European level.

Furthermore we think that in order to mitigate unintentional and undesirable effects of data analysis it might actually be necessary to process relevant sensitive data, in order to develop profiling methods that correct parts/elements in the profiling model or datasets that can lead to prejudices or other irregularities. Such derogation for the processing of sensitive data only in relation to the development or auditing of profiling techniques (or automated individual decision making including profiling) could be added to the other exceptions in Article 9 GDPR. This of course only in a strict research setting and if strict safeguards and conditions are met. For that reason we would like to evaluate whether such a provision could and should be added to the GDPR to enhance the justified application of certain AI.

2.3 Profiling: price discrimination

A specific form of profiling that is currently under close scrutiny of the Dutch government, is the use of algorithms in order to personalize offers for goods and services. Companies can use personal data of subjects in order to profile them and personalize offers to their digital profile.

This might manifest itself in multiple ways. The most straightforward example is that prices can be personalized, but another scenario is that companies will install extra barriers for an individual to buy a certain good or to obtain certain services, for example by asking more detailed financial information before offering someone an insurance policy. Another form in which this might manifest itself, is that people are completely ruled out from buying certain products, simply because it is more interesting or profitable for companies to only offer their services to certain categories of people. For the sake of clarity, we would like to classify all these forms of discrimination under the umbrella term 'offer discrimination'.

The Dutch government has been conducting research into the legal framework regarding this phenomenon. Since algorithms almost always make use of personal data, this would, in our preliminary view, mean that companies have to ask for explicit consent before using data to apply any form of offer discrimination or even when they compile different profiles using personal data in the first place. Furthermore, in Dutch law it is prohibited to discriminate on a limited number of grounds, such as race, gender or sexual preference. One could therefore argue that individuals are already fairly well protected against offer discrimination and that companies are otherwise free to contract with whomever they want under the conditions that the two parties agree upon.

Nevertheless we also observed that there are situations in which offer discrimination is legal, but in which it will lead to unjust and stigmatizing consequences, especially in the long term. This would especially be the case when offer discrimination is being applied because someone is put into a certain profile, instead of an offer being personalized based on for instance the individual's own actions in the past or factual characteristics. Even though offer discrimination techniques are not yet being applied on a large scale, the Dutch government wants to prevent the use of these techniques to the extent that they will lead to these unwanted consequences.

The Netherlands is therefore looking for a balanced approach to this phenomenon in which the freedom to contract is guaranteed as much as possible and the advantages of algorithms to determine prices can be used as well, but which also prevents that people suffer from forms of offer discrimination that are unwanted and can be stigmatizing for certain groups over a long period of time.

Interestingly enough, the concept text of the new Directive on the modernization of consumer law (which still has to be formally adopted according to our information) contains a provision that introduces the obligation for companies to be transparent about the fact that they have personalized a price. We believe that the evaluation of the GDPR should consider introducing a similar transparency provision for when personal data is used for profiling in order to adjust offers to individuals, but this provision should also give data subjects insight into which aspects of their profile were decisive in the personalization of their offer. By taking an approach that relies on an enhanced transparency obligation, we would provide citizens with the necessary control to determine what forms of profiling are unwanted and which are considered to be socially acceptable.

In conclusion, the Netherlands would like the Commission to evaluate whether the GDPR properly equips European citizens with the necessary protection against offer discrimination and whether an enhanced transparency obligation would enable citizens to exercise more control over corporate profiling activities to personalize offers. Explicit consent for profiling that leads to offer discrimination can in our view only be meaningful (informed) if the information requirement for profiling also contains the obligation to be transparent about which factors have determined the content of the offer in question.

2.4 Blockchain applications

The Netherlands is critically following the use of blockchain technology, in particular when it comes to the relation of blockchain applications with the GPDR. The Netherlands believes that blockchain applications should be assessed on a case-by-case basis, thereby taking into account all characteristics of the specific use case and specifically the way in which personal data is used and stored.

Although compliance with GDPR should be assessed on a case-by-case basis, we do want to remark that the nature of blockchains may make it very difficult for data subjects to exercise certain rights, for instance the right to erasure or – until a lesser extent – the right to rectification. Moreover we foresee that it might be very difficult to identify a controller in blockchains, (especially in public permissionless blockchains) who is actually capable, alone or together with other controllers, to do what is necessary to fulfill all the obligations of the GDPR.

The Netherlands believes that it is necessary to clarify how certain GDPR principles and rights, as for example the ones mentioned above, are to be interpreted in light of blockchain applications. We are therefore eagerly awaiting more guidance on blockchain applications by the European Data Protection Board.

Nevertheless, we do not rule out that there is a insurmountable tension between the system of the GDPR and the nature of so-called 'permissionless' blockchains that can hardly be resolved by interpreting the norms and principles in the GDPR. Even though the GDPR is intended to be technologically neutral and is formulated accordingly, distributed ledger technology might need to be regulated by introducing more specific norms. Consequently, the Netherlands wants to evaluate whether the GDPR is suitable to regulate blockchain applications in a way that protects data subjects rights but also allows for the use of blockchain technology in certain forms, but possibly also enhances the possibilities for data subjects to exercise their rights.

3. Observations on the functioning of specific provisions of the GDPR

3.1 Consistency of other directives and regulations with the GDPR

The Commission has stated in it's Commission Communication of July 29th of this year that (p. 2):

"One key objective of the Regulation was to do away with a fragmented landscape of 28 different national laws that existed under the previous Data Protection Directive and to provide legal certainty for individuals and businesses throughout the EU. That objective has been largely met".

While the Netherlands shares this positive sentiment, we would like to stress that the abolishment of the (former) fragmented legal landscape at the national level should go hand in hand with the prevention of a (future) fragmented legal landscape at the EU level. All EU directives and regulations dealing wholly or partly with data protection issues should be consistent with the GDPR. Otherwise, we risk the return of a fragmented legal landscape at the national level through the implementation of new directives and regulations which are inconsistent with the GDPR. However, in our experience so far new (initiatives for) EU directives and regulations are not always fully consistent with the GDPR. We have seen this for instance with regard to the implementation of the EU information systems on interoperability: EES, ETIAS, SIS, VIS, ECRIS-TCN and EURODAC. The different regulations pertaining to these information systems all have extensive norms on data protection. The Netherlands wants to implement these regulations in coherence and deal with these data protection issues in a consistent and logical way. However, the different data protection regimes contained in these different regulations pose a challenge in this regard.

3.2 Age of consent (Article 8 GDPR)

The Netherlands considers it necessary that only one uniform age of consent applies within the whole of the EU. The current situation, where multiple age limits apply across member states, leads to a problematic lack of legal certainty for all parties concerned; parents, children and controllers alike.

Parents and children have difficulty knowing at what age they have to give, respectively ask, for consent since that depends on the law of the Member State where the controller, that offers the specific information society service, coincidentally is established. Considering the cross-border nature of data processing as such and these information society services in particular, this lack of uniformity is also worrisome in light of one of the main goals the GDPR purports to achieve: the free flow of data.

Moreover, the freedom left to Member States to choose an age limit has had the unfortunate and unforeseen side-effect that various Members States have stretched the territorial scope of their implementation acts so as to cover not only controllers established within their Member State (establishment criterion), but also all processing activities concerning data subjects residing within their Member State (residency criterion). These Member States have done so in order to ensure that the age limit of their choice applies to all children living in their country. As a consequence sometimes two different sets of national implementation rules are both applicable at the same time to one cross-border processing. In case of incompatible or conflicting national rules regarding the age of consent, this poses a significant problem for the controller as to what to apply, since there is no rule of conflict for such a situation. This goes against one of the main goals the GDPR is trying to serve, namely to make things simpler, especially for controllers, through the imposition of uniform rules.

It is important to note that this conflict of implementation laws extends far beyond the different choices that can be made with regard to this age limit; regarding *every* subject where the GDPR leaves room for national choices (for instance regarding special categories of personal data) this situation potentially occurs. The Netherlands therefore strongly pleas for a specific provision prohibiting the use of the residency criterion to delineate the territorial scope of national implementing legislation. Of course this measure is closely linked to the previous point, because the moment there would be just one uniform age limit applicable throughout the whole of the EU, there would probably be no more need for such an expanded territorial scope.

The next question is *what* that uniformed minimum age should be. In the Netherlands, nothing has been decided on the minimum age yet. We are, amongst other things, still awaiting a scientific study regarding the position of children in Dutch law in general. Generally speaking, 13 year old children are probably sufficiently able to oversee the consequences of giving consent. Moreover, this age limit aligns with a growing tendency in Dutch law to give children from the age of 12 control over decisions affecting them (e.g. medical treatment or parental custody). On the other hand, the parental obligation to protect their children (and their wish to do so) must also be taken into account. After all, a parent has no longer any legal say in the matter when a child has lawfully consented. Might a lower age limit then 16 years be decided upon, then that age would only have to apply to the processing of regular personal data. As far as the Netherlands go, when special categories of personal data are concerned, it might be necessary to set a higher age limit or to leave room for a national choice on that specific subject. Having said that, given the problems mentioned before, the Netherlands stresses that in any case reaching a consensus between all Member States about one (any) uniform age limit is far more important than the question what age limit to settle on.[6]

One last point, that is related to the age of consent, the Netherlands likes to put forward, has to do with discussions in our Parliament regarding the right to privacy of children. For instance, the question has arisen to what extent and under which conditions a child can invoke his GDPR-rights against a controller (erasure, access, rectification, withdrawal of consent etc.), regardless whether the child has reached the age to give consent on its own. One could argue that all articles concerning the GDPR-rights are evenly applicable to a child because the child, after all, still is the data subject. On the other hand the following can be read in the guidelines of the Working party 29 on consent: *"After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3)."* [7] The Netherlands believes that the position of children in this respect requires more attention, explanation and perhaps regulation.

---

6 Ideally that uniform age limit should also be applicable to the other instances where consent is a condition for processing. If the consent is required because of Article 6 (1) (a) GDPR where there is no 'offer of information society services' concerned. But also when automated decision-making is at hand (Article 22 (2) (c) GDPR), and in the case of the transfer of personal data on the basis of Article 49 (1) (a) GDPR. If the consent is given on behalf of Article 9 (2) (a) GDPR it might still be a necessary to leave room for national choices concerning at what age that consent can be considered given lawfully.

7 Article 29 Working Party. Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2019 (17/EN WP259 rev.01), p. 27.

3.3 Records of processing activities and the derogation for SME's (Article 30 (5) GDPR)

In the Netherlands, a large part of the criticism of the GDPR focusses on the (supposedly) increased "bureaucratic burden" for small businesses and/or businesses that do not process data on a large scale. The same goes for sports and other associations and, for example, churches. Most of them are of good will, but still face a relatively large extra workload.

The discontentment of small businesses in any case concerns the derogation to the obligation to maintain a record of processing activities. Numerous worries and complaints about this subject have already been received.

Article 30 (5) of the GDPR exempts enterprises or organizations employing fewer than 250 persons of the requirement to maintain a record of processing activities, but only under a set of stringent and cumulative prerequisites. This means that in practice the exemption hardly ever applies. In particular the condition that 'the processing is not occasional' limits the possibilities for invoking this derogation too much, because processing activities, even the simplest, are almost always structural. After all, even if the amount of personal data processed is very limited (for instance only data concerning customers or members/employees), this processing will still have a structural character and these (limited) databases will form the basis for their activities.

The Netherlands believes that this was never the intention of the European legislator in the first place and therefore advocates that the exemption should be given a larger scope. Furthermore, according to recital 13, Member States and their supervisory authorities 'are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation'. The fact that Article 30 does not allow Member States to provide, at the national level, for a broader scope of the application of the derogation, makes it very difficult for Member States and their supervisory authorities to heed this recommendation.

3.4 Certification

As Article 42 (1) points out, all actors involved (Member States, supervisory authorities, the Board as well as the Commission) are to encourage the establishment of data protection certification mechanisms and of data protection seals and marks, in particular at Union level. The GDPR makes an approach at Union level possible in various ways. Article 42(5) GDPR renders the option for the EDPB to approve the certification criteria using the consistency mechanism, resulting in a common certification, the European Data Protection Seals. In addition Article 43 (8) GDPR empowers the Commission to adopt a delegated act specifying the requirements to be taken into account for the certification mechanisms. However under Article 42 (5) GDPR the different national supervisory authorities may also approve those certification criteria at the different national levels. The use of certification mechanisms that are only valid at national levels seems to be counterproductive, because they thwart further harmonization. The Netherlands would like these certification processes to be part of the evaluation. Depending on the outcome of the evaluation, we may have to reconsider the possibility of applying a certification mechanism that is only valid in a national context, or restrict that possibility to only those situations where they do serve a legitimate purpose.

3.5 The monitoring of approved codes of conduct (Article 41 GDPR)

The European Data Protection Board (EDPB) has recently adopted new guidelines on the subject of codes of conduct. In those guidelines it is stated that a code owner 'must be able to demonstrate, amongst other things, that his code provides effective mechanisms allowing appropriate monitoring of the rules (e.g., regular audits and reporting requirements, concrete sanctions and remedies in the case of a violation of the code) and identifies a monitoring body' (underscore added). In other words, according to the EDPB, there is an obligation to institute a monitoring body to be able to make use of the instrument of a code of conduct.

The Netherlands believes that the text of the GDPR is ambiguous on this subject and that the interpretation of the EDPB, as laid down in the aforementioned guidelines, is therefore questionable. We believe that the text of the GDPR should, at least be, clarified on this point and we further argue that the institution of a monitoring body in case of a code of conduct should explicitly be made facultative. We believe this solution does justice to Recital 98, which states that the drawing up of codes of conduct should be encouraged. An obligation to institute a monitoring body will have the opposite effect. The requirement will most likely act as an disincentive because it inevitably constitutes a threshold due to the additional costs involved.

3.6 Other instances of ambiguous language in the GDPR-text and the need for more guidance

Guidance on and examples of "suitable and specific measures"

In several instances, the GDPR allows for derogations to be laid down in Member State law but only when "suitable and specific measures to safeguard the fundamental rights and the interests of the data subject" have been put into place as well (for instance in Article 9(2) (g) (i) (j), Article 10 and Article 22 (2) (b) (3) (4) GDPR). The same applies to the controller who is sometimes allowed to process personal data under the condition that he ensures "appropriate safeguards" (for instance in Article 9(2) (d), Article 40 (3) and Article 46 GDPR).

It is unclear what those measures and safeguards should or could entail. So far, almost all additional safeguards that are generic enough to be enshrined in national law, such as strict(er) retention periods, specific security precautions, authorization and access restrictions, are in fact refinements of safeguards that already have a basis in the GDPR.

Controllers are obliged to take more precautionary measures depending on the specific risks the processing entails. The moment special category personal data are being processed, the controller has to take extra safeguarding measures tailored to the specific situation. Some guidance in the GDPR itself or otherwise in a guideline from the EDPB could be very helpful for both national legislators and in some cases for controllers as well.

The meaning of 'necessary for entering into a contract' in the context of Article 22'

A general prohibition in Article 22 is made in relation to automated decision-making processes that have similar or legal effects on individuals. There is uncertainty about the listed derogation in the second paragraph under a; under what circumstances can an automated decision making process be considered 'necessary for the entering into a contract'? This lack of clarity could make businesses hesitant to try out new solutions and to innovate. More guidance from the EDPB on the interpretation of Article 22 would be most welcome.

The scope of the obligation to provide ‘a copy of the personal data undergoing processing’ in article 15 (3)

A lot of questions have arisen and still arise from the obligation of a controller to provide the data subject with a copy of the personal data undergoing processing. In The Netherlands several courts have already been confronted with these kind of cases. Guidance on how to act with regard to all kinds of documents containing personal data would be useful.

3.7 Practicalities

In addition to the important task of the EDPB to issue guidelines, recommendations and best practices on various topics and by doing so clarifying the meaning of the terms used in the GDPR for the sake of day to day practice, it would be - also on a practical level - very helpful if the EDPB could ensure that only one harmonized form is issued to notify personal data breaches because controllers are now confronted with forms that vary from Member State to Member State.

3.8 Technicalities

The Netherlands would like to draw the Commissions’ attention to four technical issues, some of which may possibly be resolved in the horizontal corrigendum that we understand is being prepared at the moment:

1. In Article 83 (5), point (a), of the GDPR the reference to Article 10 GDPR seems to be missing. Consequently, the data protection authority cannot impose an administrative fine if it concludes that an infringement of Article 10 has taken place. We have corrected this omission in Dutch implementing legislation making use of the possibility that Article 84 GDPR provides, but it is preferable to correct this in the GDPR itself.

2. This raises the question whether a reference to Article 10 may also be missing in Article 22 (4) of the GDPR, because such a reference in the context of profiling seems logical.

3. In the last sentence of Article 28 (3) of the GDPR, reference is made to 'point (h)' where 'point (a)' must have been envisioned because otherwise this provision has no clear meaning.

4. Article 7 (e) of the Data Protection Directive (95/46/EC) allowed for the processing of personal data by public sector entities when the processing was necessary "in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed". In Article 6 (1)(e) GDPR the last phrase (underscore) has been deleted. In practice, this can lead to difficult issues, for example when an administrative body wants to declare a potential crime to the police. Prior to the GDPR, the administrative body could simply invoke the official authority vested in the police – the third party to whom the personal data is disclosed – as the legal basis for the necessary data processing. Under the GDPR it seems that, as a consequence of this new formulation, the administrative body has to invoke a separate new legal basis.

4. Information requested by the European Commission

4.1 Adequacy decisions

Adequacy decisions are an important instrument to facilitate (frictionless) international transfers of personal data, while at the same time ensuring a high level of protection of personal data. In addition, it should be noted that the prospect of adequacy decisions may in practice lead to an improved level of protection of personal data - in the spirit of the GDPR - in third countries, taking into account that third countries need to ensure an "essentially equivalent" level of protection for an adequacy decision to be adopted.

With regard to the 11 adequacy decisions adopted based on Directive 95/46, it should be noted that these decisions will be evaluated by the Commission in order to review compliance with the GDPR. In this regard, it may be necessary to adopt additional measures in order to achieve a level of protection that is, in fact, "essentially equivalent" to the level of protection provided in the GDPR.

Dutch trade organizations submit that the following countries could be a potential future candidate for an adequacy finding:

- Generally speaking: all countries that have ratified and implemented the modernized Convention 108 ('Convention 108+');
- Singapore, Colombia, Mexico, South-Africa, Serbia;
- Dubai International Financial Centre (DIFC).

4.2 Independence and budget of our DPA

Independence

Article 52(2) of the General Data Protection Regulation (GDPR) stipulates that the members of the DPA shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

First of all, it should be noted that the Dutch DPA is – both legally and in practice – fully independent to plan, execute and enforce its tasks and powers, without taking any instructions. In this regard the Dutch DPA is, for instance, fully independent to set its own priorities, as well as to establish and carry out its own working program.

In order to fully guarantee the DPA's independence in exercising its supervisory powers some Article s of the Independent Administrative Bodies Framework Act (*Kaderwet ZBO*) were excluded, in whole or partially, for the DPA.

Article 13(1) of the Act to implement the GDPR for the Dutch DPA (*Uitvoeringswet AVG*) stipulates that Articles 21 and 22 of the Independent Administrative Bodies Framework Act (*Kaderwet zbo's*) are not applicable for the DPA. This means the minister is neither allowed to establish policies on the exercise of the supervisory powers of the Dutch DPA, nor is he allowed to annul any decisions made by the DPA in its supervisory capacity.

Article 13(2) of the Act to implement the GDPR for the Dutch DPA stipulates that Article 23 of the Independent Administrative Bodies Framework Act (*Kaderwet zbo's*) is not applicable for the DPA. This limits the influence of the ability of the Minister to take necessary measures in case of neglect of duties by the Dutch DPA to matters concerning financial or administrative management only.

Finally, legal personality has been granted to the DPA from 1 January 2019 (see Article 6 (1) of the Implementing Act of the GDPR). From that date the DPA is no longer part of the public legal entity the State of the Netherlands. The DPA has herewith the option of being independently authorized to perform legal acts under private law, without ministerial authorization. Moreover, acquiring its own legal personality means that the DPA can continue to appoint its own staff, even after the civil service law has entered into force that requires an employment contract to be concluded with its employees. In this way, an additional contribution is made to the requirement of Article 52 (5) of the GDPR, on the basis of which the supervisor authority must have its own, self-selected staff.

Budget

Article 52(4) of the GDPR determines that Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

Article 11 (paragraph 1 to 3) of the Implementing Act of the GDPR clarifies that the DPA has its own budget as part of the national Central Government Budget in accordance with Article 52 (4) of the GDPR. To clarify that the DPA is provided with the financial resources necessary for its independent performance of its tasks, Article 11 (2) of the Implementing Act of the GDPR explicitly states that each year a budget is allocated to the DPA at the expense of the national Central Government Budget. For 2019 this amounts to a budget of 18.6 million euros.

At the moment constructive discussions regarding the budget are ongoing between the Dutch DPA and the Ministry of Justice and Security. This month the Minister for Legal Protection announced to the Dutch Parliament a joint external research. The aim of the research is to establish a shared view on a sound financial basis for the exercise of the supervisory powers by the Dutch DPA as laid down in the GDPR.

4.3 Cooperation and consistency mechanisms

The cooperation and consistency mechanisms are key instruments to ensure a high and consistent level of protection of personal data throughout the EU. It is expected that the application of these mechanisms will result in a number of important decisions and guidance documents in the near future, thereby contributing to a clear understanding and consistent application of the GDPR. Most importantly, the one stop shop mechanism (Art. 60 GDPR) and the Opinions and Decisions of the EDPB (Art. 64 and 65 GDPR) are, in practice, effective instruments to ensure a clear interpretation and application of the GDPR.

Taking into account that the cooperation and consistency mechanisms have only been applied for a relatively short amount of time, not all procedures have been applied yet. This is expected to change in 2020.

While the cooperation and consistency mechanisms are valuable tools, there is still room for improvement. With regard to the one stop shop mechanism the following observations can be made:

1. First of all it should be noted that the one stop shop mechanism plays a vital part in the creation of the single market for data. The one stop shop mechanism not only removes barriers for controllers carrying out cross-border processing operation, but also provides a high level of protection for data subjects by enabling them to file complaints at their national supervisory authority. Taking into account that supervisory authorities need to closely cooperate within the one stop shop mechanism, the European supervisory authorities have become - even more than before - mutually dependent. This means that it is of the utmost importance that all EU supervisory authorities are provided with sufficient means to carry out their tasks. Since all supervisory authorities are obliged to handle cases for which they are the European Lead supervisory authority, there is a risk that cases will not be dealt with in a timely manner, when the Lead supervisory authority does not have the means to take on these cases. This will, in turn, undermine the one stop shop mechanism as a whole.

2. Further to the matter described above, there may be incentives for forum shopping on the side of personal data controllers, inherently in the current system. Perhaps it is worth exploring additional scenarios, cooperation forms, or regulatory powers, that enable a Lead supervisory authority to prioritise its workload, while also ensuring that appropriate enforcement can be put in place, for example through settlements with a controller, merging of individual cases or to entrust other authorities with handling the matter to the extent appropriate and with all necessary competences with regard to the case. The same can be noted with regard to requests for mutual assistance as described in Article 61 (4): Perhaps a third exception could be added, in order to enable the authority that receives such a request to offer alternative ways to handle a matter appropriately, without activating paragraph 8 of Article 61 jo. Article 66(1) per se.

3. One of the benefits of the cooperation mechanism is that it fuels the creation of a uniform application of the GDPR throughout the Member States, through close cooperation in case handling and decision making. At the same time, the GDPR is also applied in non-cross-border cases on a daily basis. For example, the majority of GDPR fines imposed to date, are about non-cross-border issues. The risk of disparities in application of the GDPR between rulings in cross-border-cases versus cases on Member State level, is something to keep in mind, even though such cases may be materially similar.

4. Lastly, some key concepts of the one stop shop mechanism still need further clarification. This is for instance the case with the concept of "main establishment", which needs additional clarification in relation to the complex corporate structures that supervisory authorities may encounter in practice. Although, EDPB may be able to provide further guidance on how to interpret the concepts of "establishment", "main establishment" and "cross border", there may also be room for additional clarification in the GDPR text.

With regard to the consistency mechanism, the following observations can be shared:

1. The consistency mechanism, as well as the EDPB, play a vital part in the consistent interpretation and application of the GDPR. By applying the consistency mechanism, the European supervisory authorities are able to jointly address important and complex legal questions, thereby contributing to a better and more consistent understanding and application of the GDPR.

2. However, taking into account that the GDPR provides for strict legal deadlines (for instance for issuing EDPB Opinions or Decisions), a tension exists between short legal deadlines on the one hand and achieving the highest level of quality needed to address complex legal questions on the other hand. Taking into account that EDPB Opinions and Decisions may have far reaching consequences, both in individual cases, as well as for European companies, data subjects and public authorities, it may be advisable to allow for extended legal deadlines, in a limited amount of cases where this is strictly necessary.

5. Closing remarks

The Netherlands looks forward to discussing these observations and remarks further with the Commission, the Finnish Presidency and the other Member States.

We acknowledge that the GDPR has only been applicable for a relatively short time and that more experience needs to gained on the application of the GDPR before certain issues can be resolved. However, even with the limited experience that has been gained so far, in the Netherlands several practical issues regarding the application of the GDPR have already come to the forefront. We believe it is important that these issues – and any other issues other Member States have encountered so far – should be taken fully into account during the first review of the GDPR. If a 'quick win' solution is ripe for the taking, we believe the Commission should not shy away from developing appropriate proposals to amend the GDPR. The Netherlands believes such proposals can only help to further increase the public acceptance and legitimacy of the GDPR.

Furthermore we believe the EU is best placed to resolve the complex issues arising from the developments in information technology and information society. These developments and the tech companies behind them materialize and operate on a global scale, while the processing of data in this digitalized age often has a cross-border nature. We believe it is important to always keep a watchful eye at these developments, because in the 'never ending competition' between legislation and technological progress, stagnation means decline

AUSTRIA

Chapter I: General provisions

It is not clear if and in how far the provisions of the GDPR, in particular concerning the supervisory ahuthority's competence, apply to the legislator.

Chapter III: Rights of the data subject

Art. 23(2) GDPR provides that legislative measures restricting the scope of obligations and rights shall contain specific provisions at least, "where relevant", as to the issues listed in lit. (a) to (h). Due to the term "where relevant", it is not clear in how far and under which circumstances such specific provisions are obligatory.

Chapter IV: Controller and Processor

Articles 26 and 28

In cases where a controller is, by law, obliged to use a processing system that is run by another person or body, it is sometimes difficult to establish the roles (controller/processor) of the persons/bodies involved. In the public sector, such cases occur e.g. when courts process personal data within public registers such as the commercial register or the land register. In these cases, the courts are solely responsible for the personal data to be processed within the register, thus qualifying as controllers. However, the registers themselves are established and run by the Minister of Justice, who thus decides on the technical means of the courts' processing. It is not fully clear if the person responsible for the system would, in such cases, qualify as a joint controller, or as a processor.

Article 27

Practice has shown that some controllers established in third countries do not comply with their obligation to designate a representative in the Union pursuant to Art. 27 GDPR. In such cases, the supervisory authority lacks the legal means to prosecute the controller. This issue could be resolved by allowing the supervisory authority to designate, at the controller's cost, a representative, or to request the designation of a controller by a court. Such a designation could be notified to the EDPB and remain effective until the controller designates, in accordance with Art. 27 GDPR, a representative.

Articles 40(4), 41(1)

Pursuant to Art. 40(4) GDPR, a code of conduct (Art. 40(2) GDPR) shall contain mechanisms which enable the body referred to in Art. 41(1) GDPR to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to comply with it. In contrast, pursuant to Art. 41(1) GDPR, the monitoring of compliance with a code of conduct (Art. 40 GDPR) may be carried by a body accredited for that purpose by the competent supervisory authority.
Art. 40(4) and 41(1) GDPR thus appear to be contradictory as to whether it is mandatory or optional to establish a monitoring body. It is difficult to resolve this contradiction by way of interpretation.

Chapter V: Transfers of personal data to third countries or international organisations

In practice, data transfers to international organisations currently cannot be based on Art. 45-47 GDPR because the requirements set out therein are not met. In particular, it appears that international organisations are not ready to sign standard contractual clauses. As a consequence, such transfers are based on Art. 49 GDPR. However, this provision is designed to be an exception and not a rule. Adequacy decisions relating to international organisations could facilitate such transfers.

Chapter VII: Cooperation and consistency

The GDPR does not provide collision norms concerning the procedural law applicable in cases where supervisory authorities from more than one member state are involved. This can hamper cooperation between supervisory authorities, for example where provisions regarding legal standing or access to files differ in national procedural laws. Non-compliance with procedural obligations could result in the supervisory authority's decision being quashed at a party's appeal, in particular when the supervisory authority adopts a decision under Art. 60(8) GDPR.

Chapter VIII: Remedies, liability and penalties

The GDPR provides that data subjects have both the right to lodge a complaint with the supervisory authority (Art. 77 GDPR) and the right to an effective judicial remedy against a controller or processor (Art. 79 GDPR) if the processing of their personal data infringes the GDPR. Such a dual recourse causes difficulties, as both the supervisory authority and the courts are fully independent and underly different codes of procedures. Moreover, the possibility to lodge a complaint with the supervisory authority and at the same time bring the very same matter before a court can provoke fragmentation of the interpretation of the GDPR. In particular, issues of res iudicata are likely to occur. More clarity on whether and in how far the GDPR allows for national collision rules (such as suspension rules, inadmissibility in res iudicata cases) would be desirable.

POLAND

These are preliminary comments as the process of inter-governmental consultations regarding the application of the GDPR in Poland is still ongoing.

Poland has identified the following issues that should be subject to special scrutiny:

- **Art. 42 and 43 GDPR (certification and certification bodies)**

Poland, already now, only one year after the GDPR is being applicable, has serious concerns whether certification as set in articles 42 and 43 GDPR will work in practice. From the perspective of the Polish government it is quite clear that the mechanism as it was designed in the GDPR does not provide sufficient incentives for data controllers/processors and do not sufficiently encourage them to apply for certification. Another reason might be lack of guidance regarding what exactly can be subject to certification. It should be noted that there were no applications for certification in Poland. We would be however interested to learn how the situation in this respect looks in other Member States.

- **Article 2 para 2 letter a) and 23 para 1 GDPR (reference to national security)**

The relation between both articles causes interpretation problems, not only for controllers/processors but also for national law-makers. The reference to national security in Art. 23 para 1 GDPR requires clarification or should be removed, as the GDPR is not applicable to processing of personal data for the purposes related to the national security.

- **Art. 23 para 2 letter g) GDPR (risks to the rights and freedoms)**

Article 23 causes more interpretation issues. Also, interpretation of Art. 23 para 2 letter g) poses certain challenges, as it is not clear how to understand "the risks to the rights and freedoms of data subjects". This was something Polish legislator was carefully analysing during the work on our national data protection laws and could not achieve sufficient clarity in this respect.

- **Art. 12 para 7 and 8 GDPR (standardised icons)**

Poland is curious what steps the Commission takes regarding the so called "pictograms" (delegated act).

- **Art. 13 para 4 and 14 para 5 GDPR (information to be provided to a data subject)**

In Poland's opinion further guidance is needed on how to prove that a data subject already has the information that otherwise should be provided by a controller. We need to ensure that data subjects receive information they need but at the same time, avoid providing them with too much unnecessary data.

- **Art. 6 GDPR (lawfulness of processing)**

Poland believes that a legal basis similar to the one in Art. 9 para 2 letter e) GDPR – i.e. data manifestly made public by the data subject, would be of use. Lack of such a legal basis in Art. 6 causes practical problems.

- **Art. 6 para 1 letter c) GDPR (compliance with a legal obligation to which the controller is subject)**

In Poland's opinion legal provisions may impose duties but also grant rights. Granting rights may require processing of personal data, but is not covered by Art. 6 para 1 letter c). Such a situation causes practical problems.

- **Recital 14 GDPR (natural person acting as unincorporated entity)**

Under the Polish civil law we have unincorporated entities with legal capacity, in particular sole proprietorships. It is a very popular form of doing business by micro-entrepreneurs in Poland, but such persons are not formally considered legal persons, therefore processing of their data is subject to the GDPR. Again, this causes some practical problems.

- **One-stop-shop mechanism**

As regards the one-stop-shop mechanism, in Poland's opinion there is a need to take a closer look and check whether it properly mitigates the risk of so called forum shopping. In this respect asking the European Data Protection Board to provide DAPIX with information on the number of cases in which each of the Member States' DPAs is a lead authority could be of use. It would allow us to see how the decision making process within the one-stop-shop mechanism looks in practice.

- **New technologies, including blockchain**

The GDPR should be future-proof and should balance fundamental rights with innovation. A new technology of possibly great importance that creates challenges from a data protection perspective is blockchain. The Council document should touch upon the issue of how to execute data subject's rights without hindering the development of this technology.

PORTUGAL

To comply with the request by the Presidency addressed to the delegations in document 11292/19, Portugal hereby makes the following observations:

The General Data Protection Regulation (Regulation) has been applicable as of 25 May 2018. A little over a year later, it is prudent not to change the existing legal framework. In fact, many operators are still involved in the process of implementing the Regulation, and it is not convenient to change an existing regulation still being implemented for many operators. It should be noted that a normative assessment should focus on fully implemented rules, which is not the case, at least in Portugal, whose law implementing the Regulation dates from August 2019. The course of time will therefore dictate the possible need for a revision of particular provisions. Good legislative technique advises against changes to recently approved diplomas.
Notwithstanding, we can already foresee that the objective of harmonizing the Regulation has not been achieved, which could entail a legislative change in the near future.

In fact, the Regulation allows national legislators to approve specific legislation on a variety of subjects, namely with regard to:

- Lawfulness of processing: article 6;
- Conditions applicable to child's consent in relation to information society services: article 8;
- Processing of special categories of personal data: article 9;
- Processing of personal data relating to criminal convictions and offences: article 10;
- Information to be provided where personal data have not been obtained from the data subject: article 14 (5);
- Right to erasure (“right to be forgotten”): article 17;
- Automated individual decision-making, including profiling: article 22;
- Restrictions: article 23;
- Joint controllers: article 26;
- Processor: article 28;

- Processing under the authority of the controller or processor: article 29;
- Security of processing: article 32 (4);
- Data protection impact assessment: article 35 (10);
- Prior consultation: article 36 (5);
- Designation of the data protection officer, especially the extension of the obligation to designate and consecrate the obligation of secrecy or confidentiality: articles 37 and 38;
- Regarding international transfers of personal data, certain derogations for specific situations: article 49;
- Representation of data subjects: article 80;
- Penalties: article 84.

If all Member States make use of such legislative permissions by approving specific rules, we will then see a panoply of applicable rules, thereby undermining the desired uniformity. This leads us to conclude that the harmonization objective will not be achieved.

The adoption of specific national rules in the areas allowed by the Regulation will create a problem in law enforcement. In fact, the Regulation does not address the question of which law applies where cross-border data processing takes place and where different Member States adopt specific legislation. Is it the law of the country in which the controller or processor is established? Or is it the legislation of the country where the data subject is located?

In line with has been defended by stakeholders, who draw attention to the need for a higher level of harmonization, Portugal is of the opinion that the current diversity of national legal solutions with regard to the implementation of the provisions of the Regulation allows for flexibility is problematic and could soon dictate a legislative change.

Concerning the issue of international data transfers, we should stress our reservations regarding the intention of the European Commission to introduce data exchange and data protection clauses in trade agreements (p. 12 of COM (2019) 374 final). In this respect, it should be noted that the Regulation creates its own mechanisms, such as the adequacy decision. We are in principle against the inclusion of clauses on the fundamental right to data protection in trade agreements because interests and rights underlying trade and data protection rights are complex, difficult to reconcile, possess different scopes and should therefore be treated separately.

ROMANIA

1. Information Member States would like to share on the use of adequacy decisions by their stakeholders and/or relevant developments in countries or territories benefiting from a Commission's adequacy decision.

Until now, the Data Protection Authority did not have a case involving using the adequacy decisions to transfer personal data to a third country or international organizations.

2. Information concerning the independence and resources of the Data Protection Authorities (DPAs). This includes notably their capacity to exercise their powers provided by the GDPR and to comply with their obligations in the context the cooperation and consistency mechanisms.

One way of proving the independence of the DPA refers to the appointment of its president. Thus, according to Article 6 paragraph 1 of Law no. 102/2005, republished, the president and vice-president of the DPA are appointed by the Senate for a mandate of 5 years. Their mandate can be renewed once.

Article 6 paragraph 2 of the same law stipulates that any person holding the Romanian citizenship that has graduated from an academic institution with legal specialization can be appointed as president or vice-president. The president and vice-president are persons politically independent, having a solid professional competence, including in the field of data protection, of at least 10 years in this field, a good reputation and that enjoy a high civic probity.

In order to renew the mandate of president or vice-president of the DPA, the same procedure used for their appointment applies, as stipulated in Articles 6 and 7 of Law no. 102/2005.

Referring to the budget of the authority, Article 27 of Law no. 102/2005 mentions that:
(1) The DPA has its own budget which is part of the state budget.
(2) The DPA, after consulting the Government, shall approve its own budget and forwards it to the Government in order to include it in the state budget. The comments of the president on the budget draft made by the Government shall be submitted to the Parliament for solving.

Regarding the human resources available to the DPA, Law no. 129/2018 was adopted in order to amend Law no. 102/2005 for setting up, organizing and functioning of the DPA. Thus, the number of positions inside the DPA was increased to 85 from 50. This increase was necessary due to the new competences of the DPA as set out in the GDPR.

3. Information which would allow verifying the effectiveness of the coherent interpretation and application of the GDPR throughout the EU by the cooperation and consistency mechanism provided by the GDPR.

According to Article 60 and the following ones of the GDPR, the DPA cooperates with the other DPAs by using IMI (Internal Market Information System) made available by COM. The most popular cooperation requests are the ones based on Article 56 (referring to the competence of the main DPA) referring to the ex officio controls, namely solving the complaints. Another popular topic is Article 61. (referring to mutual assistance).

SLOVENIA

Chapter 5 - Transfers of personal data

In terms of the provisions on decisions on the appropriate level of protection issued by the European Commission, the Information Commissioner of the Republic of Slovenia (IC) has no specific comments at the moment, but at the same time stresses out that an assessment can only be made after the adoption of the new legislative framework on personal data protection in Slovenia.

In general terms, the problem lies in the definition of transfers in relation to the definition of the territorial jurisdiction of the GDPR, in case where the GDPR applies to a data controller, who in fact only has a representative in the EU and is therefore practically impossible to perform a supervision on the implementation of the GDPR. Undoubtedly, this case too should refer to transfers (EDPB has already agreed to this, but there is no exact demarcation yet).

Article 46(4) requires the use of a compliance mechanism in case where adequate protection of personal data when transferred to third countries is ensured by means of contractual provisions between the controllers and processors under Article 46(3)a. The requirement for use of a compliance mechanism in case of contractual provisions, which concern only one Member State or which have no EU component, seems excessive and imposes disproportionate costs on authorities and causes an administrative burden.

Contractual provisions may concern only the Slovenian controller and e.g. a processor from Serbia or Bosnia and Herzegovina. There are no restrictions on the language of the contractual provisions, which means that they may be written in a third-party language – in this case in Serbian or Bosnian language. Thus, the contract has a very limited regional reach, at the same time though the supervisory bodies for data protection should, at the time of issuing, treat it in accordance with the compliance mechanisms. This means it should be transmitted to EDPB, who, within its competence, would entrust the writing of an opinion on the compliance of specific contractual clauses to one of its professional sub-groups (for data transfers), in which the employees of the supervisory authorities (including the Information Commissioner) participate and prepare documents. Preparation of an opinion is complex and takes time and input in terms of human resources, and as stated before, at the same time the contract example does not have a specific EU component.

The working language for decision-making in compliance procedures is English, so Information Commissioner (or the data controller) would face additional contract translation costs.

Chapter 7 - Cooperation and consistency

Processes of cooperation and compliance (and other EDPB activities) represent a significant burden for the supervisory authority in terms of human resources (for the Information Commissioner specifically about 25% full time employees in the field of personal data protection). Particularly from the perspective of compliance processes, it is questionable to what extent these processes are economical proportionally the impact. A problematic field is the provision of document translations, revision of machine-translated documents etc., which represents a huge additional cost to the authority. Additional difficult aspect is setting deadlines in all proceedings under Chapter 7, especially in the case of cross-border proceedings under Articles 60 and 61. At first glance, they are clear, but in practice, each supervisory authority appears to be working in accordance with its own national procedures (General Administrative Procedure Act, etc.), and it is often impossible to agree on the exact procedural details, e.g. since when is the deadline counted, how is it with the establishment of powers, etc. The regulation is unclear to the extent that it allows for different interpretations. The EDPB is, of course, taking the stance on these issues, but in fact, from the point of view of legal certainty, the big question is how will the court decide on the completed cooperation cases.

a) Cooperation

According to the Information Commissioner, the cooperation in cross-border cases of supervision and assistance under Articles 60 and 61 is solid but at the same time requires considerable resources from the supervisory authority, in case of the Information Commissioner, approximately 5 full-time employees (approx. 15% personal data protection employees).

Because cooperation takes place through internal market information (IMI), which is rather opaque in this respect, this requires human resources by the administration itself - that is, receiving messages about new requests in IMI, filtering them and comparing them with the national case management system for the supervisory authority to determine whether a particular communication or process transmitted through IMI relates to a nationally operated procedure, filing claims in IMI which have specific rules, etc. A particular difficulty represents the linking of cases in IMI, which in the light of the increased effectiveness of certain bodies acting as lead authorities, present considerable difficulties for other bodies subject to the search for information on cases where the relevant supervisory authority is in related registers in IMI. Additionally, issues of judicial protection arose in cases of final decisions in cross-border cases.

Conducting the collaboration process through IMI requires additional human resources due to the complexity and length of the procedures in order to provide document translations (documentation, e.g. submission, can encompass an entire report - 30~50 pages). All documentation must be translated before it can be forwarded to the lead supervisory authority, a high level of English proficiency is required, more complex is the coordination of national inspection and decision-making practices in appeal procedures with decisions in cross-border cases. A lot higher is the use of resources for the internal coordination of cooperation processes and national practices in oversight and complaints, for training on the technical functionality of IMI, on conducting cross-border procedures, on unifying practices and on-going monitoring of practices evolving in the use of IMI.

b) Compliance

As the Chapter 5 example above shows, the compliance mechanism is prescribed in many cases, but in cases where only one or a limited number of member states are concerned it can be restrictive and disproportionate burden to the controller or processor and to the supervisory authority, both in terms of the use of human resources and costs. Participation of Information Commissioner in EDPB processes (in the area of preparation of compliance opinions, guidelines and other activities) requires approximately 4 full-time employees (approx. 10% of employees).

When a document, prepared by the data controller, the processor, the association, etc. (standard contractual clauses, codes of conduct, etc.), is required to pass the compliance process it represents an extension of the decision-making time for the EDPB (it may take it more than 3 months to prepare an opinion), all the while a language barrier and the issue of translation cost remain (borne by the supervisory authority or the applicant?). Where the document concerns only a limited number of member states, this obligation appears disproportionate and its effect limited.

The resource requirement of the supervisory authorities in cases of the compliance mechanism are greatly increased, on one hand in terms of documents handled (translations, coordination), which are required to pass the compliance process, and on the other hand, since the IC employees also participate in EDPB expert groups preparing opinions on specific documents in the compliance process – here they are bound by deadlines (approx. 3 months), which in terms of coordination of all EDPB member states represent the creation of additional meetings (either in Brussels or via audioconferences) solely for the purpose of creating these types of opinions. Consumption of resources is so much higher. Even a smaller supervisory authority who have a hard time devoting such quantities of human resources to EDPB opinions, will most likely need to take over leading roles in writing opinions, given the ongoing discussions on the rotation system in some expert subgroups. As already stated above, a document can only concern the situation in one Member State or with a limited geographical reach, which raises a question on the effectiveness of such a system (for example, EDPB will have to provide separate opinions on each standard contract clause to be transmitted to the compliance process by a different member state – Slovenia will thus participate in the preparation of an opinion on the Danish clauses, the French clauses, etc.). At the same time, the GDPR requires an exchange of views on specific documents and situations, and it is therefore impossible to adopt opinions designed as guidance for similar cases.

SWEDEN

Following the general discussion on 3 September in DAPIX, the delegations have been asked to send in writing their observations on the experiences obtained from the application of the GDPR and their initial positions on and suggestions for items to be included in the Council report.

Sweden would like to thank the Finnish Presidency for this opportunity and agrees with the Presidency on the reminder that the GDPR has only been applicable for a relatively short time and that several issues could be resolved when more experience has been gained on the application of the GDPR.

Initially, Sweden wants to confirm that the cooperation between the DPA's in the Member States has increased and is mainly satisfactory. This cooperation is fundamental to achieve an effective and a coherent interpretation and application of the GDPR throughout the EU.

Sweden would like to point out several issues that can be taken into account in composing the Council report. Sweden has in the preparation of our comments particularly looked at the requirements in article 97 in the GDPR.

Sweden has no information to share when it comes to the use of adequacy decisions by stakeholders or relevant development in our country or territory benefiting from a Commission's adequacy decision. No complaints in any substantial degree has been forwarded to the Swedish DPA and thus the DPA has not particularly focused its supervision on this matter.

Regarding the cooperation between Member States, Sweden has noted some difficulties related mostly to cases of cross-border relevance. For instance, Member States view differs on some points, such as to which extent the DPA should act in relation to a complaint and also the meaning of article 57.f of the GDPR that eg states that the supervisory authority shall "investigate, to the extent appropriate". Also, the Swedish DPA has stated that the DPA's view on handling of complaints when the controller or processor establishes a main establishment within the Union or changes its main establishment varies between Member States.

Lastly, Sweden would like to highlight the question relating to exporting companies screening of personal data relating to criminal convictions and offences against sanction lists. In Sweden a couple of organizations have complained on the lack of uniformity in this matter. In light of these reactions it would be desirable to frame some uniform guidelines so that organizations within the Union can process data on equal terms on this point.

When it comes to the independence and resources, the Swedish DPA received an increase of their appropriations for 2018 by SEK 30 million, to cover the tasks that was added to their assignments due to the implementation of the GDPR. In 2019, the DPA received a further increase of SEK 6.2 million for its assignment in the field of camera surveillance. In its budget proposal to the Riksdag, the Government has proposed that the DPA's appropriations for 2020 should be increased by an additional SEK 14 million to further strengthen operations. All of the Swedish authority's resources are reviewed annually as part of the government's ambition to ensure that they have the funds they need to carry out their tasks and in accordance with the GDPR.