COUNCIL OF THE EUROPEAN UNION

Brussels, 28 February 2014

6762/1/14 REV 1

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 30
JAI 102
MI 191
DRS 26
DAPIX 25
FREMP 28
COMIX 110
CODEC 503

NOTE

from:	Presidency
to:	Council
No. prev. doc.:	17831/13 DATAPROTECT 201 JAI 1149 MI 1166 DRS 223 DAPIX 158 FREMP 209 COMIX 700 CODEC 2973 5879/14 DATAPROTECT 13 JAI 46 MI 91 DRS 14 DAPIX 7 FREMP 12 COMIX 68 CODEC 230 5881/14 DATAPROTECT 15 JAI 48 MI 93 DRS 16 DAPIX 9 FREMP 14 COMIX 70 CODEC 232 5344/1/14 REV 1 DATAPROTECT 4 JAI 22 MI 38 DRS 7 DAPIX 4 FREMP 4 COMIX 28 CODEC 91
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading] - Orientation debate on certain issues

I. Introduction

1. The Council deals with the data protection package presented by the Commission on 25 January 2012 as a matter of key priority. The data protection package comprises two legislative proposals based on Article 16 TFEU. The first proposal, for a General Data Protection Regulation is intended to replace Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The second proposal, for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is intended to replace Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

2. The European Council of 24-25 October 2013, which focused on the digital economy, innovation and services concluded that "the timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

3. During the first two months of its term, the Presidency, building upon the work of the Danish, the Cyprus, the Irish and the Lithuanian Presidency, has conducted in-depth discussions of certain important aspects of the reform. The Presidency has devoted more than 10 full-days meetings to the data protection legislative package (Regulation and Directive).

4. At informal discussions of Justice Ministers held in Athens, on 23-24 January 2014, Ministers expressed their overall satisfaction with the provisions of the draft Regulation as regards international issues and encouraged the possible strengthening of these models with other alternative models. Such provisions are key in today's globalised world to ensure the continuity of the high protection offered to EU citizens when they are targeted by companies established outside the EU and where their personal data are being transferred to third countries or international organisations.

5. The General Data Protection Regulation builds on the proven system and principles of the Data Protection Directive (Directive 95/46/EC). The Commission may decide, in the framework of comitology, with the involvement of both Member States representatives and the European Parliament, whether the level of protection ensured by a third country – including certain territories or processing sectors - or an international organisation is adequate. The European Data Protection Board will be consulted and express its opinion. One of the adequacy decisions adopted by the Commission concerns data transfers for commercial purposes between the EU and the US (Commission Decision 250/2000/EC), the so-called "Safe Harbour" decision. The Commission presented in November last year a Communication on rebuilding trust in EU-US data flows and is in intensive discussions with US counterparts on the Safe Harbour Scheme aiming at reinforcing it by the Summer.

6. The draft Regulation also provides that transfers to third countries can take place if the data controller or the processor applies appropriate safeguards including Binding Corporate Rules (BCR'S) and contractual clauses. The role of approved codes of conduct and approved certification mechanisms has been strengthened. Such transfers should take place on an equal footing as those based on adequacy decisions. Transfers can also be based on restricted derogations in specific situations.

7. On the basis of the outcome of the June 2013 Council, specific aspects of Chapter I to IV have been further examined in the Working Party on Data Protection and Exchange of Information (DAPIX). Extensive discussions took place on the right to data portability and profiling as well as on pseudonymisation and controller/processor obligations. Following these discussions, the Presidency has endeavoured to further redraft specific points of Chapter I to IV.

8. The Presidency attaches the text on the territorial scope, Chapter V (International transfers) and specific important items of Chapters I to IV mentioned above (…). The text set out in Annexes I and II reflects the outcome of the discussions during the Danish, the Cyprus, the Irish, the Lithuanian and the Hellenic Presidency.

9. Significant further progress has been achieved in the negotiation of the draft Regulation under the Greek Presidency. Discussions on the one-stop-shop mechanism are proceeding on the basis of indications provided by Ministers at the 2013 October and December JHA Councils.

II. Territorial scope and key principles of international transfers

10. During the January 2014 informal discussions of Athens, Ministers expressed their overall satisfaction with the provisions of the draft regulation on international transfers and with the territorial scope of the Regulation, highlighting the need to broadly ensure the application of Union rules to controllers not established in the EU when processing personal data of Union residents.

    Ministers also underscored the exceptional nature of the transmission of personal data to third countries or international organisations based on derogations (i.e. when not based on findings of adequacy/appropriate safeguards including binding corporate rules or contractual clauses) and the need to provide safeguards to ensure the fundamental rights and freedoms as regards the protection of personal data as enshrined in Article 8 of the EU Charter.

    As regards possible future new models (alternative) that could be envisaged for international transfers, the Presidency considers that these can and should inscribe themselves in the logic of the - multifaceted but yet coherent - system currently proposed, which relies on transfers based on adequacy findings, appropriate safeguards and derogations for which Ministers have given their support during the informal discussions in Athens. The current compromise is future-proof and provides sufficient possibilities to accommodate new models based on appropriate safeguards ensuring the protection of individuals whose data are transferred abroad.

III. Key provisions - Chapters I to IV

The four topics to be discussed address some of the key technological developments of recent years. In each case, the aim of the Presidency is to ensure that the full potential of the proposed Regulation is developed in a way that enhances trust in the EU single digital internal market.

Pseudonymisation

11. The pseudonymisation of personal data is a common operation in the digital world and is one of the most important means of achieving data protection in the context of a risk-based approach. For this reason pseudonymisation should be encouraged while such data remain personal data. Discussion at technical level has led to the insertion of "pseudonymisation" in the Regulation in order to limit the impact on the individual rights and strengthen data security. It will help striking the right balance between the protection of fundamental rights and freedoms of concerned individuals and the need of the public and private sector to process large amounts of data. An example of pseudonymisation would be the case where medical data from patients suffering from cancer go through a process of removal of directly identifying elements such as their names, and attributing randomly serial numbers to each patient, so that this resulting information could be used for medical research or public health purposes.

Portability of personal data

12. The aim of the right to data portability is to allow individuals to transfer their own personal data from one provider to another one when they decide to opt for another provider (e.g. transmission of an individual's data related to his or her work experience from general purpose social network to a professional career-oriented network). The discussions have shown the importance of the right to data portability to give control to individuals on their own data especially on the internet and to modernise the current framework. The Presidency has addressed the concerns expressed by some delegations by removing the public sector from the scope of this right and by refining its scope in order to avoid overburdening data controllers. The compromise ensures the protection of other concerned individuals and takes into account the need for technological neutrality.

Obligations of controllers and processors

13. Today service providers play a far more important role in the digital economy than in 1995. New technological developments, notably in cloud computing, call for the improvement and clarification of the role and obligations of controllers and processors (including sub-processors) in data processing. The Presidency has sought to clarify the relationship between controllers and processors, including through the inclusion of a reference to optional "standardised" contracts between controllers and processors. Discussions at technical level have shown that there is support for this.

Automated decision making based on profiling

13. The processing of personal data is absolutely essential to a knowledge-based economy. In the digital age many economic activities are based on the establishment and use of certain profiles. Thus internet advertising, which in itself is an important economic bedrock of the internet, is often based on the creation and use of certain profiles for marketing purposes. The establishment and use of customer profiles can also be used to protect customers, e.g. from credit card or other types of fraud in a digital environment.

However, processing intended to evaluate (i.e. analyse and predict) certain aspects relating to performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements (profiling) may entail severe risks for the rights and freedoms of the individuals. Under the 1995 Directive (Article 15) there is already a provision on the right of an individual not to be subject to decision which is based solely on automated processing and which produces legal effects concerning him or significantly affects him and in view of some of the above aspects. The decision in question could cover activities like automatic refusal of an on-line credit application without any human intervention. The focus of this provision is thus on avoiding that individuals are subject to automated decision-making without human intervention.

The current compromise does not introduce a specific regime governing profiling activities as such. It submits these activities to the general rules governing processing of personal data (legal grounds of processing, data protection principles) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases (Articles 33 and 34) or provisions concerning specific information to be provided to the concerned individual. The European Data Protection Board would have the possibility to issue guidance in this context.

The Presidency intends to ensure that the individual should be protected against decisions taken solely on the basis of automated processing, including profiling which produces legal effects concerning him or her or (which) severely affects him or her.

The current text seeks to prohibit the decision-making based on automated processing, namely (but not exclusively) through profiling, but not the creation and use of profiles as such.

Automated decision-making should be allowed if necessary for the entering and performance of a contract, on the basis of explicit consent of the data subject or when explicitly authorised by Union or Member State law, including for fraud and tax evasion prevention and monitoring purposes.

Profiling and automated decision-making based on special categories of personal data should only be allowed under specific conditions.

IV. Questions

The Presidency is aware that support for any issue is conditional in the sense that no part of the draft Regulation can be finally agreed until the whole text of the Regulation is agreed.

In view of the above, the Council is invited

A. *to discuss whether, following the discussions of the Informal Ministerial meeting in Athens, it confirms its broad support on the draft provisions as regards the territorial scope of the Regulation (Article 3(2)) (see annex I);*

B. *to discuss whether, following the discussions of the Informal Council in Athens, it confirms its understanding on the key principles of Chapter V (annex II) as a basis for the Working Party on Data Protection and Exchange of Information (DAPIX) to finalise technical discussions on this Chapter;*

C. *to confirm that the Working Party on Data Protection and Exchange of Information (DAPIX) should continue working on the basis of the progress achieved so far and finalise the work on:*

   1) *Pseudonymisation as an element of the risk-based approach (see annex III).*
   2) *Portability of personal data for the private sector (see annex IV)*
   3) *Obligations of controllers and processors (see annex V).*

D. *to discuss whether the draft Regulation, like Directive 95/46/EC, should*

   a. *limit itself to regulating automated decision-making namely (but not exclusively based on profiles that provide legal effects or significantly affect individuals; or*
   b. *should provide also for a specific regime regarding the creation and use of profiles?*

TERRITORIAL SCOPE

19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not, **(…)** which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union **(…)**.

21) The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union. In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

ANNEX II

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to **recipients in** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to **recipients in** another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

80) The Commission may **(…)** decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of participation in a suitable international data protection system established in third countries or a territory or a processing sector. **The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations.**

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. **The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.**

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. **They should relate in particular to compliance with the general principles relating to personal data processing, the availability of data subject's rights and effective legal remedies are available and the principles of data protection by design and by default.**

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for the protection of (…) reasons of public interest, for example in cases of international data exchange, either spontaneous or on request, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, or between competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. **In the absence of an adequacy decision or of appropriate safeguards, Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…).

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, **in particular on the level of protection in third countries or international organisations,** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

Article 4

Definitions

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(21) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

(…).

Article 41

Transfers with an adequacy decision

1. A transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…), data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…);
   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country, or to which an international organisation is subject, with responsibility for ensuring compliance with the data protection rules **including adequate sanctioning powers** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, **in particular** in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…).** The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

3a. *Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission* **in accordance with the examination procedure referred to in Article 87(2). (…)**

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3). **(…)**

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44. (…)The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards *in a legally binding instrument* with respect to the protection of personal data **or where the controller or the processor has obtained prior authorisation for the transfer by the supervisory authority in accordance with paragraph 5.**

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
   (a) binding corporate rules **referred to in** Article 43; or
   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority pursuant to paragraph 4; or

(e) an approved code of conduct pursuant to Article 38; or

(f) a certification mechanism pursuant to Article 39:

3. A transfer based on *binding corporate rules or standard data protection clauses* as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 (…), the controller or processor shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…).

5. Where, notwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor **(…)**shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).

5a. If the transfer referred to in paragraph 4 (…)is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority.*

Article 43

Transfers by way of binding corporate rules

1. The competent supervisory authority shall *approve binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they:
   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;
   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall **contain a description of** at least the following elements:
   (a) the structure and contact details of the group concerned and of each of its members;
   (b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
   (c) their legally binding nature, both internally and externally;
   (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35, including monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 41, of appropriate safeguards pursuant to Article 42, **or of binding corporate rules pursuant to Article 43** a transfer or a category of transfers of personal data to **a recipient or recipients in** a third country or an international organisation may take place only on condition that:
   (a) the data subject has consented to the proposed transfer, after having been informed **that** such transfers **may pose** *risks* due to the absence of an adequacy decision and appropriate safeguards; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, *where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. (…)

4. Points (a), (b), (c) **and (h)** of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the national law of the Member State to which the controller is subject. **Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…).

6a. (…)

7. (…).

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;
   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;
   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission **and supervisory authorities** shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VII

SECTION 3

EUROPEAN DATA PROTECTION BOARD

Article 66

Tasks of the European Data Protection Board[r]

(referred only the provisions that relate to international transfers)

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

   (cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to **in Article 41**;

   (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

   (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67

Reports

1. (…).

2 The European Data Protection Board *shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

_____

PSEUDONYMISATION

23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes. The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person.

Pseudonymised data, which could be attributed to a natural person only by the use of additional information, should be considered as information on an identifiable natural person, taking into account all the means reasonably likely to be used either by the controller or by any other person to identify the individual. The principles of data protection should also apply when an individual may be identified by the use of additional information, taking into account all the means reasonably likely to be used either by the controller or by any other person to identify the individual.

39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. **The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes can be regarded as carried out for a legitimate interest.**

45) If the data processed by a controller do not permit the controller to identify a natural person **(…)** the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. (…). However, the controller should not refuse to take **additional** information provided by the data subject **in order to** support the exercise of his or her rights.

Article 4

Definitions

For the purposes of this Regulation:

[...]

(3b) 'pseudonymisation' **means the** processing of **personal data in such a way that the data can** no longer **be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.**

Article 14 a

Information to be provided where the data have not been obtained from the data subject

4. Paragraphs 1 to 3 shall not apply where and insofar as:

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests; or

Article 23

Data protection by design and by default

1. Having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall (…), implement (…) technical and organisational measures appropriate to the processing activity being carried on and its objectives, including **pseudonymisation of personal** data, in such a way that the processing will meet the requirements of this Regulation and (…) protect the rights and freedoms of (…) the data subject.

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context**,** scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, including **pseudonymisation of personal** data, to ensure a level of security appropriate to these risks.

Article 32

Communication of a personal data breach to the data subject

3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if**:**

   a. the controller (…)has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption **(…)**; or

Article 38

Codes of conduct

1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(bb) the **pseudonymisation of personal** data;

_____

PORTABILITY OF PERSONAL DATA

51) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, where possible for what period, which recipients receive the data, what is the logic involved in any automatic data processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates. **To further strengthen data subject right of access to their own data, the data subject should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format.**

55) To further strengthen the control over their own data **(…), w**here the processing of personal data is carried out by automated means, the data subject should also be allowed to withdraw the personal data, which he or she has provided, **in a commonly used format** from one automated processing system and transmit those data, (…) into another **automated processing system.**

This **right** should apply where the data subject provided the personal data to the automated processing system, based on ~~their~~ his or her consent or in the performance of a contract. **It should not apply where processing is based on another legal ground** other than consent or contract. **By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of a official duty vested in the controller.**

Where, in a certain set of personal data, more than one data subject is concerned, the right to withdraw and transmit the data into another automated processing system should **be without prejudice to the requirements on the lawfulness of the processing of personal data related to another data subject in accordance with this Regulation**. **This right should also not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and** should **in particular not** imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. **(…)**

Article 18

Right to data portability

1. (…)

2. Where the data subject has provided personal data and the processing, (…) based on consent or on a contract, is carried on in an automated processing system [provided by an information society service], the data subject shall have the right to withdraw these data in a **commonly used format and** to transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn, **without prejudice to Article 17**.

2a. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights **in relation to the processing of the data in the automated processing systems**.

[2b. The right referred to in paragraph 2 shall not apply to processing on the basis of points (c), (d), (e) and (f) of Article 6(1).]

[3. The Commission may specify (…) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]

4. (…)

OBLIGATIONS OF CONTROLLERS AND PROCESSORS

63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures **which** will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated by means of adherence of the processor to a code of conduct or a certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act binding the processor to the controller, setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are either adopted by the Commission or by a supervisory authority in accordance with the consistency mechanism and adopted by the Commission, or which are part of a certification granted in the certification mechanism. If a processor processes personal data other than as instructed by the controller, the processor should be considered as a controller in respect of that processing. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; in that case the processor should implement appropriate measures to ensure the security and confidentiality of the personal data and should not actively process the personal data anymore.

Article 26

Processor

1. (…)The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…).

1a. The provision of sufficient guarantees referred to in paragraphs 1 and 2a may be demonstrated by means of adherence **of the processor** to a code**s** of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller, setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects and stipulating in particular that the processor shall:

(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject and in such a case, the processor shall notify the controller unless Union law or the law of the Member State to which the processor is subject prohibits such notification on important grounds of public interest;

(b) (…)

(c) take all (…) measures required pursuant to Article 30;

(d) determine the conditions for enlisting another processor (…), such as a requirement of specific prior consent of the controller;

(e) as far as (…) possible, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;

(f) determine how the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) return or delete, at the choice of the controller, the personal data after the completion of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; in that case the processor shall implement appropriate measures to ensure the security and confidentiality of the personal data;

(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article.

2a. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the other processor shall provide sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation.

2aa. Where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, in a contract or other legal act the same obligations shall be imposed on that other processor as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2.

2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2aa may be based, in whole or in parts, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.

2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and in accordance with the examination procedure referred to in Article 87(2).

2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and in accordance with the consistency mechanism referred to in Article 57.

3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.

4. (…)

5. (…)