



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 24 April 2013**

**8825/13**

---

**Interinstitutional File:  
2012/0011 (COD)**

---

**LIMITE**

**DATAPROTECT 49  
JAI 312  
DAPIX 74  
MI 320  
FREMP 43  
DRS 79  
CODEC 895**

**NOTE**

---

from:	Presidency
to:	COREPER
Prev. No.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219 16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 274
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) - Specific issues

---

**I. General**

1. The comprehensive data protection package was adopted by the Commission on 25 January 2012. This package comprises two legislative proposals based on Article 16 TFEU, the new legal basis for data protection measures introduced by the Lisbon Treaty.

The first proposal, for a General Data Protection Regulation, seeks to replace the 1995 Data Protection Directive<sup>1</sup>. The second proposal, for a Directive of the European Parliament and of the Council on data protection in the field of police and judicial cooperation in criminal matters, is intended to replace Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters<sup>2</sup>. Even though Article 16 TFEU also offers a legal basis for adopting data protection measures applicable to EU institutions, the Commission has chosen to propose new measures only for the Member States.

During the first three months of its term, the Presidency, building upon the work accomplished by the Danish and the Cyprus Presidency, has finalised a first examination of the entire proposal and has conducted in depth discussions of certain important aspects of the Regulation. During the month of April, the Presidency intends to finalise the second examination of Chapters I to IV of the draft Regulation.

2. The second examination has allowed the Presidency to identify a number of pivotal issues, the resolution of which requires political guidance. The following items are submitted to COREPER for consideration:
  - Material scope
  - Territorial scope
  - Definition of consent
  - Data processing principles
  - Freedom of expression and access to public documents.

---

<sup>1</sup> OJ L 281, 23.11.1995, p. 31.

<sup>2</sup> OJ L 350, 30.12.2008, p. 60.

## II. Material scope

3. Article 2 of the draft regulation defines its material scope. Under paragraph 2, certain areas of processing of personal data are excluded from the scope of the Regulation. A number of these exclusions have turned out to be particularly problematic.

### *Activities outside the scope of Union law*

4. The first is the exclusion of personal data processed in the course of an activity which falls outside the scope of Union law. While many Member States sought clarity in relation to such activities, a listing of such excluded areas was not possible in light of relevant Treaty provisions and related case law. The Presidency draws attention to recital 14, which refers to this matter.

### *EU institutions, agencies bodies and offices*

5. The second is the exclusion of personal data processed by '*Union institutions, bodies, offices and agencies*'. The consequence of this exclusion is that Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data<sup>3</sup> remains unaffected. In the course of the discussions in the Working Party on Information Exchange and Data Protection (DAPIX) it has become clear that Member States take issue with the point of view of the Commission that there is a more pressing need to reform the data protection rules applicable to Member States than there is with regard to the data protection rules applicable to the EU institutions.
6. The Presidency sees different avenues for accommodating the widespread concern regarding this difference in treatment between the Member States and the EU institutions.
7. The most radical option would be to amend Regulation No 45/2001 through this Regulation, which would substantially alter the scope of this instrument. So far no delegation has requested this and neither does it seem feasible to extend the scope of the Commission proposal to cover EU institutions.

---

<sup>3</sup> OJ L 8, 12.1.2001, p.1.

8. A second option, which has been argued for by several delegations, is to delete point (b) of paragraph 2 of Article 2, as a consequence of which 'Union institutions, bodies, offices and agencies' would no longer be excluded from the scope of the Regulation. This would imply that these institutions, bodies, offices and agencies, most of which are currently governed by their own specific data protection rules, would also become bound by the General Data Protection Regulation. Regardless of the political expedience of such a solution, this would create a very complicated legal situation with legal uncertainty resulting from the coexistence of specific data protection regimes (*leges speciales*) with a general data protection rule (*lex generalis*), with the former predating in many cases the latter. In many cases these specific data protection regimes differ from that proposed in the General Data Protection Regulation and even in its recent proposal for a Europol Regulation, the Commission has proposed a data protection regime which, at least on some points, differs from that in the General Data Protection Regulation. The Presidency thinks that this legal uncertainty should be avoided.
9. Therefore other alternatives have been looked into by which it would be ensured that the data protection rules from the draft General Data Protection Regulation will in the future also be applied to 'Union institutions, bodies, offices and agencies'. The Commission could be invited to give an undertaking – through a declaration to be made upon the adoption of the Regulation – to propose new data protection rules for the EU institutions within for example six months following the adoption of this Regulation. The Presidency deems that such a declaration should be combined with a recital along the lines of recital 14a) which would mean that the goal of adapting Regulation (EC) No 45/2001 is enshrined in the preamble of the Regulation.

### *The household exemption*

10. A third exclusion from the material scope of the draft Regulation which has provoked a considerable amount of discussion concerns the so-called household exemption. Article 2(2)(d) of the Commission proposal excludes processing of personal data *'by a natural person without any gainful interest in the course of its own exclusively personal or household activity'*. Under the 1995 Directive, the processing of personal data *"by a natural person in the course of a purely personal or household activity"* has been excluded from its scope. As the criterion of lack of 'gainful interest' and the reference to 'exclusively' gave rise to interpretation difficulties and controversy, both have been deleted and the current draft now refers to processing *'in the course of a personal or household activity'*. Whilst most delegations appear to find this acceptable, some delegations would prefer to build on the notion of a 'consumer', for example *'by a natural person acting for purposes which can be regarded as outside his trade or profession'*.
11. The distinction between these two alternatives is especially important for processing in the online world which, since the adoption of the 1995 Data Protection Directive, has experienced an exponential development. Today, individuals voluntarily supply large amounts of personal data when purchasing goods and services on the Internet and using other online services. Moreover, many actively publish and share personal data about themselves and, frequently, about other family members and friends on social networking sites.
12. In the Lindqvist case<sup>4</sup> the ECJ clarified the meaning of the household exemption and held that the communication of personal data to an indefinite number of persons by a private individual is not covered by the household exemption (even though the communication was not for financial gain). With regard to social networking sites, this implies that individuals who use social networking sites with a limited number of contacts come within the household exemption. However, if a person used a social networking site for the purposes of a gainful interest he/she would come within the scope of the Regulation.

---

<sup>4</sup> Case C-101/01, judgment of 6 November 2003, ECR, p. 12971.

13. The Commission proposal would most probably not affect this ECJ interpretation of the household exemption. It would imply that the processing of personal data on the internet in many cases is not covered by the General Data Protection Regulation, but when the processing activities are commercial in nature, for example, if an individual decided to sell a musical instrument or rare book online, he or she would fall outside the scope of the household exemption and the provisions of the Regulation would apply.
14. If one were to phrase the household exemption in such a way that it would refer to processing 'outside trade or profession', this would imply that the Regulation would never apply to individuals acting in a private capacity, even if they pursue a gainful interest, as long as they were not acting in a commercial capacity (trader).
15. With a view to reaching a broadly acceptable solution, the Presidency has also redrafted recital 15 in order to highlight the fact that social networking and online activity carried on in the context of personal and household activity are also covered by the exclusion. The Presidency is therefore of the opinion that this strikes a good balance between the situation as it exists under the 1995 Data Protection Directive and the new realities of the digital online world .

***The law enforcement exemption***

16. The 1995 Data Protection Directive excludes data processing 'in the course of State activities relating to the area of criminal law'. In 2008 the Council adopted a Framework Decision on data protection in the framework of police and judicial cooperation in criminal matters<sup>5</sup>. The current Commission proposal excludes processing

*'(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'*

---

<sup>5</sup> Council Framework Decision of 27 November 2008 on the protection of personal data in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p.60.

17. This point (e) of paragraph 2 of Article 2 of the draft Regulation marks the delimitation with the proposed Directive on data protection in the field of police and judicial cooperation in criminal matters. Several delegations have argued that this 'boundary marker' should be moved and that also other activities related to ensuring public order and security should be exempted from the Regulation and brought within the scope of the proposed Directive.
18. The main argument in favour of such a change is that it would allow all Member State authorities involved in some kind of law enforcement activity to be subject to a single data protection regime, namely that of the Directive. Especially in the area of prevention it may be very hard to distinguish activities aimed at preventing or limiting certain risks (e.g. public disorder) from the prevention or even detection of criminal offences. From a practical point of view it would in some instances indeed be very onerous on public authorities if they have to examine which data protection regime they are subject to when exercising certain powers, especially at moments when it may not be clear whether criminal activity is involved or not.
19. The Commission has argued that Article 21 of the draft Regulation already allows Member States to adopt national laws to restrict the scope of some obligations and rights of the Regulation as necessary and proportionate measures to safeguard public order. This may allow Member States to use the transposition legislation of the future 'police/criminal' Data Protection Directive to specify the data protection regime of authorities involved in maintaining public security. However, this would probably only go some way towards accommodating delegations concerns as Article 21 only allows for restrictions of the obligations and rights flowing from parts of the Regulation (Articles 5, 11 to 20 and 32), but does not allow Member States to provide for restrictions regarding the obligations of controllers (in this case the public authorities tasked with maintaining public order) or the role of data protection authorities. Even an extensive use of Article 21 will not detract from the fact that point (e) of paragraph 2 of Article 2 of the draft Regulation, as proposed by the Commission, implies two data protection regimes for public authorities which have both a role in maintaining public order and in the prevention, investigation, detection or prosecution of criminal offences, as is the case for many police authorities.

20. Therefore, subject to the views of the Council Legal Service, the only way to accommodate this concern may be to extend the exemption of point (e) of paragraph 2 of Article 2, for example by adding '*and for the maintenance of public order*'. It has to be acknowledged, however, that this may be viewed as risking an extension of the scope of what is understood to be police and judicial cooperation in criminal matters and that this may considerably complicate the transposition of the of the future 'police/criminal' Data Protection Directive notably by those Member States bound by Protocols 21 and 22 to the T(F)EU .

***Other Matters***

21. Several Member States expressed their concerns in relation to the application of the proposed/draft Regulation to the courts. The Presidency draws attention to the new recital 16a), which clarifies that, in order to safeguard the independence of judges in the performance of their judicial functions, the competence of supervisory authorities should not cover the activities of courts when acting in their judicial capacity and acknowledges the role of Member State law in relation to the specification of processing operations and processing procedures by courts and other judicial authorities.
22. Several Member States referred to the role of private entities in the field of law enforcement and requested recognition of this in the text. The Presidency draws attention to the amended recital 16 which recognises that certain obligations and rights under the Regulation may be restricted by law in such cases e.g. in the framework of anti-money laundering activities pursuant to Article 21.



### III Territorial scope

23. The draft Regulation is very ambitious in its territorial scope in that it would not only apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union but also, under paragraph 2 of Article 3, 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".*

24. Paragraph 2 is novel as compared to the 1995 Data Protection Directive. The Presidency has endeavoured to further clarify and delimit the meaning of point (a) in recital 20, by including reference to elements (inspired by the ECJ *Alpenhof* case law<sup>6</sup>) which should help to determine whether a particular offer of goods or services is geared towards EU residents. Point (b) of Article 3(2) is more problematic, notwithstanding the qualification added by the Presidency that the *'behaviour takes place within the European Union'*. This aspect of the Commission proposal appears to be aimed primarily at online tracking of consumer profiles of EU data subjects on the internet.

25. Many delegations doubt the enforceability of this provision, which imposes all the obligations of the General Data Protection Regulation on controllers outside the EU which offer goods or services or even merely track the online behaviour of data subjects within the Union. This applies in particular to the obligation in Article 25 to appoint a representative in the Union. It may indeed be doubtful if and to what extent these controllers will be aware of and be willing to apply EU data protection rules. Of course one may argue that the application of a fundamental right to data protection should not be dependant on the territory from which the controller operates, but this does not detract from the practical enforcement difficulties which can be expected to arise.

---

<sup>6</sup> Cases C-585/08 and C-144/09, judgment of 7 November 2010, ECR, P. I-12527.

26. The Presidency draws attention to the revised text of recitals 20 and 21 which seek to clarify the territorial scope of the draft Regulation.

### III. Definition of consent

27. Data subject consent is one of the most important bases for lawful data processing (Article 6(1)(a)). The Commission proposal defines the data subject's consent in a strict way as *'any freely given, specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'* (Article 4(8)).

Recital 25 clarifies that what is required is *'a statement or ... a clear affirmative action by the data subject, ... including by ticking a box when visiting an Internet website'* and that silence or inactivity should not constitute consent. Article 7 sets out further conditions for consent. Consent is also referred to in Article 8 (regarding the processing of personal data of a child) and Article 9(2) (regarding the processing of special categories personal data).

28. The proposed definition goes beyond the requirements of the 1995 Data Protection Directive. The Commission argues that the new definition merely clarifies the 1995 Directive and that the latter does not allow for silent or implicit consent. Many delegations view the additional requirements for 'explicit' consent in all cases as unrealistic and have queried the added value. The requirement for explicit consent has met with objections by Member States, who have argued that in reality this may lead to 'click fatigue'. In particular on the internet, the mere ticking of boxes could result in a situation where, in case of litigation, the controller rather than the data subject is protected as the consent would meet all the legal requirements.
29. It appears therefore preferable to replace the word 'explicit' by another word, such as 'unambiguous' in the case of personal data other than the special categories referred to in Article 9. The explicit consent threshold should be maintained in respect of the latter.

30. Many Member States objected to paragraph 4 of Article 7 on the grounds that it would create legal uncertainty and doubt. The Presidency has therefore dropped this paragraph from Article 7. The revised recital 34 provides that consent may not be valid where, in the circumstances of a specific case, there is a clear imbalance between the parties and this makes it unlikely that consent has been freely given.

#### **IV. Data processing principles**

31. Article 5 sets out the main data protection principles applicable to all forms of data processing within the scope of the Regulation. These principles are to a significant extent copied from Article 6 of the 1995 Data Protection Directive, and have been redrafted during the discussions in the DAPIX Working Party. A new principle of data security and confidentiality has been added (Article 5 (ee)).
32. Any agreement on the drafting of these principles is without prejudice to further discussion on specific regimes for the processing of data for historical, statistical or scientific purposes and for archiving purposes.

#### **V. Articles 80 and 80a: freedom of expression and access to public documents**

33. The right to the protection of personal data co-exists with other fundamental rights, notably the right to freedom of expression which is also included in the Charter. The relationship between these rights is recognised in Article 80. However, many Member States consider that the references to exemptions or derogations from data protection rules in this article may give a false impression that freedom of expression ranks lower than protection of personal data.
34. Many Member States are also unhappy with the reporting requirements in paragraph 2 which, at least in some cases, would require the submission of national constitutions, and associated constitutional case law, to the Commission for vetting.
35. In light of these concerns, the Presidency has redrafted Article 80 to make it clear that the law of Member States shall contain rules to reconcile the right to protection of personal data with the right to freedom of expression.

36. Recital 18 of the draft Regulation allows the principle of public access to official documents to be taken into account when applying its provisions. However, the Regulation does not contain a corresponding article.
37. In order to meet the concerns of several Member States in relation to this matter, the Presidency has drafted Article 80a which provides for the disclosure of personal data in official documents in the public interest. Such disclosure may be in accordance with Union law or Member State law which reconciles public access to such documents with the right to the protection of personal data pursuant to the Regulation. The text of recital 18 has also been expanded.

## **VI. Conclusion**

38. *In view of the above, the Presidency invites the COREPER to agree that:*
- 1) *The Commission should be invited to give an undertaking – through a declaration to be made upon the adoption of the regulation – to propose new data protection rules for the EU institutions for example within six months following the adoption of this Regulation. Such a declaration should refer to recital 14a) of the draft Regulation;*
  - 2) *Regarding the material scope of the Regulation, the annexed version of Article 2 should be agreed; read together with the annexed versions of recitals 14 to 16a;*
  - 3) *Regarding the territorial scope of the Regulation, the annexed version of Article 3 should be agreed; read together with the annexed versions of recitals 19 to 22;*
  - 4) *Regarding consent, the definition of in Article 4(8) and Articles 7 and 9(2)(a) as set out in the annex; read together with the annexed version of recitals 25 and 31 to 34 should be agreed;*

- 5) *The data protection principles as set out in the annexed version of Article 5 should be agreed; read together with the annexed version of recital 30 and subject to future changes regarding historical, statistical or scientific and archiving purposes;*
  - 6) *The relationship between this Regulation and freedom of expression should be governed by the annexed version of Article 80; and*
  - 7) *The relationship between this Regulation and the right of access to documents should be governed by the annexed version of Article 80a, read together with the annexed version of recital 18.*
-

.....

- 14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, taking into account Articles 3 to 6 of the Treaty on the Functioning of the European Union (...) or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
- 14a) This Regulation does not cover the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001<sup>7</sup> and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation (...).
- 15) This Regulation should not apply to processing of personal data by a natural person, in the course of a (...) personal or household activity, (...) and thus without any connection with a professional or commercial activity. Personal and household activities include social networking and on-line activity undertaken within the context of such activities. However, this Regulation should (...) apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.
- 16) 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 as well [as for the purposes of maintaining public order], and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYYY).

---

<sup>7</sup> OJ L 8, 12.1.2001, p. 1.

When processing of personal data by (...) private entities falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering (...).

- 16a) While this Regulation applies also to the activities of courts and other judicial authorities, Union or Member State law could, within the limits of this Regulation, specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks.
- 17) Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation. This Regulation should therefore be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.
- 18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body may be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject, and the data subject's legitimate interests or fundamental rights and freedoms in the particular case are not prejudiced.

- 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, or to the monitoring of the behaviour of such data subjects, 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, or to the monitoring of the behaviour of such data subjects.
- 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.

.....

25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

.....

30) Any processing of personal data should be lawful and fair. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant (...) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (...).

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.

- 31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.
- 32) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that, and the extent to which, consent is given.
- 33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.
- 34) In order to safeguard that consent has been given freely, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. (...)

*Article 2*

***Material scope***

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
  - (a) in the course of an activity which falls outside the scope of Union law (...);
  - (b) by the Union institutions, bodies, offices and agencies;
  - (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;
  - (d) by a natural person (...) in the course of (...) a personal or household activity;
  - (e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [and for the maintenance of public order.]
3. (...).

*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.

*Article 4*

***Definitions***

For the purposes of this Regulation:

....

- (8) 'the data subject's consent' means any freely given, specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

*Article 5*

***Principles relating to personal data processing***

1. Personal data must be:
- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
  - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83;
  - (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed (...);
  - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed (...) for historical, statistical or scientific (...) purposes pursuant to Article 83 (...);
  - (ee) processed in a manner that ensures appropriate security and confidentiality of the personal data;
  - (f) (...).
2. The controller shall be responsible for compliance with paragraph 1.

*Article 7*

***Conditions for consent***

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that consent was provided by the data subject .
2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (...) from the other matters.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (...).
4. (...).

*Article 9*

***Processing of special categories of personal data***

.....

2. Paragraph 1 shall not apply if one of the following applies:
  - (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

*Article 80*

***Processing of personal data and freedom of expression***

1. Member State law shall provide for rules (...) in order to reconcile the right to the protection of personal data pursuant to this Regulation with the rules governing freedom of expression, including artistic and or literary expression.
2. (...).

*Article 80a*

***Processing of personal data and public access to official documents***

Personal data in official documents held by a public authority may be disclosed by the authority in accordance with Union law or Member State law to which the public authority is subject in order to reconcile public access to such official documents with the right to the protection of personal data pursuant to this Regulation

---