Opinion no. 35/2012 of 21 November 2012[1]

Subject: Opinion of the CPP's accord on the draft 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[2]

The Commission for the Protection of Privacy;

Having regard to the Belgian Act of 8 December 1992 *on the protection of privacy in relation to the processing of personal data* (hereinafter DPAct), in particular article 29;

Having regard to the report by Mr Willem Debeuckelaere, President and Mr Stefan Verschuere, Vice-President;

Has issued the following opinion on 21 November 2012:

I. INTRODUCTION

[1] Unofficial English translation provided by the secretariat of the Belgian data protection authority.

[2] COM (2012)11 final

1. Subject of the present opinion

1. On 25 January 2012, the European Commission (EC) presented its proposal for an updated legal framework for data protection in the European Union (Data Protection Package)[3]. The new protection scheme envisaged consists of two legislative proposals:

   - A 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[4] (hereinafter called "the draft regulation") and;

   - A 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[5].

2. The Commission for the Protection of Privacy (hereinafter CPP) has examined these proposals and discussed them during its sessions on 8 February, 29 February, 14 March, 21 March, 11 April and 18 April, 25 April, 23 May , 17 October and 21 November 2012.

3. The present opinion of the CPP's own accord concerns, however, only the draft regulation. It is a first analysis – mainly by article – and the CPP reserves the right to issue, if any, an additional opinion at a later time.

4. The CPP would like to draw the attention to the fact that the present opinion is based on the French and Dutch texts of the draft regulation. This is mentioned because the CPP has found that there are some differences in the text depending on the language in which it was written[6].

2. Background

[3] COM (2012)9 final.

[4] COM (2012)11 final

[5] COM (2012)10 final

[6] As an illustration: The last sentence of Article 47.3 has a different meaning in French and Dutch:

-"Les membres de l'autorité de contrôle (…), n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

- De leden van de toezichthoudende autoriteit (…) verrichten gedurende hun ambtstermijn geen andere al dan niet bezoldigde beroepswerkzaamheden".

A. The communication of the European Commission of 4 November 2010

5. In a communication of 4 November 2010 entitled " *A comprehensive approach on personal data protection in the European Union*", the European Commission sums up the objectives of the reform[7]:
    - Strengthening individuals' rights: increasing transparency for data subjects, enhancing control over one's own data, ensuring informed and free consent, protecting sensitive data, making remedies and sanctions more effective, increasing the number of awareness-raising activities to make data subjects aware of their rights;
    - Enhancing the internal market dimension, for example by reducing the administrative burden, enhancing the data controllers' responsibility by encouraging self-regulatory initiatives and exploring EU certification schemes;
    - Revising the data protection rules in the area of police and judicial cooperation in criminal matters (directive proposal);
    - Taking the global dimension of data protection into account: clarifying and simplifying the rules for international data transfers;
    - Strengthen the institutional arrangement for better enforcement of data protection rules: increase the independence; strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities and improve the cooperation and coordination between them.

6. The explanatory memorandum to the draft regulation formulates the motivations for the initiative and the EC objectives as follows: "*The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.*"[8]

B. Earlier positions of the CPP

[7] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union; COM (2010)609 final

[8] COM (2012)11 final

a) CPP contribution to the public consultation of the European Commission (November 2010 – January 2011)

7. In its letter of 14 January 2011 – which constitutes a contribution to the public consultation following the aforementioned Communication of 4 November 2010 – the CPP submits 9 comments to the European Commission. The first comment concerns the choice of instrument: directive or regulation. The CPP recalls the need to respect the subsidiarity and proportionality principles[9] when making this choice. In consequence, the CPP isolates "multinational and transnational" data processing operations – data processing operations that are carried out in a similar manner across the borders of Member States or carried out by a single controller (multinational) in different Member States – for which a harmonised European set of rules at the highest level seems appropriate.

8. For the same processing operations the CPP is in favour of the creation of a European Data Protection Authority. This Authority would handle trans-/international[10] issues at European level without interfering with the internal organisation of the public authorities of a Member State. The CPP also called for a unique European notification system for European multinationals, but this comment is no longer relevant because the draft regulation does away with all prior notifications to the Data Protection Authority.

9. The CPP also mentions in this letter of 14 January 2011 to the European Commission that the new legal framework should promote (1) the function of Data Protection Officer as well as (2), in the context of increasing cross-border data flows, the mechanism of binding corporate rules (BCR) and that of mutual recognition as applied by a number of Data Protection Authorities in the Union[11].

[9] Minimum explanation of these principles: the principle of subsidiarity allows the execution of a competence conferred to the Union: it is a condition for the entry into force of the competence. See Article 5.1 and 5.2 of the Treaty on European Union (TEU):1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.(art.5.3.): Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

[10] Swift, Google, Facebook…

[11] Mutual recognition is an agreement that was concluded between different authorities to accelerate the European cooperation procedure for BCR. According to this agreement, once the lead authority is satisfied that the BCR meet the requirements determined in the working documents and its analysis has been checked by two other different authorities, the other participating authorities accept that this analysis constitutes a sufficient basis for their own national authorisation or approval of the BCR, or to issue a favourable opinion to the organism that has to issue the authorisation.

10. With respect to genetic data, the CPP emphasises their extreme sensitivity. The CPP believes that the processing should be limited to health care and scientific research or forensic medicine. Any processing operation in a contractual, political, social or commercial context should be excluded.

11. The CPP favours the introduction of mandatory data protection impact assessments since all effective and proportionate security measures should be based on the risk that is caused by data processing. These measures should allow for reasonable risk management without obstructing efficient and effective services to the public and enterprises, or without undermining the proper functioning of the latter or the public services.

12. Based on the knowledge acquired during the organisation of the "Privacy and Research: from Obstruction to Construction" conference the CPP makes several recommendations to the European Commission originating from the CPP's conclusions, which are meant to safeguard the necessary protection of data of research subjects, as well as the legitimate interests of the researchers. Clarifications with respect to the application of the rules on deceased persons and clarifications of the conditions under which research can be carried out in Europe and with respect to invoking other legal grounds than the authorisation are, amongst others, part of the formulated suggestions.

b) Hearing of the CPP Presidency by the Justice Committee of the Belgian House of Representatives

13. A year later at the beginning of March 2012, the CPP Presidency draws the attention of the Justice Committee of the House of Representatives to the choice made by the European Commission to regulate all data processing operations through a regulation (with the exception of "police" and "justice" data processing operation which are covered by the proposal for a directive).

14. In general the CPP warns the Belgian legislator for the important changes caused by the regulation after its adoption. The CPP is especially concerned about the fate of the existing sector committees (for example Social Security and Health Sector Committee, Federal Government Sector Committee, Statistic Supervisory committee and National Register Sector Committee) with regard to their prior authorisation power, because the regulation limits the cases in which prior authorisation has to be requested from the Data Protection Authority (article 34). The mechanism of authorisations granted by the aforementioned sector committees does not appear to have been established in the provisions of the draft. Similarly,

the CPP has questions about the future use (authorised or unauthorised) of the National Register number.

15. In order to support these considerations the CPP asks the Belgian House of Representatives to exercise its competence of political oversight, granted to the House since the Treaty of Lisbon by article 6 of Protocol no. 2 on the application of the principles of subsidiarity and proportionality, annexed to the Treaty[12].

16. On 20 March 2012 the CPP's president, vice-president and commissioner B. De Schutter were heard by the Justice Committee of the Belgian House of Representatives[13].

17. In conclusion of its opinion on subsidiarity the Justice Committee of the Belgian House of Representatives takes the following position:

Regarding subsidiarity

- The cross-border dimension of data protection, combined with increased internationalisation and the omnipresent internet justifies taking action at European level;
- Member States should be able to transpose the European rules in their own legal system at their discretion;
- The choice of a regulation raises objections regarding subsidiarity because by opting for a regulation, which is directly applicable in national legal systems and does not need further transposition into these systems, the European Commission ignores the existing practice and characteristics specific to the organisation of data protection in Belgium;
- A directive is desirable, a regulation can only be used for certain specific subjects for which Member States support the use of a regulation (like data exchange with countries outside the EU);
- The European Commission's competence to suspend decisions of Data Protection Authorities is regarded as excessive (outside its scope); strengthening the European Data Protection Board – EDPB is preferred;
- Pursuant to article 62 of the draft regulation the European Commission would have greater powers with respect to the elaboration of implementing legislation. The regulation, however,

[12] Article 6 of Protocol no. 2: *"Any national Parliament or any chamber of a national Parliament may, within eight weeks from the date of transmission of a draft legislative act, in the official languages of the Union, send to the Presidents of the European Parliament, the Council and the Commission a reasoned opinion stating why it considers that the draft in question does not comply with the principle of subsidiarity.(…)"*

[13] 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 COM (2012) 0011; 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 COM (2012) 0010, opinion on subsidiarity of 6 April 2012, on behalf of the Justice Committee by R. Landuyt, Belgian House of Representatives, Parl. Doc. DOC 53 2145/001, p. 13-16. (No English version)

should already be as complete as possible in order to ensure the involvement of all actors, the European Parliament and the Council.

Regarding proportionality

- The existing personal data processing operations of the public sector would be influenced or changed as a whole by the draft regulation (supervisory mechanism of the Sector Committees);
- If the proposed regulation is approved, authorisations issued by Sector Committees prior to the processing of some data would no longer be allowed;
- Member States should determine by law which data processing operations require prior authorisation;
- One might wonder whether the use of a unique means of identification, like the National Register number, could become problematic: Member States should be able to determine the conditions in national law under which a national identification number or any other general means of identification may be used for data processing purposes;
- The regulation should also be applicable to the European institutions.

II. ANALYSIS OF THE DRAFT REGULATION BY ARTICLE

1. Territorial scope (article 3)

18. Pursuant to article 3.1 the draft 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. In the case where a controller established outside the EU makes an appeal to a processor established inside the EU, the CPP believes that it should be clarified whether only the activities of the processor are subject to the application of the draft regulation, or whether also the controller is subject to all the obligations determined by the draft regulation.

19. Article 3.2 aims at the application of the draft regulation in cases where the controller is not established in the Union. The fact that the data processing is linked to the offering of goods or services to data subjects resident in the Union (or involves monitoring their behaviour), is in that case the criterion for the territorial scope of the draft regulation.

20. The criterion of "equipment" used by Directive 95/46/EC (article 4.1.c) has frequently led to interpretation issues and the new criterion aims to avoid these difficulties while still protecting European citizens in a more targeted manner. It would be nevertheless useful to clarify the concept "offering of goods or services" in order to limit this to those situations where goods

are not easily obtainable for European citizens, but where the offering of goods or services is clearly addressed to them, which results for example from the use of domain names by EU Member States, from the fact that special delivery options are provided and/or from the fact that the offer takes into account the language/culture/traditions/practices of a certain Member State etc. (so-called "target approach"). This is done to avoid that every foreign commercial website is part of the scope of the draft regulation.

2. Definitions (article 4)

A. General observation

21. The CPP wonders why the definitions are not mentioned earlier than in article 4 of the draft regulation. Articles 1 to 3 use many notions which are not defined until article 4. The CPP believes that the instrument would be drawn up more logically if the section on definitions was incorporated in the first article.

B. Personal data and data subject

22. The CPP is in favour of the adjustment of the definitions for "personal data" and "data subject' and in particular of the specification that account should be taken of all the means that are reasonably likely to be used to identify the data subject, either by the controller or by someone else. This clarification was provided for in preamble 26 of Directive 95/46/EC and is now introduced in the definition itself, which provides for more clarity and legal certainty.

C. Data relating to health

23. The definition of article 4.12, has to be read in the light of preamble 26[14] which provides for a very broad definition of the concept: not only are data relating to physical or mental health concerned but also all the information on providing health care services to a person (like patient registration for care provision, information on payments).

24. The CPP believes that the definition proposed by the draft regulation is (far) too broad and does not take sufficient account of the numerous contexts in which the processing of such

[14] Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

data can occur, nor does it take sufficient account of the intended purpose of the data processing operation. This definition threatens to have undesirable, far-reaching consequences. As an illustration:

a. Video footage of surveillance cameras shows a person with a broken leg. On the basis of the definition in the draft regulation this is data relating to health.
b. A public service is authorised to grant tax reductions or other social benefits to persons with a disability. The fact that this public service stores in its databases that a person belongs to this category (without specifying the disability), is sufficient to claim that this service processes data relating to health pursuant to the draft regulation.

25. Finally, in the Dutch text, article 4.12 (definitions) uses the term "gegevens over gezondheid", but the rest of the Dutch draft regulation regularly uses the formulation "gegevens betreffende de gezondheid". A uniform terminology/translation should be proposed.[15]

D. Main establishment

26. In case the data processing takes place as part of the activities of a controller or processor established in several Member States, the draft regulation states that only the authority located in the same location as the main establishment is regarded as the competent authority (see below).

27. The draft regulation also provides for a criterion of main establishment for processors, and here it concerns the location of the central administration in the Union (article 4.13, in fine).

28. The CPP has some reservations about this because there is no certainty that a central administration, such as the registered office or "headquarters" of a group of enterprises acting as processor, is actually involved in the data processing or the agreement that binds the processing enterprise to the controller. Similar to what the draft regulation establishes for controllers, the designated competent authority for processors should be as close as possible to the available information (location where data processing takes place or technical or organisational decisions on the processing are taken) and legal responsibility (person legally bound to the processing agreement). Assuming that the central administration (or headquarters) has no knowledge of the processing agreement and is in no way involved in the execution of this agreement, the competent authority will nonetheless have to consult its colleagues in order to gain information about the agreement.

[15] Translator's note: the English version of the draft regulation mostly uses the formulation 'data concerning health', only preamble 26 uses a diferent formulation: 'data relating to health'.

E. Binding corporate rules

29. The CPP appreciates the explicit recognition of binding corporate rules. It should, however, be ensured that this solution can also be applied to enterprises that are not established in the Union but are nevertheless obliged under the draft regulation to provide for adequate safeguards in the context of data transfers originating from the European Union (see article 4.17)[16].

F. Children

30. Preamble 29 clarifies that "*to determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child*". Since most EU Member States have ratified the Convention on the Rights of the Child, the choice of this referential definition seems "democratically" relevant[17]. According to article 4.18 a child is defined as "any person below the age of 18 years". However, the full text of the UN convention clarifies "unless under the law applicable to the child, majority is attained earlier". Consequently, preamble 29 and the definition of the child as mentioned in article 4.18 should be made more coherent.

31. An age-based definition has the advantage of legal certainty. Still, the CPP is of the opinion that the random determination of age (age of majority) with respect to the protection of personal data is difficult to reconcile with the reality of use, for example of the internet, by (sometimes very) young people. In analogy to what has been provided in *recommendation Rec(2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes* the CPP either recommends informing, consulting children and taking into account their desires from a certain age or gradually involving them in the decisions that have to be taken for example with respect to the exercise of their rights, depending on their power of judgment. This approach reflects the CPP's aim of encouraging young people to adopt a well-informed, responsible and respectful (of themselves and others) attitude when using information and communication technologies[18].

[16]The Model Clauses 2010/87/EU provide for example a legal solution for the data transfers to enterprises that are established in third countries and act as a processor. It should be avoided that binding corporate rules for processors can only be offered to enterprises established in the Union while they can make use of Model Clauses.

[17] Belgium ratified the International Convention on the Rights of the Child in 1991.

[18] See in this context Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 February 2009, WP 160

3. Principles relating to personal data processing (article 5)

32. Although the CPP fully supports the principle that personal data have to be adequate and not excessive in relation to the purposes for which they are processed (the existing proportionality principle), the CPP believes that the minimisation principle in article 5.c goes too far. This principle implies that the data processed must be limited to the necessary minimum and that it must be verified if the purposes could not be achieved without personal data processing. Such a principle is too restrictive in the eyes of the CPP, since in some cases it could hinder the achievement of the purpose by prohibiting the processing of data that do not seem essential at first, but later appear to be indispensable for processing (for example in the context of scientific research).

4. Lawfulness of processing (article 6)

33. Firstly, the CPP would like to draw the attention to the fact that the term "lawfulness" could lead to confusion in this context. After all, it could lead to thinking that processing operations which are in accordance with one of the grounds in article 6.1 are automatically completely in conformity with the draft regulation, while this is obviously not the case. The CPP therefore recommends using the term "admissibility". The latter concept has a more limited scope than "lawfulness" and therefore conveys much better that article 6 is only a first step in assessing whether a data processing operation complies with the obligations set out in the draft regulation.

34. Furthermore, the CPP has concerns regarding article 6.1.f of the draft regulation, in which public authorities are prohibited to justify processing operations if they act on basis of their legitimate interests that override the interests and rights of data subjects. The CPP believes that this admissibility basis for processing operations should not be deleted. It is quite likely that situations will arise where a public authority has no other choice than to base some processing operations on its legitimate interests (for example in the context of personnel management).

35. More in general, the CPP has also elaborated a note in which it has gathered elements of reply to the question whether a separate, legal, regulatory framework is needed for the public and private sectors. This note was annexed to the present opinion.

36. Finally, the CPP has some remarks on article 6.4 of the draft regulation, which states the following: *"Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one*

of the grounds referred to in points (a) to (e) of paragraph 1. (…).″ Either the processing operation is compatible, or it is not, and in the latter case it constitutes a new processing operation that has to meet all legal requirements and that by consequence should have different legal basis. All hypotheses of article 6.a to 6.f should be applicable in this case, and therefore the CPP does not understand why the draft regulation only mentions the hypotheses referred to in points a) to e). The CPP is also of the opinion that article 5.b of the draft regulation should include a clear reference to article 6.4. Both provisions are closely connected.

5. Data Subject consent (article 7)

37. When controllers justify their processing on the basis of consent, the draft regulation stipulates that consent should be given explicitly (article 4.8) and that the controller clearly bears the burden of proof (article 7.1). Preamble 25 clarifies that consent can be given by any appropriate method, either by a statement or by a clear affirmative action or by any other statement which clearly indicates the acceptance of the proposed processing of personal data in the given context. These adaptations aim to strengthen the rights of data subjects and to make controllers aware of their responsibilities with respect to storing evidence.

38. The draft regulation also provides that consent can be withdrawn at any time without any justification or motivation. This provision is presented as a means to strengthen the rights of data subjects and the control that data subjects should be able to maintain of the use of their data. The CPP notes, however, that a possible unilateral and unjustified withdrawal of a legally sanctioned consent affecting the interests of a third party, could undermine the activities of controllers and that this rule threatens the balance created by Directive 95/49/EC between data subject rights and controller interests. This possible unilateral withdrawal should also be assessed in the light of the right to object to processing operations and of the conditions to exercise this right (see below).

39. The CPP considers in general that an overvaluation of consent should be avoided. Consent is allowed as a basis for legitimacy but one should remain vigilant to its vulnerability and not want to base all processing operations on data subject consent. Numerous provisions in the draft regulation have consent as a legitimacy basis, like in article 8.1 which concerns the consent of minors in the context of information society services (see above). Now, in that context subscription contracts are concluded much more often, in which case one cannot really use the term 'consent'.

40. The draft regulation also excludes consent as a valid legal basis for the processing when there is a significant imbalance between the data subject and the controller (article 7.4). Preamble

34 clarifies that this is the case where the data subject is in a situation of dependence on the controller, for example when his personal data are processed by his employer in the employment context. This is a formal recognition that the free nature of a consent may be a problem in a professional context due to the existence of a relationship of subordination[19].

41. If the use of consent in a professional context was excluded in all cases, the CPP believes, however, this could lead to increased legal uncertainty for the controller for processing operations that are not strictly necessary for the execution of the employment contract. In order to make processing operations admissible in those cases, the controller has to balance his interests beforehand (article 6.1.f of the draft regulation), with the risk of being disciplined by a judge afterwards.

42. According to the CPP, an employee's consent should therefore be a valid legal ground in some cases. Inspiration can be found in the existing Belgian regulating framework. Article 27 of the Belgian Royal Decree of 13 February 2001, implementing the Belgian Data Protection Act provides for the prohibition for the employer to base the processing of **sensitive** data solely on consent, **except when the processing is intended for the data subject to benefit from**. The CPP calls for copying this exception in the draft regulation.

6. Processing children's personal data (article 8)

43. The draft regulation introduces the principle of a specific protection for minors (children) "*as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data*" (preamble 29).

44. The CPP is favourable to this initiative, which is particularly appropriate in the context of online activities, social networks and marketing activities aimed specifically at young people. The CPP recalls the initiative it took in this context with its special website for minors (children and adolescents) and their parents and teachers[20], which the CPP anticipates the encouragement of the proposal for a regulation to organise awareness campaigns for this category of data subjects (article 52).

45. Concerning the guarantees provided for in the draft regulation, the CPP is satisfied with the clarification of article 6.f. This provision states that the fact that a person is a minor should be taken into account when assessing interests, freedoms or fundamental rights possibly prevailing over the legitimate interests of the controller. Similarly, the CPP shares the desire

[19] See in this context recommendations no. 01/2002 of the CPP and working documents WP48 and WP168 (paragraph 66) of the Article 29 Working Party.

[20] 'I decide' website: http://www.ikbeslis.be (Dutch), http://www. jedecide.be (French)

of the European Commission to subject large databases concerning minors to a prior data protection impact assessment (article 33), to promote awareness campaigns by Data Protection Authorities (article 52), to draw up specific codes of conduct (article 38) as well as to request the controllers to do what is required to obtain verifiable consent when information society services are offered (article 8).

46. With regard to the direct offer of information society services to children, article 8 states that in the context of this regulation processing data of a child below the age of 13 is only lawful if and to the extent that consent is given or authorised by the child's parent or custodian (article 8.1). Yet, article 8.2 states the following: "*Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.".*

47. The CPP sees this provision as an invitation to make a distinction between the lawfulness (based on consent) of processing data of a minor below the age of 13, and the lawfulness of their contractual obligations in the context of national (civil) law. It would be useful to include a confirmation of this interpretation and an illustration of what is meant by "the offering of information society services directly to a child" in the preambles.

48. Moreover, the CPP wonders how the strict validity requirements of an authorisation under article 7 of the draft regulation are compatible with the consent of a minor over the age of 13.

49. Finally, the CPP would like to point out that, regardless of any specific protection, account could and should be taken of the particular situation of children in the application of the provisions of the draft regulation (example: the information should be understandable, which means that the controllers should adapt their language when specifically addressing children). The same goes for other categories of persons, for example persons who are not very familiar with computer applications and information and communication technologies (elderly people, digital gap)[21].

50. In this regard the CPP also notes that the draft regulation could provide for a general provision concerning the representation of people who are legally incapacitated. This provision could stress the fact that when their representatives give their consent, it should not be forgotten that they give consent for a third party, and not for themselves, and that in this context the protection of the person they represent should be their guideline.

[21] Although rules on "data protection" in general have gradually become more complex and *processing* and *data* are currently at the centre of attention (economically and legally), it should not be forgotten that the purpose of regulating this fundamental right is in the first place the protection of *individuals* (with respect to the processing of their data).

7. Processing of special categories of personal data (article 9)

51. Article 9.1, which defines the special categories of personal data (sensitive data), also mentions genetic data. This was not the case in article 8.1 of Directive 95/46/EC. The CPP is pleased with this insertion.

52. The CPP has a lot more reservations with respect to the change in the description of judicial data as stated in article 8.5 of Directive 95/46/EC and more specifically with respect to the deletion of the term "offences". The latter notion, however, allowed for the qualification of administrative offences or civil convictions as legal data (see article 8 §1 of the Belgian Data Protection Act).

53. Furthermore, the CPP has found that the number of cases where the processing of judicial data is authorised, has increased considerably compared to article 8.5 of Directive 95/46/EC. For example, data subject consent or data disclosure by the data subject are, pursuant to article 9.2.a and 9.2.e of the draft regulation, grounds of exceptions on the prohibition of processing, while these grounds cannot be found in the Directive. The CPP also questions the motivation for this loosening of the rules.

54. The CPP's point of view with respect to the processing of data relating to health has been stated above.

8. Processing not allowing identification (article 10)

55. Article 10 of the draft regulation states that when the data do not permit the controller to identify a natural person, the controller shall 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. The CPP believes that the intentions behind this provision should be clarified and that the interpretation that the controller is no longer bound to any obligation should be ruled out.

9. Transparency (articles 11 and 14)

56. The CPP welcomes the general obligation to have transparent, complete and easily accessible policies and is positive about the fact that every provision of information or communication from the controller has to be done in clear and plain language adapted to the data subject (article 11).

57. The draft regulation also provides for a broader content of the information that has to be provided by the controller (compare article 14.1 to 14.3 of the draft with articles 10 and 11 of Directive 95/46/EG).

58. The CPP appreciates the additional information on the origin of the data (article 14.3) which de facto immediately allows data subjects to maintain greater control of their data.

59. With respect to the provision of information on the rights of data subjects (article 14.1.d), the CPP believes that information should also be given on the new rights created by the draft regulation (right to be forgotten, right to portability, profiling measures). Also, the provision of information on international data transfers (14.1.g) should include the adequate safeguards provided by the controller, as these safeguards often create rights for data subjects.

60. The CPP also notes that the draft regulation (article 14.1.c) establishes the principle that when information is provided to data subjects also the envisaged retention period of the processed data is mentioned. The CPP shares the idea that this principle would lead to a higher degree of transparency of data processing in cases where the controller has got a clear view of the retention period in advance (e.g. because it has been established by law), but would like to point out at the same time that in practice it is often impossible for the controller to determine the exact retention period in advance. This can be illustrated by the numerous deliberations of the Sector Committee of the Federal Government.
    The CPP therefore fears that this new rule will often make it impossible for the controller in practice to come up with anything more than a rough estimate of the storage period. "Just to be on the safe side", the controller will probably ask for a longer period than strictly necessary.

61. Lastly, the CPP would like to draw the attention to the fact that – pursuant to article 14.5.c of the draft regulation – the obligation of information is not applicable when (the data are not collected from the data subject and) recording or disclosure has <u>expressly</u> been laid down by law.

62. The CPP believes that on the one hand this provision seems make the rules more strict compared to Directive 95/46/EG, because the word "*uitdrukkelijk*"[22] has been added (compare article 11.2, at the end of Directive 95/46/EG). On the other hand, this provision also seems to make the rules more flexible , because the obligation for Member States – in article 11.2, at

[22] This remark concerns only the Dutch text, given that in the English version of Directive 95/46/EC the word "expressly" was already included: "*Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is* ***expressly*** *laid down by law*."

the end of Directive 95/46/EC – to "*provide appropriate safeguards"* for the cases where the present exception to the obligation of information can be invoked, has not been copied in the draft regulation.

63. The CPP wonders whether it was the European Commission's intention to make any changes with respect to the current situation when editing article 14.5.c. In other words, what does the Commission have in mind? Does it wish to make the rules more strict or flexible, or does it aim at a status quo?

64. In any case, the CPP is of the opinion that stricter rules for this exception to the obligation of information could have the implication that many data flows in the Belgian public sector will become subject to the obligation of information, while up to now the exception could often be invoked as soon as a legal ground for the processing had been found. The draft regulation could therefore have important implications for data processing in the public sector. Large scale reflection will probably be required to check whether the regulating framework of each domain is sufficient to justify the exception to the obligation of information, or whether legal interventions are necessary, or whether data subjects will nevertheless have to be informed.

65. The CPP has serious doubts on the desirability of such a test and therefore recommends the preservation of the current situation in article 14.5, point c of the draft regulation, as already provided for by article 11.2, in fine, of Directive 95/46/EC.

10. Procedures and mechanisms for exercising the rights of the data subject (article 12)

66. The CPP appreciates the obligation of the controller to provide the data subjects with means to exercise their rights and submit their requests electronically when personal data is processed by automated means (article 12.1), the introduction of a reply term (12.2) and the principle that the exercise of one's rights is free of charge (except in case of misuse)(12.4).

11. Access to data (articles 15 and 20)

67. The CPP believes that the right of access (article 15) should also apply to the appropriate safeguards that were provided for in the context of international data transfers. The existing safeguards like binding corporate rules and the model clauses of the European Commission often enable data subjects to have access to content, seeing that these safeguards often provide for data subject rights (as third beneficiaries).

68. The draft regulation provides for the possibility for processors to take appropriate measures (article 42). Since they are not necessarily in contact with data subjects, the CPP believes that

increased transparency and access by data subjects to the appropriate safeguards offered by processors should be included in the draft regulation[23].

69. Incidentally, article 12 of Directive 95/46/EC provides for the mandatory communication to data subjects of the logic involved in the automatic processing of their data, at least for the automated decisions referred to in 15(1) . The "automated measures" for which article 15 of Directive 95/46/EG has laid down specific rules, are combined with "profiling measures" in article 20 of the draft regulation. The CPP considers, however, that there could also be automated processing operations that are not carried out in the context of profiling (see above). It regrets that for those cases the draft regulation does not establish any specific rule that obliges the controller to inform the data subjects on the logic behind the automated processing of their data.

12. Right to rectification (article 16)

70. The CPP believes that when data are objectively inaccurate, easy rectification should be possible. The possibility to add a rectification, provided for in article 16, should only be applicable, however, when the data are related to subjective information (an assessment for example) and the data subject, contrary to the controller, considers them to be incorrect (in practice, this allows storing both versions of the data).

13. Right to be forgotten and to erasure (article 17)

71. A clear distinction should be made between the right to be forgotten and the right to erasure (article 17), given that two different concepts are concerned.

72. Furthermore, the CPP notes that article 17 provides for the right of data subjects to have their data erased when the data are no longer necessary in relation to the purposes for which they were collected or when the authorised retention period has expired while there is no other legal ground for the processing of the data. According to the CPP, the data subject should not have to request erasure in these cases, since this should be done automatically. The CPP consequently thinks that the lack of automatic erasure leads to a certain weakening of data subject protection compared to the current situation.

73. Lastly, the CPP shares the view that it should be closely monitored that data of minors remain accurate, up to date and that they are erased when storage is no longer justified. However, no legal consequence is attached to the phrase "especially in relation to personal data which

[23] Which would ensure that controllers have to make the measures taken by processors available.

are made available by the data subject while he or she was a child" (article 17.1). This lack of legal consequences could lead to confusion and a certain sense of legal uncertainty.

14. Right to data portability (article 18)

74. The CPP welcomes this principle – which aims to strengthen the position of the data subject by giving them more control of their data – but believes that vigilance will be required when establishing the implementing measures of this principle. According to the CPP, the conditions currently provided for in the draft regulation are insufficiently elaborated to apply this article in practice.

15. Right to object (article 19)

75. When the regulation enters into force the right to object provided for by the Belgian Data Protection Act will disappear in cases where the data subject's consent constitutes the legal basis of a processing operation[24]. This is unacceptable because it would entail a weakening of the rights of data subjects. The right to object is essential since it implies that the controller can no longer process data for which data subjects have exercised their right to object.

76. The right to object currently provides for stronger safeguards than the possibility of withdrawal of consent provided for in the draft regulation, which states the following: "*The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal*". In any case, one must assume that the withdrawal of consent can only have practical consequences in the future. Such a provision significantly weakens the protection provided by the exercise of the current rules of the right to object.

---

[24] Pursuant to article 14 of directive 95/46/EG, Member States were obliged to provide for a right to object in at least a certain number of cases (especially the cases referred to in article 7.e and 7.f, and direct marketing), but otherwise they could freely introduce this right in other cases (all processing operations regardless of their legal basis).

In the Belgian Data Protection Act the actual choice was made to expand this right to other cases. Article 12 of this act states the following: "*In addition any person shall have the right to object against the processing of data relating to him for serious and legitimate reasons that have regard to his particular situation, unless the lawfulness of the processing is based on grounds referred to in Article 5 b(if processing is necessary for the performance of a contract) and c (if processing is necessary for compliance with an obligation to which the controller is subject)*".

In short, the Belgian Data Protection Act provides for two additional hypotheses compared to the minimum required by Directive 95/46/EC, namely when processing is necessary in order to protect the vital interests of the data subject (art. 5d) Belgian Data Protection Act) and when processing is justified by data subject consent (art. 5a) Belgian Data Protection Act).

The draft regulation, on the other hand states the following (art.19): "*The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d),*

(e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject."

Accordingly, the right to object is excluded in case of processing operations based on consent (art. 6 a), contracts (6.1.b) and the law in general (6.1.c) – legal obligation of the controller).

77. Finally, when exercising the right to object, the draft regulation gives the controller the possibility to invoke compelling legitimate grounds for the processing which override the interests or fundamental rights and fundamental freedoms of the data subject (article 19.1). At first sight this appears to strengthen the rights of data subjects who in the context of the exercise of their right to object, no longer have to give substantial and legitimate reasons related to their particular situation (see 14.a of Directive 95/46/EC). Instead, the draft regulation now wants to give the controller the possibility to refuse the exercise of this right. The CPP believes that this new rule may lead to controllers constantly invoking their legitimate interest in order to refuse the exercise of the right to object by the data subject[25].

78. The CPP also expresses its concern about the fact that article 19.3 also seems to question the unconditional nature of the right to object with respect to direct marketing ("without reason") provided for in article 12, paragraph 3 of the Belgian Data Protection Act, since it states: *"Where an objection is upheld pursuant to paragraphs 1 and 2 (direct marketing)…."*.

16. Profiling (article 20)

79. The CPP believes that safeguards for the data subjects should always include the right to human intervention (which is currently only provided for in article 20.2.a of the draft regulation). In addition, data subjects should always have the right to put forward their point of view (article 15.2.a of Directive 95/46/EC). Both safeguards should therefore clearly be applicable in all cases of article 20.2 of the draft regulation (in case of a contract, implementation of law or consent).

80. When reading article 20 of the draft regulation it is in fact not easy to determine whether profiling for direct marketing purposes in the form of specific advertising messages is part of the scope of this article, since there are no legal consequences for the data subject (except when a reduction and therefore a price offer are included) and does not necessarily affect him in an important way. Nevertheless, the CPP believes that this kind of profiling should be subject to the specific conditions set out in article 20.

81. The CPP regrets that the draft regulation is limited to mentioning in a preamble that profiling must not concern children (preamble 58). The CPP advocates including this in article 20 (measures based on profiling) and prohibiting that a child's consent is seen as a ground for processing, since it is of the opinion that in the context of profiling it is impossible to meet the condition that there is no imbalance between the interests of the data subject (child) and the controller (article 7.4: conditions for consent).

[25] Article 19.3 does not offer any solution since it states: "*Where an objection is upheld (…), the controller shall no longer use or otherwise process the personal data concerned".*

82. Finally, article 20.3 aims to exclude automated data processing intended to evaluate certain personal aspects relating to a natural person, when it is solely based on special categories of data (sensitive data). The CPP wonders to what extent public authorities will be limited by this provision in their public policies on health care and believes that a solution could be found in the context of the implementation of article 21. Moreover, the CPP wonders to what extent such a processing operation can solely be based on sensitive data.

17. Responsibility of the controller (article 22)

83. The CPP appreciates the inclusion of the responsibility principle for controllers which obliges them to provide for measures intended to prevent that data protection is compromised in any way. It is better to deal with this problem in advance by using mechanisms that prevent violations, than to be bound by principles and possible sanctions in case of non-compliance. This principle is currently applied in binding corporate rules.

84. The CPP notes a lack of consistency, however, because of the fact that the principle only concerns controllers (article 22.1), while the list of measures for the implementation of the responsibility principle is also directly related to processors (article 22.2).

85. The CPP also believes that the obligations referred to in article 22.3 should be clarified. This article is about a mandatory audit and it is not clear if the "proportionality" mentioned in the last sentence of article 22.3 should be applied to the obligation itself (the audit would in other words only be obligatory when justified by the situation) or only to the fact that it will be carried out by internal or external auditors (i.e.: depending on the situation the obligation will (not) require any intervention by external auditors). The differences in the translations of the draft regulation only create more confusion.

86. Furthermore, the CPP thinks that the controller is in the best position to assess – taking into account the nature of data processed, the risks, the existence of other protection mechanisms, if any, etc. - whether an external audit of his organisation is a useful measure, or whether internal control is sufficient.

18. Data protection by design and by default (article 23)

87. The CPP supports the introduction of these principles but stresses that the development of processing systems is sometimes not in the hands of controllers but of product and software developers.

19. The Representatives (article 25)

88. In case of application of article 3.2[26], article 25 of the draft regulation provides for the appointment of a representative in the Union.

89. The role of representatives should be clarified. Will they only be a contact person for the Data Protection Authorities within the Union or do they also have a role as legal representative? Article 4.14 states that he may be addressed by **any** supervisory authority. This role as contact person is confirmed by article 53.1.c on the powers of Data Protection Authorities (under this provision DPAs can order him to provide all useful information), and also by articles 28.3 and 29. With regard to legal responsibility it is at least surprising that article 78, on the possibility for Member States to impose sanctions, can also be applied to representatives, although no references are made to them in article 79 (administrative sanctions) or in article 77 (civil liability). Furthermore, by not clearly defining that the legal obligations of the controller also apply to the representative, the introduction of direct criminal responsibility could cause problems, since normally one cannot be made criminally responsible for the mistakes of others[27].

90. Furthermore, the draft regulation provides for several exceptions of the obligation to appoint a representative (article 25.2) and the CPP has a number of concerns about this aspect.

91. Firstly, the CPP believes it is always useful to appoint a representative, even in cases where the controller is established in a third country offering an adequate level of protection (article 25.2 a). The CPP agrees with the opinion of the ICO[28], which states that a controller established in a third country with an adequate level of protection could breach the

---

[26] *"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 to such data subjects in the Union; or

(b) the monitoring of their behaviour."

[27] With the exception to legal responsibility of legal persons, but in this case a specificity is concerned.

[28] Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework, 27 February 2012, p. 17

requirements of the regulation without necessarily breaching the law of the third country in which it is located.

92. Secondly, the draft regulation also provides for an exception for enterprises with less than 250 employees (article 25.2.b), although the number of employees, according to the CPP, cannot be a relevant criterion for assessing the risks (see below).

93. Moreover, with regard to the exception for controllers only occasionally offering goods or services to data subjects residing in the Union (article 25.2.d), the criterion "occasionally offering goods or services", could cause difficulties of application (one collection of sensitive data concerning 1,000,000 individuals could be occasional?).

94. Finally, the CPP advocates for the full deletion of every exception to the obligation to appoint a representative in cases where sensitive data is processed.

20. Documents (article 28)

95. The CPP can accept the deletion of the mandatory notification in order to replace it by mandatory internal documentation of processing operations. The essential elements of data processing operations should be easily accessible to data subjects and should remain available for the DPAs. For example through the Data Protection Officer or through a website.

96. The CPP has been able to certify that the particular importance of the notification does not really consist of the transparency they create (given that few citizens consult the public register) but od the fact that notification obliges controllers to ask themselves pertinent questions about the intended data protection. It is therefore important to ensure that this occurs every time when setting up and deploying of a processing operation. Drawing up, updating and maintaining internal documentation preserves the advantages of a notification (awareness of the necessity to comply with the law). The disadvantages of a mandatory notification (unnecessary red tape, maintenance costs of a register that is not often consulted) can be avoided.

97. The CPP observes that the exceptions provided for the mandatory documentation (4) are too extensive given that each controller should keep basic documentation with the most important elements related to data processing: the contact details of the controller and of the person who in practice can immediately be addressed by data subjects for the exercise of their rights (but also the identity of processors, of possible representatives, of the Data Protection Officer, a short description of the processing operations (purposes, categories of personal data and recipients)).

98. The aforementioned exception cannot be applied to 'sensitive personal data'.

99. In any case, it must be ensured that the DPA can be quickly and fully informed when requesting documentation and information (which indeed has to be elaborated further and in a uniform manner by the Commission, as provided in (5) and (6) (following the opinion of the DPAs)).

100. Finally, it should be pointed out that the list of information data in article 28 (2) is far-reaching. And for some processing operations difficult if not impossible to apply. The CPP is of the opinion that it is not possible for the controllers to always determine in advance how long they will keep the data. Accordingly, the requirement will have to be written, elaborated and enforced in a sufficiently flexible manner in order to allow for practical case-by-case application. Controllers or processors must be given some room to not provide certain information as long as there are reasonable grounds motivating why this information is difficult or impossible to provide. This does not mean that basic elements will not have to be documented at all times. It is important that the regulation makes this distinction.

21. Co-operation with the supervisory authority (article 29)

101. The CPP appreciates the introduction of this principle (article 29), but the mandatory disclosure of information should not be restricted to the research hypotheses (53.2a). It should be broader and relate inter alia to article 53.1c.

102. For all of its control and mediation tasks, the DPA has to be enabled to make a binding request for all relevant information to the controller or processor.

103. Also, information should be provided on how and who has to reply with respect to the one-stop shop (application of article 51.2) and on the formal role of other DPAs. In order to avoid gaps, there should be provision stipulating that each DPA can rely on this obligation to co-operate, making it impossible to deny jurisdiction.

22. Security of processing: article 30

104. The CPP appreciates that the draft regulation also imposes the obligations related to security on the processor (article 30.1). In practice this coincides with our national rules (article 16 §4 DPAct).

105. The CPP also emphasises the benefit of explicitly requiring that the instructions given to the processor are documented in writing (article 26.3) and believes that this should also be the case for the level of the service or of the safeguards related to the security measures imposed by the controller.

106. Article 26.4 also provides that when a processor processes personal data in any other way than instructed, he shall be considered to be a controller and be subject to the rules on joint controllers. Article 24, which lays down the rules on joint controllers, stipulates that they determine their respective responsibilities by means of a mutual arrangement and that non-compliance can be penalised with a fine up to 500,000 EUR, or in case of an enterprise up to 1% of its annual worldwide turnover (article 79.5.e). However, the CPP points out that when processors use data for the realisation of a purpose of their own, they will not necessarily inform the initial controller about these activities. Consequently, (and although the CPP supports the idea that the processor in the present situation should be considered the controller), care should be taken that the initial controller – who, as mentioned, did not know of these new processing operations – cannot be punished for not concluding an agreement, within the meaning of article 24 of the draft regulation.

107. With regard to the conditions that allow the processor to appeal to another processor (article 26.2d), the CPP wishes to emphasise that in addition to the prior authorisation of the controller, this additional subcontractorship should also become the subject of an agreement imposing the same obligations on the subsequent processor as an initial processor. This principle is set out in Model Clauses 2010/87/EU which were approved by the European Commission, and more specifically in article 11. This article also states that in case of shortcomings by the subsequent processor of the data protection to which he is bound by agreement, the initial processor will remain fully responsible to the controller.

23. Notification of a personal data breach to the DPAs and data subject: articles 31 and 32

108. The draft regulation does not specify whether each security breach (data breach) has to be reported to the Data Protection Authority. The text delegates the task of determining in which circumstances the controllers are required to notify the personal data breach (article 31.5) to the European Commission. One could be right in thinking that this means that in the absence of approval of delegated acts, every security breach should be reported to the Data Protection Authority, which could become an obligation that is too broad and unworkable. It is also up to the European Commission to define the circumstances in which violations could constitute data breaches or infringe upon the privacy of data subjects. With these criteria breaches that also have to be reported to data subjects could be determined.

109. The CPP is of the opinion that clear criteria should be inserted in the text itself and not be determined afterwards through delegated acts. First of all, excessive notification of small breaches to the DPAs should be avoided so that only breaches with serious consequences or breaches with an impact on a large number of persons are reported. What is more, also the risks of financial losses should be included in the criteria that require a notification to data subjects.

110. Furthermore, the draft regulation provides for an exception to the notification of a personal data breach to the data subject if controllers demonstrate to the satisfaction of the DPA that they have implemented appropriate technological protection measures to ensure that the data are rendered unintelligible to any person who is not authorised to access it (encryption measures). The CPP stresses the fact that the encryption measures should technically not have the consequence of rendering the data totally unintelligible[29] for everybody; this actually the objective. . The requirement should rather be that this objective is aimed at, including compulsory characteristics linked to the nature of the data, the state of the art and the costs.

111. Lastly, the CPP believes it would be useful if the agreement between the controller and processor provided that in case of a security breach, the controller and the processor would work together to find the cause of the incident and take palliative or corrective measures.

112. The CPP considers that the current text still raises so many questions that an approval of this text will lead to impossible situations, for the DPA, controller and processor, but also for the data subject. The so-called data breach notification is rather new and still requires a lot of research and experiments. The CPP is therefore of the opinion that for its implementation a realistic roadmap should be drawn up so that this obligation can be introduced gradually. Also, careful monitoring of the advantages and disadvantages of the mechanism, the administrative and financial consequences and the implications for data subject rights should be provided for. The limited experiences of the CPP in this context are not exactly positive. The CPP therefore makes a serious reservation and expects sufficient prior research on the feasibility and effectiveness of this mechanism, with one key question: will the public benefit from it?

24. Data protection impact assessment: article 33

[29] The CPP suggests replacing the term 'unintelligible' by 'inaccessible'.

113. In addition to the circumstances stated in 33.1, it is appropriate to grant the DPA the power to impose a data protection impact assessment in a reasoned decision. This should allow the DPA to take action in a modulated and appropriate manner.

114. The CPP does not understand what the specific risks in 33.2.c would be: nowadays publicly accessible areas are excellent places that are monitored by optical-electronic devices. Except in exceptional conditions in which the DPA can intervene and impose a data protection impact assessment, it is hard to understand why (large-scale) video surveillance in publicly accessible areas (scope of the concept?) would create specific risks (except when special applications would be used, like for example facial recognition or when cameras and/or footage would not be used in a manner in line with the expectations of the public) . This is in any case not consistent with the CPP's experiences with video surveillance.

115. Article 33.4. is unclear and can be interpreted in many ways or ignored. This provision should be deleted or clarified.

116. The CPP wonders why article 33.5 refers to processing operations carried out in the framework of EU legislation and not also that of Member States. A data protection assessment should always be made when adopting national law (see preamble 73). The CPP therefore sees no reason why only EU legislation and not other legislative instruments (adopted by a parliamentary assembly) are exempted. This exception should be applied to each legislation, but should be compensated by obligatory opinions of the involved DPA (article 52.1.f: with regard to this consultation the authorised DPA will decide whether a data protection impact assessment is useful and necessary, and how it should be implemented).

117. The CPP is in favour of the instrument "data protection impact assessment'. The principle is therefore fully supported by the CPP.

118. The CPP knows from experience, however, that a good data protection impact assessment should not become too extensive and should not be diluted into a sterile style exercise where a lot is written by highly paid consultants. On the contrary, every step should be taken to ensure that the data protection impact assessment is an accurate and practical instrument that indicates as clearly and impartially as possible the intentions, the purpose of the intended processing operation, the risks, the options, how the controllers or processors have fulfilled their obligations. The key question with regard to this aspect should always be whether it benefits or harms the public, the data subjects, and what actions are taken to strengthen the rights and freedoms of the public.

119. The manner in which this obligation is further elaborated in articles 33.6 and 33.7 is therefore important. The CPP again requests a well thought-out introduction and regular monitoring. By analogy, see above.

25. Prior authorisation and prior consultation of Data Protection Authorities (article 34)

120. The draft regulation wants to limit the competence for prior authorisation by Data Protection Authorities to international data transfers (article 34.1). The current Belgian rules on privacy protection, however, provide for a system of prior authorisations for certain data transfers by Belgian public services. Hence, article 34 threatens to put this system at risk.

121. The protection measures and procedures that were elaborated in Belgium provide for, inter alia, the establishment of sector committees (Social Security and Health, National Register, Federal Government, Statistics, Phenix (Justice), Crossroads Bank of Enterprises) that have a prior authorisation competence. These committees were established under the aegis of our DPA, but they are mixed, because they consist partly of members of the CPP and partly of experts of public authorities. The committees have to monitor data processing by public administrations, especially through prior authorisations. Before these public administrations can make certain personal data available to other administrations or third parties, an authorisation is needed from one of these committees. This is for example the case for access and use of the National Register number and access to population registers.

122. The prior authorisation procedure of these committees can provide useful guidance to the public sector during the introduction of a personal data flux. These committees fulfil the role of guide for the controllers. Not only can they fully authorise or deny access, they can to grant authorisations to which (suspensive) conditions are linked.

123. The introduction of prior consultations, as provided for by the draft regulation will lead to either a lack of reaction by the authority (which creates legal uncertainty for the controller) or a prohibition[30] of processing operations, when they are not in accordance with the law (article 34.3). Moreover, such a prohibition could even be imposed in cases where the processing is defined by an act, which is excessive.

[30] Article 34, paragraph 3, does provide for the obligation of the DPA to make "appropriate proposals" in case of a prohibition "to remedy such incompliance". Today, the Belgian sector committees can – in cases where room for improvement regarding privacy protection is detected - immediately grant an authorisation with a (suspensive) condition attached. In the system of the draft regulation the Data Protection Authority will always have to refuse every time in such situations and make "appropriate proposals" which implies de facto that the applicant will have to submit a new application, which is not very flexible and inefficient…

124. The CPP also notes, as a subsidiary remark, that in article 34.4 of the draft regulation the Data Protection Authorities are given the choice to draw up a list of processing operations that require a prior consultation. The CPP believes that this is an excessive competence, since such decisions have to be made democratically (and thus by the legislator).

125. **In summary, the CPP believes that the Belgian system of sector committees, established for the protection of personal data in the public sector, should be fully maintained** and that the draft regulation should not affect purely national systems that do not impede the free movement of data. The present draft regulation does not provide for this possibility (neither in article 34, nor in Chapter IX). Allegedly, the representative of the European Commission has, however, declared – in context of DAPIX meetings – that there is understanding for this Belgian stance. The CPP therefore calls for an adaptation of the draft regulation in this respect.

26. The Data Protection Officer (articles 35 to 37)

126. The draft regulation dedicates an entire section of the chapter on the obligations of the controller and processor to the function of Data Protection Officer (articles 35 to 37).

127. The CPP welcomes this formal recognition of the Data Protection Officer and his assisting role[31] to the controller and the processor in fulfilling of the various obligations incumbent on them pursuant to the regulation. The appointment of a Data Protection Officer shall contribute to the implementation of the principle of "accountability" and the "internal privacy management" approach of the regulation, while a close link with the Data Protection Authority and the data subjects will continue to exist.

128. If the draft regulation becomes effective one day, the role and status of the "Data Protection Officer" in the sense of article 17bis will finally be specified; a specification which the CPP has been insisting upon with the Belgian executive for many years[32].

129. The CPP notes with satisfaction that the Data Protection Officer can be a person that is employed by the controller or a third person (article 35.8) and that he is also assigned the role of contact person for data subjects when exercising their rights. The information that has to be provided by the controller and processor is essential in this respect.

[31] Note on the translation: the CPP notes that the wording « monitor the implementation and application of the policies..» that is used in article 37 §1 b) was translated into French by « contrôler la mise en œuvre..». The Commission believes that this translation is not suitable. The wording «veiller à (surveiller) et assister» (in the sense of for example a heart monitor) is preferred.

[32] See, inter alia, CPP Opinion 15/2002 of 2 May 2002 on the Draft Royal Decree in implementation of Article 3, § 6 of the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data (§ 17). (Only Dutch and French)

130. With respect to collaboration with the Data Protection Authority, the CPP shares the vision of the draft regulation (article 37 §1). A relation, for example regarding the exchange of information, seems to be essential.

131. The CPP is also generally pleased with the safeguards of independence that are required by the draft regulation and it also approves of the obligations imposed on controllers and processors in order to allow the Data Protection Officer to fully carry out his duties (article 35 § 5, 6, 7 and article 36). Those safeguards are an addition to those the CPP repeatedly requested when exercising its competence to deliver an opinion[33]. The CPP notes, however, the complete lack of mechanisms/procedures/safeguards against the dismissal of the officer pursuant to the exercise of his functions. It would at least have considered it useful if the Data Protection Authorities would be informed on the matter and/or that the Data Protection Officer would be offered the possibility of referral to the Data Protection Authority in case of (planned) dismissal[34].

132. In accordance with its case law, the CPP is furthermore of the opinion that the function of Data Protection Officer can be exercised along with another function, as long as the Data Protection Officer has sufficient freedom and independence in this capacity to successfully carry out his tasks[35]. The CPP stresses to this respect that the independence of the Data Protection Officer cannot reasonably be absolute, if only because the Data Protection Officer, at least in some cases, is bound by a contract to the controller.

133. **Notwithstanding the preceding favourable assessment, the CPP does not favour the option of making the appointment of a Data Protection Officer obligatory in some cases.** The CPP believes that the appointment of a Data Protection Officer should remain optional. The appointment of a Data Protection Officer is a measure – among all the other measures contributing to accountability - that the controller should be able to take freely, taking into account the processing operations carried out, the nature of the data processed, the risks, the existence of other protection mechanisms and the actual benefit that the appointment of a Data Protection Officer would imply for data protection in that case.

[33] See opinions 01/2007, 16/2007 and 39/2008 (Only in Dutch and French).

[34] See for example the French Act 78-17 of 6 January 1978 relative à l'informatique, aux fichiers et aux libertés (Chapitre IV) and the décret d'application 2005-1309 of 20 October 2005.

[35] CPP, Opinion 33/2002 of 22 August 2002 on the Bill establishing the Belgian Health Care Knowledge Centre (paragraph 21). In the same sense, CPP, Opinion 19/2002 of 10 June 2002 on a (1) Bill amending the Act of 8 August 1983 establishing a National Register of natural persons and the Act of 19 July 1991 on the population registers and the identity cards and amending the Act of 8 August 1983 establishing a national register of natural persons. (2) Draft Royal Decree on the identity cards. (3) Draft Royal Decree laying down transitional measures in relation to the electronic identity card in Belgium; CPP, Opinion 23/2006 of 12 July 2006 on the Bill on a framework for of negative lists (paragraphs 42-44).

134. In subsidiary order, the CPP also has remarks on the criteria set out in the draft regulation to determine whether a Data Protection Officer is mandatory or not:

a. One of the criteria is the situation in which the processing is carried out in a company with at least 250 employees. The CPP is of the opinion that the number of employees is not a good criterion to determine whether a Data Protection Officer is needed. After all, a company can employ 1000 employees and barely carry out any (sensitive) data processing operations, while a small company with 10 employees could process a large amount of sensitive data.

b. The CPP wonders how the phrase in article 35, paragraph 1, c) should be interpreted: *"(…)processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.* The CPP requests that, in the text of article 35, or at least in a recital, there is a clarification on what is meant by this phrase. Since this is a case which requires the mandatory appointment of a Data Protection Officer, this clarification has to be made before the delegated act reserved by the European Commission in article 35.11, is approved.

27. Codes of Conduct

135. The CPP believes that it should not be the competence of the European Commission but the competence of the European Data Protection Board to determine whether or not a code of conduct is generally applicable within the territories of the European Union (article 38.4).

28. Transfer of personal data to third countries or international organisations

136. The CPP believes that the draft regulation provides a clearer definition of the rules concerning cross-border data transfer. This is particularly the case for the definition of the assessment criteria for adequate safeguards offered by third countries or for the explicit recognition of binding corporate rules.

137. The CPP also supports the desire to simplify the obligations for enterprises through the elimination of mandatory national authorisations when binding corporate rules or standard contractual clauses are used.

138. The CPP believes that article 42.5 lacks clarity. This article appears to concern the public sector and it should be limited to that subject only. It is essential that solutions are provided for international data flows for the public sector. Standard contractual clauses or binding

corporate rules are not meant to be used in the public sector. The cooperation agreements or unilateral commitments that are used in the public sector, should continue to exist and even should be recognised explicitly in the text.

139. Regarding binding corporate rules the draft regulation aims to list the conditions that have to be met based on the existing requirements in the documents of the Article 29 Working Party[36]. The draft regulation does not copy the existing requirement regarding the necessity to introduce within a group of enterprises an internal system for complaint handling of the data subjects, as well as the introduction of a suitable training programme[37]. These obligations are not laid down clearly and can only be found within the task description of the data protection officer. Even if the latter has to be informed about complaints regarding personal data, it does not necessarily mean that he has to fulfil these tasks (complaint handling[38], employee training) and moreover, the explicit reference to article 35 in article 43.2.h does not always guarantee existence. The Article 29 Working Party documents , for that matter, demand that the members of the group of enterprises commit themselves to accepting that internal transparency (within the group) is necessary during a conflict between a foreign legislation and the binding corporate rules and that, in case of doubt, they should consult the European Data Protection Authorities[39]. This condition was not copied in article 43 of the draft regulation. And as is stressed above, the application of well-defined binding corporate rules should not be limited to multinationals that have an establishment inside the Union.

140. The derogation in article 44.1.h concerning the possibility that controllers can make their assessment of the circumstances surrounding a data transfer and adduce appropriate safeguards, is not only in breach with the system of "ad hoc" binding corporate rules and with that of BCR that require an intervention of the public authorities, but also endangers both systems.

29. Data Protection Authorities (articles 46 to 54)

[36]Mainly WP153 but also WP74 and WP108

[37] Points 2.1. and 2.2. of WP153.

[38] Complaint management must however be entrusted to a person or department that has an adequate level of independency while carrying out his or its duties (see WP 153 of the Article 29 Working Party but also CPP recommendation 01/2006 concerning whistleblowing).

[39] Point 6.3. of WP153.

141. Chapter VI of the draft regulation is completely dedicated to the supervisory authorities (Data Protection Authorities). Their status, the rules on their establishment, competences, duties and powers are more amply and explicitly described than in Directive 95/46/EC .

142. The draft regulation aims to strengthen the independence of the Data Protection Authorities and takes into account the judgment of 9 March 2010 of the Court of Justice of the European Union v. the Federal Republic of Germany[40].

143. The CPP is positive about the requirements in article 47 of the draft regulation concerning the independence of the Data Protection Authorities, in particular the *all-encompassing nature* of this independence: independence of its members (CPP commissioners), sufficient human resources and own staff (CPP secretariat), technical resources, adequate financial resources subject to financial oversight that does not threaten independence and the making available of the necessary offices and infrastructure to properly carry out its duties and powers. On this point the CPP would like to draw the attention of the competent Belgian authority to the new functions the Belgian DPA will be intrusted with and the resulting consequences for human and financial resources. The following examples can be given: prior data protection impact assessment (article 33), the handling of notifications of personal data breaches and the inquiry into the question whether the controller has taken the appropriate measures to prevent harmful consequences (articles 31-32), assistance to its European counterparts, co-operation with the latter and participation in the European Data Protection Board (chapter VII), as well as its new power to impose administrative sanctions (article 53.4 and articles 79.4, 5 and 6).

144. In relation to the general conditions applicable to the members of the supervisory authority (article 48), the CPP has two comments:

    a. Firstly, it considers that the consequences related to the fact that a member no longer meets the necessary conditions for the exercise of his function or has committed a serious error, should be left to the national legislator's consideration. The CPP deems that it is outside the European Commission's scope of competence to provide that a member can resign or is deprived of his pension rights and other benefits.

    b. Secondly, the CPP considers that the members of the supervisory authorities should always be appointed by parliament and not by government (article 48, paragraph 1, leaves this choice to the Member States). After all the parliament consists of representatives of all political groupings, which guarantees a better democratic control. According to the CPP, the appointment of members by parliament is more in

[40] European Court of Justice (Grand Chamber) , 9 March 2010, case C-518/07.

accordance with the conditions on independence stated in the Court of Justice judgment of 9 March 2010.

145. When the data processing takes place in the context of the activities of a controller or processor established in more than one Member State, the draft regulation states that only the authority of the "main establishment" of the controller shall be the competent authority (article 51.2). The European Data Protection Authorities have described this as a **one-stop-shop** for the controllers.

146. Although at first sight this is an attractive principle[41], the CPP has serious doubts on its practicability.

147. The concept of "main establishments" is one of the crucial elements in article 52 and the definition given for this concept (article 4, point 13) is anything but clear, especially regarding the following phrase: "(…) *if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place.(…)*". The CPP also wonders how conflicts of jurisdiction between DPAs - which inevitably will arise based on this unclear Article 52 - will be solved.

148. Furthermore, the CPP is concerned about the legal and practical consequences of the designation of one competent authority in a specific case. It believes that this concern can best be illustrated using some examples:

c. A Belgian employee who is employed in Belgium for a company with its "main establishment" in Ireland, submits a complaint against his employer to the Belgian DPA because his phone is being tapped. The Belgian DPA refers the case to the Irish DPA, which would be the competent authority in this case. Assume that the Irish DPA comes to an settlement between the employer and the employee. Should the Irish DPA in this case- in addition to the draft regulation – take account of, for example, Belgian social and criminal law?

   If the answer is yes, this implies that the Irish DPA has to apply Belgian law. A consistent application of such an approach would also imply that every DPA possibly has to be able to apply the laws of each of the 26 EU Member States when it has been appointed as the competent DPA, according to article 51, and when the case in question does not only affect the privacy regulation, but also other national laws

[41] The CPP understands the intention of introducing a one-stop shop in general, which provides that for a single processing operation that is performed in different Member States, different parallel authorities would have jurisdiction and therefore different decisions could be taken.

(which is often the case). The CPP has serious doubts about the feasibility of such a system.

If the answer is no, it is highly likely that in the example the settlement of the Irish DPA will conflict with Belgian binding legal provisions in social and criminal law. In the latter case, a Belgian judge will not be able to respect the settlement made by the Irish DPA[42].

d. A Chinese company has a branch in Belgium that sells products to Belgian citizens on the telephone. The company has several branches in the EU, of which the Polish branch is the "main establishment". The company proposes to record all telephone conversations between employees and customers, and explains that its sole aim is to improve the employee education and training. The unions fear, however, that the recorded conversations will be used for entirely different purposes (surveillance of employees) and they ask the Belgian DPA to mediate. The Belgian DPA –best acquainted with the social relations, social problems, the language of the people involved – will have to ask the union to address the Polish DPA.

e. An American IT company with several branches in the EU and the "main establishment" in Paris installs a cloud application together with a Belgian company. In this context a security breach arose and personal data of Belgian citizens are made public. Which DPA is has jurisdiction? Probably the French DPA. Does the Belgian DPA need to redirect all affected Belgian citizens to the CNIL?

149. In summary, the CPP fears that article 52, paragraph 2, will cause endless conflicts and discussions on jurisdiction between Data Protection Authorities and also thinks that this rule of jurisdiction will lead to illogical and unworkable situations. **The CPP therefore rejects the criterion of "main establishment".**

150. The CPP is also aware of the fact that this is a difficult exercise for which a lot of reflection will be necessary. In order to make a first contribution to this discussion, the CPP emphasises that this could be one of the possible alternative criteria: a DPA has jurisdiction in cases where controllers' activities target a certain customer base/market on the territory of the Member State where this DPA operates.

[42] This example also draws the attention to another problem, namely the fact that the rules of jurisdiction regarding DPAs are not consistent with those of the judiciary. Moreover, it is rather rare that the actions of a violation of the regulation are only related to data protection: the criminal offences mostly consist of several breaches of which one aspect is related to data protection and the other aspects can only be judged by the judiciary. A specific dispute must however be looked at as a whole (regardless of which legal branches it concerns and regardless of which DPA/court has jurisdiction) in order to come to a good solution.

30. Co-operation and consistency (articles 55 to 72)

151. Considering the globalisation of the processing of personal data, the CPP deems it useful to strengthen the existing co-operation systems between the European authorities through mutual assistance mechanisms (article 55), joint operations (article 56) and consistency mechanisms (articles 57 to 63).

152. The CPP, however, is of the opinion that the European Commission's possibility to request the suspension of a DPA measure, which according to the CPP threatens to lead to an incorrect or inconsistent application of the regulation (article 60), goes too far. How can a Data Protection Authority take any independent decisions, if they can be questioned by the executive power afterward? Such an approach, according to the CPP, conflicts with article 8, paragraph 3 of the Charter of Fundamental Rights of the European Union.

153. Considering the increasing number of topics dealt with by the Article 29 Working Party, the CPP thinks the establishment of a permanent secretariat for the Article 29 Working Party (future European Data Protection Board – EDPB) would be useful. The CPP nevertheless expresses its doubts on the term that was established for the approval of opinions by the EDPB (1 month) (article 58.7).

31. Penalties (articles 78 and 79)

154. First of all, the CPP has serious doubts about the usefulness of a uniform system of administrative sanctions to be executed by the Data Protection Authorities. The CPP wonders why this is proposed today, because it does not perceive the current situation as problematic. As an example, the CPP refers to the Google Street View case and the illegal obtention of data from internet connections (Wi-Fi), where the involved Data Protection Authorities applied, according to their own policy and legislation, the control system and the available penalty system when, if any, without any difficulties: the Dutch Data Protection Authority punished Google with a penalty payment, the French CNIL imposed a fine and the CPP referred the file to the public prosecutor who proposed an amicable settlement of 150,000 euros to Google.

155. Furthermore, the CPP opposes the fact that it would have the power to impose sanctions, especially because of its attachment to the principle of separation of powers. In relation to this the CPP would like to know if the combination of the powers granted to the CPP by the draft regulation are compatible with the impartiality requirement that is at least necessary for the execution of certain competences. This question would need to be thoroughly investigated, especially in the light of the jurisprudence of the European Court of Human

Rights[43]. A thorough reorganisation of CPP would be required (at organisational level, for example through separate chambers, modelled on the system that the French CNIL has introduced).

156. In this regard the Commission also notes that

a. from a constitutional point of view only the judiciary is authorized to check compliance with the law and to punish non-compliance. Independent magistrates have thus been intrusted with this power.

b. it is rather rare that the facts of constituting a violation of the regulation are solely related to data protection: criminal offences mostly consist of several infringements of which one aspect is related to "data protection". In those cases the scope of the Data Protection Authority will prevent the latter from dealing with the facts in a global manner. They will be limited to the aspect "data protection", because the CPP at its level cannot appeal to the concurrence of offences technique, according to which the maximum penalty is applied to facts under dispute. Only courts and tribunals may rely on this technique and handle criminal offences as a whole.

157. The CPP also wonders whether article 78 targets administrative or criminal penalties. In this article the following is stated: "*Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this regulation and shall take all measures necessary to ensure that they are implemented.(…)The penalties provided for must be effective, proportionate and dissuasive."*

158. Having regard to the choice for a regulation (instead of a directive) and after having read article 78 with the legal basis for the draft regulation in the preamble, the CPP decides that the Member States' task consists of providing for administrative penalties. After all, if the EU wants to instruct Member States to incorporate criminal penalties in their national law, article 83.2 of the Treaty on the functioning of the EU[44] needs to be used as legal basis. This article clearly requires that minimum standards related to criminal penalties have to be adopted by using a *directive* (and not a *regulation*).

159. The CPP also has serious doubts about the qualification of the sanctions established by article 79. Although these sanctions are explicitly described as "administrative sanctions", the

[43] Dubus v. France Judgment of 11 June 2009.

[44] "(…) If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned.(…)"

CPP is of the opinion that they are criminal sanctions, and having regard to the case law of the European Court of Human Rights[45] and the EU policy[46]. The importance of determining whether criminal sanctions are concerned, essentially relates to the fact that article 6 of the European Convention on Human Rights and article 6 of the Treaty on the European Union stipulate that in such a context sufficient legal safeguards must be provided (for example the possibility to appeal to an independent judge). The text of the draft regulation does not mention this at all.

160. Regardless of whether administrative of criminal sanctions are concerned, it is clear that the draft regulation introduces two systems (articles 78 and 79) and according to the CPP the combination of the two will cause problems. The CPP believes that a cumulative application of two penalty schemes can lead to a violation of the general legal principle according to which no-one can be prosecuted or punished on the basis of the same offences (non bis in idem).

161. In support of its analysis, the CPP would like to mention the judgment of 10 February 2009 of the Grand Chamber of the European Court of Human Rights (Zolotoukhine v. Russia), establishing that when an administrative and a criminal penalty are combined, there is a violation of Article 4 of Protocol No 7 which states: "*No one shall be liable to be tried or punished again in criminal proceedings under the jurisdiction of the same State for an offence for which he has already been finally acquitted or convicted in accordance with the law and penal procedure of that State.*"

In this case the Court considered that the procedure initiated against the plaintiff, although it was qualified as administrative national law, had to be considered as a criminal procedure, particularly because of the nature of the offence and the severity of the punishment.

162. The CPP also points out that according to the rule of law violations can only be penalised when they have been sufficiently defined, regardless of whether criminal or administrative penalties are imposed. The CPP has observed that many violations referred to in article 79, paragraph 4 to 6,or the violations for which the national legislator will impose sanctions, if any, as application of article 78, are a repetition of general obligations and are described in general or even vague terms that leave controllers at least a significant margin of discretion. What about predictability in this context? The CPP would like to mention article 5a) (lawful, fair and transparent processing), article 5e) (inexcessive retention period based on achievement of purposes), article 5f) (processing under the responsibility and liability of the

[45] See Engel Judgment of 8 June 1976.

[46] See article 6.3 of the Treaty on European Union, which leads to the conclusion that the EU supports the criteria used by the European Court of Human Rights to distinguish criminal cases from other cases. The European Court of Justice explicitly confirmed this in the Spector judgment of 23 December 2009 (§ 42, C-45/08)

controller, who ensures compliance for each processing operation), article 6e) (processing necessary for the performance of a task carried out in the public interest) and article 6f) (legitimate interest of the controller which does not prevail over the interests or fundamental rights and freedoms of data subjects).

163. Finally, the CPP would like to remark that article 79 of the draft regulation leaves DPAs little room for appreciation. Particularly, they cannot take into account the specific circumstances in which the violations were committed. Only in a limited number of cases in which a controller commits a first accidental violation, a sanction can be replaced by a warning. The CPP believes that more flexibility would be recommendable here.

32. Provisions relating to specific data processing situations (articles 80 to 85)

A. Existing national rules for the public sector

164. Chapter IX is related to the various sectors that differ nationally, and these divergences are considered to be justified by the difference in culture and legal traditions, for example in the area of free speech, the processing of data concerning health, social security or employment. States have therefore been requested to elaborate national legislation related to these aspects.

165. Since the introduction and development of fundamental rights, more specifically the right to the protection of privacy in general and the right to the protection of personal data in particular, many European countries have specifically strived towards an incorporation of these rights in their administrative and constitutional tissue. These rules on the protection of privacy in the context of data processing operations carried out by public authorities present so many national differences that the CPP believes that the existing systems of each Member State should be preserved.

166. In the field of health data processing, some room to manoeuvre has been given to Member States for medical purposes, national health or social security. Not so in this chapter for the processing of other data (than related to health) in the context of social security (and the data processing operations in this sector are obviously not only related to the simple reimbursement of health care costs; they can also be related to unemployment fees or pensions).

167. A second example is the Belgian system of sector committees, which was established to protect personal data in the public sector. The CPP believes that it should be fully maintained (see above).

168. The CPP is therefore of the opinion that it should be possible to declare certain provisions in the draft regulation inapplicable to data processing operations in the public sector, to ensure that national systems – with specific privacy protection safeguards (for example prior authorisations) that were established in the legal framework through the years - are not compromised an can be further regulated on Member State level.

B. Use of the National Register identification number

169. The CPP regrets the deletion of article 8.7 of Directive 95/46/EG, which allows states to determine the conditions under which a national identification number or any other general means of identification can be processed. This provision has been deleted without any explanation and has not been replaced by a specific rule related to this particular matter.

170. As a consequence it is feared that it will no longer be possible to use the identification number of the National Register in Belgium. This number is, however, one of the cornerstones of the most important existing e-government projects and a prohibition on its use *de facto* undermines all these projects, while there is no real justification for it based on privacy considerations. Belgian legislation provides for a special protective system of control and authorisation for the use of the National Register identification number. As mentioned above, the CPP wishes for this system of prior authorisations to be maintained.

171. Allegedly, the representative of the European Commission declared during the DAPIX meeting that the old system mentioned in 8.7. of Directive 95/46/EC should indeed be copied and that it was not the intention to obstruct the creation and use of identification numbers. The CPP is pleased with this statement and insists that the draft regulation is adjusted to this effect.

C. Processing of personal data concerning health

172. Article 81 of the draft regulation contains specific provisions on data processing operations relating to health.

173. These provisions should be read together with the definition of the notion of "data concerning health", mentioned in article 4.12. The latter provision should in turn be read with reference to preamble 26[47]. This reading shows that a very broad interpretation of this

[47]Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number,

concept is given: it does not only concern data relating to physical or mental health, but also any information about the provision of a health service to a person (such as patient registration for care provision, information on payments or eligibility of a patient for health care).

174. Firstly, the CPP is of the opinion that the definition given by the draft regulation is (far) too broad and does not sufficiently take into account the numerous contexts in which processing operations related to such data can occur.

175. Furthermore, the CPP notes that article 81 also enforces specific conditions (obligatory existence of a specific legal basis, obligatory professional secrecy or an equivalent obligation of confidentiality) to process such data, and these stipulations raise questions:

    a. The CPP considers that the requirement that for example data processing operations for the purpose of hospital invoicing services must have a specific legal framework, is rather useless/unrealistic.

    b. It is important to the CPP that the concept of "equivalent obligation of confidentiality" (article 81.1, a)) is not perceived as being limited to professional secrecy, since this would entail that all these processing operations would require the supervision of a health care professional (also data processing operations related to social security and the reimbursement of health care).

    c. The relationship between Article 81 and Article 9 of the draft regulation is entirely unclear according to the CPP. The latter article provides for a list of grounds for exceptions allowing for the processing of health data. One of these grounds is mentioned in article 81 (article 9.2.h) and it seems that article 81 is only related to this specific situation. However, medical data can also be processed on basis of other grounds, mentioned in article 9.2, and these data processing operations are not linked in any way to article 81. Moreover, there is an overlap between some of the other grounds for exceptions stated in article 9.2 and the three grounds listed in article 81.1, without any specific motivation for this. As a consequence, the CPP requests a thorough review of the link between articles 9 and 81.

---

symbol or particular assigned to an individual to uniquely identify the individual for health purposes;
[45]any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease
risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

D. Processing for historical, statistical or scientific purposes

176. The draft Regulation dedicates a complete article to historical, statistical or scientific research (article 83), which definitely facilitates the reading of the legal conditions for processing data related to scientific research[48]. The conditions set forth in article 83.1, which encourages the use of anonymous or encoded data in scientific research, are perfectly in line with our national legislation and other international standards[49]. Nonetheless, the CPP believes that the text of article 83.1 should express more clearly that data processing operations should be carried out on the basis of anonymous data as much as possible, and if this is impossible, processing operations should be based on encoded data and if also that is impossible, the processing of identifiable data can be admissible.

177. The CPP also considers it useful that historical, statistical or scientific research has been recognised as a legal basis for the processing of sensitive data (Article 9.2.i) [50]. Directive 95/46/EC allowed Member States to recognise scientific research as reasons of substantial public interest (preamble 40) and there were several national implementations in this context.

178. The CPP has more reservations about article 6.2. that seems to allow the processing of non-sensitive data for scientific purposes without complying with paragraph 1 of article 6. According to the CPP it is nevertheless of major importance that every research project undergoes this obligatory test of lawfulness in order to prevent the authorisation of unethical research projects.

179. Article 5.e. provides for the explicit possibility for longer data retention periods for historical, statistical or scientific purposes, it legitimises public archives and copies article 6.1.e. of Directive 95/46/EG. Pursuant to this article, Member States have to provide for appropriate safeguards and these safeguards are directly presented in the text of the draft because it is the intention that it this is applicable immediately. The condition is that periodic reviews are carried out to assess the necessity of continued storage. The CPP thinks it is useful to add other safeguards, such as the necessity of honouring the purpose of the research and the introduction of security measures, so that access is only possible in the context of the historical, statistical or scientific research.

---

[48] Currently the useful information is spread across Directive 95/46/EC, in particular in preambles 29, 34 and 40, and in articles 6.1.b, 6.1.e, 11.2, 13.2).

[49] Chapter II of the Belgian Royal Decree of 13.02.2001, but see also article 40 of the German Federal Law, article 46 of the Austrian Federal Law (DSG 2000), article 16 of the Estonian law and article 3 of Recommendation Rec (2006)4 of the Council of Europe on research that makes use of biological materials of human origin.

[50] The international conference on scientific research organised by the CPP in November 2010 also led to this finding.

180. The CPP is surprised that the exceptions related to the exercise of data subject rights (articles 11.2 and 13.2) included in Directive 95/46/EC, are no longer to be found in the draft regulation, unless in the form of a possible approval of delegated acts (article 83.3). The exceptions should be mentioned in the text itself, to guarantee their existence as of the date of entry into force, and they should contain the appropriate safeguards provided for by Member States today. Considering the experience gained in the scope of the international conference "Privacy and Research: from Obstruction to Construction", organised by the CPP in November 2010[51], the CPP has a concrete text proposal:

- *In addition to the circumstances referred to in Article 14(5), paragraphs 1 to 4 of Article 14 shall not apply where the data are directly[52] or indirectly obtained from the data subject, under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research[53]. From the moment that the information is not any more likely to render impossible or seriously impair the achievement of the objectives of the scientific research, the data subject shall be informed without delay.*
- *Article 15 shall not apply under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research, unless the interests of the research are overridden by the interests or the fundamental rights and freedoms of the data subject. From the moment that the information is not any more likely to render impossible or seriously impair the achievement of the objectives of the scientific research, the controller or processor shall grant the data subject access to the data without delay.*

E. Data protection rules of churches and religious associations

181. The CPP wonders which is the scope of article 85 of the draft regulation.

33. Delegated acts and implementing acts

[51] http:/www.privacyandresearch.be/

[52] An exemption in case of direct collection already exists in different national legislations such as the German Federal Law (Art.33), the Portuguese law (Art. 10) and the Luxembourg law (art. 27).

[53] Giving clear information on the specific purposes of the research can obviously influence and therefore compromise its findings .A similar exception is found in Polish legislation (Art. 25 of the Act of August 29, 1997) for the indirect collection of data.

182. The draft regulation is characterised by a large number of delegated and implementing acts (articles 86 en 87).

183. The CPP is of the opinion that in almost all cases, the envisaged delegations do not comply with the conditions under which delegated acts are allowed (article 29 §1, 1st subsection TFEU). The object of a delegated act should normally be aimed at completing a legal act by specifying certain technical elements, or aimed at altering the non-essential elements of the legal act itself. Notwithstanding the strict interpretation given to the concept of essential elements and the consequential extensiveness of authorised delegations[54], the CPP believes that in this case the European Commission exceeds its competences given the number of authorised delegations (article 86.2), their objects and the fact that in the absence of some of them, the provisions in the draft regulation cannot have any (useful) effect.

184. The draft regulation does not provide any information on the intention, if any, of the European Commission to approve these numerous delegated acts, nor about the term for their possible approval. What is to be done pending these delegated acts? It cannot be the intention to replace an existing system that is working well with new legal rules that still require many crucial points on delegated or implementing acts (of which the content and timing is very unclear) before they can be put into practice?

185. The CPP therefore strongly insists on strictly limiting delegated acts and implementing acts to non-essential elements. This consequently implies that almost all articles of the draft regulation that allow for such acts, should be revised.

Annex: Considerations on the public-private distinction following the proposal for a data protection regulation COM(2012)11 of 25/01/2012

[54] N. de Sadeleer, I Hachez " Hiérarchie et typologie des actes juridiques de l'Union européenne", in *les innovations du Traité de Lisbonne : incidences pour le praticien,* Brussels, 2011.

1.1. The main question is whether a separate, legal, regulatory framework is needed for the public and private sectors. Concerning this issue, the specific needs for police and justice are disregarded as these were already presented in another instrument[55].

1.2. Such an approach needs to be avoided as much as possible. All arrangements, both the basic principles and the actual elaboration, should be unified to every extent possible. This especially goes for the basic principles (the basis for the elaboration, the principles, the rights of the person concerned, law enforcement, international data exchange). But the same instrument and legal framework should also apply for the actual elaboration, procedures, independent supervisor, exceptions and so forth.

Today the international regulatory texts concerning privacy and personal data protection, do not make this distinction and they are intended to be applicable in both the private and public sectors.

On this issue, Convention no. 108 of the Council of Europe (1981) can be quoted, more specifically article 3, §1 (scope), which explicitly states: "*The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.*" An application in the public and private sectors has not been questioned in any way in the current modernisation/revision process of Convention no. 108.
The explanatory report of Convention no. 108 gives an explicit formulation of the broad scope (paragraphs 33 and following):
"*According to paragraph 1 the convention applies to the public as well as the private sector. Although most international data traffic occurs in the private sector, the convention is nevertheless of great importance for the public sector and this for two reasons. First, Article 3 imposes obligations on the member States to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country.*
The distinction public sector/private sector is not found in the other provisions of the convention, especially since these terms may have a different meaning in different countries. ***But it may play a role in the declarations which the Parties may make with regard to the scope of the convention (paragraph 2).***"

Certain countries make use of the possibility offered in Article 3, §2 to deviate from the scope in the Convention (also see the explanatory report above), namely for certain files from the

[55] Which immediately will cause numerous problems because no clear boundaries were made between the world of police and the judiciary, and the private actors that have a role in it (lawyers, notaries, bailiffs, GAS (administrative penalties), private security, private detectives, etc.). In any case, there is a need for a legal instrument to frame this.

public sector[56]. Taking the explanations in the footnote into account, it appears that this exclusion from the scope has taken place when national law created a type of framework for these type of files (flexibility for the public sector – role of national law).

It is interesting to know that the Belgian state has not made use of this possibility. However, it has to be said that at the time the protection of personal data was only in its infancy (the first binding, legal instrument) and that it concerned an international Convention that "had to be transposed into national law" (see the declaration of Belgium on 28/05/1993).
http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=&DF=&CL=FRE&VL=0
English:http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CV=1&NA=21&PO=999&CN=999&VL=1&CM=9&CL=ENG

European Directive 95/46/EC covers the public and private sectors in the same manner (with the nuance in 1.1. concerning police and justice and the domains that are not within the authority of the European legislator but within national sovereignty). This is not only stated literally and explicitly in Convention no. 108 but is also deduced from the provisions in the directive. See for example the definition for the responsible authority for the elaboration that also implies the "public authorities". This option is not questioned in the proposal for a regulation by the European Commission and was not seen as problematic in the Commission's evaluation report.

The choice of instrument by the European Commission, namely a directly applicable regulation, (instead of a directive that has to be transposed into national law) is also included in the analysis. Where a conversion – which is necessary due to the nature of a directive – gave the national legislator certain room to manoeuvre, in particular for potential data processing activities of the public sector, the directly applicable property of a regulation does not allow any nuances, unless the regulation itself would provide specific, nuanced or sufficiently flexible provisions which take the particularities of this sector into account. The reading of the regulation draft and the explanations that were given by European Commissioner V. Reading on the matter, indicate that the text was first conceived for companies and multinationals from a desire for simplification, legal certainty and free movement of data in a global context. If one looks at what the Council of Europe stated in

[56]Examples of reservations concerning "public sector": see the declaration of Andorra: no application of the Convention on the "public records explicitly regulated by law in Andorra". Liechtenstein on its part has removed the processing operations by the Ministry of Finance, the Parliamentary Assemblies and Committees from the scope (ditto for Switzerland for the parliamentary assemblies). See also the Luxembourg Declaration which dropped the application of the Convention on **databases that are accessible to the public by law or regulation**. The Netherlands made in turn the same reservations about numerous files: **archives designated by law, files that are used for the implementation of the electoral law, the register of civil status, the central register of students in higher education, drawn up in the framework of the law on university education** (As a more classical example, many countries excluded the data related to national security, public safety and criminal violations).

1981, namely that most of the (international) data flows is related to the private sector, the desire from the EU becomes meaningful. That does not mean that a certain flexibility with respect to data processing in the public sector - very clearly identified and defined processing – should stand in the way of the realisation of these objectives by the private sector. The protection of personal data in/by the public sector, should respect the regulation through specific adaptations and the national regulations should be taken more into account (traditionally more applicable to that sector, or at least more than in the private sector).

1.3. One of the difficulties that one always encounters when making such a distinction, is the question which criterion should be used. Will people work organically, or will they prefer a material approach. And what about intermediary institutions and tasks (public & private). The case law of the Council of State and the Court of Cassation (attribution conflicts) on, for example, whether free educational institutions are administrative authorities or not, is a good example of a discussion that will never really be settled: a never ending story. But there are of course many other examples: social security, health care ...

2.1. This does not mean that public institutions, administrative bodies, administrations or what else belongs to the public authority *sensu strictu or lato* have no need for their own arrangements. The public sector has specific characteristics that are unique to the government: privilège du préalable, direct execution power, monopoly rights, democratic control from legislative and executive power, etc. This should be taken into account in the actual elaboration of the basic principles and especially with the procedures and forms of supervision and law enforcement.

2.2. Another aspect is to monitor and maintain the acquis: many public institutions have a sophisticated toolbox for processing personal data. In many cases, this processing consists also of privacy and security arrangements. In many cases, these mechanisms work satisfactorily, not to say very well. As an example, a reference may be made to the whole functioning of the Crossroads Bank for Social Security.

To question this system without letting the theoretical principles of the proposed EU regulation on personal data processing prevail threatens to cause huge administrative problems and the destruction of a refined and workable toolbox for personal protection. Take a similar look at the act on the National Register and the Sector Authorisation Committee, an additional mechanism in accordance with the requirements of the Directive 95/46/EC on the framework for the processing of unique means of identification (see below).

2.3. Neither can we ignore the merits of Directive 95/46: it makes no sense to simply set aside the qualities of this directive. As an example: article 8 point 7[57], which set the basis for the continued use of the National Register number and the further development of the National Register. Of course in a legal and regulated manner, amongst others through the Sector Committee of the National Register. It concerns an important instrument in administrative law: e-government, which is meant for the public sector[58]. This is just one example of the quality of the earlier directive which, unfortunately, currently has not been repeated in the European proposal. In the context of specific arrangements for both private and public applications, it would be preferable to continue building on the achievements of Directive 95/46.

2.4. Respect for democratic achievements and control. Here one can refer to the Belgian generally binding collective agreements that have made, through social dialogue, significant contributions to the privacy protection and the acceptance by the sectors. But the same applies for example to the social security: it is managed through equal representation and under control of the Sector Committee of Social Security. In the totality of the privacy protection, there are many examples of privacy protection that were developed, not by the government sensu stricto but by civil society, social partners and all of the actors in a certain sector: see in that regard the health sector. To replace these achievements by "delegated acts" is a clear degradation of democratic achievements. See article 81 and 82 of the EU proposal in this regard.

3. Practical problems concerning p&p in the actual proposal for a regulation

3.1. Article 6.1.f (balanced interests): it is difficult to understand why article 6, lawfulness of processing, excludes "public authorities" for this processing ground. Preamble 38 specifies that "*Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks."* This motivation cannot convince the CBPL. See the argumentation in the draft opinion on the proposal for a regulation.

[57] Member states determine the conditions under which a national identification number or another general identification number may be used for processing purposes.

[58] Authorisations are granted to public and private institutions of the Belgian law for the information they require to perform general interest tasks entrusted to them by or under a law ... or for tasks that are explicitly recognized as such by the aforementioned Sector Committee (Article 5, first paragraph, 2 ° of the Law of 8 August 1983 National Register).

3.2. What about article 21 of the proposal?

3.3. The article of the proposal that causes us most concern is article 34: prior authorisation and prior consultation. A sustained application of the mind of this provision should lead to the prohibition of the whole of prior authorisations on which the system of sector committees and regional supervisors is based. The basic mechanism is indeed a prior authorisation to a request by the controller, building up a dossier, satisfying basic requirements (including security), advice from reference institutions and assessment by an equally constituted governing body.

The "solution" for the Belgian Commission for privacy protection to make use of the possibility stated in article 34 §4 (consultation mechanism), can, according to the Commissioners, in the present text definitely offer the same amount of protection as the mechanism of the existing sector committees.

After all, article 34 §4 stipulates: *"The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board."*

Article 34, §2 b) states that the controller or processor will consult the data protection authority if: "*the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4."*

HOWEVER…

- The Belgian authorisation mechanism of sector committees is not solely based on risk (in some cases it is even based on the non-existence of risks, for example the Crossroads Bank of Enterprises) but also/especially on a sectoral approach;
- With regard to the composition which partly is a reflection of the sector concerned, one could question its compatibility with article 47 §3 (independence) of the proposal for a regulation which mentions that *"Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not";*
- And ESPECIALLY, the list of processing operations which would be approved by the CBPL (and which is a reflection of the competences of the current sector committees) is (pursuant to article 58, §2 c) has been submitted to the European Committee for

data protection for an opinion and consequently for a possible opinion and a potential suspension measure by the European Commission (articles 59 et seq., chapter that deals with co-operation and a consistency mechanism).

3.4. Article 51.2, competence: the one-stop shop principle: causes particular problems for authorities, in particular with relations, contracts, co-operation in international enterprises and organisations (for example ICT, especially clouds, pharmaceutics, financial…). As in many cases the authorized DPA will not be the national supervisor, this poses the problem how a foreign DPA will deal with the proper administrative, constitutional structure of all these other countries…

3.5. Chapter IX, provisions relating to specific data processing situations in the field of personal data processing, especially articles 81, 82, and to a certain extent 83 en 85 pose particular questions and problems for the public sector. At first sight they offer possibilities for the authorities to act in certain domains based on their mission as a public authority. They are nevertheless formulated as exceptions, which results in the fact that in the whole concept of the regulation no room is provided for other domains in which the government operates. Moreover, these exceptions are formulated in such a sharp and restrictive manner that they rather become a kind of straitjacket than an actual possibility for interventions by national governments.

4. A basic problem that goes far beyond the purpose of this p&p note stems from the totalitarian claim of the EU proposal.

4.1. The processing of personal data is not a stand-alone activity. The protection of personal data is a transversal and relative fundamental right. Transversal because this right relates and has to be applied to almost all human activities. Relative because the law almost never stands alone but has to be balanced and equilibrated with other rights and freedoms.

4.2. Formulating a universal system for personal data protection that does not leave room (anymore) for other rights and freedoms, embedded in the constitutional, administrative and organisational structure of a state, community and society is threatening to collide with those other foundations and fundamental rights.

For the Administrator (on leave) ,

Patrick Van Wouwe

The President,

Willem Debeuckelaere