Opinion No. 10/2014 of 5 February 2014

Subject: own-initiative opinion 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, as voted by the LIBE Committee of the European Parliament on 17 October 2013 (CO-A-2014-001)

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 Privacy Act), in particular Article 29;

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

Issued the following opinion on 5 February 2014:

Summary

On 21 November 2012, the CPP presented a critical own-initiative opinion on the 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* (hereinafter the "Draft Regulation") filed by the European Commission.

In line with the objections and comments expressed in Opinion 35/2012, the CPP has set forth below its point of view in relation to the draft text adopted by the European Parliament's "Civil Liberties, Justice and Home Affairs" (LIBE) lead Committee on 17 October 2013.

The CPP would like to draw the attention of both competent MEPs and (Belgian) politicians - today and following the upcoming elections - to the implications of the guidelines adopted by the lead Committee. Particular attention is paid to certain concepts that are not included in the proposal submitted by the European Commission (pseudonymous data), which take on another dimension in the eyes of the MEPs of the LIBE Committee (certification, BCR Processor) or which are widely discussed at all relevant levels of the European Council (profiling, the "one-stop-shop" principle and remedies, processing for historical, statistical and scientific research).

Enhanced protection of the rights of the data subjects? One of the stated objectives of the data protection reform consists in strengthening the rights of the data subjects, especially in the digital age and in the face of the (European and non-European) giants of the Internet. In its Opinion 35/2012, the CPP immediately raised doubts as to the actual strengthening that would be provided by the draft regulation, in particular in relation to the acquis of Directive 95/46/EC.

Actual protection does, of course, involve the content of the law but also its effective implementation (particularly its having to be practicable for controllers) and, *ultimately,* the means available made available to the data subject to assert their rights vis-à-vis the controller, the supervisory authority and the judiciary. The CPP has made the following comment in support of this assumption.

I. Adequate scope

1. The processing of data carried out through the use of social networks cannot fully escape the application of the draft Regulation. This must be included in its *scope* and the scope of the exception for purely personal and domestic activities must be defined to cover it (paragraphs 6 et seq.)

2. The CPP opposes the inclusion of the concept of *"pseudonymous data",* whether they are the result of encoding or a means of identification in the digital environment. The inclusion of a subcategory

of personal data in the draft regulation further complicates the interpretation of current concepts of "personal data" and "anonymous data" on which the existing system is based. By providing an unclearly "reduced" protection system for this category of personal data, the proposed reform would result in an unacceptable reduction of the safeguarded level of protection (paragraphs 9 et seq.).

II. Adequate definitions

3. The CPP calls for a definition of data relating to health that recognizes the context in which the processing of such data takes place (paragraph 15 et seq.). As these data are processed for the purposes of developing therapies; it is opposed to the obligation of Member States to adopt specific legislation to enable their processing (paragraphs 129 et seq.).

III. Adequate derogation scheme

4. The LIBE Committee limits the possibility of exemptions from the application of the Regulation, whether through articles which may be waived or through the grounds on which the Member State may establish a derogation scheme. In this regard, the CPP would like to alert the reader to the deletion of the concept of "general interest of the Union or of a Member State" and its replacement by the words "taxation matters" (paragraphs 56 et seq.).

IV. Effective rights, strengthened (or at least safeguarded in respect of the acquis of Directive 95/46/EC) for the data subjects

5. The CPP welcomed the changes made by the LIBE Committee as regards the content of the *provision of information* to data subjects, particularly as regards the data retention term, the security measures put into place, the logic behind the processing, the elements relating to profiling and safeguards for cross-border flows. It is not convinced, however, of the added value of the symbols that have been put forward. Finally, it is also opposed to the abolition of the exercise of certain rights of the data subjects in cases where the controller is subject to professional secrecy (paragraphs 18 et seq.).

6. The CPP regrets that the deletion of the words "right to be forgotten" in the title of Article 17 is not accompanied by further *clarification as to the exact scope of the right to erase* which this article confirms. In particular, the CPP believes that the obligation for data controllers to contact all third parties who have legally re-disclosed the initially processed data will be difficult to implement (paragraphs 24 et seq.)

7. The CPP notes that the LIBE Committee does not provide a comprehensive fix to the weakening of the *right to object.* The right to object enshrined in the Privacy Act (Privacy Act) disappears in cases where the data subject's consent constitutes the legal basis for the processing of data. The balance of

interests to be carried out by controllers - which can lead to them denying data subjects the exercise of a right - creates the unacceptable risk that the controllers continually invoke their legitimate interests to oppose the exercise of the right to object (paragraphs 31 et seq.).

8. As to the proposed framework for *profiling,* the CPP calls for a protection system which constitutes a framework for both processing operations based on a profile and automated individual decisions currently covered by Article 15 of Directive 95/46/EC. As to profiling in itself, creating a profile on the one hand as well as the application of profiles on the other should be regulated, in the spirit of the Recommendation of the Council of Europe Convention on profiling, and the "right to anonymity" it introduces (paragraphs 33 et seq.).

9. The CPP regrets the reduction to the barest minimum of the obligation to provide *mandatory documentation*. In this form the obligation no longer requires the controller to consider the relevant issues with regard to the envisaged processing as is the case with the current notification requirement which it intends to replace. The CPP believes that the documentation should at least include, in addition to contact details of the possible controllers, processors, representatives and Data Protection Officers and recipients of the data, a description of the purposes of the processing operations and of the categories of data processed (paragraphs 60 et seq.).

10. The CPP requests that the *system of sector committees and their competence of prior authorisation* of specific data processing operations be maintained under the new EU regulation. It is convinced that such committees' analysis is essential and that the conditions included in their authorisations adequately frame (mainly) public sector data streams. It strongly advocates maintaining such a beneficial mechanism for the protection of citizens' privacy and personal data (paragraphs 68 et seq.).

11. In other words, the CPP regrets that the practices and the positive experiences of some Data Protection Authorities in the implementation of their national regulations have not been taken into consideration. On top of the mechanism of authorisations issued by the above-mentioned sector committees, the CPP regrets the loss of the provision of current Directive 95/46/EC allowing for a framework for access and use of the *national register number*. It calls for the continuation of this situation (paragraphs 127 et seq.).

12. With its experience in the field, the CPP also proposes a number of amendments to the framework for *historical, statistical and scientific research* which aim at an adequate balance between the interests of researchers on the one hand and the necessary respect of the protection of privacy and personal data in this sector on the other hand (paragraphs 131 et seq.).

13. As for the *bodies and remedies available* to data subjects, the CPP cannot support the elaboration of the one-stop shop principle in the proposal for a regulation (see below).This principle is accompanied by a variety of administrative and judicial remedies available to data subjects, both in the Member State where they have their residence and abroad. According to the CPP, the complexity of the system of remedies offered by the draft regulation - particularly in the version adopted by the LIBE Committee - does not offer sufficient safeguards to conclude that Articles 16 of the TFEU, 8 and 47 of the Charter of Fundamental Rights of the Union, and 6 (right to a fair trial) and 13 (right to an effective remedy) of the European Convention on Human Rights as having been fully implemented (paragraphs 115 et seq.).

14. The CPP welcomes the LIBE Committee's attempt to provide a solution to the transfer of data to non-adequate third countries, in particular those identified in the SWIFT case (and transfers of data to the UST (U.S. Treasury)), and more recently by E. Snowden's revelation of extensive monitoring programs carried out by the U.S. Secret Service (NSA - National Security Agency). The CPP opposes, however, the role intended for Data Protection Authorities, including giving them the power to authorise such transfers, and has serious doubts as to the desirability and feasibility - both from a practical and legal point of view - of providing individualized information to data subjects about such transfers (paragraphs 95 et seq.)

V. Obligations which companies can carry out and which are beneficial to the protection of data subjects' data – risk-based approach

15. As mentioned in its Opinion 35/2012, the CPP advocates a system of coherent obligations based on a specific assessment of the actual risk induced by processing operations.

16. The CPP believes that *data breaches* which require notifications – either to the Data Protection Authority or to the data subject – are not (sufficiently) defined. This lack of precision could lead to the ineffectiveness of this obligation and the related useful information it aims to provide to the supervisory authority and to individuals (paragraphs 62 et seq.), and this right from the start.

17. The CPP supports the deployment of the function of *Data Protection Officer* provided that the appointment of such an Officer remains an option for the controller. This function should be seen as an accountability measure which the controller should be able to take freely, considering the processing operations carried out, the actual risks, the existence of other protection mechanisms and the actual benefit they would provide to the protection of data. Accordingly, the CPP cannot agree with the LIBE Committee's approach which further extends the circumstances in which the appointment of an Officer is mandatory, *a fortiori* in hypothetical cases based on risk criteria that do not appear relevant (paragraphs 76 et seq.).

18. In the same context of supporting incentives to the dissemination and the implementation of a true culture of corporate data protection, the CPP regrets that the LIBE Committee has omitted *the Processor BCR* (Binding Corporate Rules for processors). These rules provide a high level of data protection in the event of transfers of data processed initially by a multinational group acting as a processor. Opposing them would only create legal uncertainty and push companies to opt for less protective tools that do not offer the advantages of BCR to promote European data protection rules abroad (paragraphs 86 et seq.).

19. The CPP insists that the criteria and requirements for *certification* schemes, including the conditions for granting, revoking and recognizing within the EU and in third countries as well as the criteria for the accreditation of certifiers are determined by Data Protection Authorities. Under those conditions alone, it could accept that certification includes the same sufficient safeguards for data transfers to a non-adequate third country in the same way as model clauses or BCR. It is, however, opposed to a system of reduced sanctions for certified companies which have been found guilty of a breach of the draft regulation (paragraphs 75-81 and 85).

VI. An accessible Data Protection Authority

20. As for its own role, the CPP believes it is certainly likely to evolve, regardless of the fate of the draft regulation submitted by the European Commission. Several of the above comments highlight some of the CPP's concerns about the role that is intended for it, about the competences that it would be entrusted with (certification, authorisation of certain data transfers outside the European Union (Article 43a)), the removal of the competence to authorise data flows in the public sector). Its independence as well as its mission to raise awareness, guide and assist the general public and companies must be preserved.

21. As for *sanctions,* the CPP is particularly concerned about maintaining the primary objective of its work, which entails ensuring the compliance of processing operations with the requirements of the data protection rules. Based on its experience, it favours mediation over sanctions, particularly so for reasons related to the need to respect the principle of separation of powers. The excessively high amounts, even if these are maximum amounts, of administrative fines planned by the LIBE Committee reinforce this position (paragraphs 123 et seq.).

22. Finally, the CPP believes that regular and structured cooperation between (European) Data Protection Authorities is essential. However, it favours the creation of a *European Data Protection Authority* (with a legal personality, established in the European Union and with the power to take decisions binding on all the States of the Union) for cases relating to "cross-border" processing operations (i.e. processing operations common to several EU Member States). In this respect, it is in favour of

strengthening the role of the European Data Protection Board (EDPB – paragraphs 109 et seq.), including in the preparation of delegated acts (paragraphs 141 et seq.). Alternatively, it rather defends the concept of a lead authority associated with a co-decision procedure than that of a one-stop shop with an exclusive role for the lead authority of the main establishment of the controller, which would take decisions binding on all protection authorities involved. The Data Protection Authority should remain a local contact, especially for citizens who wish to lodge a complaint (paragraphs 104 et seq.).

I. Introduction, background, scope and aim of this opinion

1. On 21 November 2012, the CPP issued a critical own-initiative opinion on the *proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Regulation on data protection - hereinafter referred to as the "Draft Regulation") filed by the European Commission on 25 January 2012.

2. In line with the objections and comments expressed in Opinion 35/2012, the CPP has set forth below its point of view in relation to the draft text adopted - as part of the co-decision procedure – on 17 October 2013 by the European Parliament's "Civil Liberties, Justice and Home Affairs" lead Committee (hereinafter "the LIBE Committee").

3. The CPP has not conducted a systematic review of each of the numerous amendments adopted by the LIBE Committee. Its analysis does not purport to be exhaustive.

4. The CPP does however wish to draw the attention of competent MEPs and (Belgian) politicians - today and following the upcoming elections – to the implications of the guidelines adopted by the lead Committee. Particular attention is paid to certain concepts that are not included in the proposal submitted by the European Commission (pseudonymous data), which take on another dimension in the eyes of the MEPs of the LIBE Committee (certification, processor BCR) or which are widely discussed at all relevant levels of the European Council (profiling, the "one-stop-shop" principle and remedies, processing for historical, statistical and scientific research). The CPP has closely monitored the European debate on the document, providing independent technical support to the Minister and the Federal Public Service of Justice, especially during the meetings of the DAPIX working group (Working Group on Information Exchange and Data Protection).

5. As already mentioned, the comments below are in line with those expressed by the CPP in relation to the draft regulation submitted by the European Commission in its Opinion 35/2012. Where appropriate, explicit reference is made to the latter opinion.

II. Analysis of certain key concepts and provisions

1. Chapter I: General Provisions

1.1. Material Scope (Article 2)

6. The LIBE Committee considers that the exception for purely personal and domestic activities also covers data disclosures which can reasonably be expected to be accessible only to a limited number of people.

7. This position is in line with the jurisprudence of the Linqvist judgment of the Court of Justice of the European Union[1] and allows us to consider, for example, that the processing operations carried out by individuals in the context of their use of social networks are *included* in the scope of the draft regulation, if the information is made accessible to an indefinite number of people. Although the practical implementation of all of the obligations of the draft regulation by individuals may pose some practical problems, the CPP nevertheless supports the idea of the principle according to which such processing operations should remain within the scope of Personal Data Protection law. A system, if any, adapted to the specificity of social networks and taking into account freedom of expression and information, could be put into place.

8. Considering the risks resulting from the use of social networks, particularly the loss of control of information, and given the harmful consequences of such data processing operations (corroborated by the number and nature of the complaints the CPP receives in this context), it is inconceivable for the CPP that such operations are not at all part of the scope of the regulation on the protection of personal data and that data subjects are deprived of any remedy in this regard.

1.2. Pseudonymous data (Article 4.2a)

9. The LIBE Committee introduced the concept of "pseudonymous data" in Article 2a) by defining them as *"personal data that cannot be attributed to a specific data subject without additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution".* The LIBE Committee also provides a number of specific conditions for the processing of such data (see below), including exceptions which have caused the CPP to express the below thoughts and comments.

[1] Case C-101/01, ECJ, 6 November 2003.

The concept of pseudonymous data: a multi-faceted reality

10. The identification of a person is not limited to the mere possibility of knowing their civil identity (surname, name, address, etc.) but also includes the **ability to be able to recognize them or distinguish them from others** *(the person is "singled out").* Under the personal data protection system individuals must be protected as soon as they can be singled out given that starting from this moment, they can be treated individually/differently, with a risk of discrimination. According to the CPP, **the concept of pseudonymous data in practice covers very different situations:**

11. *Pseudonymisation of data (e.g. encoded data):* the data relating to the civil identity of an individual are replaced by an alias or a code. This minimization process is frequently used in the context of scientific research, **where the aim is not to take individualized measures** with regard to any particular person but rather to **increase the overall knowledge of society. The pursuit of that legitimate objective has led to an adapted and separate system** in the current rules (Directive 95/46/EC and the Privacy Act). **In this context, pseudonymisation[2] is subject to the requirements of proportionality:** if it is not practicable to achieve the research objective using anonymous data[3], the use of pseudonymisation is permitted.

12. *"Digital" pseudonyms as an alternative form of identification:* the development of the information society enables private companies to single out individuals without necessarily needing to know their civil identity. Other identifiers are used (a login, a code linked to a phone or to a computer, a smart card or a fingerprint). These identifiers are used to obtain and collect accurate information on consumer habits, travel, employment, standard of living etc. of data subjects which have been singled out. **These processing operations directly aim to treat people in an individualized manner,** by providing them with personalized information, by offering different prices, by granting or restricting access to certain services.

[2] ISO 29100 defines pseudonymisation as follows: *"Pseudonymisation: process applied to personally identifiable information (PII) which replaces identifying information with an alias. Note 1 to entry: Pseudonymisation can be performed either by PII principals themselves or by PII controllers. Pseudonymisation can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use. Note 2 to entry: Pseudonymisation does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymised data which are able to determine the PII principal's identity based on the alias and data linked to it"*.

[3] See Chapter II of the Royal Decree of 13/2/2001 implementing the Privacy Act.

An unclear reduced protection system? Rejection by the CPP

13. In both cases, pseudonymous data are personal data. This important qualification stems from the definition given by the LIBE Committee and the CPP considers it to be essential. **However, the CPP rejects the idea of including a definition of "pseudonymous data" in the new rules for two main reasons:**

- Including a new concept of pseudonymous data which differs from the definition of personal data - even though pseudonymous data is personal data - will only create more confusion in the interpretation of the concepts of personal and anonymous data;

- Some amendments (see below) suggest that pseudonymous data should generally be subject to a reduced data protection scheme (a "light scheme"), which seems simply unacceptable to the CPP. Although the particular context of scientific research can justify a modified scheme possibly including derogations in certain respects, such derogations are not justified for all pseudonymous data, quite the opposite in fact. According to the CPP, digital identity must benefit from the same protection as civil or traditional identity. It is essential that the processing operations referred to in paragraph 12 above are fully subject to data protection law, which safeguards the balancing of represented interests and transparency in respect of individuals.

  On this last point, the CPP refers in particular to recital 38 as voted by the LIBE Committee, which provides that pseudonymous data processing operations are, *ipso facto,* to be considered as meeting the reasonable expectations of the data subjects, which could lead to the elimination of the balancing of represented interests under Article 6.1.f of the draft regulation. Recital 58a raises the same issue by stressing that profiling performed exclusively through pseudonymous data processing should be presumed to not significantly affect the rights or freedoms of the data subjects. Data pseudonymisation is solely a technical measure that can be taken into account when balancing represented interests, but cannot in itself replace the analysis of other contextual elements (see also below paragraph 54 under Article 20 on profiling).

1.3. <u>The concept of "profiling" (Article 4.3a)</u>

14. This key concept in the digital era and that of data warehouses, which does not appear in the European Commission's original draft, is defined by the LIBE Committee. Reference is made in this regard to the analysis of Article 20 which deals with the framework for profiling (paragraphs 39 to 44).

1.4. Definition of data related to health (Article 4.12)

15. In its 2012 opinion, the CPP drew attention to the fact that the definition of "health data" contained in the European Commission's proposal is (much) too broad and did not sufficiently take into account the multiple contexts in which the processing of such data may occur[4]. The definition adopted by the LIBE Committee poses the exact same problem. To take just one example: imagine that footage from video surveillance cameras shows that a person has a broken leg; on the basis of the definition contained in the text adopted by the LIBE Committee, this would constitute a processing of data related to health which is therefore subject to a special protection system.

16. In order to avoid such absurd situations, the CPP advocates for rules focusing on processing operations as well as on their purpose (and not on the nature of the data processed)[5]. In this way, far fewer processing operations would be subject to the processing prohibition, which could thus be limited to those cases in which processing operations involve an actual risk. Specifically, the CPP proposes the following wording:

"Article 4 (12) "données concernant la santé" : toute information relative à la santé physique ou mentale passée, actuelle ou future de la personne concernée ;"

(TR: ""Article 4 (12)"data related to health" means any data relating to the past, current or future physical or mental health of the data subject;")

"Article 9, point 1. Le traitement des données à caractère personnel visant à révéler (…) des données concernant la santé (…) sont interdits."

(TR: "Article 9, paragraph 1. The processing of personal data aimed at revealing (…) data related to health (…) shall be prohibited."[6]

[4] Paragraphs 23 to 25 of Opinion No. 35/2012

[5] This would be in line with the notion of the processing of data related to health in the context of the modernization of Convention No. 108. Without prejudice to the principle of a definition "by nature", an alternative would consist of taking the context into account when determining the *conditions* under which the processing of data related to health could take place.

[6] Note: if this approach were to be adopted, the recitals relating thereto would also have to be reviewed (see recital 26, for instance).

2. Chapter III: Rights of the data subject

17. The European Commission states that the reform it proposes aims to strengthen the rights of data subjects in the digital age. In its Opinion 35/2012, however, the CPP shows that this goal is not always achieved; neither through certain new provisions nor through certain amendments to existing rights. In general, the CPP is opposed to any curtailing of the rights enshrined in Directive 95/46/EC and transposed into Belgian law by the Privacy Act. It is in light of these concerns that it makes the following remarks in relation to the direction taken by the LIBE Committee.

2.1. Right of information (Articles 13a and 14)

18. The CPP supports the changes made by the LIBE Committee regarding the content of the information to be provided to data subjects in relation to, more specifically relating to: the data retention term (which can now be determined in a flexible manner by referring to certain parameters and no longer only in terms of a quantified duration - Article 14.1.c)), the security measures implemented (Article 14.1.b)), the logic involved in the processing (Article 14.1.gb)), the specific elements of information in the event of profiling (Article 14.1.ga) - See, however, the request for explanations in paragraph 45 below), the safeguards for cross-border data flows (Article 14.1.g)) and the information that data were communicated to a public authority during the previous 12 months under Article 43a) (see paragraph 100 below for this particular item).

19. Conversely, the CPP has serious doubts about the added value in terms of actual information provided to the data subject of the 6 symbols the controller mandatorily has to provide in addition to the elements referred to in Article 14 (Article 13a)). In addition to the fact that they represent an undeniable administrative burden for the controller, the first 3 symbols imply a necessarily positive self-assessment by controllers (if not, the latter would not meet the obligations imposed upon them by the draft regulation), while the following three symbols are intended to provide factual information to the data subject. According to the CPP, this dual perspective is likely to be more confusing than useful when informing the data subject.

20. The CPP has noted that controllers bound by professional secrecy often invoke this obligation in order to try to be exempted from the application of the Privacy Act, in particular as regards the rights of the data subject and the supervisory competence of the CPP. Although professional secrecy and the regulations on data protection protect the confidentiality of data, the latter goes

beyond preserving confidentiality (namely in its principles of purpose limitation, of proportionality, of data security, etc.).

21. Consequently, the CPP welcomes the LIBE Committee's attempt to reconcile the demands of professional secrecy (which can vary from one Member State to another) with those of data protection.

22. However, the way in which the LIBE Committee attempts to take into account the obligation of professional secrecy to which controllers would be subject is also unsatisfactory and the CPP deems it to be a largely unjustified exception to the right of information (Article 14.5.da)). Abolishing the right of information for data subjects, even if it were only in the event of indirect collection, on the grounds that the controller is subject to professional secrecy or any other obligation of secrecy seems plainly indefensible. Under Belgian law at least, the opposability of professional secrecy is aimed at *third parties* and not the person who relying on it. Whether collection is performed in a direct or indirect manner seems to be irrelevant; professional secrecy prohibits the *disclosure* to *third parties* of the data covered by this secret, with certain exceptions to this rule. Generally speaking, the CPP calls for a provision reconciling "data protection" and "professional secrecy", so that those bound by professional secrecy wull not have to violate it to implement data protection regulations.

2.2. Right of access and data portability (Article 15)

23. The CPP welcomes the clarification provided by the LIBE Committee regarding the right of access on the one hand and data portability on the other.

2.3. Right of erasure (Article 17)

24. The CPP notes with satisfaction that the title of Article 17 has been amended: the text of the LIBE Committee no longer contains the title "right to be forgotten in the online environment and of erasure", but only "right of erasure". This amendment meets the wishes expressed by the CPP in its Opinion 35/2012. It believes that the right to be forgotten and the right of erasure should be clearly distinguished. While the right to erase data is a given when the processing is not performed in accordance with applicable provisions, it is unclear which additional rights and obligations would arise from the introduction of a right to be forgotten.

25. The latter concept is not understood in the same sense in the various legal systems. In addition, it is often jurisprudential in nature and not formally enshrined in law; most often it concerns the press sector and judicial data and its scope is uncertain[7].

26. The CPP considers that the text as amended by the LIBE Committee does not solve the problems raised by the text proposed by the European Commission. The new provision does not clarify whether Article 17 establishes a new right, or whether it only modifies the right to erasure of unlawfully processed data (and a related obligation). In addition, the CPP believes it will be difficult to put into practice the requirement for controllers to contact all third parties who have legally re-disclosed data which were initially disclosed lawfully.

27. The compatibility and effectiveness of this right of erasure which the data subject may exercise with regard to third parties must also be examined in the light of Directive 2000/31 on electronic commerce, which particularly prohibits measures providing general surveillance measures with regard to the intermediaries of the information society, such as search engines for instance[8].

28. Finally, the difference between the two cases referred to in Article 17.1 and 17.2 is not obvious: in fact, the new version of Article 17.1, as amended by the LIBE Committee, adds third parties as the intended addressees of the obligation of erasure, in addition to the controller. Such third parties were already covered by Article 17.2, but this provision stipulates that the controller must take all reasonable steps to erase the data, including third-party erasure. It seems that third parties therefore have no *direct* obligation to erase data in this case.

29. However, the new Article 17.3 provides that the controller, but also the third parties, must erase the data without delay, except in the cases mentioned in the same article. It seems that the obligation of erasure is therefore aimed at third parties, either in the case mentioned in Article

[7] This is clear in the case currently pending before the ECJ (Case C-131/12, Google v. Spanish Data Protection Agency), in which the Advocate General issued an opinion which concluded not only that the current scheme of Directive 95/46 does not establish the existence of a right to be forgotten but also questioned the qualification of search engines, which could not be considered to be controllers within the meaning of Directive 95/46/EC.

[8] Recital 17 of the draft regulation provides that this Regulation should apply without prejudice to Directive 2000/31/EC, and in particular to its Articles 12 and 15 relating to the liability of intermediary service providers. However, difficulties arising from the simultaneous application of both texts are not to be excluded. See the judgement of the ECJ in Sabam v. Tiscali, Case C-70/10, 24 November 2011 confirming that European law, and in particular the above-mentioned Directive 2000/31 preclude an injunction made to an Internet Service Provider from setting up a filtering system for all electronic communications passing through its services, including through the use of "peer-to-peer" software, which applies equally in respect of all its customers, as a preventive measure, exclusively at its expense and without limitation in time. The effectiveness in time of a request for erasure shall be reduced if the third party shall not have to make sure that the disputed data has reappeared after having erased said data.

17.1 (data first disclosed without legal justification) or in the case mentioned in Article 17.2 (data made public by the controller without any justification based on Article 6.1).

30. For these reasons, the CPP believes that the system established by Article 17 is unclear and inconsistent, rendering its application even more difficult.

2.4. Right to object and direct marketing (Article 19)

31. In its Opinion 35/2012 (paragraphs 75 to 78), the CPP underlined that with the entry into force of the draft Regulation, the right to object provided by the Privacy Act disappears in cases where the consent of the data subject constitutes the legal basis for the processing of data. The text adopted by the LIBE Committee provides no fix for this weakening of the rights of the data subject.

32. The cases in which the controller has the ability to demonstrate the existence of compelling and legitimate reasons for the processing, which override the interests or fundamental rights and freedoms of the data subjects are nevertheless restricted: when the processing is based on the Article 6(1) f) as voted by the LIBE Committee (the processing is based on the legitimate interest of the controller), the right to object is set out unconditionally. With regard to direct marketing which would be recognized as a legitimate interest within the meaning of Article 6(1) f), the possibility for the controller to refuse the exercise of the right to object no longer exists. However, in cases where this possibility persists, the CPP believes that the balancing of interests to be carried out by the controller with regard to the exercise of a right by the data subject creates the unacceptable risk of controllers continually invoking their legitimate interests to resist the right to object exercised by the data subject.

2.5. Profiling

Reminder of the European Commission's initial proposal

33. In its Communication of 25 January 2012[9], the European Commission stated that *"personal data has become an asset for many businesses. Collecting, aggregating and analysing the data of potential customers is often an important part of their economic activities. In this new digital environment, individuals have the right to enjoy effective control over their personal information."*

34. Article 20 of the draft regulation submitted by the European Commission is entitled "Measures based on profiling" and enshrines the right of every person not to be subjected to a measure producing legal effects or significantly affecting them that is taken on the sole basis of an automated processing operation intended to evaluate certain aspects of his personality or to analyse or predict in particular that natural person's professional performance, economic situation, place of residence, health, personal preferences, reliability or behaviour.

35. Article 20 is based on article 15, paragraph 1 of Directive 95/46/EC on automated individual decisions, which it completes and to which it adds additional safeguards. It also takes into account the recommendation of the Council of Europe on profiling. It seems that the European Commission intends for this new provision to extend the protection already afforded by Article 15 of Directive 95/46 to certain types of profiling.

36. The CPP shares the European Commission's observation (see paragraph 33 above). In line with its Opinion 35/2012, it pays particular attention to this concept of profiling. It will address the following aspects below:

- ✓ The link with (and its distinction from) the principle of the prohibition of automated individual decisions
- ✓ The definition of profiling
- ✓ Conditions for the processing of personal data in the context of profiling
- ✓ A specific aspect: profiling and (non-) discrimination
- ✓ The right to anonymity

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2012) 9 final).

Profiling and automated individual decisions: two concepts to be distinguished

37. The CPP regrets that the term "profiling" in Article 20 include the current system of automated decisions from Article 15 of Directive 95/46. It is possible that automated decisions are taken without establishing a profile beforehand.[10] Conversely, it is possible to create profiles or to profile individuals without taking measures which significantly affect them or produce legal effects in relation to them.[11]

38. Therefore, the CPP believes that dividing Article 20 into two parts, keeping the system governing automated decisions as enshrined in Directive 95/46/EC on the one hand, and adding a specific system for regulating profiling on the other, would provide better protection for individuals. Otherwise, it seemed that the regulation proposes a protection system below that provided by Article 15 of Directive 95/46/EC. The CPP considers the weakening of the level of protection to be unacceptable.

Definition of profiling (Article 4.3a))

39. The term "profiling" is not defined independently by the draft regulation submitted by the European Commission. The new Article 4.3a of the LIBE Committee's draft defines it as *"any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour."*

40. The CPP believes that there is a difference between collecting data for the purpose of creating profiles, creating profiles (whether abstract or individual), and the application of such profiles to an individual. These three operations require data processing operations which may fall within the definition of profiling as defined by Article 4.3a of the draft text of the LIBE Committee.

41. However, the definition of profiling is ambiguous and does not establish whether it includes both the creation of a profile and its application to an individual. In addition, the CPP notes that Article 20 is no longer titled "Measures based on profiling", but rather "Profiling", which might suggest that the scope of Article 20, as proposed by the LIBE Committee's text, is wider.

---

[10] For example, a multiple choice questionnaire (MCQ) in which the criteria for granting bank loans do not necessarily require the establishment of a preliminary profile.

[11] An abstract profile can be based on information from several categories of persons, as part of data mining operations. In addition, an individualized behavioural profile of a person can be created without taking action against him.

42. In support of the above, the CPP believes that it is necessary to clarify this aspect by stating that *all* operations relating to profiling (data collection, creating abstract or individual profiles, application of such profiles in order to draw conclusions and / or develop approaches with regard to the person profiled) must be regulated.

43. In this respect, the CPP believes that the draft text should be in line with that of the Recommendation of the Council of Europe on profiling and include - but not be limited to - the definition of a profile, defined as "a set of data characterising a category of individuals that is intended to be applied to an individual"[12].

44. The CPP also believes that it is important to define the profile as being a set of data without requiring that such data be personal data, given that a profile can also be established from anonymised data or information. However, such profiles can also be applied to an individual.

Conditions for the processing of personal data in the context of profiling

45. The CPP believes that in all cases, individuals should be informed of the fact that their data will be used to establish profiles. In this case, it should be clear from the draft regulation that it constitutes a new data processing operation. Article 14 (ga) proposed by the LIBE Committee should be adapted accordingly given that it seems to target only the *application* of a profile ("profiling") and not its creation.

46. Article 20 as amended by the LIBE Committee provides that any individual may object to any form of profiling. Article 20.2 also provides for a stricter scheme regarding profiling activities leading to measures which produce legal effects for the data subject or significantly affect their interests, rights or freedoms.

47. The CPP welcomes the fact that Article 20 applies to *all types* of profiling, and not just those leading to measures which produce legal effects for the data subject or significantly affect their interests, rights or freedoms. The way in which this provision is worded enables profiling for direct marketing purposes to be covered (see paragraph 80 of Opinion 35/2012).

[12] According to the CPP, a profile should also comprise any data characterising the behaviour of a particular individual and the data relating to such person.

48. In the cases referred to in Article 20.2, profiling can only be based on a contract, the consent of the data subject or legislation. Appropriate safeguards must also constitute the framework for profiling. As mentioned by the CPP in its previous Opinion 35/2012, there should always be human intervention in each of the cases in Article 20.2 of the draft regulation (paragraph 79 of Opinion 35/2012).

A specific aspect: profiling and (non-) discrimination

49. The CPP also has questions about the scope of Article 20.3, which prohibits profiling that would have the effect of discriminating against individuals on the basis of their race, ethnic origin, political opinions, religion or beliefs, union membership, sexual orientation or gender identity, or that results in measures that would have such an effect.

50. This is because the concept of discrimination is not defined in the draft regulation. Several European texts refer to this concept[13], but the draft regulation does not. In addition, it is clear that profiling is specifically designed to treat individuals differently depending on their characteristics, which could be the characteristics listed in Article 20.3.

51. Moreover, insofar as discrimination is prohibited under other laws, the CPP does not see the added value of Article 20.3 given that it only prohibits what is already prohibited. It therefore recommends deleting the text as such or making it more specific by referencing specific texts or a specific definition of discrimination.

52. Article 20.3 proposed by the European Commission states that profiling cannot be based solely on the specific categories of personal data referred to in Article 9. The CPP recalls in this regard that it stated in its previous Opinion 35/2012 that this provision could exclude processing operations performed by some public authorities in their public policies on health care (paragraph 82 of Opinion 35/2012).

53. Finally, the CPP notes that recital 58a establishes the presumption that profiling based solely on the processing of pseudonymous data will not be considered as significantly affecting the interests, rights and freedoms of data subjects. The CPP refers in this regard to paragraph 13 above concerning pseudonymous data specifically and adds that the sole fact that pseudonymous

[13] For example, Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

data are used is not sufficient to exclude the risks linked to profiling, including the risk of discrimination.

54. In addition, the last sentence of recital 58a seems to assume that pseudonymous data cannot be attributed to a specific data subject, which is not the case. This recital stems from a misunderstood definition of pseudonymous data, which in any case remain a form of personal data. Therefore, the CPP proposes the deletion of recital 58a.

Right to anonymity

55. The CPP believes that Article 20 should introduce a principle enshrining the right to receive a product or service without having to disclose personal data, unless the required service requires knowledge of the data subject's identity. This principle was introduced by the Recommendation of the Council of Europe on profiling. Additionally, in order to ensure free, specific and informed consent to profiling, the text should provide that Information Society service providers should ensure, by default, non-profiled access to information about their services.

2.6. Restrictions (Article 21)

56. The LIBE Committee restricts the articles which can be derogated from exceptionally (Article 21). The basic principles set out in Article 5 a)-e) remain applicable in all circumstances, as well as Article 20 (profiling), which was not the case in the original text of the European Commission. In the same spirit of enhanced protection, the LIBE Committee added a number of elements to be included in derogating national legislation, on the basis of the constant jurisprudence of the European Court of Human Rights. The reasons for which a Member State may adopt a derogation scheme relative to the provisions of the draft regulation are also limited. Thus, the reference to the public interest is reduced to "taxation matters" only.

57. In a first reading, any restriction of the right to derogate from a protection system seems likely to be *welcomed, especially* by a Data Protection Authority such as the CPP. However, an unworkable system in the absence of adequate exemptions entails, among other adverse effects, the risk of systematic circumvention of the provisions and a wrong or deliberately biased interpretation of such provisions. In other words, it is better to have a protection system which provides appropriate exceptions rather than an unclear, *theoretically* applicable system which is unworkable in practice, for instance for the public sector. In this regard, the CPP would like to

alert the reader to the deletion of the concept of *"general interest of the Union or of a Member State"* (Article 21.1 c)) and its reduction to *"taxation matters"* only."[14] The CPP is in favour of maintaining the exemptions in Article 13 of Directive 95/46/EC, the relevance of which has not been questioned, at least not to the CPP's knowledge.

3. Chapter IV: Obligations of the controller

58. In the spirit of its Opinion 35/2012 and as a starting point for Chapter IV of the European Commission draft regulation, the CPP questions the actual and tangible added value of the obligations imposed upon controllers and processors for the protection of data subjects with regard to the processing of data concerning them. This observation takes into account the feasibility and costs of the accountability measures developed. In other words, the CPP advocates a system of coherent obligations based on a specific assessment of the actual risk induced by the processing operations performed. It is in light of these criteria that some of the obligations imposed on the controller and the processor, as well as other measures aimed at making them accountable, are discussed below, starting from the version provided by the LIBE Committee.

3.1. Controller and processor (Article 26)

59. The issue of further processing and the corresponding conditions are referred to below in paragraphs 91 to 92 on processor BCR.

3.2. Documentation (Article 28)

60. The LIBE Committee reduces the obligation of documentation to the strict minimum. Any controller and processor must keep documentation stating the following few elements only: name and contact details of the controller, of any possible joint controller, of the processor and of the representative, if any; identity and contact details of the possible Data Protection Officer as well as of the controllers to whom the data have been disclosed.

[14] The CPP believes, for instance, that social security should be recognized as a general interest of a Member State of the Union and should justify a derogation for certain aspects of the processing operations performed in this sector which is often regulated very specifically at national level. The CPP particularly recalls the Social Security and Health Sector Committee's competence in this area. Social security could usefully be included in a recital relating to Article 21. In any event, the CPP pleads for a clarification of the rules for processing personal data in this area given that the combined reading of Articles 21, 81.1c) and 82a as proposed by the LIBE Committee is confusing.

61. In its Opinion 35/2012, the CPP states that it is in favour of the obligation of internal documentation instead of the prior notification of processing provided that the particular interest of this notification - being the requirement for notifiers to ask themselves the relevant questions with regard to the principles of data protection concerning their processing - remains. This reflection process disappears in the minimalist obligation of documentation laid down by the European Parliament's LIBE Committee. The CPP believes that this documentation should also include: a brief description of the processing operations incorporating the objectives pursued and the categories of data processed (paragraph 97 of Opinion 35/2012).

3.3. Security and data breach notifications (Articles 30, 31 and 32)

62. In Article 30 (1a.), the CPP welcomes the clarifications regarding the contents of the security policy.

63. As regards data breach notifications, the LIBE Committee maintains the distinction proposed by the European Commission between (1) notifications to Data Protection Authorities (Article 31) and (2) notifications to data subjects (Article 32). Although the LIBE Committee urges controllers and processors to notify security breaches no longer within 24 hours but rather "without delay" - which is welcomed by the CPP - it does not specify any more than the European Commission (or inadequately so) exactly which violations must be notified. As stated in its Opinion 35/2012, the CPP believes that the text as it stands will generate "impossible" situations for Data Protection Authorities, for controllers, for processors and for the data subjects themselves. This lack of precision could lead to ineffectiveness of this obligation and the related useful information it aims to provide to the supervisory authority and to every party involved, and this right from the start.

3.4. Respect to risk (32a)), Data Protection Impact assessment (Article 33), Data protection compliance review (Article 33a))

64. With the adoption of Article 32a) entitled "Respect to risk", the LIBE Committee shows its intention to justify the obligations to appoint a representative within the Union (Article 25), to appoint a Data Protection Officer (Article 35) and to perform a Data Protection Impact assessment (Article 33 - DPIA) in relation to the specific risks arising from certain processing operations.

65. The CPP, however, is not convinced by the way the LIBE Committee justifies its conclusions - theoretically, *a priori,* putting itself in the place of the controller or processor. Thus, while Article

32a.1. evokes processing operations *"likely to present specific risks"* and Article 32a.2. lists the measures to be taken *"according to the result of the risk analysis"* (the designation of a representative, of a Data Protection Officer, or the performance of a DPIA), the articles which detail the cases in which these obligations must absolutely be implemented leave no discretion to the controller. Article 32 a.1. seems to be more of a textual construct than an actual implementation of the "risk-based approach" by the controller that the CPP calls for.

66. In general, the CPP questions the qualification of *"risky"* or *"with specific risks"* used for certain processing operations identified as such. It refers in this regard to its Opinion 35/2012 (paragraphs 113 et seq.).

67. As for the "Data Protection Impact assessment" as an actual instrument, the CPP is in favour of its existence insofar as it relates to processing operations which have been properly identified as being particularly "risky" (see above), and are carried efficiently, concretely and in the most unbiased way possible. With the same requirements, it welcomes the principle of "data protection lifecycle management" (title of section 3) and that of the periodic assessment of the impact assessment (Article 33a).

3.5. Prior authorisation and prior consultation (Article 34)

68. In its Opinion 35/2012, the CPP noted that the draft regulation of the European Commission intends to limit the competence for prior authorisation by Data Protection Authorities to the sole area of international data transfers. Consequently, the CPP pleads for the Belgian system of sector committees set up for the protection of personal data in the public sector to be fully maintained (Social Security and Health, National Register, Federal Government, Statistics, Crossroads Bank of Enterprises). The prior authorisation procedure of these committees can provide useful guidance to the public sector for personal data flows. These committees fulfil the role of guides for the controllers. They can grant or deny access, but also grant authorisations to which conditions precedent or subsequent are linked (paragraphs 120 et seq. Opinion 35/2012).

69. The CPP notes that the text voted by the LIBE Committee does not respond to its concerns. Prior consultation (sometimes presented as an adequate palliative) does not enable such a system to be maintained - not in the "European Commission" version and not in the version amended by the LIBE Committee.

70. The CPP therefore suggests the insertion of the following amendment:
"Notwithstanding paragraph 2, Members States may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health".

3.6. The Data Protection Officer (Articles 35 et seq.)

71. As is the case in the European Commission's original proposal, the LIBE Committee makes the appointment of a Data Protection Officer an *obligation* for the controller and the processor in a number of cases. The LIBE Committee added a fourth case to those already in the original proposal: when the core activities of the controller consist of processing operations a) of sensitive data, b) of location data, c) of data relating to minors or to employees in large-scale filing systems.

72. The LIBE Committee also changed one of the cases in which a representative must be designated. The criterion of *"an enterprise employing 250 persons"* was thus replaced by the number of people affected by the processing operations performed annually by the controller (5000 - Article 35.1.b)). In its Opinion 35/2012, the CPP highlighted the lack of relevance of the criterion of the number of persons employed by the controller, a criterion that does not take into account the risks arising from the processing operations performed. The number of data subjects - other than seeming hardly feasible - is open to the same criticism.

73. In general, the CPP believes that, given the 4 cases in which the appointment of a Data Protection Officer is mandatory, few processing operations will not justify the appointment of a Data Protection Officer. The CPP believes that the appointment of a Data Protection Officer must remain optional. Introducing such a function 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 applicable protection mechanisms and the actual benefit for data protection provided by such an appointment. It is in this sense that the CPP favours that controllers and processors can decide on this, as mentioned in the text under discussion at the Council (DAPIX).

74. The CPP finally notes that the LIBE Committee provides in Article 34.2. that where such exists, prior consultation may be carried out with the Data Protection Officer instead of the supervisory

authority. According to the CPP, such measures could be introduced - even in a system of non-compulsory nomination of a Data Protection Officer - as an incentive to their nomination.

3.7. Certification (Article 39)

75. The LIBE Committee offers a more comprehensive body of rules on certification. Designed by the European Commission as an information tool *"allowing data subjects to quickly assess the level of data protection provided by controllers and processors"* (Article 39.1. of the COM's proposal), certification entails a number of practical consequences under the text voted by the LIBE Committee.

76. Thus, Article 42.2 (aa) describes the "European Data Protection Seal" as an adequate safeguard for the transfer of data to controllers established outside the European Union in the absence of a decision on the adequacy of the regulations applicable to them (see paragraph 85).

77. Article 79.2b) concerning administrative sanctions, commented below (paragraphs 123 to 126), indicates that sanctions would only be imposed on the recipient of such a label in a small number of cases. The CPP emphasizes that is it objects to this.

78. The CPP is consequently even more convinced of the need to provide that the criteria and requirements applicable to certification mechanisms, including the conditions for granting, revoking and recognizing in the EU and in third countries, as well as the criteria for the accreditation of certifiers, are determined by the Data Protection Authorities, grouped within the European Data Protection Board (EDPB), if any. Consultation of the EDPB by the European Commission when preparing the delegated act on this subject is a minimum.

79. Based on these criteria and requirements, certified (by the Data Protection Authorities and/or the EDPB) external certifiers will respond positively or negatively to applications for certification from controllers and processors. This division of roles between supervisory authorities and certifiers aims to preserve the independence of the Data Protection Authorities and their full supervisory competence, also with regard to certified controllers and processors.

80. As for the personal data breach register (Article 31.4.), the CPP supports the idea of a public register of certificates issued and withdrawn (Article 39.1h)).

81. Finally, the CPP notes that Article 23 makes *"data protection by design"* a selection criterion for public procurements. It seems therefore that the European Data Protection Seal might play a significant role in this, in line with the current provisions of Directives 2004/17/EC and 2004/18/EC on procedures for awarding certain public contracts. The CPP will remain attentive to developments in this regard.

4. Chapter V: Cross-border flows

4.1. Transfers of data based on appropriate safeguards (Article 42)

The fate of existing authorisations

82. The CPP regrets that the LIBE Committee proposes that decisions taken under Article 26.2 of Directive 95/46/EC (data transfer authorisations on the basis of *ad hoc* contracts, model clauses or BCR) will only remain valid for two years subsequent to the entry into force of the draft European regulation.

83. This position will entail a significant and unnecessary administrative burden for both the European Data Protection Authorities who will have to review all of the decisions already granted (even though they will certainly have more essential tasks to perform) and for companies who will have to make new authorisation requests for transfers that had already been authorised.

84. This also induces a significant *legal uncertainty* and implies that companies are currently reluctant to invest in data protection tools which only have a limited term of validity. This measure will have (and already has at present) a completely counter-productive effect. For these reasons, the CPP strongly opposes it.

A new safeguard: certification

85. The CPP notes that the labelling of controllers or processors – also to the benefit of controllers and processors established outside the European Union - using the "European Data Protection Seal" is listed among the adequate safeguards allowing for data transfers to a non-adequate third country (Article 42.2. aa)). The CPP refers in this regard to the above paragraphs 75 to 81 relating to certification and believes that it is under those terms, and those terms only as stated in those paragraphs, that such certification may result in the authorisation of a data transfer without any other additional safeguards.

4.2. Binding Corporate Rules (BCR) for processors (Article 43)

86. In its Opinion 35/2012 on the draft European Regulation[15], the CPP welcomed the proposal to explicitly recognize Binding Corporate Rules (BCR). They have been used by multinationals for several years[16] in order to provide adequate safeguards for their intra-group transfers of personal data.

87. However, although the vote of the LIBE Committee maintains the use of BCR, it appears to abolish the possibility of using "BCR Processor"[17]). The CPP opposes this position for the following reasons:

88. This abolishment is a vector of legal uncertainty for companies already using this solution. Since January 2013, "Processor BCR" can be the object of a European cooperation procedure [18] and several cases are already under review[19].

89. In addition, abolishment would do away with a tool currently offering the most protective safeguards in terms of data protection for international data transfers to processors and the best way to promote the European principles of data protection abroad. Companies would have no alternative but to sign model clauses 2010/87/EU or to limit themselves to calling on processors established in the European Union or in a country considered as offering adequate protection (for instance, companies established in the USA having subscribed to the Safe Harbor[20] principles). BCR go beyond the basic legal obligations under model clause 2010/87/EU because they impose,

---

[15] http://www.privacycommission.be/sites/privacycommission/files/documents/Opinion_35_2012.pdf

[16] In fact, they have been used since 2003, when the WP29 acknowledged the possibility for enterprises to make use of BCR.

[17] " Controller BCR " are tools for the supervision of transfers of data processed initially by the group's companies acting as data controllers (E.g. data relating to the group's employees or clients); " Processor BCR " govern the transfer of data processed initially by the group acting as processors (e.g. a group offering outsourcing to third companies such as the management of data relating to the employees or clients of these third companies).

[18] The WP29 established the framework for the use of " Processor BCR " in June 2012 (WP195 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf) and it has been possible for companies to submit their application for a European cooperation since January 2013 (http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf).

[19] To our knowledge, there are already eight pending European cooperation procedure applications, but the companies currently making the prior investments necessary for the formal introduction of their application must also be added to that number.

[20] Application of the Safe Harbor principles for processors nevertheless poses some difficulties (see FAQ 10) and the legal framework is not without criticism, see in this respect the European Commission Communication of 27 November 2012 "on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU."

among other things, the implementation of measures to ensure the effective implementation of legal obligations (regular audit, employee training, internal system for complaint handling, etc.)[21].

90. A criticism sometimes levelled against " Processor BCR " (and which would justify its deletion by the LIBE Committee?) is the lack of safeguards as a framework for further data processing. However, the CPP believes that the proposed safeguards are adequate. As already provided in model clauses 2010/87/EU, processing companies may, under strict conditions[22], call on further processors and provide the contractual safeguards necessary for these activities. The conditions are intended to ensure transparency in respect of controllers (client companies belonging to the group) and maintain supervision on the possible intervention of further processors[23]. Moreover, contracts will have to be the framework for further processing activities carried out outside the group[24].

91. Moreover, it would be totally inconsistent to object to "Processor BCR" citing the lack of strict conditions governing further processing, given the very weak conditions[25] governing further processing within the EU currently provided by the text of the LIBE Committee itself (Article 26.2d)). The stringent conditions of the "Processor BCR" as a framework for further processing outside the EU[26] should rather be a model of inspiration to the European Parliament and the European Council in the adoption of rules for further processing within the Union[27].

92. It is a fact that multinationals providing processing services are currently calling on the services of further processors. The autonomy afforded to processors enabling them provide a legal framework for their further processing has been legally recognized by the Member States, the European Commission and the European Data Protection Authorities since the adoption of model clauses 2010/87/EU. It is not by banning "Processor BCR" that we will be able to stop this

[21] Measures of accountability, also supported in the draft European data protection regulation.

[22] See paragraph 6.1 of WP195.

[23] This procedure can only be carried out with their consent. Depending on the sensitivity of the activities involved, the parties may freely decide to provide for specific consent for each further processor or to consider general consent as sufficient. In the latter case, the controller must always have the possibility to object to the intervention of a subsequent processor and to terminating the contract in such case.

[24] The safeguards to be provided by further processors should be modelled on the safeguards offered by the principal processor in respect of the client company. In any event, principal processor will be liable towards their clients for any possible inadequacies of further processors.

[25] Article 26.2.d does not provide that a contract necessarily be signed between the processor and further processors, and it stipulates that such further processing may occur without the prior permission of the controller, which will certainly be an obstacle to the necessary controller supervision. In addition, the principal processor is not liable for the misconduct of further processors.

[26] See in particular paragraphs 6.1.vi and vii of "Processor BCR" (WP195) but also Article 11 of model clauses 2010/87/EU.

[27] Article 26.2.d. on further processing within the EU.

development, including cloud computing. The law is not aimed at limiting technological developments but rather at providing a framework for them as much as possible.

93. Another reason sometimes put forward, which might explain the (LIBE Committee's) objection to "Processor BCR", is the risk relating to access to data by foreign authorities. BCR are intended as a framework for commercial activities, and by definition they cannot restrict the powers of foreign authorities[28]. However, in case of a conflict of law, the "Processor BCR" include strict transparency requirements in relation to controllers but also in respect of the European Data Protection Authorities that must intervene[29]. The safeguards provided by "Processor BCR" are therefore along the same lines as Article 43a as proposed by the LIBE Committee, and certainly go beyond those currently laid down in model clauses 2010/87/EU or in the Safe Harbor principles, for instance.

94. In conclusion, besides the fact that the substantive arguments justifying the deletion of "Processor BCR" are untenable according to the CPP, opposing them only creates legal uncertainty and pushes companies to opt for less protective tools that do not offer the advantages of BCR for the promotion of European data protection rules abroad.

4.3. Transfers and disclosures not authorised by Union law (Article 43a))

95. The CPP believes that a general, large-scale and systematic surveillance of Belgian and European citizens is unacceptable in a democratic society. Accordingly, the CPP positively welcomes the LIBE Committee's initiative in Article 43a. and Recital 82 attempting to provide solutions to the practices - and consequences for the protection of privacy and personal data - revealed in the press in recent months.

96. In short, Article 43.a) provides that the Data Protection Authority is responsible for assessing the compatibility of an application for the transfer of data to third countries (application based on a court decision of this state, for instance the SWIFT case, Snowden, the eDiscovery requests or the American SEC (Security Exchange Commission) requests) with the Regulation and to authorise, where appropriate, said transfer. It is also the Data Protection Authority that will inform "the competent national authority."

[28] The best way forward would probably be to introduce authorisations for European public authorities for the transfer for such purposes and to conclude international agreements. Industrial and policy solutions are also preferred.

[29] See paragraph 6.3 of WP195.

97. However, the CPP considers it necessary to conclude international agreements aimed at regulating the actions of third States in the fight against serious offences, and to the benefit of national security. In this regard, the reference made in Article 43a. to the mutual assistance treaties is certainly useful in the fight against such offences.

98. Although the CPP believes that Data Protection Authorities cannot reasonably be totally discarded or left in total ignorance of this type of data transfer, it does not, however, believe that they are best placed or have even been established to determine that a foreign judgment or administrative decision may or may not be accepted.

99. It is surprising in this regard that Article 43a. as it is proposed only entrusts the Data Protection Authorities (which inform the competent national authorities) with powers, while Recital 90 refers to the intervention of the European Commission which shall ensure that EU law will always take precedence, which shall attempt to resolve jurisdictional conflicts with third countries and which shall provide information and assistance to the controllers and processors involved. There is some confusion regarding the respective role of Data Protection Authorities and the European Commission which undoubtedly demonstrates that Data Protection Authorities are neither equipped nor have they been established for the political role intended for them under Article 43a. The entity responsible for assessing applications could be the entity designated in the relevant international agreement.

100. Although the CPP deems it useful that general information be provided in respect of applications made in the last 12 months, it has more doubts about the option to provide specific information to data subjects. Imposing such transparency does not solve the potential conflict of laws that a company could find itself tied up in if such transparency is prohibited by foreign authorities.

101. Moreover, the sole reference to foreign courts or administrative authorities is not sufficient, given that in the case of PRISM, they are not systematically involved. It would be useful to extend the scope of the Article to public authorities in general.

102. Finally, the CPP welcomes Recital 82 which explicitly states that the fact that foreign legislation allows for extraterritorial access to personal data processed in the EU without authorisation granted under Union or Member State law, should be considered as an indication of non-conformity.

4.4. Exceptions (Article 44)

103. For the reasons already developed in its previous opinion on the draft regulation (Paragraph 140 of Opinion 35/2012), the CPP welcomes the deletion of paragraph h of Article 44.1. It also wishes to emphasize that, in general, the derogations provided for in Article 44 must be interpreted restrictively and cannot concern large-scale or repetitive data transfers, nor serve as a basis for data transfers that take place in such a way that they cannot be considered necessary and proportionate in a democratic society.

5. Chapter VII: Cooperation and consistency

5.1. The "one-stop shop" principle (Article 51)

104. The text of the LIBE Commission recasts the "one-stop shop" mechanism as included in the European Commission's proposal. The first paragraph of Article 51 remains almost unchanged, but specifies that each supervisory authority shall be competent to exercise its powers in its own territory, without prejudice to Articles 73 and 74, which relate to the right *to lodge a complaint* with the supervisory authority of their place of residence and the right to challenge the decisions of a supervisory authority in court. In addition, Article 51.1 states that the processing operations carried out by public authorities shall be the exclusive competence of the supervisory authority of the Member State in question. The CPP welcomes these clarifications.

5.2. The "lead authority" (Article 54a)

105. A new article 54 a provides for a framework for the designation of a so-called "lead authority" in the event of cross-border processing, as stipulated in Article 51.2 of the European Commission's proposal. This new article refers to the concept of the main establishment, as defined in Article 4 (13), itself amended.

106. The main establishment is now defined as *" the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the main decisions as to the purposes, conditions and means of the processing of personal data are taken."* Various additional objective criteria mentioned in this article are useful for determining more specifically what will be the controller's main establishment.

107. Despite the reservations already expressed by the CPP in its previous opinion on the concept of the main establishment (paragraphs 18 et seq. of Opinion 35/2012), the amendments made by the LIBE Committee lead to simplification in the sense that the main establishment will be determined in the same way for controllers and processors, which was not the case in the European Commission's proposal. In addition, the indicative and non-exclusive criteria for determining the main establishment are more flexible.

108. It is in the case of "cross-border processing" that the designation of a lead authority will be required (Article 54a adopted by the LIBE Committee). Such processing is defined as a personal data processing operation in the context of the activities of a controller or a processor established in the Union, but in several Member States, *or as a processing operation concerning personal data of residents of different Member States.* The CPP welcomes this end-of-sentence addition, given that a lead authority will also be designated in cases where data are processed relating to data subjects not residing in the Member State where the controller is established. In these cases it is necessary that all the supervisory authorities of Member States whose inhabitants' data are processed receive a role in the supervision of the processing operations in question.

5.3. Strengthening the role of the European Data Protection Board

109. The CPP notes with satisfaction that the text as amended by the LIBE Committee allows for disputes on the designation of the lead authority to be submitted to the European Data Protection Board (EDPB). In this regard, paragraph 3 of Article 54a and paragraph 4 of the same article seem contradictory since paragraph 3 states that the EDPB may issue an *opinion* in this regard, while paragraph 4 provides that the EDPB may *decide* on the identification of the lead authority. The text should be clarified in this regard.

110. Once the lead authority has been designated, the text specifies that it will consult all the other competent supervisory authorities pursuant to Article 51.1, before taking the measures necessary to supervise the activities of the controller. In the case where the leading authority wishes to adopt a measure which produces binding legal effects with regard to the controller, the other competent authorities may oppose such a measure. In such a case, the matter will be submitted to the EDPB, which may adopt a final binding decision with respect to the supervisory authority.

111. However, the CPP rejects the idea of allowing a lead authority to adopt binding decisions with respect to processing operations for which other supervisory authorities are competent. A co-decision procedure involving all of the competent supervisory authorities is more appropriate in

this case, since the decision adopted by the lead authority will be shared by all other competent authorities.

112. In any event, instead of a lead authority system (whether or not with a co-decision procedure), the CPP prefers that a specific body, such as the European Data Protection Board (EDPB), be empowered to supervise cross-border processing operations as defined in Article 54 a.

113. More generally, the CPP is in favour of creating an independent European body in charge of *at least* settling disputes of jurisdiction between supervisory authorities (if the system of the lead authority were to be retained), or for adopting binding decisions in some cases (such as taking binding measures in the event of cross-border processing operations, in the event that the lead authority system is abandoned). Such a body could, for instance, take the form of an agency, which should also have legal personality in order to be authorised to take decisions.

114. The CPP also notes that the draft regulation does not mention the possibilities of appeal against the EDPB's decisions, while any decision taken by a supervisory authority must be able to be challenged in court, in accordance with Article 74. The text should therefore provide that proceedings may be instituted against the EDPB's decisions at the Court of Justice of the European Union.[30]

6. Chapter VIII: Remedies, liability and sanctions

6.1. Complexity of the system of remedies

115. Data subjects confronted with a violation of their fundamental right to the protection of their personal data may find themselves facing different jurisdictions of several Member States. These may be:

- The local supervisory authority located in the Member State where the data subject lodges a complaint (Article 73 of the draft regulation)
- The lead supervisory authority in the Member State where the controller has its main establishment (Article 54(a) of the draft regulation)

[30] As provided for in Article 263 TFEU.

- The courts of the Member State in which the lead authority[31] is established (place of the controller's main establishment), for appeals against the decisions of the lead supervisory authority (Articles 54a and 74 combined),
- The courts of the Member State that is a data subject's habitual place of residence, for a legal action brought against the controller (Article 75).[32]
- The courts of the Member State of the authority receiving the complaint, for legal actions against local authorities.

116. Unlike Directive 95/46/EC, which is based on the approximation of laws to promote the internal market (Article 114 TFEU), the draft regulation intends to base itself on Article 16 TFEU which sanctions a fundamental right, notably the protection of citizen's fundamental rights. It reproduces Article 8 of the Charter of Fundamental Rights of the European Union. The CPP believes that Article 16 TFEU aims to protect the fundamental rights of citizens, and was not intended to enable controllers to process their data more easily, notably by having access to a single point of contact which would supervise their activities (the one-stop shop principle).

6.2. Lack of effective legal remedies as guaranteed by the EU Charter of Fundamental Rights

117. By allowing the lead supervisory authority to be different from the one receiving a complaint, data subjects who filed a complaint will be confronted with a foreign supervisory authority which may be geographically very distant, speaking a language other than their own, and which is subjected to a different procedure. These obstacles, together with the costs likely to arise from such a procedure, are likely to contravene Article 16 TFEU by making this procedure extremely difficult.

118. In addition, it should be recalled that Article 47 of the Charter of Fundamental Rights of the European Union enshrines the right to an effective remedy before a court. This article includes what is stipulated in Articles 13 and 6(1) of the ECHR. This effective access to a national authority is interpreted *specifically* by the European Court of Human Rights.[33]

119. However, in case of application of Article 74, any appeal against a decision taken by a lead authority located abroad should take place before the courts of that authority. This makes access

[31] I.e. the courts of the Member State in which the controller has its main establishment within the meaning of Article 4 (13).

[32] These cases are not restrictive, since, for example, Article 74.2 enables a data subject to go to court in the Member State where the supervisory authority is established in order to force it to deal with a complaint.

[33] See ECHR, judgment No. 12964/87, 16 December 1992, *de Geouffre de la Pradelle v. France.*

to an effective remedy against a decision concerning a fundamental right is extremely difficult for the data subject. It is true that Article 74.4 provides that individuals affected by a decision adopted by a supervisory authority in another Member State may request the supervisory authority of their place of residence to institute proceedings on their behalf against the foreign supervisory authority. However, this provision is not particularly clear (Who shall bear the costs? Can the authority refuse to institute such proceedings? What type of proceedings are referred to?), and its implementation may not compensate for the difficulties data subjects will be faced with if they wish to institute proceedings against a decision of a foreign authority.

120. The same holds true for Article 75, which provides for the right to initiate proceedings against the controller in the country of its main establishment, or in the Member State of the data subject's place of residence. Accordingly, it is possible for multiple proceedings to be instituted in different Member States, all of them relating to the *same* violation of the provisions of the Regulation. In addition to this difficulty, an appeal can be made before another court against the decision of a supervisory authority. In these cases, a jurisdictional dispute is sure to arise.

121. Although paragraphs 2 and 3 of Article 76 suggest certain principles aimed at trying to avoid conflicts of judicial decisions, the CPP believes that it is clear that the system's complexity does not allow for effective remedies for data subjects in order to enforce their rights, which is in contradiction with Articles 47 and 8 of the Charter of Fundamental Rights of the European Union, and 16 TFEU.

122. For these reasons, the CPP has considerable reservations concerning the appeals system as proposed by the draft regulation, combined with the one-stop shop mechanism. The exercise of citizens' fundamental right to privacy is weakened as a result, and the system's consistency cannot be ensured if the proposed jurisdiction rules remain unchanged.

6.3. Administrative sanctions (Article 79)

123. The CPP notes that the text voted by the LIBE Committee (Article 79.2a)) provides that in the event of a violation of the Regulation, the Data Protection Authority will impose at least one of the 3 following sanctions: a warning (in the event of a first unintentional violation), "data protection" audits to be performed at regular intervals or an administrative fine amounting to a maximum of 100 million Euros or to 5% of the world-wide turnover. These amounts will be updated by means of a delegated act. Finally, if the controller and the processor have been

awarded the European Data Protection Seal, there will only be an administrative penalty in cases of intentional or negligent violation (see paragraph 77 above).

124. The CPP would like to reiterate the objections in its Opinion 35/2012 concerning the European Commission initial draft (paragraphs 154-163). It continues to oppose an administrative sanction competence to Data Protection Authorities (whatever form such administrative sanctions may take, and regardless of whether the different forms of sanctions were to be presented gradually).

125. The CPP is particularly anxious to preserve the primary objective of its work, which is ensuring that processing operations comply with the requirements of the data protection rules. Based on its experience, it can confirm that mediation can, in most cases, achieve such compliance but also leads to parties' greater acceptance of the applicable rules and consequently also more awareness of the issues surrounding the protection of privacy and personal data. In the rare event of a failure of mediation, the CPP believes it is incumbent on judicial authorities to take over in accordance with the rules of the separation of powers. The CPP therefore has a clear preference for course set out by the Council (DAPIX), giving the Data Protection Authorities the *possibility* (not the obligation) to impose administrative fines. However, it also believes that measures such as warnings or organizing regular audits can be valuable supervisory tools and can increase compliance. Concerning the amounts of the fines, the CPP judges them to be excessive, even if they are maximum amounts. The percentage of the world-wide turnover, meanwhile, is impossible to calculate in the absence of further details on the concept of "world-wide turnover".

126. Finally, the CPP is opposed to the preferential treatment granted to certified controllers and processors (Article 39). Instead, it believes that awarding this seal should encourage those receiving it to commit to strictly respecting the rules. It believes that breaches of trust must, *a fortiori* , be more severely punished.

7. Chapter IX: Special Provisions

7.1. National Register number

127. In its Opinion 35/2012, the CPP regrets the deletion of Article 8.7. of Directive 95/46/EC allowing Member States to define the conditions under which a national identification number or any other identifier of general application may be processed. It fears that the Belgian National Register identification number could no longer be used (paragraphs 169 to 171).

128. Consequently, the CPP calls for the introduction of an amendment authorising the processing of the National Register number as regulated by the Belgian Act of 8 August 1983 organizing a National Register of natural persons, including the cases in which such processing operations are subject to authorisation by the competent sector committee (see above paragraphs 68 to 70).

7.2. Processing of data related to health for the purpose of therapies (Article 81)

129. The CPP draws attention to the unnecessarily stringent formulation of the legal basis for the processing of data related to health for the purpose of therapies. In the current legislation, the processing of data related to health is always admissible in this context. Article 81, paragraph 1 a) of the text adopted by the LIBE Committee, however, states that such processing operations shall only be admissible if they are subject to specific European or national legislation. The CPP does not understand how a specific mandatory legislation could help to actually improve the protection of citizens' privacy in all cases. It considers that this will create unnecessary red tape in many situations.

130. However, the CPP believes that the pursuit of the purpose of therapies combined with the safeguard of professional secrecy (or any other equivalent obligation of secrecy) is, in principle, sufficient to justify the admissibility[34] of the processing of data related to health for the purpose of therapies and therefore proposes to formulate Article 81, paragraph 1 a) as follows:

"Within the limits of this Regulation and in accordance with Article 9, paragraph 2, sub-paragraph h), the processing of personal data related to health must be necessary:

(a) for the purposes of preventive medicine, medical diagnosis, the provision of care or treatments or the management of health services, provided that the data are processed by a health professional subject to professional secrecy, or by another person also subject to an equivalent obligation of confidentiality under Union or Member State law or following rules adopted by the competent national authorities; Union or Member State law may provide for suitable specific measures to protect the legitimate interests of the data subjects;"

[34] In the event of admissibility of a processing operation, it is self-evident that all other criteria included in the new Regulation (purpose, proportionality, security, etc.) will also have to be complied with.

7.3. Data processing for historical, statistical and scientific research purposes (Article 83)

131. Processing operations performed for historical, statistical and scientific (HSS) research purposes are currently subject to a favourable system[35] and it is necessary for this system to remain in place, but also for the rules and safeguards to be further harmonized in order to permit their application at European level. More and more research projects go beyond the purely national level and it is essential to facilitate the work of scientists by avoiding differences in national legislation as much as possible.

Retention term

132. Just as the European Commission's initial draft, the draft text voted by the LIBE Committee makes it possible to retain data longer for HSS research purposes (Article 5.e). The LIBE Committee adds *archiving* as a purpose and provides, as a further safeguard, that security and organisational measures must be taken in order to ensure that data are accessible only for those purposes. The CPP welcomes these additions (the reference to security measures was also specifically suggested by the CPP in its Opinion 35/2012[36]).

Compatibility in the event of further processing operations

133. The CPP believes, however, that it would be useful to include the exception currently provided in Article 6 of Directive 95/46/EC, which states that further processing operations for historical, statistical or scientific purposes (adding the purpose of archiving) are not deemed incompatible (in accordance with the safeguards laid down in Articles 83 and 83a).

Article 5.b: collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation); Further processing of data for historical, statistical, scientific or archive purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83 and 83a;

134. The CPP does not support the proposed amendment to Recital 126 which states that the data processed for HSS research purposes could be processed for any other purposes with the consent of the data subject or on the basis of Union or Member State law. According to the CPP, this

[35] The relevant information is currently scattered in Directive 95/46/EC, in particular in Recitals 29, 34, 40; and Articles 6.1.b, 6.1.e, 11.2, 13.2.
[36] Paragraph 179.

amounts to restoring part of Article 6.4 for which the LIBE Committee, however, proposes deletion[37].

Recital 126. ***Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***

Legal grounds: consent

135. With regard to the legal grounds, the LIBE Committee provides for the reintroduction of the need for consent in the processing of data related to health for HSS research purposes. As stipulated in Directive 95/46/EC, Member States may provide for an exemption from the requirement of consent in the context of research that serves high public interest[38]. Despite the possibility for the European Commission to adopt delegated acts to further specify this high public interest objective, the CPP believes that the principle of reintroducing the requirement of consent is not a good thing and that this proposal will clearly result in divergence between national laws.

Article 81

1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.

1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.

1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes shall be permitted only with the consent of

[37] Paragraph 36 Opinion 35/2012.
[38] Recital 34 of the Directive.

the data subject, and shall be subject to the conditions and safeguards referred to in Article 83.

~~2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interests, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.~~

136. In addition, the CPP does not understand why Article 83a concerning archives provides that national law must refer to the issue of consent. The CPP absolutely does not support the idea that processing operations performed by archiving services should require consent.

Article 83a

1 Once the initial processing for which they were collected has-been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object

137. Although the need for consent should be avoided, each research project should lead to a balancing of interests. This is why, as already explained in its previous Opinion 35/2012, "*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.*"

Article 6.2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

Processing conditions

138. Concerning the conditions to be met in the context of HSS research, Article 83.1 justly promotes the use of anonymous pseudonymised data in scientific research, which is fully in line with our national legislation and other international standards[39]. However, the CPP believes that the text of Article 83, paragraph 1, should allow the use of directly identifiable data where it is impossible to make use of anonymous data or pseudonymisation. If not, the draft text will push controllers to turn to other legal grounds than those specified in Articles 6.2 and 9.2.i and ia (which would amount to them avoiding the application of the other safeguards - which are useful - provided for in Articles 81 and 83). One cannot seriously imagine that historical research should necessarily be limited to anonymous data or should opt for pseudonymisation given that, by its very nature, knowing the identity of the persons who are the subjects of the research is often necessary. It is therefore necessary to add the terms originally proposed by the European Commission *"as long as these purposes can be fulfilled in this manner."*

Article 83

In accordance with the rules set out in this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects, as long as these purposes can be fulfilled in this manner.

Rights of the data subjects

139. Concerning exceptions to the exercise of the rights of the data subjects, the CPP welcomes the intention of including them directly in the Regulation[40]. However, it regrets the lack of an exception to the right of access and to the right to rectification (although currently provided for in Article 13.2 of Directive 95/46/EC).

[39] Chapter II of the Royal Decree of 13/02/2001; see also Art .40 of the German Federal Act, Article 46 of the Austrian Federal Act (DSG 2000), Article 16 Estonian Act and Article 3 of the Recommendation Rec(2006)4 of the Council of Europe on research on biological materials of human origin.

[40] See paragraph 180 of Opinion 35/2012 which criticizes the European Commission's intention to address this problem through a delegated act.

Article 15 and 16 shall not apply under condition that the information or part of the information referred to in Article 15 or the rectification is likely to render impossible or seriously impair the achievement of the objectives of the scientific, statistical or historical 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.

140. The exception to the right of information is provided for by the LIBE Committee (Art. 14.5.b). The CPP believes that it could be extended to statistical purposes (Art. 81a)[41]. In addition, an exception to the duty of information should also be provided for direct data collection[42] if this would render impossible or seriously compromise the scientific objectives pursued. Information could be provided as soon as transparency no longer jeopardizes the objectives. The idea is, for instance, to avoid being forced to clarify prior to the collection of information that a psycho-sociological study focuses on possible racist behaviour of individuals. It is obvious that stating this purpose will have an impact on responses, which could skew the results[43]. The CPP provides a draft text in this regard, already put forward in Opinion 35/2012:

Article 14

5. Paragraphs 1 to 4 shall not apply, where:

(b) the data are processed for historical, statistical or scientific research purposes or for archive services subject to the conditions and safeguards referred to in Articles 81 and 83, are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort and the controller has published the information for anyone to retrieve; or

14.5.ba: data are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83 and the provision of such 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

[41] The same applies for the exception to the right of erasure (17.3.c).

[42] An exemption in the event of direct collection is already provided for in various national legislations, such as the German Federal Act (Art.33), the Portuguese Act (Art. 10) and the Luxembourg Act (art.27).

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

of the scientific, statistical or historical research. 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 17.3.ca
for archive services in accordance with Article 83a;

8. Chapter X: delegated acts and implementing acts

8.1. Delegated acts (Article 86)

141. For the many reasons contained in Opinion 35/2012 (paragraphs 182 to 185), the CPP has been opposed from the start to the large number of delegated acts provided for by the draft regulation submitted by the European Commission. The LIBE Committee's reflection in this regard does not appear to be have been concluded. The list of delegated acts under Article 86 thus remains open. However, the CPP welcomes the use, in several provisions, of the European Data Protection Board's (EDPB) competence to deliver an opinion as well as prior consultation of the latter in cases where the adoption of a delegated act is maintained.

p.p. the Chief Administrator, The President,

(Sgd.) Patrick Van Wouwe (Sgd.) Willem Debeuckelaere