Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

Adopted on 12 March 2019

TABLE OF CONTENTS

The European Data Protection Board

Having regard to article 63 and article 64(2) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to article 10 and article 22 of its Rules of Procedure of 25 May 2018, as amended on 23 November 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the Board) is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. Article 64(2) GDPR provides that any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one Member State.

(2) On 3 December 2018, the Belgian Data Protection Authority requested the European Data Protection Board to examine and issue an Opinion on the interplay between the GDPR and the ePrivacy Directive, in particular regarding the competence, tasks and powers of data protection authorities.

(3) The opinion of the Board shall be adopted pursuant to article 64(3) GDPR in conjunction with article 10 (2) of the Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. On 3 December 2018, the Belgian DPA requested the European Data Protection Board to examine and issue an opinion on the interplay between the ePrivacy Directive[1] and the GDPR, submitting the following questions :

   a. Regarding the **competence, tasks and powers** of data protection authorities[2], whether
      i. data protection authorities are able or not able to exercise their competence, tasks and powers in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive; and if so, whether
      ii. data protection authorities may or should take into account provisions of the ePrivacy Directive and/or its national implementations when exercising their competences, tasks and powers under the GDPR (e.g., when assessing the lawfulness of processing) and if so, to what extent.
   b. whether the **cooperation and consistency mechanisms** can or should be applied in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive; and
   c. the extent to which processing **can be governed by provisions of both** the ePrivacy Directive and the GDPR and whether or not this affects the answers to questions 1 and 2.

2. The Board considers that these questions concern a matter of general application of the GDPR, as there is a clear need for a consistent interpretation among data protection authorities on the boundaries of their competences, tasks and powers. Clarification is particularly needed to ensure, amongst other, a consistent practice of mutual assistance in accordance with article 61 of the GDPR and joint operations in accordance with article 62 of the GDPR.

3. This opinion does not relate to any such division of competences, tasks and powers of data protection authorities under the proposal for the ePrivacy Regulation.

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

[2] As set forth by articles 55-58 GDPR. The term "data protection authorities" (as opposed to "supervisory authorities") shall be used throughout this Opinion in order to clearly distinguish the "supervisory authorities" envisaged by the GDPR from other types of supervisory authorities, such as the national regulatory authorities mentioned in Directive 2002/58/EC.

2 LEGAL CONTEXT

2.1 Relevant provisions of the GDPR

4. According to article 2(1), the GDPR applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*."
Article 2(2) of the GDPR states that the GDPR shall not apply to the processing of personal data:

> *"(a) in the course of an activity which falls outside the scope of Union law;*
>
> *(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;*
>
> *(c) by a natural person in the course of a purely personal or household activity;*
>
> *(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".*

5. Article 5, entitled "Principles relating to the processing of personal data", contains the principles applicable to any processing of personal data, including the requirement that any processing of personal data shall be lawful and fair.[3] Article 6 describes the circumstances in which processing of personal data shall be lawful, one of which relates to the consent of the data subject. Article 7 further specifies the conditions for valid consent within the meaning of the GDPR.[4]

6. Article 51(1) sets forth the legal mandate of data protection authorities, which is to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Articles 55, 57 and 58 specify the competences, tasks and powers of each data protection authority. Chapter VII of the GDPR, entitled 'Cooperation and Consistency', specifies the different ways in which data protection authorities shall cooperate in order to contribute to a consistent application of the GDPR.

7. Article 94, entitled 'Repeal of Directive 95/46', states that

> *"1. Directive 95/46/EC is repealed with effect from 25 May 2018.*
>
> *2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation."*

[3] See also recital (39) GDPR ("*Any processing of personal data should be lawful and fair. […]*").
[4] See the WP29 Guidelines on consent under Regulation 2016/679, WP259 rev.01, endorsed by the EDPB on 25 May 2018.

8. Article 95, entitled 'Relationship with Directive 2002/58/EC', stipulates that

> *"This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC."*

9. Recital (173) of the GDPR stipulates that:

> *"(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à- vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation."*

2.2 Relevant provisions of the Framework Directive

10. Article 2(g) of the Framework Directive[5] defines a 'national regulatory authority' as

> *"the body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives."*

11. Article 2(l) of the Framework Directive states that

> *'"Specific Directives' means Directive 2002/20/EC (Authorisation Directive), Directive 2002/19/EC (Access Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)."*

12. Article 3(1) of the Framework Directive provides that

> *"Member States shall ensure that each of the tasks assigned to national regulatory authorities in this Directive and the Specific Directives is undertaken by a competent body."*

2.3 Relevant provisions of the ePrivacy Directive

13. Article 1(2) of the ePrivacy Directive stipulates that

> *"The provisions of this Directive particularise and complement [Regulation (EU) 2016/679] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons."*[6]

[5] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[6] In accordance with article 94(2) of the GDPR, all references to Directive 95/46 in the ePrivacy Directive have been replaced with "[Regulation (EU) 2016/679]" and references to the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC" have been replaced with "[European Data Protection Board]".

14. Article 2(f) of the ePrivacy Directive states that

> *"'consent' by a user or subscriber corresponds to the data subject's consent in [Regulation (EU) 2016/679]"*

15. Article 15(2) of the ePrivacy Directive stipulates that

> *"The provisions of [Chapter VIII on remedies, liability and penalties] of [Regulation (EU) 2016/679] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.*"

16. Article 15(3) of the ePrivacy Directive stipulates that

> *"The [European Data Protection Board] shall also carry out the tasks laid down in [Article 70 of Regulation (EU) 2016/679] with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.*"

17. Article 15a, entitled 'Implementation and enforcement', stipulates that

> *"1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. […]*
>
> *2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.*
>
> *3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.*
>
> *4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.*
>
> *The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the [European Data Protection Board], make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures."*

18. Recital (10) of the ePrivacy Directive states that

> *"In the electronic communications sector, [Regulation (EU) 2016/679] applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. [Regulation (EU) 2016/679] applies to non-public communications services.*"

3 SCOPE OF THIS OPINION

19. The GDPR has the objective to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union.[7] To achieve this objective, the GDPR lays down common rules on data processing, so as to ensure consistent effective protection of personal data throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market. The rules serve to ensure a balance between the (potential) benefits of data processing and the (potential) drawbacks.

20. The ePrivacy Directive has the objective to harmonise the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.[8] The ePrivacy Directive seeks therefore to ensure respect for the rights set out in articles 7 and 8 of the Charter. In this regard, the ePrivacy Directive aims to "particularise and complement" the provisions of the GDPR, with respect to the processing of personal data in the electronic communication sector.[9]

21. The questions referred to the Board are limited to processing that triggers the material scope of both the GDPR and the ePrivacy Directive. In order to further clarify the scope of this opinion, the following sections clarify:

    - where there is no interplay between the GDPR and the ePrivacy Directive because the matter falls outside of the scope of the GDPR;
    - where there is no interplay between the GDPR and the ePrivacy Directive because the matter falls outside of the scope of the ePrivacy Directive; and
    - where there is an interplay between the GDPR and the ePrivacy Directive because the processing triggers the material scope of both the GDPR and the ePrivacy Directive.

[7] Article 1 of the GDPR.
[8] Article 1(1) of the ePrivacy Directive.
[9] Article 1(1)-(2) of the ePrivacy Directive, to be read in light of article 94(2) GDPR.

3.1 Matters outside the scope of the GDPR

22. In principle, the material scope of the GDPR covers any form of processing of personal data, regardless of the technology used.[10] The GDPR shall not be applicable when:

- no personal data are being processed (e.g. a phone number of an automated customer service of a legal person, or the IP address of a digital photocopier in a corporate network do not constitute personal data);
- the activities fall outside of the material scope of the GDPR, taking into account article 2(2) and (3) GDPR; or
- the activities fall outside the territorial scope of the GDPR.[11]

3.2 Matters outside the scope of the ePrivacy Directive

23. A particularity of the ePrivacy Directive is that two of its provisions have a wider scope of application than the other provisions, for which the scope of application is limited to the provision of publicly available electronic communications services in public communications networks. Consequently, as outlined in the following sections, two questions need to be answered to determine whether an activity falls inside or outside the material scope of the ePrivacy Directive.

3.2.1 The general material scope of the ePrivacy Directive

24. According to its article 3, the ePrivacy Directive applies to "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices*".

25. As such, the ePrivacy Directive in first instance addresses publicly available electronic communication services and electronic communication networks.[12]
The Electronic Communications Code[13] provides that services which are functionally equivalent to electronic communications services are covered.

[10] See also recital (46) of the ePrivacy Directive.
[11] Article 3 GDPR. See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 16 November 2018.
[12] Commission Staff Working Document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, COM SWD(2017)005 report, p. 20 ; Report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, p. 24 ff.
[13] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

26. For purposes of its general material scope, the ePrivacy Directive applies when each of the following conditions are met:

- there is an electronic communications service (ECS)[14];
- this service is offered over an electronic communications network[15];
- the service and network are publicly available[16];
- the service and network are offered in the EU.

27. Activities which do not meet all of the above criteria are generally out of scope of the ePrivacy Directive.

Examples:

A corporate network which is accessible only to employees for professional purposes does not constitute a "publically available" electronic communications service. As a result, the transmission of location data via such a network does not fall inside the material scope of the ePrivacy Directive [17]

A clock synchronisation service sends a signal over an electronic communications network to all clocks which adhere to its synchronisation protocol (undetermined number of recipients). This service is a broadcast service instead of a communication service in the current context and would also fall outside the material scope of the ePrivacy Directive.

[14] Article 2(d) ePrivacy Directive specifies that 'communication' means "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service" and excludes broadcasting services which may - in theory - reach an unlimited audience. The term 'electronic communications service' is currently defined by article 2(d) Framework Directive, though with effect from 21 December 2020 it shall be defined by article 2(4) of the Electronic Communications Code.

[15] 'Electronic communications network' is currently defined by article 2(a) Framework Directive, though with effect from 21 December 2020 it shall be defined by article 2(1) of the Electronic Communications Code.

[16] A service for the public is a service available to all members of the public on the same basis, and not only publicly owned services. Compare: EDPS, Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), p. 12 and Communication by the Commission to the European Parliament and the Council on the status and implementation of Directive 90/388/EEC on competition in the markets for telecommunications services, COM(95) 113 final, 04.04.1995, p. 14.

[17] Commission Staff Working Document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, COM SWD(2017)005 report, p. 21 , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN; Report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, p. 14, https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

3.2.2 The extended material scope of articles 5(3) and 13 ePrivacy Directive

28. The overarching aim of the ePrivacy Directive is to ensure the protection of fundamental rights and freedoms of the public when they make use of electronic communication networks.[18] In light of this aim, articles 5(3) and 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g. for cookies) or other businesses (e.g. for direct marketing).[19]

> Examples:
>
> Search engine services which store or access cookies on the device of a user fall within the extended material scope of article 5(3) ePrivacy Directive.[20]
>
> Unsolicited electronic mail sent by a website operator for the purposes of direct marketing also fall within the extended material scope of article 13 ePrivacy Directive.[21]

3.3 Matters within the material scope of both the ePrivacy Directive and the GDPR

29. There are many examples of processing activities which trigger the material scope of both the ePrivacy Directive and the GDPR. A clear example is the use of cookies. In its opinion on online behavioral advertising, the Article 29 Working Party stated that

> "*If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then,* ***in addition*** *to Article 5(3), Directive 95/46/EC will also apply.*"[22]

30. Case law of the Court of Justice of the European Union (CJEU) confirms that it is possible for processing to fall within the material scope of both the ePrivacy Directive and the GDPR at the same time. In *Wirtschaftsakademie*[23], the CJEU applied Directive 95/46/EC notwithstanding the fact that the underlying processing also involved processing operations falling into the material scope of the ePrivacy Directive. In the pending *Fashion ID* case, the Advocate General expressed the view that both set of rules may be applicable in a case involving social plug-ins and cookies.[24]

31. Whilst the GDPR replaced Directive 95/46/EC on 25 May 2018, the analysis undertaken by the CJEU and the Article 29 Working Party according to which both legal acts may apply at the same time are

---

[18] Article 1(1) ePrivacy Directive provides: "*This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.*"

[19] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, section 3.2.1 p. 9. Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12. ; Report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, p. 9.

[20] Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12

[21] Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12.

[22] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 9. See also Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12-139.

[23] CJEU, C-210/16, 5 June 2018, C-210/16, ECLI:EU:C:2018:388. See in particular paragraphs 33-34.

[24] Opinion of Advocate General Bobek in Fashion ID, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039. See in particular paragraphs 111-115.

relevant. Recital (30) of the GDPR elaborates on the definition of "online identifiers" in a way that supports the interpretation that processing of personal data may trigger the material scope of both the GDPR and the ePrivacy Directive:

> "*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*"

32. Worth noting in particular is that 'IP addresses' and 'cookie identifiers' are mentioned in recital (30), which states that IP addresses and cookie identifiers might be combined with other "unique identifiers" and other information received by the servers to create profiles of natural persons.

33. In other words, the GDPR itself explicitly refers, when clarifying its own material scope (the concept of personal data), to processing activities which also trigger, at least in part, the material scope of the ePrivacy Directive.

34. Another example of an activity which triggers the material scope of both the ePrivacy Directive and the GDPR is the customer relationship between electronic communications service providers and natural person that is a user of its services, which involves personal data processing about customers on the one hand, and are also governed by specific rules for instance on subscriber directories, itemised billing, calling line identification. Traffic data and location data generated by electronic communications services may also involve personal data processing, insofar as they relate to natural persons.

35. Finally, article 95 of the GDPR and recital (173) GDPR confirm the lex generalis-lex specialis relationship between the GDPR and the ePrivacy Directive, with article 95 providing that the GDPR shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the EU in relation to matters for which they are subject to specific obligations with the same objective set out in the ePrivacy Directive.

***

36. This opinion aims to provide clarity on the competence, tasks and powers of data protection authorities, with regards to cases which trigger the material scope of both the ePrivacy Directive and the GDPR as briefly laid out in the previous sections. The following sections describe some instances of interplay between the provisions of the ePrivacy Directive and the GDPR and how each sets of rules relate to one and other.

4 INTERPLAY BETWEEN THE EPRIVACY DIRECTIVE AND THE GDPR

37. Although an overlap in material scope exists between the ePrivacy Directive and the GDPR, this does not necessarily lead to a conflict between the rules. Besides this becoming apparent from reading the various provisions side by side, article 1(2) of the ePrivacy Directive expressly provides that "*the provisions of this Directive particularise and complement Directive 95/46/EC* (…)"[25]. To properly understand the interplay between the ePrivacy Directive and the GDPR, it is necessary to first clarify the meaning of article 1(2) of the ePrivacy Directive. After that, the meaning and implications of article 95 GDPR shall be clarified.

4.1 "To particularise"

38. A number of provisions of the ePrivacy Directive "*particularise*" the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector. In accordance with the principle *lex specialis derogate legi generali*, special provisions prevail over general rules in situations which they specifically seek to regulate.[26] In situations where the ePrivacy Directive "particularises" (i.e. renders more specific) the rules of the GDPR, the (specific) provisions of the ePrivacy Directive shall, as "*lex specialis*", take precedence over the (more general) provisions of the GDPR.[27] However, any processing of personal data which is not specifically governed by the ePrivacy Directive (or for which the ePrivacy Directive does not contain a "special rule"), remains subject to the provisions of the GDPR.

39. One example of where the ePrivacy Directive "particularises" the provisions of the GDPR can be found in article 6 of the ePrivacy Directive, which concerns the processing of so-called "traffic data". Ordinarily speaking, the processing of personal data can be justified on the basis of each of the lawful grounds mentioned in article 6 GDPR. However, the full range of possible lawful grounds provided by article 6 GDPR cannot be applied by the provider of an electronic communications service to processing of traffic data, because article 6 ePrivacy Directive explicitly limits the conditions in which traffic data, including personal data, may be processed. In this case, the more specific provisions of the ePrivacy Directive must take precedence over the more general provisions of the GDPR. Article 6 of the ePrivacy Directive does not however, curtail the applications of other provisions of the GDPR, such as the rights of the data subject. Nor does it negate the requirement that processing of personal data must be lawful and fair (article 5(1)a GDPR).

40. A similar situation occurs with regards article 5(3) of the ePrivacy Directive, insofar as the information stored in the end-user's device constitutes personal data. Article 5(3) of the ePrivacy Directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user.[28] To the extent that the

[25] Article 94.2 GDPR provides that references to the repealed Directive 95/46 shall be construed as references to the GDPR.
[26] Judgement of the CJEU in Joined Cases T-60/06 RENV II and T-62/06 RENV II, 22 April 2016, ECLI:EU:T:2016:233, at paragraph 81.
[27] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 10.
[28] Pursuant to article 5(3) information in the terminal equipment of a subscriber or user may also be stored or accessed insofar as its consists of technical storage or access for the sole purpose of carrying out the transmission

information stored in the end-users device constitutes personal data, article 5(3) of the ePrivacy Directive shall take precedence over article 6 of the GDPR with regards to the activity of storing or gaining access to this information. The outcome is similar in the interplay between article 6 of the GDPR and articles 9 and 13 of the ePrivacy Directive. Where these articles require consent for the specific actions they describe, the controller cannot rely on the full range of possible lawful grounds provided by article 6 of the GDPR.

41. A corollary of the "*lex specialis*" principle is that there shall only be a derogation from the general rule insofar as the law governing a specific subject matter contains a special rule. The facts of the case must be carefully analysed to find how far the derogation extends, especially in cases where data undergoes many different kinds of processing - either in parallel or sequentially.

> Example:
> A data broker engages in profiling on the basis of information concerning the internet browsing behaviour of individuals, collected by the use of cookies, but which may also include personal data obtained via other sources (e.g. "commercial partners"). In such a case, a subset of the processing in question, namely the placing or reading of cookies must comply with the national provision transposing article 5(3) of the ePrivacy Directive. Subsequent processing of personal data including personal data obtained by cookies must also have a legal basis under article 6 of the GDPR in order to be lawful.[29]

4.2 "To complement"

42. The ePrivacy Directive also contains provisions that "*complement*" the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector. For example, several of the provisions of the ePrivacy Directive seeks to protect "subscribers" and "users" of a publicly available electronic communications service. Subscribers of a publicly available electronic communications service may be natural or legal persons. By supplementing the GDPR, the ePrivacy Directive protects not only the fundamental rights of natural persons and particularly their right to privacy, but also the legitimate interests of legal persons.[30]

4.3 The meaning of article 95 GDPR

43. Article 95 of the GDPR stipulates that the GDPR "*should not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.*" (emphasis added).

---

of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

[29] While data protection authorities cannot enforce article 5(3) of the ePrivacy Directive (unless national law confers this competence to them), they should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection in order to avoid undermining this protection.

[30] Recital (12) of the ePrivacy Directive.

44. The aim of article 95 GDPR is therefore to avoid the imposition of unnecessary administrative burdens upon controllers who would otherwise be subject to similar but not quite identical administrative burdens. An example that illustrates the application of this article relates to the personal data breach notification obligation, which is imposed by both the ePrivacy Directive[31] and the GDPR[32]. They both provide for an obligation to ensure security, as well as an obligation to notify personal data breaches to the competent national authority and the data protection authority, respectively. These obligations are applicable in parallel under the two different pieces of legislation, according to their respective scopes of application. Clearly, an obligation to notify under both acts, once in compliance with the GDPR and once in compliance with national ePrivacy legislation would constitute an added burden without immediate apparent benefits for data protection. Following article 95 of the GDPR, the electronic communications service providers who have notified a personal data breach in compliance with applicable national ePrivacy legislation are not required to separately notify data protection authorities of the same breach pursuant to article 33 of the GDPR.

4.4 Co-existence

45. Where specific provisions exist which govern a particular processing operation or set of operations, the specific provisions should be applied (*lex specialis*), in all other cases (i.e. where no specific provisions govern a particular processing operation or set of operations), the general rule will apply (*lex generalis*).

46. Recital (173) confirms that, in respect of the processing of personal data to which the specific obligations of the ePrivacy Directive do not apply, the GDPR shall remain applicable:

> "*to all matters concerning the protection of fundamental rights and freedoms vis-à- vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons*".[33]

47. Recital (173) to the GDPR reiterates that, which is already stated in recital (10) to the ePrivacy Directive, which provides that: "*In the electronic communications sector, [Regulation (EU) 2016/679] applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals*."

48. For example, a provider of a public communications network or publicly available electronic communications service must comply with national rules transposing article 6(2) of the ePrivacy Directive concerning traffic data when processing data necessary for the purposes of subscriber billing and interconnection payments. Due to the absence of specific ePrivacy provisions on, for example, the right of access, the provisions of the GDPR apply. Likewise, recital (32) of the ePrivacy Directive confirms that where the provider of an electronic communications service or of a value added service

[31] Article 4 ePrivacy Directive.
[32] Articles 32-34 GDPR.
[33] Recital (173) goes on to state that "In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation." That review process is still ongoing.

subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the GDPR.

***

49. The previous sections described how the provisions of the ePrivacy Directive and the GDPR interact in case of processing which triggers the material scope of application of both instruments. The following sections turn to the resolving the questions referred to the Board regarding the competence, tasks and powers of data protection authorities, with regards to cases which at least in part fall within the scope of the ePrivacy Directive.

5 ON THE COMPETENCE, TASKS AND POWERS OF DATA PROTECTION AUTHORITIES

50. The Belgian SA referred two questions concerning the competence, tasks and powers of data protection authorities – as set out by articles 55-58 of the GDPR – to the Board, which can be paraphrased as follows:

- Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of data processing operations that should be excluded from their consideration, and if so to what extent?
- When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive (e.g., when assessing the lawfulness of processing), and if so to what extent? In other words, should infringements of national ePrivacy rules be taken into account or set aside when assessing compliance with the GDPR, and if so, under which circumstances?

51. As a preliminary matter, it should be noted that Member States are required to ensure full effectiveness of EU law, notably by providing for appropriate enforcement mechanisms. This obligation is founded on the principle of sincere cooperation established in article 4(3) TFEU.[34] The following sections describe in brief the enforcement provisions of the GDPR and ePrivacy Directive respectively and the interplay between them.

[34] Article 4.3 TEU provides: "*Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.*
The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.
The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives."

5.1 Enforcement of the GDPR

52. The GDPR provides for enforcement of its provisions by independent data protection authorities. In this regard, it should also be noted that article 8 of the Charter of Fundamental Rights of the EU (the Charter) provides that the processing of personal data shall be subject to control by an independent authority:

> "***Article 8 – Protection of personal data***
>
> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with **these** rules shall be subject to **control by an independent authority**.*"

53. Data protection authorities are given a legal mandate in this regard, as set forth in article 51(1) GDPR, which is to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.

54. The GDPR contains one exception and one possibility to derogate this mandate:

- the competence of the supervisory authorities shall not cover the processing of personal data when courts are acting in their judicial capacity (article 55(3) GDPR);
- for processing carried out for journalistic purposes or for the purpose of academic, artistic or literary expression, Member States may provide for exemptions and derogations from amongst others Chapters VI (independent supervisory authorities) and VII (cooperation and consistency) of the GDPR (article 85 GDPR);

In addition, the powers of the data protection authorities may be extended in line with article 58(6) GDPR and may in particular grant the power to fine public authorities and bodies, should a Member State provide so in the national legislation (article 83(7) GDPR).

Being exceptions to the general rule, these provisions must be narrowly construed.

55. Where the GDPR limits or allows for derogations on the competences, tasks and powers of data protection authorities, it has done so explicitly. The GDPR also does not exclude data protection authorities in any way from exercising their competences, tasks and powers in relation to processing to the extent it triggers the material scope of the GDPR. The question therefore becomes whether the EU legislature has envisaged or allowed a derogation on the general competence of data protection authorities in cases where provisions of the ePrivacy Directive apply to the processing at issue.

5.2 Enforcement of the ePrivacy Directive

56. The enforcement of the provisions of the ePrivacy Directive is closely linked to the Framework Directive[35], which stipulates in article 3(1) that "*Member States shall ensure that each of the tasks assigned to national regulatory authorities in this Directive and the Specific Directives is undertaken by a competent body*[36]*.*"

57. Article 2(g) of the Framework Directive defines a 'national regulatory authority' as

> *"the body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives.*"

58. Member states have chosen different ways of allocating the task of enforcing national ePrivacy rules to one or more entities.[37] This level of variation is possible, as the ePrivacy Directive only sets out some general goals to be achieved by the member states on this matter.

59. The ePrivacy Directive does not state that only one national body shall be competent to enforce its provisions. In fact, article 15a of the ePrivacy Directive explicitly provides that more than one national body may be competent to enforce its provisions. Article 15a also provides for the implementation and enforcement of the Directive by Member States including the obligations that Member States shall lay down rules on penalties, grant power to order cessation of infringements, grant investigative powers and resources etc. as follows:

> *"1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.*
>
> *2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority* ***and, where relevant, other national bodies*** *have the power to order the cessation of the infringements referred to in paragraph 1.*
>
> *3. Member States shall ensure that the competent national authority* ***and, where relevant, other national bodies*** *have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.*
>
> *4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive*

[35] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended.

[36] Article 2(l) of the Framework Directive clarifies that "'*Specific Directives' refers to Directive 2002/20/EC (Authorisation Directive), Directive 2002/19/EC (Access Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*"

[37] Report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, p. 33 ff.

and to create harmonised conditions for the provision of services involving cross-border data flows."

60. In addition article 15(2) of the ePrivacy Directive contains a provision referring to the provisions of Directive 95/46/EC on judicial remedies, liability and sanctions, now to be read as a reference to the GDPR:

> "*The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.*"

61. Article 15(3) of the ePrivacy Directive also provides:

> *"The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector."*[38]

5.3 Enforcement where GDPR and ePrivacy intersect

62. The ePrivacy Directive particularises and complements the GDPR and moreover refers to the latter's provisions on judicial remedies, liability and sanctions (article 15(2) of the ePrivacy Directive read in light of article 94 of the GDPR)..

5.3.1 Question one: are certain processing operations "off limits" for data protection authorities?

- *Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of processing operations they should exclude from their consideration, and if so which processing operations shall be excluded?*

63. Under the GDPR, Member States must have appointed one or more supervisory authorities. Member States may have appointed the same authority to be competent for (part of) the enforcement of the national implementation of the ePrivacy Directive, but may also have opted for one or more other authorities, for example a national telecommunications regulatory authority (NRA), a consumer protection organisation, or a ministry.

---

[38] Art. 15(3) of the ePrivacy directive provides "*The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.*"
Article 94.2 GDPR provides that "*References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.*"
Consequently, Article 30 of Directive 95/46 shall be construed as a reference to the relevant sections of article 70 GDPR (Tasks of the Board).

64. The ePrivacy Directive gives Member States flexibility on which authority or body to entrust with enforcement of its provisions.

65. While the ePrivacy Directive refers to the provisions of the GDPR regarding judicial remedies, liability and sanctions (article 15(2) of the ePrivacy Directive), article 15a(1) of the ePrivacy Directive details the "Implementation and enforcement" provisions of the ePrivacy Directive. For example, article 15a(1) provides that "*Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented...".* As such, the ePrivacy Directive explicitly provides Member States discretion with respect to penalties and article 15(2) does not interfere with the discretion offered to the Member States on enforcement (i.e., to determine who enforces the provisions of the ePrivacy Directive).[39]

66. In case national law confers competence for the enforcement of the ePrivacy Directive on the data protection authority, the law should also determine the tasks and powers of the data protection authority in relation to the enforcement of the ePrivacy Directive. The data protection authority cannot automatically rely on the tasks and powers foreseen in the GDPR to take action to enforce national ePrivacy rules, as these GDPR tasks and powers are tied to the enforcement of the GDPR. National law may assign tasks and powers inspired by the GDPR, but may also grant other tasks and powers to the data protection authority for enforcement of national ePrivacy rules in accordance with article 15a of the ePrivacy Directive.

67. Discretion exists only within the requirements and limits set forth in higher rules. Article 8(3) of the Charter demands that compliance with personal data protection rules is subject to control by an independent authority.[40]

68. When the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, data protection authorities are competent to scrutinize subsets of the processing which are governed by national rules transposing the ePrivacy Directive only if national law confers this competence on them. However, the competence of data protection authorities under the GDPR in any event remains unabridged as regards processing operations which are not subject to special rules contained in the ePrivacy Directive. This demarcation line may not be modified by national law transposing the ePrivacy Directive (e.g. by broadening the material scope beyond what is required by the ePrivacy Directive and granting exclusive competence for that provision to the national regulatory authority).

69. Data protection authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.

[39] Note that Article 15a(1) of the ePrivacy Directive was introduced by 2009/136/EC (i.e. an amendment to the ePrivacy Directive).

[40] The case law of the CJEU concerning article 28 of Directive 95/46 has clarified the requirements as regards independence: see e.g. Judgement of 9 March 2010, C-518/07 (Commission v. Germany), paragraph 17 and following; Judgment 16 October 2012, C-614/10 (Commission v. Austria), par. 36 and following; Judgment of 6 October 2015, C-362/14 (Safe Harbour), par. 41 and following; Judgment of 21 December 2016, C-203/15 and C-698/15 (Tele2/Watson), par. 123.

70. Where exclusive competence has been given to a body other than the data protection authority, national procedural law determines what should happen when data subjects nevertheless lodge complaints with the data protection authority regarding for instance the processing of personal data in the form of traffic or location data, unsolicited electronic communications or the collection of personal data by use of cookies without also complaining about a (potential) infringement of the GDPR.

5.3.2 Question two: Are national ePrivacy provisions "off limits"?

- *When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive* (e.g., when assessing the lawfulness of processing)*, and if so to what extent? In other words, should infringements of national ePrivacy rules be taken into account or set aside when in assessing compliance with the GDPR, and if so*, under which circumstances*?*

71. An example illustrates the difference with question one. Consider a data broker, who engages in profiling on the basis of information obtained from two distinct sources. The first source is data collected concerning the internet browsing behaviour of individuals, through the use of cookie identifiers and/or other device identifiers. The second source is data obtained via commercial partners, who share data about participants in prize draws or cash-back programs.

72. Profiling of individuals on the basis of personal data generally falls within the scope of the GDPR and therefore within the competence of data protection authorities. If a data protection authority receives a complaint regarding the profiling activities undertaken by the data broker, what consideration may data protection authorities give to specific rules, in this case national ePrivacy rules, when assessing compliance with the GDPR?

73. Worth noting is that ePrivacy Directive is a specific example of a law which offers special protection to particular categories of data which may be personal data. Other legal texts also offer particular protection to specific kinds of data which may be personal data for various reasons (e.g. the context of the processing, the nature of the data or the risks for data subjects).[41]

74. Member States are obligated to appoint one or more authorities to supervise compliance with the national law transposing the ePrivacy Directive, and such authority(-ies) is then responsible for enforcement of this law. The national law transposing the ePrivacy Directive applies to the specific processing operation(s) governed by the ePrivacy Directive (e.g. a processing operation which consists of the storing of or access to information stored on the end-users device).

[41] An example can be found in the financial sector: Specific protection is afforded to data used to assess a person's creditworthiness or the publicity to be given to administrative penalties. See: Article 21(1) in Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010; Articles 68-69 in Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.
Another example can be found in the rules on clinical trials: see articles 28 - 35 of Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.

75. Unless national law gives them such competence, data protection authorities cannot enforce the provisions (of national law implementing) the ePrivacy Directive as such when exercising their competences under the GDPR. However, as indicated earlier, the processing of personal data which involves operations subject to the material scope of the ePrivacy Directive, may involve additional aspects for which the ePrivacy Directive does not contain a "special rule". For example, article 5(3) of the ePrivacy Directive contains a special rule for the storing of information, or the gaining of access to information already stored, in the terminal device of an end-user. It does not contain a special rule for any prior or subsequent processing activities (e.g., the storage and analysis of data regarding web browsing activity for purposes of online behavioural advertising or security purposes). As a result, data protection authorities remain fully competent to assess the lawfulness of all other processing operations that follow the storing of or access to information in the terminal device of the end-user.[42]

76. An infringement of the GDPR might also constitute an infringement of national ePrivacy rules. The data protection authority may take this factual finding as to an infringement of ePrivacy rules into consideration when applying the GDPR (e.g., when assessing compliance with the lawfulness or fairness principle under article 5(1)a GDPR). However, any enforcement decision must be justified on the basis of the GDPR, unless the data protection authority has been granted additional competences by Member State law.

77. If national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR (otherwise it does not).

78. As a general comment, where several authorities are competent for the different legal instruments, they should ensure that enforcement of both instruments is consistent inter alia to avoid a breach of the non bis in idem principle in case infringements of provisions of the GDPR and ePrivacy Directive which took place in the context of one processing activity are strongly linked.

[42] In this regard, reference should be made to the Opinion of the WP29 on legitimate interest (06/2014) and the WP29 opinion on purpose limitation (Opinion 03/2013), which clarify that certain forms of behavioural advertising require consent of the data subject, not just because of article 5(3). Opinion on purpose limitation states:
"The second potential scenario is when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers. In these cases, free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."
Opinion on legitimate interests states:
"Instead of merely offering the possibility to opt out of this type of profiling and targeted advertisement, an informed consent would be necessary, pursuant to Article 7(a) but also under Article 5(3) of the ePrivacy Directive. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing."

6 ON THE APPLICABILITY OF THE COOPERATION AND CONSISTENCY MECHANISMS

79. The third question submitted by the Belgian Data Protection Authority to the Board can paraphrased as follows:

- *to what extent is the cooperation and consistency mechanisms applicable in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive?*

80. Following Chapter VII of the GDPR, the cooperation and consistency mechanisms available to data protection authorities under the GDPR concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the provisions contained in the ePrivacy Directive as such.

81. In any event, article 15(3) of the ePrivacy Directive provides:

> *"The [European Data Protection Board] shall also carry out the tasks laid down in [article 70 of Regulation (EU) 2016/679] with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector."*

82. Regarding cooperation between authorities competent for the enforcement of the ePrivacy Directive, article 15a(4) of the ePrivacy Directive provides that "*the relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross- border data flows (…)*."

83. Such cross-border cooperation between authorities competent for the enforcement of the ePrivacy Directive, including data protection authorities, national regulatory authorities and other authorities, may take place to the extent that relevant national regulatory authorities adopt measures to allow such cooperation.

84. It should be noted that the cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a "special rule" contained in the ePrivacy Directive). For example, even if the processing of personal data (e.g. profiling) in part relies on access to information stored in the end-user's device, the data protection rules which are not provided by the ePrivacy Directive (e.g. data subject rights, principles of processing) for any processing of personal data that takes place following the access to information stored in the end-user's device shall be subject to the provisions of the GDPR, including the cooperation and consistency mechanisms..

85. In practice, data protection authorities will have carefully select which 'line of communication' to use, especially if they are not only enforcing the GDPR but also competent to enforce (part of) the national transposition of the ePrivacy Directive. The default 'line of communication' - as detailed in Chapter VII (Cooperation and Consistency) of the GDPR - shall be used for any and all parts of a procedure that envisage using the enforcement powers granted by the GDPR in response to an infringement of the GDPR.

The discretionary 'line of communication' may be used by data protection authorities in the context of their distinct enforcement powers granted by the national transposition of the ePrivacy Directive and only insofar as the procedure aims to respond to infringements of national ePrivacy rules governing the specific behaviours regulated by the ePrivacy Directive. As soon as it concerns matters falling within the scope of the GDPR, data protection authorities are obliged to apply the cooperation and consistency mechanism provided by the GDPR.

7 CONCLUSION

- *Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of data processing operations they should set aside, and if so when?*

86. When the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, data protection authorities are competent to scrutinize the data processing operations which are governed by national ePrivacy rules only if national law confers this competence on them, and such scrutiny must happen within the supervisory powers assigned to the authority by the national law transposing the ePrivacy Directive.

87. Data protection authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.

- *When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive, and if so to what extent? In other words, should infringements of national ePrivacy rules be set aside when in assessing compliance with the GDPR, and if so when?*

88. The authority or authorities that are appointed as competent in the meaning of the ePrivacy Directive by Member States is exclusively responsible for enforcing the national provisions transposing the ePrivacy Directive that are applicable to that specific processing operation, including in cases where the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive. Nevertheless, data protection authorities remain fully competent as regards any processing operations performed upon personal data which are not subject to one or more specifics rules contained in the ePrivacy Directive.

89. An infringement of the GDPR might also constitute an infringement of national ePrivacy rules. The data protection authority may take this factual finding as to an infringement of ePrivacy rules into consideration when applying the GDPR (e.g., when assessing compliance with the lawfulness or fairness principle under article 5(1)a GDPR). However, any enforcement decision must be justified on the basis of the GDPR, unless the data protection authority has been granted additional competences by Member State law.

90. If national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR (otherwise it does not).

- *To what extent is the cooperation and consistency mechanisms applicable in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive?*

91. The cooperation and consistency mechanisms available to data protection authorities under Chapter VII of the GDPR, concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the national implementation of the ePrivacy Directive. The cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a "special rule" contained in the ePrivacy Directive).

***

92. The Board acknowledges that the interpretation above is without prejudice to the outcome of the current negotiations of the ePrivacy Regulation. The proposed Regulation addresses many important elements, including as regards the competences of data protection authorities, but also as regards a range of other very important issues. The Board reiterates its position that the adoption of an ePrivacy Regulation is important.[43]

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[43] The EDPB has called upon the European Commission, Parliament and Council to work together to ensure a swift adoption of the new ePrivacy Regulation (EDPB statement published on 25 May 2018).