European Data Protection Board

Johannes Gungl

BEREC Chair 2018

Jeremy Godfrey

BEREC Chair 2019

Brussels, 3 December 2019

Ref: OUT2019-0055

Subject: Data protection issues in the context of Regulation (EU) 2015/2120

Dear Mr Gungl, Dear Mr Godfrey,

I refer to your letter of 13 November 2018 regarding consultation of the European Data Protection Board ('EDPB') on some issues on traffic management and zero-rating that concern privacy aspects, also in connection with Regulation (EU) 2016/679 ('GDPR') and Directive 2002/58/EC ('ePD').

In the attached Annex, you will find the Board's replies to the questions submitted by BEREC concerning certain terminological elements, as well as applicable rules related to personal data processing and privacy and specific obligations regarding transparency, consent and legal conditions for the processing of personal data.

In summary, the Board wishes to point out that the terms "specific content" and "monitoring" are not explicitly defined in the data protection legislation currently in force. Nevertheless, this or similar terminology is in use in jurisprudence and important principles regarding general monitoring of communications have been set out in the case law of the Court of Justice of the European Union ('CJEU'). In particular, in Case C-70/10 *Scarlet Extended*, the Court and the Advocate General have undertaken a thorough analysis of traffic analysis and monitoring operations. The analysis of a filtering system in that case led to the conclusion that any such filtering system would create an interference with the fundamental rights established by Articles 7 and 8 of the Charter.

Furthermore, in order to determine whether and to what extent traffic monitoring may be lawful, Articles 4, 5 and 6 ePD are relevant. The ePD generally provides that communications related data may not be stored, tapped or otherwise intercepted without the consent of all end-users concerned[1]. In the case of a network service that is based on the internet protocol (IP), the EDPB is of the view that the IP header information constitute traffic data within the meaning of Article 2(b) ePD, and that all other parts of the packet must be considered content or

[1] The ePD provides for exemptions to this requirement in Art 5 ePD for "technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.", for "any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication", in Art 6(2) ePD and in Art 15(1) ePD.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

"specific content". In some cases, transport headers could also be considered traffic data. The communications service provider must not process the content of an IP packet for purposes other than technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality, including elements serving as control information for other protocol layers, e.g. http headers or URLs. This interpretation appears to be reflected correctly in the BEREC's Net Neutrality Rules (BoR (16) 127 69), as reported in BEREC's letter.

As established in C-70/10 and C-582/14 *Breyer*, also traffic data (including IP addresses) constitute personal data when associated to a natural person. Consequently, the relevant GDPR provisions apply[2]. The GDPR transparency requirements complement those laid down in the Regulation (EU) 2015/2120 (hereinafter *"TSM Regulation"*)[3] Article 4, which have a different scope and purpose. Furthermore, the GDPR's definition of 'consent' and its provisions on consent also apply in cases where the ePD requires consent.

As BEREC correctly recognizes in its letter, the ePD requires consent for the processing of traffic data of all end-users concerned in order to provide value added services. It should be taken into account that the domain names and URLs can provide revealing insights on a wide variety of aspects of a person's life. For reasons set out in the annex, the Board considers that **processing of data such as the domain name and URL by internet access services providers for traffic management and billing purposes is unlawful, unless consent of all users is obtained**. The EDPB remains open to discuss how traffic management and zero-rating offers could be also implemented using other technical means, such as those suggested in the annex.

Finally, the Board would like to thank the BEREC for this consultation on these very important data protection related issues.

Yours sincerely,

Andrea Jelinek

[2] EDPB 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

[3] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012, OJ L 310, 26.11.2015, p. 1–18

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Annex

a. Is the term "specific content" commonly used in privacy context, and how would this term in that case be defined in EU privacy rules?

Background

According to Regulation (EU) 2015/2120 (hereinafter *"TSM Regulation"*)[4] Article 3(3) '*[the traffic management] measures shall not monitor the specific content and shall not be maintained for longer than necessary.*'

The BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules defines *'specific content'* as the transport layer protocol payload[5]. Therefore, both network layer (e.g. IP packet) headers and transport layer (e.g. TCP or UDP) headers are considered generic content.

Answer

Both traffic data and content are part of the communications data as defined by article 2 ePD.

There is no definition of the term *'specific content'* neither in the ePrivacy Directive[6] ('ePD)' nor in the GDPR[7].

Article 2 ePD defines the term *'communication'* as '*any information exchanged or conveyed between a finite number of parties by means of publicly available electronic communication service (...)'. 'Traffic data'*, are defined as *"any data processed for the purpose of conveyance of a communication on an electronic communication network or for the billing thereof'.*

The EDPB considers that network layer (e.g. IP packet) headers and transport layer (e.g. TCP or UDP) headers should be considered traffic data, while the transport layer protocol payload should be considered contents of the communication.

[4] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012, OJ L 310, 26.11.2015, p. 1–18

[5] 69. In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content (i.e. transport layer protocol payload).
70. Conversely, traffic management measures that monitor aspects other than the specific content, i.e. the generic content, should be deemed to be allowed. Monitoring techniques used by ISPs which rely on the information contained in the IP packet header, and transport layer protocol header (e.g. TCP) may be deemed to be generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video).

[6] 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) OJ L 201, 31.7.2002, p. 37–47

[7] Regulation (EU) 2016/679 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 (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

b. Is the term *"monitoring"* commonly used in privacy context, and how would this term in that case be defined in EU privacy rules?

Background

The term *'monitor'* or *'monitoring'* is used in Recital 10[8] and Article 3(3) of the Regulation (EU) 2015/2120. In both cases the monitor term is used in the context of IAS providers' traffic management activities while preventing the monitoring of '*specific content*'.

The BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules also refers to monitoring in its paragraph 85, where it is described as '*monitoring of the integrity and security of the network*'.

Answer

Although the term *'monitoring'* is commonly used in the context of privacy and data protection, there is no definition of the term neither in the ePD nor in the GDPR which would apply in the present context.[9]

However, general principles for monitoring of communications have been developed in the case law of the Court of Justice of the European Union ('CJEU'). For example, the case C-70/10 *Scarlet Extended*[10], which involved balancing the protection of fundamental rights: on the one hand, the protection of the intellectual property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information . In this case the CJEU ruled that *"Preventive monitoring (…) would (…) require active observation of all electronic communications conducted on the network of the ISP concerned and, consequently, would encompass all information to be transmitted and all customers using that network"*. In this case, the Court and the Advocate General undertook a thorough analysis of traffic analysis and monitoring operations. The analysis of a filtering system in that case led to the conclusion that any such filtering system would create an interference with the fundamental rights established by Articles 7 and 8 of the Charter. As the AG recognized in his opinion[11], this interpretation was also held by the European Data Protection Supervisor[12] (EDPS) and the

[8] Recital 10 of Regulation (EU) 2015/2120. '*Reasonable traffic management does not require techniques which monitor the specific content of data traffic transmitted via the internet access service.*'

[9] In the context of the GDPR, "monitoring" individuals' habits or preferences is one of the situations that trigger high risks for data subjects' rights and freedoms to the extent that a prior data protection impact assessment is mandatory before a processing operation entailing a "monitoring" is put in place, see e.g. Art. 3(2) b) or Art. 35 (3) c GDPR.

[10] Judgement of the Court of Justice of the European Union of 24 November 2011, Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)), ECLI:EU:C:2011:77

11 Opinion of Advocate General Cruz Villalón delivered on 14 April 2011, Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)), ECLI:EU:C:2011:255

12 Opinion of the European Data Protection Supervisor of 10 May 2010 on the proposal for a directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (OJ 2010 C 323, p. 6, paragraph 11).

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Article 29 Working Party (WP29), the predecessor of the European Data Protection Board (EDPB) [131415].

c. Which rules follow from EU privacy law for practices concerning traffic management?

Background

According to Article 3(4) of the Regulation (EU) 2015/2120 processing of personal data shall be carried out in accordance with the ePD and with the Directive 95/46/EC (since replaced by Regulation (EU) 2016/679 (GDPR)).

Answer

Recital 9 of the TSM Regulation provides that *'[t]he objective of reasonable traffic management is to contribute to an efficient use of network resources and to an optimisation of overall transmission quality responding to the objectively different technical quality of service requirements of specific categories of traffic, and thus of the content, applications and services transmitted.*'

The EDPB understands that by *"traffic management*" one should intend an intervention of the network operator so that, based on predefined criteria communications flowing into the network are routed in a different way. Recital 9 of the TSM Regulation clarifies that such routing '*differentiation should be permitted only on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth) of the specific categories of traffic, and not on the basis of commercial considerations*'. From a privacy and data protection perspective, processing that involves scrutiny of packet flows might amount to monitoring of electronic communications and must be approached with caution. In addition, the choice of criteria for traffic management is important, since this is where the impacts on individuals' rights and freedoms may be generated.

In the context of traffic management, it is particularly important to highlight that the content of communications and the traffic data are both protected by the right to the confidentiality of communications, which is a fundamental right, guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 of the Charter of Fundamental Rights of the European Union.

13 Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECLI:EU:C:2011:255, Opinion of AG Cruz Villalón. para 76

14 EDPS Opinion of the European Data Protection Supervisor of 22 February 2010 on the Anti Counterfeiting Trade Agreement (ACTA), OJ 2010 C 147, p. 1, paragraph 24; EDPS Opinion of the European Data Protection Supervisor of 10 May 2010 on the proposal for a directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, OJ 2010 C 323, p. 6, paragraph 11

15 Article 29 Working Party "Privacy on the Internet - An integrated EU Approach to On-line Data Protection-" WP 37, 21 November 2000, p. 22

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Confidentiality is further protected in secondary EU legislation, in particular, Article 5 ePD. Article 5 (1) ePD sets out the general rule that *'(...) listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users*' is prohibited without the consent of the users concerned, allowing two exceptions, a legal authorisation in line with ePD Article 15(1) and the '*technical storage which is necessary for the conveyance of a communication*'.

Article 6 (2) ePD allows the processing of traffic data for the purposes of subscriber billing and interconnection payments.

Article 2(b) defines "traffic data" as "any data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof".

Further, Article 5(1) states in respect of national legislative measures on confidentiality of communications that they "...shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

In order to benefit of this last exception for traffic management, the processing should be clearly demonstrable as being strictly necessary and proportionate. To be strictly necessary, such data processing should be required, unconditional and without alternative. To be proportionate, the processing should strike the right balance between the means used and the intended aim. Service providers need to be able to provide this demonstration whenever and however they under-take such processing.

On this aspect, it is worth recalling that the processing of personal data retained in the context of traffic management must also respect other principles that derive from the GDPR and the ePD. In particular, the data minimization principle (personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed), and the principle of lawfulness, fairness and transparency (personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject).

In addition, as the ePD complements and particularises the GDPR and Art 2(f) ePD refers to the definition of consent in GDPR[16], whenever the two exceptions in articles 5(1) and article 6(2) do not apply and consent is the legal basis for the processing, this must be interpreted in line with Article 4 (11) GDPR as *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*' The Article 29 Working Party's guidelines on consent[17] provide general guidance on how to obtain users consent.

[16] 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]"*

[17] Article 29 Working Party. "Guidelines on Consent under Regulation 2016/679" adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

d. How would the obligation to be transparent on traffic management measures relate to obligation to inform under EU privacy law?

Background

According to Article 4(a) of the Regulation (EU) 2015/2120, '*providers of IAS* shall ensure *that any contract specifies [...] the information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data.*'

Answer

Providers of IAS must also provide their customers with the information foreseen in Articles 12 and 13 GDPR. The purposes for which Regulation (EU) 2015/2120 allows traffic monitoring (compliance with *legislative acts, preservation of network integrity and security and prevention or mitigation of network congestion*) are different from the purpose of fulfilling the contract or conveying the message. The subscriber should be informed of such purposes and of the associated legal grounds envisaged in ePD. Such information should be provided in a precise, transparent, comprehensible and easily accessible form. It may be provided together with the contractual terms.

Furthermore, providers of IAS bear a responsibility for informing customers about any update or changes to their traffic management policies.

e. When applying traffic management for IAS, from a data protection perspective, is it allowed to process data such as the domain name and URL?

Background

Article 3(4) of the Regulation (EU) 2015/2120 sets out the requirements to process personal data for traffic management.

On the one hand it requires that the processing will be carried out in accordance with the ePD and with the GDPR. On the other it allows such processing only if necessary and proportionate to achieve the objectives set out in Article 3(3) paragraph 3 of the Regulation (EU) 2015/2120.

Answer

The confidentiality of communications enshrined in Article 5(1) ePD, as said, prohibits *'technical storage which is necessary for the conveyance of a communication'* without the consent of the users concerned, allowing two exceptions: a legal authorisation in line with ePD Article 15(1) or for the '*technical storage which is necessary for the conveyance of a communication'.*

The relevance of confidentiality is of high importance as the domain names and URLs, in conjunction with other data relating to electronic communications, can provide revealing insights on a wide variety of aspects of a person's life. In fact, they can be as revealing as the actual contents of the communication.

IAS service providers do not require information included in the transport layer payload (like domain names or URLs) to convey a communication on an electronic communication network.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Therefore, domain names and URLs cannot be considered 'traffic data' as defined in Article 2(b) ePD and they cannot be processed under the provisions in Article 6 ePD.

Article 5(1) ePD allows for the '*technical storage which is necessary for the conveyance of a communication*'. However, domain names and URLs are not necessary for IAS service providers to convey a communication.

Even the option of basing traffic management on consent is not unconstrained. Consent, in fact, must be interpreted in the light of Article 4 (11) GDPR as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*. In the light of this definition, no possibility exists for setting vague purposes, and any open-ended traffic management processing operations would be in breach of the law. IAS providers should also consider that freely given consent can be withdrawn anytime. The Article 29 Working Party's guidelines on consent[18] provide general guidance on how to obtain users consent.

The EDBP considers that the processing of communications and related traffic data on the basis of the Article 5(1) ePD for purposes of traffic management requires the consent of all end-users of an IAS provider.

IAS providers would need to perform deep packet inspection to gain access to the domain names and URLs that are included in the transport layer payload.

As already mentioned, a filtering system that would require an ISP to carry out general monitoring of the information in Case C-70/10 Scarlet Extended led the CJEU to the conclusion that any such filtering system would create an unjustifiable interference with the fundamental rights established by Articles 7 and 8 of the Charter.

Considering the interference that the general monitoring of end-users' communications content would create, **the EDPB is of the view that the use of deep packet inspection to extract the domain names and URLs for traffic management is unlawful, unless consent of all users is obtained.**

IAS provider could achieve the objectives of traffic management standardizing and using data available at the IP header like the Explicit Congestion Notification[19] (ECN) or the Differentiated Services Code Point[20] (DSCP). Therefore, the EDPB is of the view that processing of domain names and URLs by providers of IAS is not necessary to conduct traffic management.

The EDPB encourages the IAS providers and BEREC where relevant to define and agree on less invasive and more standardized ways to manage internet traffic, interoperable throughout different IASs, which are not based on the use of URLs and domain names.

[18] Article 29 Working Party "Guidelines on Consent under Regulation 2016/679" adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB
[19] https://tools.ietf.org/html/rfc3168
[20] https://tools.ietf.org/html/rfc2474

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

f. On zero-rating offers, how can providers of IAS obtain user consent on monitoring all visited domain names and websites for billing purposes?

Background

According to the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules[21], a zero-rating offer *'is where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the IAS).'*

Answer

Art 5(1) ePD prohibits '*listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.*'

If billing is the purpose of the processing of electronic communication data, legislative measures referred in Article 15(1) ePD would not be applicable. Consequently, freely given and specific consent of the users would be required to process visited domain names and websites for billing purposes[22].

As mentioned in the previous answer, domain names and URLs cannot be processed under the traffic data provisions in Article 6 ePD.

For the mentioned purpose, the IAS will need to obtain consent of all end-users. The same argument as provided in the answers to question c and e relating to consent still apply in this case[23].

For an IAS to obtain consent in a way that will fully meet all the requirements stipulated by the GDPR will be challenging.

For the same reasons expressed in the previous answer, the EDPB is of the view that **monitoring all visited domain names and websites for billing purposes is unlikely to be possible in a lawful manner**.

[21] https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

[22] Article 29 Working Party "Guidelines on Consent under Regulation 2016/679" adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB

[23] The Art 29 Working Party Guidelines state "that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time." (emphasis added)

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

g. On zero-rating offers, how can providers of IAS lawfully monitor traffic of third parties for billing purposes (red arrow in the figure above)?

Answer

As mentioned in the reply to the previous question, Article 5(1) ePD requires the user's consent to legitimise the processing.

The EDPB is of the view that whenever non-contractual parties are involved, consent as in art 5(1) ePD is needed to legitimise the processing.

Consent must be obtained from all users involved in the processing of communications data (senders and recipients)[24]. Therefore, according to Article 5(1) ePD, the legal ground to monitor traffic for billing purposes can only be consent of all involved end-users (to be understood as the individuals actually using the service).

In the case of the communication represented by the red arrow in the figure, the sender of an electronic communication has not consented the monitoring of his or her traffic. Therefore, **monitor of traffic of such third parties for billing purposes would be unlawful**.

The data contained in headers of transport, network or data link layers, if properly standardized, could be considered traffic data and processed by the IAS providers for billing purposes in line with the provisions in Article 6 ePD. However, following the data minimization principle, the data included for billing purposes in the mentioned headers should be adequate, relevant and limited to what is necessary (e.g. to count or not a packet against the data cap).

Again, the EDPB encourages the IAS providers and BEREC where relevant to define and agree on less invasive and more standardized ways to bill internet traffic, based on labelling the type of communication, interoperable throughout different IASs, which are respectful of the data minimization principle and do not require traffic monitoring.

[24] See also 29 Working Party Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, p.3 and p.13

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels