European Parliament
2014-2019

Committee on Petitions

2.5.2017

NOTICE TO MEMBERS

Subject: Petition No 1998/2014 by S. K. (German), on the handling of personal data by PayPal

1. Summary of petition

The petitioner claims that the payment service PayPal in Luxembourg is infringing Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. According to the petitioner, PayPal does not delete personal data when the contract is terminated and the deletion of the data is requested. The petitioner also claims that PayPal blocks accounts in an unannounced and arbitrary way as soon as a large amount of money is deposited. The petitioner considers this to be confiscation of funds. In order to release the money, PayPal demands very personal information, such as bank statements, copies of accounts, contracts from suppliers, etc. Another arbitrary measure is the setting of a minimum reserve, where PayPal retains each payment until a certain amount has been reached. The company gives no reasons for setting a minimum reserve, nor for determining the amount of the reserve. Moreover, citizens cannot hold PayPal liable. According to the petitioner, the German regulatory authorities such as the Bundeskartellamt and the Bundesanstalt für Finanzdienstleistungsaufsicht cannot supervise PayPal either and refer to the Luxembourgish regulatory authority which, in its turn, refers to PayPal's general terms and conditions which are subject to the law of the United Kingdom. However, a complaint against PayPal in Luxembourg on the basis of UK law is unaffordable for most PayPal customers. The petitioner requests the intervention of the EU.

2. Admissibility

Declared admissible on 24 June 2015. Information requested from Commission under Rule 216(6).

3. **Commission reply**, received on 29 February 2016

In the European Union the right to the protection of personal data is guaranteed under Article

8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union. The right is elaborated, in particular, in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[1] Directive 95/46 establishes a legal framework for national data protection law in the Member States of the European Union. The Member States are obliged to implement the provisions of the Directive into their own national legislation.

Under Directive 95/46/EC personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Personal data must also be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Article 6). Personal data may be processed only if the data subject has unambiguously given his consent; if the processing is necessary for the performance of a contract to which the data subject is party; if the processing is necessary for compliance with a legal obligation to which the controller is subject; if processing is necessary in order to protect the vital interests of the data subject; if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or if processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interest are overridden by the interests for fundamental rights and freedoms of the data subject (Article 7).

A data subject has a right, under certain conditions, to request his data be rectified, erased or blocked[2] and/or to object processing of his personal data.[3] Those rights have been interpreted by the CJEU in *Google Spain* case, confirming that when personal data appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue, it should not be (further) processed.[4]

In as far as PayPal qualifies as obliged entity in the sense of Directive 2015/849 it will be subject to obligations to process personal data for the purposes of the prevention of money laundering and terrorist financing.[5] The processing of personal data on the basis of that directive for those purposes is considered to be a matter of public interest under Directive 95/46/EC (see Article 43 of Directive 2015/849). The collection and subsequent processing of personal data should be limited to what is necessary for the purpose of complying with the requirements of Directive 2015/849 and personal data should not be further processed in a way that is incompatible with that purpose.

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995, p. 31 – 50.

[2] Article 12(b) of Directive 95/46/EC. Data subject can request the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.

[3] Article 14(a) of Directive 95/46/EC. Under Article 14(a) of Directive 95/46/EC, the rights to object processing relate at least to those two latter cases. Data subject can object processing at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

[4] Judgment of the Court of 13 May 2014 in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, paras 94, 98-99.

[5] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal L 141, 5/6/2015, p. 73 – 117.

PayPal being a payment service provider, it is also subject to the requirements of the Payment Services Directive (2007/64/EC). The processing of personal data by payment service providers is permitted when it is necessary to safeguard the prevention, investigation and detection of payment fraud. The PSD does not provide specific rules on the retention time of the data for that purpose but follows the rules of Directive 95/46/EC.

In order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities under Directive 2015/849 should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to fulfil the requirements relating to the protection of personal data, the retention period is fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary and proportionate, Member States can allow or require the further retention of records for a period not exceeding an additional five years (Article 40). Specific safeguards have to be put in place to ensure the security of data and to determine the persons having access to the data retained.

Without prejudice to the power of the European Commission as guardian of the Treaties, it is in the first place for Member States to monitor the application of the national data protection rules implementing Directive 95/46/EC, primarily through their national Data Protection Supervisory Authorities. The Commission is not competent to resolve the complaints which are submitted to it by data subjects against private natural or legal persons.

Hence, if the petitioner considers that his rights as a data subject have been violated, he may lodge a complaint with the competent national data protection authority. As PayPal (Europe) offices are located in Luxembourg and the processing is carried out in the context of the activities of that establishment of the controller, it is prima facie the Luxembourgish data protection law implementing Directive 95/46/EC that applies.

If the petitioner believes that the processing of data by PayPal in his case is not in compliance with Directive 95/46/EC and the Luxembourgish data protection legislation implementing it, he can lodge a formal complaint with the Luxembourgish data protection supervisory authority, or the national data protection supervisory authority of his Member State. National data protection supervisory authorities are under an obligation under Article 28 of Directive 95/46/EC to hear complaints (within the territory of their own Member State). Where the complaint relates to a matter taking place on the territory of another Member State, in accordance with Article 28(6) of Directive 95/46/EC, the supervisory authorities of both Member States shall cooperate to the extent necessary for the performance of their duties. This was recently clarified by the European Court of Justice as to the determination of the applicable law and the competent supervisory authority as well as the exercise of the powers of the supervisory authority.[1]

The addresses of Data Protection Authorities in all EU Member States are accessible on the following website: http://ec.europa.eu/justice/data-protection/bodies/authorities/

[1] Judgment of the Court of 1 October 2015 in Case C-230/14, Weltimmo s.r.o./ Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.

Conclusion

It is primarily for the national Data Protection Supervisory Authorities to monitor the application of the national data protection rules adopted in the implementation of the Directive 95/46/EC. Should the petitioner consider that his rights under Directive 95/46/EC have been infringed, he can consider filing a formal complaint with the competent national Data Protection Supervisory Authority.

4. Commission reply (REV), received on 2 May 2017

The petition raises two separate issues in relation PayPal. The first issue concerns the violation of EU legislation on data protection, the second issues concerns the blocking of large amounts by PayPal on its customers' accounts as a minimum reserve. As regards the second issue, the petitioner has submitted a separate petition (no. 0407/2016) that specifically also targets this point, and on which the Commission transmitted its initial observations on 28 February 2017.

As regards the first issue, in the European Union the right to the protection of personal data is guaranteed under Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union. The right is elaborated, in particular, in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[1] Directive 95/46 establishes a legal framework for national data protection law in the Member States of the European Union. The Member States are obliged to implement the provisions of the Directive into their own national legislation.

Under Directive 95/46/EC personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Personal data must also be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed (Article 6). Personal data may be processed only if the data subject has unambiguously given his consent; if the processing is necessary for the performance of a contract to which the data subject is party; if the processing is necessary for compliance with a legal obligation to which the controller is subject; if processing is necessary in order to protect the vital interests of the data subject; if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or if processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interest are overridden by the interests for fundamental rights and freedoms of the data subject (Article 7).

A data subject has a right, under certain conditions, to request his data be rectified, erased or blocked[2] and/or to object to the processing of his personal data.[3] Those rights have been

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995, p. 31 – 50.

[2] Article 12(b) of Directive 95/46/EC. Data subject can request the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.

[3] Article 14(a) of Directive 95/46/EC. Under Article 14(a) of Directive 95/46/EC, the rights to object processing relate at least to those two latter cases. Data subject can object processing at any time on compelling legitimate

interpreted by the Court of Justice of the European Union (CJEU) in the *Google Spain* case, confirming that when personal data appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue, it should not be (further) processed.[1]

In as far as PayPal qualifies as obliged entity in the sense of Directive 2015/849 it will be subject to obligations to process personal data for the purposes of the prevention of money laundering and terrorist financing.[2] Data processing necessary for compliance with these obligations can be seen as having a legitimate basis in the sense of Article 7 of Directive 95/46/EC and would not require the consent of the data subjects involved (i.e. its users). The processing of personal data on the basis of that directive for those purposes could in circumstances also be considered to be a task carried out in the public interest under Directive 95/46/EC (see Article 43 of Directive 2015/849). The collection and subsequent processing of personal data should be limited to what is necessary for the purpose of complying with the requirements of Directive 2015/849 and personal data should not be further processed in a way that is incompatible with that purpose.

PayPal being a payment service provider, it is also subject to the requirements of the Payment Services Directive (2007/64/EC). The processing of personal data by payment service providers is permitted when it is necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of such personal data must be carried out in accordance with Directive 95/46/EC (see Article 79 of Directive 2007/64/EC).

In order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities under Directive 2015/849 should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to fulfil the requirements relating to the protection of personal data, the retention period is fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary and proportionate, Member States can allow or require the further retention of records for a period not exceeding an additional five years (Article 40). Specific safeguards have to be put in place to ensure the security of data and to determine the persons having access to the data retained.
Without prejudice to the power of the European Commission as guardian of the Treaties, it is in the first place for Member States to monitor the application of the national data protection rules implementing Directive 95/46/EC, primarily through their national Data Protection Supervisory Authorities. The Commission is not competent to resolve the complaints which are submitted to it by data subjects against private natural or legal persons.

Hence, if the petitioner considers that his rights as a data subject have been violated, he may lodge a complaint with the competent national data protection authority. As PayPal (Europe)

---

grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

[1] Judgment of the Court of 13 May 2014 in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, paras 94, 98-99.

[2] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Official Journal L 141, 5/6/2015, p. 73 – 117.

offices are located in Luxembourg and the processing is carried out in the context of the activities of that establishment of the controller, it is prima facie the Luxembourg data protection law implementing Directive 95/46/EC that applies.

If the petitioner believes that the processing of data by PayPal in his case is not in compliance with Directive 95/46/EC and the Luxembourg data protection legislation implementing it, he can lodge a formal complaint with the Luxembourg data protection supervisory authority, or the national data protection supervisory authority of his Member State. National data protection supervisory authorities are under an obligation under Article 28 of Directive 95/46/EC to hear complaints (within the territory of their own Member State). Where the complaint relates to a matter taking place on the territory of another Member State, in accordance with Article 28(6) of Directive 95/46/EC, the supervisory authorities of both Member States shall cooperate to the extent necessary for the performance of their duties. This was recently clarified by the European Court of Justice as to the determination of the applicable law and the competent supervisory authority as well as the exercise of the powers of the supervisory authority.[1]

The addresses of Data Protection Authorities in all EU Member States can be found on the following website:
http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

On 27 April 2016 the EU adopted Regulation (EU) 2016/679[2] 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). This Regulation will apply from 25 May 2018 and repeals Directive 95/46/EC with effect from that date.[3] The Regulation retains the basic principles, for example that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes or that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5).

As in Directive 95/46/EC, the General Data Protection Regulation allows for the processing of personal data if such processing is necessary for compliance with a legal obligation to which the controller is subject or if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6).

The Regulation will simplify the enforcement of the rights of the data subject by providing one set of rules that apply equally in all Member States and by further strengthening the cooperation between the Data Protection Authorities. Data subjects may lodge a complaint with the national data protection authority of any Member State (Article 77).

As regards the second issue, the Commission indicated in its observations to petition

[1] Judgment of the Court of 1 October 2015 in Case C-230/14, Weltimmo s.r.o./ Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
[3] 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.

0407/2016 that it will contact the Luxemburg authorities to check with them which actions the have taken or will take to ensure that the terms and conditions of this operator are in compliance with the Payment Services Directive and do not contain unfair contract terms that are in breach with EU consumer protection legislation.

Conclusion

It is primarily for the national Data Protection Supervisory Authorities to monitor the application of the national data protection rules adopted in the implementation of the Directive 95/46/EC. Should the petitioner consider that his rights under Directive 95/46/EC have been infringed, he can consider filing a formal complaint with the competent national Data Protection Supervisory Authority.

As regards the second issue, the Commission will report on the outcome of its contacts with the Luxemburg authorities in its additional reply to petition 0407/2016.