NOTICE TO MEMBERS

Subject: Petition No 0648/2020 by J. M. (German) on the storage and disclosure of private data

1. Summary of petition

The petitioner calls for a ban on services that access, store or divulge the data of third parties, indicating that certain messaging services can only be used if consent is given under the general terms and conditions to the retrieval, storage and disclosure of data in user address books. He points out that non-public data generally contained in address books is subject to data protection.

2. Admissibility

Declared admissible on 17 September 2020. Information requested from Commission under Rule 227(6).

3. Commission reply, received on 18 May 2021

The rights to protection of private life and communications and protection of personal data are laid down in Article 7 and 8 of the Charter of Fundamental Rights of the European Union. Detailed rules are provided for in the ePrivacy Directive\(^1\) and the General Data Protection Regulation (‘GDPR’)\(^2\). The GDPR provides for a comprehensive framework on the processing of personal data. The ePrivacy Directive provides for the protection of the right to confidentiality of communications and the protection of the terminal equipment of the user in

---


the sector of electronic communications. As from 21 December 2020, by virtue of the EU Electronic Communications Code definitions, the confidentiality of communications in the ePrivacy Directive will also apply to so-called Over-the-Top services, such as webmail, web-telephony or messaging services. The ePrivacy Directive particularises and complements the GDPR.

Article 5(3) of the ePrivacy Directive requires the users’ consent for the storing of information or the accessing of information already stored in a user’s terminal equipment (i.e. personal computer (PC) or smartphone), except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user. The ePrivacy Directive relies on the definition of consent in the GDPR (Article 4(11)), which requires that consent is freely given, specific, informed and unambiguous indication of the data subject’s wishes. This means that the user can refuse to give his or her consent to access information stored in his or her terminal equipment, for example the user address book, except if one of the two exceptions mentioned above apply.

Article 7(4) GDPR lays down that when assessing whether consent is freely given, utmost account should be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. If consent is given in this situation, it is presumed to be not freely given (recital 43 GDPR). Article 7(4) GDPR seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which this personal data is not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the processing of personal data, i.e. consent and contract, cannot be merged and blurred.

The ePrivacy Directive had to be transposed into the national legislation of every Member State. Without prejudice to the competences of the Commission as guardian of the Treaties, the monitoring and enforcement of data protection legislation falls primarily within the competence of national data protection authorities and courts.

In 2017, the Commission adopted a proposal for a Regulation on privacy and electronic communications which improves and strengthens inter alia the protection of the terminal equipment of users. In particular, it provides an easy way to accept or refuse the tracking of cookies, for example through privacy settings of web browsers. In addition, the proposal maintains that any interference with the end-user’s terminal equipment requires consent, except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user. The Commission’s proposal is currently under legislative negotiation.

As a result and as regards the suggestion to ban service providers from reading the smartphone’s address books of users, such a prohibition would not be necessary as the ePrivacy Directive, as well as the proposed Regulation, ensures that the user can accept or refuse that the service provider has access to the information stored in his or her smartphone.

---


Conclusion

Article 5(3) of the ePrivacy Directive provides for protection of terminal equipment. The Commission has tabled a proposal for an ePrivacy Regulation to ensure harmonisation and modernisation of the ePrivacy rules, including the rules on cookies. The proposal is under discussion by the co-legislators.

The rights to protection of private life and communications and protection of personal data are laid down in Article 7 and 8 of the EU Charter of Fundamental Rights. Detailed rules are provided for in the ePrivacy Directive and the General Data Protection Regulation (GDPR). The GDPR provides for a comprehensive framework on the processing of personal data. The ePrivacy Directive provides for the protection of the right to confidentiality of communications and the protection of the terminal equipment of the user in the sector of electronic communications. As from 21 December 2020, by virtue of the EU Electronic Communications Code definitions, the confidentiality of communications in the ePrivacy Directive will also apply to so-called Over-the-Top services, such as webmail, web-telephony or messaging services. The ePrivacy Directive particularises and complements the GDPR.

Article 5(3) of the ePrivacy Directive requires the user’s consent for the storing of information or the accessing of information already stored in a user’s terminal equipment (i.e. personal computer (PC) or smartphone), except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user. The ePrivacy Directive relies on the definition of consent in the GDPR (Article 4(11)), which requires that consent is a freely given, specific, informed and unambiguous indication of the data subject’s wishes. This means that the user can refuse to give his or her consent to access information stored in his or her terminal equipment, for example the user address book, except if one of the two exceptions mentioned above apply.

Article 7(4) GDPR lays down that when assessing whether consent is freely given, utmost account should be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. If consent is given in this situation, it is presumed to be not freely given (recital 43 GDPR). Article 7(4) GDPR seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which this personal data is not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the processing of personal data, i.e. consent and contract, cannot be merged and blurred.

The ePrivacy Directive had to be transposed into the national legislation of every Member State. Without prejudice to the competences of the Commission as guardian of the Treaties, the monitoring and enforcement of data protection legislation falls primarily within the competence of the national authorities.
of national data protection authorities and courts.

In 2017, the Commission adopted a proposal for a Regulation on privacy and electronic communications\(^8\) which seeks to improve and strengthen *inter alia* the protection of the terminal equipment of users. In particular, it seeks to provide an easy way to accept or refuse the tracking of cookies, for example through privacy settings of web browsers. In addition, the proposal maintains that any interference with the end-user’s terminal equipment requires consent, except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user. Furthermore, the proposal seeks to strengthen the enforcement powers of competent authorities, including powers to impose significant fines in case of a breach (of a similar magnitude as those set out in the GDPR). This will render enforcement more effective. The Commission’s proposal is currently under legislative negotiation.

As a result, and as regards the suggestion to ban service providers from reading the smartphone’s address books of users, the ePrivacy Directive provides a balanced approach that requires the consent of users for such access. In addition, the ePrivacy Regulation, once adopted, will make enforcement more effective.

**Conclusion**

Article 5(3) of the ePrivacy Directive provides for protection of terminal equipment by requiring the user’s consent for the storing of information or the accessing of information already stored in a user’s terminal equipment, except where such storage or access is necessary for carrying out the transmission of a communication or for the provision of an information society service explicitly requested by a user. The Commission has tabled a proposal for an ePrivacy Regulation to ensure harmonisation and modernisation of the ePrivacy rules, including the rules on cookies, and to strengthen enforcement powers. The proposal is under discussion with the co-legislators.

---

\(^8\) COM(2017) 10 final.