WISTRAND

2018-11-20

MEMORANDUM

THE RIGHT TO ERASURE UNDER THE GDPR –TECHNICAL SOLUTIONS AND THE LAW

1 INTRODUCTION

1.1 In the aftermath of the EU General Data Protection Regulation (the "**GDPR**"), which entered into force on 25 May 2018, [stakeholders] have started to examine application of technical solutions in order to adhere to obligations in relation to individuals right to erasure ('right to be forgotten') following from Article 17 of the GDPR. The following analysis, addressing some of the general legal aspects raised by this issue, has been made by Erik Ullberg (Partner) and Jeanette Jönsson (Associate), Wistrand Advokatbyrå (Gothenburg Office).[1]

2 CONCLUSION AND SUMMARY

2.1 It can be concluded that a data controller generally can achieve the objective of erasure of personal data in accordance with the GDPR in two separate ways:

i) The first option to fulfil the obligation to erase personal data is to actually delete all the personal data.

ii) The second alternative to fulfil the obligation to erase personal data is to make the personal data anonymous, i.e. making the data subject unidentifiable (anonymization).

2.2 Until case law has settled how the obligation of erasing personal data under the GDPR is to be interpreted in complex technology structures, data controllers and processors should be aware of the risk of incompliance with the GDPR when developing or applying technical structures that will include personal data of EU based individuals.

2.3 In order to be fully sure that the obligation under Article 17 of the GDPR is met, any personal data must either be i) irrevocably erased by the data controller, or ii) made anonymous, i.e. by making sure that a data subject can no longer be directly or indirectly identified by the data, and that the process cannot be reversed.

[1] NB. Other provisions and principles under the GDPR, such as any necessary legal basis for processing activities relating to anonymisation, data minimisation, the concept of privacy by design and privacy by default etc., has not been considered with within the framework of this memorandum. Moreover, this memorandum sets forth an analysis from a general context and does not constitute legal or other professional advice. No reader should act or refrain from acting based on information contained in this memorandum without seeking advice of counsel.

2.4 With regard to anonymization it is possible to argue that a practical approach could be taken in order to meet compliance. Statements with regard to blockchain technology and backups indicates that implementation of technical solutions making it, as far as possible, impossible for the public to retain personal data or putting the personal data "beyond use" may be acceptable.

2.5 It should emphasized that there is no authoritative guidance on the required level for the use of technical solutions. Nonetheless, in our opinion it is reasonable to assume that, for example, an encryption solution where the key is removed in a way that nobody will be able to decrypt the data in question can be tolerated under the GDPR (especially if used as a temporary solution pending full deletion of the data in question).

3 THE RIGHT OF ERASURE OF PERSONAL DATA

3.1 Article 17 of the GDPR provides data subjects with a right to erasure of its personal data in certain circumstances. This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. However, the right to be forgotten is not an absolute right.

3.2 It should be noted that the GDPR does not include a definition of how "erasure of data" can be obtained, but the common view is that erasure in its true sense or anonymization of the personal data in question could be used.[2]

3.3 To fulfil the requirement of erasing personal data upon a data subject's request, by actually erasing the personal data, it would mean in this context that the personal data should be irrevocably erased from a data controller's or a data processor's system. When the personal data have been erased, it should simply not be possible to recycle the data in any way back into a system.

3.4 The UK Information Commissioner's Office (ICO) published a guidance in 2014 on the requirements on the erasure of personal data. This guidance was published before the GDPR had entered into force, but the ICO has stated that the guidance still is relevant. In this guidance, ICO attempts to take a practical approach on the requirements for erasure of personal data as the ICO recognises that the irrevocable erasure of personal data in some technical environments may be difficult to achieve. Therefore, the ICO states that the ICO will be satisfied if the personal data is put "beyond use" if it cannot be irrevocably erased. For example, such a solution may be used if personal data cannot be erased in a system without erasing other data at the same time. According to the ICO, such solution putting the personal data "beyond use" is only acceptable if the following is fulfilled;

[2] See *e.g.* New European Data Protection Regulation, Rücker et al., p. 71, GDPR Juridik, organisation och säkerhet enligt dataskyddsförordningen, Frydlinger et al., p. 280 f.

(i) It is not possible, or will not attempted, by the data controller to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;

(ii) the data controller does not give any other organisation access to the personal data;

(iii) the data controller surrounds the personal data with appropriate technical and organisational security; and

(iv) the data controller commits to irrevocable and permanent erasure of the information if, or when, this becomes possible.

The ICO states, however, that it is important to note that if personal data is put "beyond use", such personal data might still be provided in response to a court order, since the personal data is not irrevocably erased.

3.5 It is further important to note that the above solution is solely the ICO's assessment and that such assessment may be contrary to any future EU assessment on how the GDPR may be interpreted as regards the erasure of personal data in technically complex environments.[3]

4 THE GDPR'S DEFINITION OF PERSONAL DATA

4.1 The GDPR only applies to data which constitutes personal data in the meaning of GDPR.[4] This means that any personal data, which is being converted into no-personal data will subsequently not fall within the scope of the GDPR. Therefore, it could also be relevant to consider the definition of personal data in the meaning of the GDPR when making an assessment on the fulfilment of the right to erasure.

4.2 Article 4 of the GDPR defines personal data very broadly and as any information relating to an identified or identifiable natural person, with "identifiable natural person" being defined to mean an individual who can be identified, directly or indirectly. According to the GDPR recital 26, sentence 3 and 4, to determine whether a natural person is identifiable, account should be taken to all the means reasonably likely to be used. To ascertain whether means are reasonably likely to be used to identify a natural person, account should further be taken of all objective factors, such as the costs of and the amount of time required for identification. Also the available technology and technological development should be taken into account.

---

[3] The ICO guidance is available here: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf.

[4] Personal data means: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (Article 4 (1) of the GDPR).

Even though data at the time of the processing may be considered to be technologically impossible to use to identify a person, account also must be taken for the technological development. Account must also be taken of which time period data are intended to be processed.

4.3 Encrypted data is an example of so-called pseudonymisation[5], since information then relates to individuals that are earmarked by a code. Irrespective of the key making correspondence between the code and the common identifiers of the individuals is being kept separately, encrypted data may still be linked to a natural person. Therefore, encrypted data related to individuals as a general rule constitutes personal data under the GDPR. This is normally true also in cases where it is virtually impossible to reverse engineer an encryption. Even when it is no longer possible to precisely retrieve the record of an individual, it may remain possible to glean information about the individual with the help of other sources of information that are available publicly or not (The Opinion 05/2014 of the Article 29 Data Protection Working Party on Anonymisation Techniques, dated 10 April 2014).[6]

4.4 Further guidance might be taken from the Court of Justice of the European Union (the "**CJEU**") judgement in case C-582/14 (*Patrick Breyer v. Bundesrepublik Deutschland*). In this case the CJEU ruled that a dynamic IP address may constitute personal data even where only a third party (in this case an internet service provider) has the additional information necessary to identify the individual. However, this should apply only under certain circumstances, for instance where there exist a legal means for a third party to obtain the additional information necessary to identify the individual.

4.5 It follows from the foregoing that the GDPR does not apply to anonymous data as such data cannot be traced back to an individual. Data which are no longer needed in a form which permits identification, could be further processed in an anonymised form. According to recital 26 of the GDPR, such anonymisation requires that the personal data is rendered anonymous in such a manner that the data subject is not or no longer identifiable.

4.6 Anonymisation of personal data can be achieved through a number of techniques that generally fall within two categories; (i) randomisation and (ii) generalisation. If the randomisation technique is used, the personal data is made anonymous by altering the accuracy of the data in order to remove the strong link between the data and the individual. If the data becomes sufficiently uncertain, it can no longer refer to a specific individual. The generalisation technique consists of generalising/diluting the

---

[5] According to Article 4 (5) of the GDPR "'*pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*"

[6] Available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

attributes of data subjects by modifying the respective scale or order of the data. However, since the EU has not provided a standard of successful anonymization, a combination of randomisation and generalisation techniques may be considered to accomplish a stronger privacy guarantee.[7] As stated above, if an anonymization is successful the GDPR does not apply. However, if a data controller or a data processor is able to restore the anonymised data with reasonable likelihood, it will be deemed personal data under the GDPR. Therefore, it is always a risk inherent to anonymisation which must be considered when assessing possible techniques to achieve anonymization of personal data.

5 TECHNICAL DIFFICULTIES AS REGARDS FULFILLING THE OBLIGATION OF ERASURE OF PERSONAL DATA

5.1 As already concluded, a data controller can generally "erase" personal data in two different ways. The first option to fulfil the obligation to erase personal data is to actually delete all the personal data. The second alternative to fulfil the obligation to erase personal data is to make the personal data anonymous, i.e. making the data subject unidentifiable effectively meaning that the data in question no longer constitutes personal data within the meaning of the GDPR thus falling outside its scope.

5.2 Since the GDPR does not include any guidance on how a data controller shall erase personal data in order to be able to objectively have fulfilled its obligation according to article 17 there is an inherent uncertainty for data controllers in relation to use of solutions where the technology limits the possibility to erase data (such as backups, blockchain technology etc.). However, in such situations alternative methods to achieve the objective of the GDPR has been recognised.

5.3 Comparisons can for instance be made with problems of erasing personal data in a blockchain. In this context the French Data Protection Authority ("**CNIL**") has recently published an opinion on how a data controller may ensure that a data subject may exercise its right of erasure of personal regardless of the practical implications to erase personal data that exists within a blockchain. The CNIL has pointed out that there are technical solutions to move towards compliance with the GDPR. For instance, this may be achieved if data, which is stored on the blockchain, is subject to a cryptographic method. In that case, the deletion of data stored outside of the blockchain and the verification elements stored on the blockchain, would render any personal data almost inaccessible and arguably that the data in question has been effectively been "anonymised".

5.4 The CNIL's somewhat practical approach also draws support from a view taken by the British Data Protection Authority ("**ICO**"). The ICO has stated that "It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the

[7] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR),* 2017, p 13–15.

data will remain within the backup environment for a certain period of time until it is overwritten." However, "The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten."

5.5 In conclusion, it should be safe to assume that a practical rather than a fundamental approach to erasure can under certain circumstances be acceptable under the GDPR. However, in the absence of specific case law on the issue at hand it is difficult to reach any firm conclusion on which steps that are necessary in order to have fulfilled obligations to erase personal data by technical measures.