Editorial

It is increasingly questionable whether the current approach to sensitive or special personal data holds in light of technological and organisational developments. In order to understand how the provisions in the GDPR came about and which regulatory alternatives exist, it is important to briefly describe the evolution of this doctrine.

Right from the earliest data protection law, reference was made to, and a special position was reserved for, sensitive data. Article 1 of Resolution 1973 (on the private sector) by the Council of Europe specified that the 'information stored should be accurate and should be kept up to date. In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.' It is interesting that these two seemingly unrelated elements are mentioned in one provision, for which no explanation is provided. The explanatory memorandum does provide as an example of data concerning a person's intimate private life information about her behaviour at home, her sexual life and her opinions and as an example of data that entails a risk for unfair discrimination data about a person's health and past criminal record. The provision basically adopted the same structure as can be seen in Article 9 GDPR, namely a prohibition of processing sensitive data, with exceptions, for example, as the memorandum provides, processing health data for counselling alcoholics or recording the political beliefs of members by political parties.

The provision was (much) stricter than the current regime on sensitive data in that it prohibited full dissemination of those data. Disseminating was not understood in a limited fashion but as 'any transfer of information by a user to a third party, for example by a credit bureau to a bank.' It was also broader in the scope as to, what later became known as, sensitive data. The text refers both to data regarding 'intimate private life',[1] thus indirectly referencing Article 8 ECHR (the provision does not regard all data regarding private life, but only regarding intimate private life - where the boundary is drawn is not made explicit), and data which may lead to discrimination, thus indirectly referring to Article 14 ECHR. That article prohibits discrimination on the basis of 'sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.' It is important to stress that not only does Article 14 ECHR contain a residual category and not only does the Memorandum to Resolution 1973 refer to 'etc.' when mentioning examples that could relate to a person's intimate private life, the fact that Article 1 of the Resolution holds a reference to both types of data equally means that it was not the attempt to define what are sen-

DOI: 10.21552/edpl/2022/3/3

1 The term as such is used very seldom by the ECtHR. ECtHR, L. and V. v. Austria, appl. nos. 39392/98 & 39829/98, 09 January 2003. ECtHR, B.B. v. the UK, appl. no. 53760/00, 10 February 2004. ECtHR, Wolfmeyer v. Austria, appl. no. 5263/03, 26 May 2005. ECtHR, Big Brother Watch and others v. the United Kingdom, appl. nos. 58170/13 and 62322/14 and 24960/15, 25 May 2021. See also: ECtHR, Smith and Grady v. UK, appl. nos. 33985/96 and 33986/96, 27 September 1999. ECtHR, Lustig-Prean and Beckett v. UK, appl. nos. 31417/96 and 32377/96, 27 September 1999.

sitive personal data exhaustively, but instead look at the (potential) effect of the data processing. The question of whether data could reveal parts of a person's intimate private life or be used for discriminatory practices was determinative for the status of the data.

Resolution 1974 (on the public sector), also by the Council of Europe, took a different approach. It also referred to both types of sensitive data, but did not contain a general prohibition, with exceptions, but only made special reference to these types of data when laying down the requirement of a legal basis, the purpose specification and the purpose limitation principle, holding that these principles must 'especially' be respected when sensitive data are processed. In a way, this should be understood as applying normal public law requirements imposed on public sector organisations to the field of data processing. It is normal that public sector bodies only exert power on the basis of a law or similar regulation; it is normal that the powers that are transferred to them by the legislative branch are to be used for specific tasks only, and it is obvious that they, in principle, can only use the powers for those tasks that are provided in the law. The Memorandum also makes clear the article making special mention of sensitive data is basically a codification of the legality principle. Consequently, it is important to underline that the early data protection instruments were very strict on the processing of sensitive data by private sector organisations, while they set virtually no additional restrictions for public sector organisations doing so. This approach can still be witnessed in the many public interest grounds for legitimately processing sensitive data and the special rules contained in the Police Directive. Though, over time, this sharp division has been toned down.

www.lexxion.eu

Convention 108 set out rules for both the public and the private sector and, in a way, applied the public sector regime of legality to both public and private sector organisations. It provides a prohibition on the processing of sensitive data, except when there is a national law, providing for appropriate safeguards. Though the explanatory report made clear that this requirement should not be limited to laws in the narrow sense, but also includes 'appropriate or specific regulations or administrative directives, as long as the necessary level of protection is secured',[2] it still imposed an important burden on private sector organisations. It meant that a slightly stricter approach was taken than the Resolution from 1973 with respect to private sector bodies processing personal data because the Resolution left room for exceptions to the general prohibition, while the Convention requires a legal basis at all times. On the other hand, Resolution 1973 placed a strict prohibition on the dissemination of data to others, while the Convention leaves room for such practice when there is a legal basis.

The biggest change entailed the types or categories of data that were deemed sensitive. The Convention mentions data regarding racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and relating to criminal convictions. What is striking is that these categories neither include

2 Explanatory report, point 46.

all previous elements mentioned with respect to intimate private life, e.g. data regarding home life is omitted, and the reference to 'opinions' is limited to specific opinions, nor includes all elements contained, e.g. in Article 14 ECHR, while it is formulated as an exhaustive list. In doing so, the Convention seems to elevate the examples provided in the Resolutions to fixed and exhaustive categories of data. The explanatory report, however, denies that such is the case: 'The list of this article is not meant to be exhaustive. A Contracting State may, in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership, for example may be considered to entail as such a privacy risk in one country, whereas in other countries, it is considered sensitive only in so far as it is closely connected with political or religious views.'[3] Thus, the Convention provides a list of data that are, in any case, to be regarded as sensitive, but allows countries to include additional categories dependent on their national context.

The explanatory report makes clear that the underlying goal of this provision was to prevent especially harmful practices from materialising, and that although such determination should normally be made in a context-dependent situation, there are exceptions. 'While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests.'[4]

In the EU Data Protection Directive 1995, the EU basically adopted the approach by the CoE, with small variations. The reference to trade union membership in the explanatory memorandum to Convention 108 was formalised, to racial origin was added ethnic origin, other beliefs (next to pollical opinions and religious beliefs) were made explicit as 'philosophical beliefs' and criminal data were mentioned separately.[5] The novelty introduced by the Directive is not that it was made clear that processing sensitive personal data should not only have a legal ground, but also serve an important public interest, or that criminal data were mentioned in a separate paragraph, but that it is made clear that sensitive data could also be processed on the basis of the data subject's consent.[6] Though this means an important shift from the legality principle, virtually no explanation was given concerning this introduction. Parliament suggested including an additional provision specifying: 'The Member States shall provide in their law for a ban on the processing of data of a strictly private nature in the private sector.'[7] But it was not accepted.

3 Explanatory report, point 48.

4 Explanatory report, point 43.

5 Parliament suggested to also provide protection to 'or significant social circumstances including criminal convictions as well as any identification number issued by the public authorities' C 94 Volume 35 13 April 1992.

6 COM(90) 314 final ~.sYN 287 and 288 Brussels, 13 September 1990.

7 C 94 Volume 35 13 April 1992.

Under the GDPR, both the definition of what qualifies as sensitive personal data and the grounds for legitimately processing those data have been revised. With respect to the definition, instead of 'processing of data concerning [] sex life', the GDPR refers to 'data concerning a natural person's sex life or sexual orientation shall be prohibited'. Thus, it includes data on the orientation itself, without actual information on sexual practices. The GDPR also adds new categories to the list: genetic data and biometric data for the purpose of uniquely identifying a natural person, next to the older category of data concerning health. These are also defined specifically in the GDPR. In addition, the grounds for legitimately processing sensitive personal data has been expanded considerably.

The Court of Justice has provided a broad interpretation of the grounds contained in the Directive. For example, in *Lindqvist*, a person had written on a blog that a colleague was working part-time on medical grounds because she had injured her foot. The question of whether having injured one's foot already qualifies as 'medical data' was only answered by the Court in a brief, staccato manner. 'In the light of the purpose of the directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual. The answer to the fourth question must therefore be that reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.'[8]

Another case, that of *V.,* concerned the transfer of a medical file within the employment context.[9] The applicant complained about the sharing of her medical file within the employment context. The Tribunal held that, although the pre-recruitment examination serves the legitimate interest of the European Union institutions, which must be in a position to fulfil the tasks required of them, that interest does not justify carrying out a transfer of medical data from one institution to another without the consent of the person concerned. It pointed out that medical data are particularly sensitive data. Thus, it seemed to make a hierarchy between various categories of sensitive personal data and seemed to attach to that fact the requirement of consent.

The question is whether the current regulatory approach holds, given the various societal and technological developments now unfolding. Increasingly, it is possible to derive sensitive data by combining two datasets that contain non-sensitive personal data or even no personal data at all. Anonymised (e.g. medical) data can often be deanonymized. Aggregated data is increasingly made available online, the tools for harvesting those data have been democratised and are increasingly used for generating insights about individuals. Perhaps most importantly, high impact decisions can be made on the basis of non-sensitive personal data or even non-personal data, such

8 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist* [2003] ECLI:EU:C:2003:596, para 50-51.

9 CJEU, C- F-46/09, *V v European Parliament* [2011] ECLI:EU:F:2011:101.

as when based on general group profiles. Though such may fall under the data protection regime when a decision impacts a natural person, her interest may not always be individualizable and evident, given that such decisions impact large groups or society as a whole. Against this background, alternative approaches could be considered.

First, like the distinction between personal and non-personal data, the legal regime makes a binary distinction between non-sensitive personal data and sensitive personal data. From a technological perspective, the binary distinction between sensitive and non-sensitive personal data may be challenged. In technological literature, it is much more common to assess each data processing operation on a case-by-case basis, taking a holistic understanding of the potential risk, the harm entailed when the risk materialises, and the possibilities to achieve the goals without the data concerned. On the basis of that assessment, the level of risk and sensitivity is determined, as well as the level of protection and security that is needed. Thus, it could be considered to take a less binary approach to the question of sensitive or non-sensitive processing operations.

Second, on a more abstract level, from a technological perspective, it is not the data as such that is determinative of the sensitivity of the data processing operation, but (also) other aspects, such as the technologies used, the amount of data, the goal of the data processing operation and the application of the data processing operation. While the legal regime suggests that processing certain types of data are risky per se, from a technological perspective, it is unclear why. There may be data processing operations that do not include sensitive personal data that are highly risky in light of individual and societal interests, and there are data processing operations that do include sensitive personal data that are clearly not risky at all. Thus, whether the very idea of basing regulation on the type and status of data makes sense can be questioned.

Third and finally, if the current approach of providing an exhaustive list of sensitive personal data should be maintained, it is unclear why the current categories should be included. In the legislative documents of the various legal instruments, no or very limited explanation is provided for why certain categories are and others are not included. In addition, some of the categories seem to be outdated. For example, at least in most west and north European countries, membership of a trade union seldom leads to negative consequences. At the same time, there are good reasons to include other types of data in the list, such as financial information, location data and metadata. Also, it might be worth including data about minors. Alternatively, it could be suggested to work with a list of non-exhaustive examples, as was originally the case with the provision on sensitive personal data.

Turning to this edition, we have four articles by leading experts. Renée Dekker and Irith Kist discus the legislative framework of data protection and health law. They observe three gaps in the individual's data protection. Jeffrey Bholasing suggests that the approach of the GDPR, where data is either in scope of the regulation or not, fails in light of recent technological developments. Emmanuel Salami discusses concerns that

might arise in AI systems in the event of data reidentification and how this might raise interesting challenges for data protection compliance. Finally, Parviz Bagheri and Nabeel Mahdi Althabhawi evaluate privacy laws in on-line contracts from the Shari'ah perspective. They show that Islamic law gives great significance to the right of privacy.

The reports section, led by Mark Cole and Christina Etteldorf, is as always packed with interesting discussions on topical developments in Europe. Carl Vander Maelen evaluates the EDPB's vision on Codes of Conduct as Tools for Transfers and Giorgia Bincoletto dives into the EDPB-EDPS joint opinion on the Commission's Health Data Space Regulation. Rowin Jansen and Minke Reijneveld compare the rules set by the Council of Europe and the European Union with respect to the processing of personal data for national security interests. Marcelo Corrales Compagnucci comments on a remarkable development in Denmark, where the DPA has banned the use of Google Chromebooks and Workspace in schools. Adrien Bottacci provides insights from a Portuguese case on metadata and data retention. Finally, in the practitioner's corner, Gaurav Pathak evaluates what counts as making datta manifestly public in light of clearview.

In the case note section, led by Maria Tzanou, there are two very interesting case notes. Our board member Marc Rotenberg evaluates the CJEU's PNR decision and Mara Paun discusses a case that has not gotten the attention it deserves, which sheds light on the notion of identifiability. Finally, in the book review section led by Gloria Gonzalez Fuster, Maria Magierska reflects on the latest book by Ari Waldman.

For those interested in submitting an article, report, case note or book review, please e-mail our Executive Editor Jakob McKernan (mckernan@lexxion.eu) and keep in mind the following deadlines:

- Issue 4/2022: 15 October 2022;
- Issue 1/2023: 15 January 2023;
- Issue 2/2023: 30 April 2023;
- Issue 3/2023: 15 July 2022.

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT) Tilburg University, Netherlands