Overview 2023:

Case Law of the CJEU and the ECtHR, Country Reports and Books of the Year

*Maria Tzanou, Bart van der Sloot, Christina Etteldorf and Gloria González Fuster**

I. Case Law of the Court of Justice of the EU

by Maria Tzanou

2023 was another exciting and productive year for data protection case-law. The data protection related judgments delivered by the Court of Justice of the EU (CJEU) have continued to increase in both volume and substantive significance. This section provides an overview of this rich case-law by focusing on the decisions delivered by the Court in the area of data protection in 2023 and their main findings.[1]

GDPR

The GDPR[2] has now reached significant maturity in its application across Member States. Unsurprisingly, therefore, the majority of preliminary reference cases rendered by the CJEU concerned the interpretation of various provisions of the GDPR.

In *Gesamtverband Autoteile-Handel*,[3] the Court stated that the VIN – which is defined by Article 2(2) of Regulation No 19/2011[4] as an alphanumeric code assigned to the vehicle by its manufacturer in order to ensure that the vehicle is properly identified- is not as such 'personal' data, but it becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person.[5] In those circumstances, the VIN constitutes personal data, within the meaning of Article 4(1) GDPR, of the natural person referred to in that certificate, in so far as the person who has access to it may have means enabling them to use it to identify the owner of the vehicle to which it relates or the person who may use that vehicle on a legal basis other than that of owner.[6]

In *Norra Stockholm Bygg*,[7] the Court clarified that the provision of Article 6(3) and (4) GDPR applies, in the context of civil court proceedings, to the production as evidence of a staff register containing personal data of third parties collected principally for the purposes of tax inspection.[8] Moreover, Articles 5 and 6 GDPR require that when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each case, the type of proceeding at issue and duly taking into account the requirements arising from the principle of proportionality as well as, in partic-

* Dr Maria Tzanou, EDPL Case notes editor, University of Sheffield, UK. Bart van der Sloot, Tilburg Institute for Law, Technology, and Society (TILT) Tilburg University, Netherlands. For Correspondence: <B.vdrSloot@tilburguniversity.edu>. Christina Etteldorf is a Senior Research Scientist with the Institute of European Media Law (EMR) and manages the Reports Section together with the responsible editor Mark Cole. For correspondence: <c.etteldorf@emr-sb.de>. Gloria González Fuster is a Research Professor at the Vrije Universiteit Brussel (VUB).

1 All the data protection related CJEU decisions are discussed, besides the ones that were deemed not to add any interpretative points to the data protection jurisprudence. The General Court (GC) decisions have been omitted.

2 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) [2016] OJ L 119/1.

3 Case C-319/22 *Gesamtverband Autoteile-Handel eV v Scania CV AB* [2023] ECLI:EU:C:2023:837.

4 Commission Regulation (EU) No 19/2011 of 11 January 2011 concerning type-approval requirements for the manufacturer's statutory plate and for the vehicle identification number of motor vehicles and their trailers and implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units [2011] OJ L 8.

5 C-319/22 *Gesamtverband Autoteile-Handel eV v Scania CV AB*, para 46.

6 C-319/22 *Gesamtverband Autoteile-Handel eV v Scania CV AB*, para 48.

7 Case C-252/ 21 *Norra Stockholm Bygg* [2023] ECLI:EU:C:2023:145.

8 C-252/ 21 *Norra Stockholm Bygg*.

ular, those resulting from the principle of data minimisation (Article 5(1)(c) GDPR).[9]

Meta Platforms and Others v Bundeskartellamt (Conditions générales d'utilisation d'un réseau social)[10] is a landmark Grand Chamber judgment delivered in 2023 where the CJEU seized the opportunity to clarify a number of different provisions of the GDPR in the context of data processing carried out by social media.

More particularly, the Court stated that where the user of an online social network visits websites or apps to which one or more of the categories referred to in Article 9(1) GDPR relate and, potentially enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data', which is in principle prohibited, subject to the derogations provided for in Article 9(2) GDPR, where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person.[11] The Court, further, clarified that where the user of an online social network visits websites or apps to which one or more of the special categories of personal data relate, the user does not manifestly make public, within the meaning of Article 9(2)(e) GDPR, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies.[12] It is where the user enters information into such websites or apps or where they click or tap on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons enabling them to identify themselves on those sites or apps using login credentials linked to their social network user account, their telephone number or email address, that the user is considered to manifestly make public, within the meaning of Article 9(2)(e) GDPR, the data thus entered or resulting from the clicking or tapping on those buttons 'only in the circumstance where they explicitly made the choice beforehand', as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to them 'accessible to an unlimited number of persons.'[13]

In *Meta Platforms and Others v Bundeskartellamt*, the Court also had the opportunity to clarify when processing of personal data by an online social network operator could be considered lawful under Article 6(1) GDPR. More specifically, the Court found that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of Article 6(1)(b) GDPR,

> only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.[14]

Furthermore, it held that the processing of personal data by the operator of an online social network can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of Article 6(1)(f),

> only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party.[15]

9 C-252/ 21 *Norra Stockholm Bygg*.

10 Case C-252/21 *Meta Platforms and Others v Bundeskartellamt (Conditions générales d'utilisation d'un réseau social)* (Grand Chamber) [2023] ECLI:EU:C:2023:537.

11 C-252/21 *Meta Platforms and Others*.

12 C-252/21 *Meta Platforms and Others*.

13 C-252/21 *Meta Platforms and Others*.

14 C-252/21 *Meta Platforms and Others*.

15 C-252/21 *Meta Platforms and Others*.

Processing of personal data by the operator of an online social network is justified under Article 6(1)(c) GDPR, where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary.[16]

Moreover, the Court found that processing of personal data by the operator of an online social network cannot in principle be regarded as necessary in order to protect the vital interests of the data subject or of another natural person, within the meaning of Article 6(1)(d) GDPR, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller under Article 6(1)(e) GDPR.[17]

Finally, the CJEU stated that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) GDPR, to the processing of their personal data by that operator (Article 6(1) and Article 9(2)(a) GDPR). However, the Court noted that holding a dominant position is, nevertheless, an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.[18]

Several preliminary references that reached the Court in 2023 related to the interpretation of Article 15 GDPR.

In *RW v Österreichische Post*,[19] the Court held that Article 15(1)(c) GDPR must be interpreted as meaning that the data subject's right of access to the personal data concerning them, provided for by that provision, entails, where those data have been or will be disclosed to recipients, 'an obligation on the part of the controller to provide the data subject with the actual identity of those recipients', unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question.[20]

In *Österreichische Datenschutzbehörde*,[21] the Court clarified that the right to obtain from the controller a copy of the personal data undergoing processing under Article 15(3) GDPR means that the data subject must be given

> a faithful and intelligible reproduction of all those data. That right entails the right to obtain copies of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data, if the provision of such a copy is essential in order to enable the data subject to exercise effectively the rights conferred on him or her by that regulation, bearing in mind that account must be taken, in that regard, of the rights and freedoms of others.[22]

Furthermore, the CJEU explained that the concept of 'information' under Article 15(3) GDPR relates exclusively to the personal data of which the controller must provide a copy.[23]

In *Pankki*,[24] the Court stated that Article 15 GDPR is applicable to a request for access to the information referred to in that provision where the processing operations which that request concerns were carried out before the date on which the GDPR became applicable, but the request was submitted after that date.[25] It went on to hold that information relating to consultation operations carried out on a data subject's personal data and concerning the dates and purposes of those operations constitutes information which that person has the right to obtain from the controller under Article 15(1) GDPR. However, the Court clarified that Article 15(1) GDPR does not lay down such a right in respect of information relating to

> the identity of the employees of that controller who carried out those operations under its authority and in accordance with its instructions, unless that information is essential in order to enable the

16 C-252/21 *Meta Platforms and Others*.

17 C-252/21 *Meta Platforms and Others*.

18 C-252/21 *Meta Platforms and Others*.

19 Case C-154/21 *RW v Österreichische Post AG* [2023] ECLI:EU:C:2023:3.

20 C-154/21 *RW v Österreichische Post AG*.

21 Case C-487/21 *Österreichische Datenschutzbehörde* [2023] ECLI:EU:C:2023:369.

22 C-487/21 *Österreichische Datenschutzbehörde*.

23 C-487/21 *Österreichische Datenschutzbehörde*.

24 Case C-579/21 *Pankki S* [2023] ECLI:EU:C:2023:501.

25 C-579/21 *Pankki S*.

person concerned effectively to exercise the rights' conferred on them by the GDPR and 'provided that the rights and freedoms of those employees are taken into account.[26]

In *FT (Copies du dossier médical)*,[27] the Court ruled that the controller is pursuant to Articles 12(5) and 15(1) and (3) GDPR under an obligation to provide the data subject, free of charge, with a first copy of his or her personal data undergoing processing, even where the reason for that request is not related to those referred to in the first sentence of Recital 63 GDPR.[28] It stated that the adoption of a piece of national legislation which, with a view to protecting the economic interests of the controller, makes the data subject bear the costs of a first copy of his or her personal data undergoing processing, is not permitted under Article 23(1)(i) GDPR. Finally, it clarified that in the context of a doctor-patient relationship, the right to obtain a copy of personal data undergoing processing under Article 15(3) GDPR means that the data subject must be given

a faithful and intelligible reproduction of all those data. That right entails the right to obtain a full copy of the documents included in their medical records and containing, inter alia, those data if the provision of such a copy is essential in order to enable the data subject to verify how accurate and exhaustive those data are, as well as to ensure they are intelligible.[29]

Regarding data relating to the health of the data subject, that right includes in any event the right to obtain a copy of the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided to them.[30]

In *SCHUFA Holding (Libération de reliquat de dette)*,[31] the CJEU ruled that Article 5(1)(a) GDPR precludes a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons in order to be able to provide information on the solvency of those persons, for a period extending beyond that during which the data are kept in the public register.[32]

It further held that the data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay where they object to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds capable of justifying, exceptionally, the processing in question. Moreover, it clarified that under Article 17(1)(d) GDPR the controller is required to erase unlawfully processed personal data as soon as possible.[33]

Finally, the Court held that a decision on a complaint adopted by a supervisory authority under Article 78(1) GDPR is subject to full judicial review.[34]

In the seminal *OQ v Land Hessen SCHUFA*[35] case, the Court was called to adjudicate on automated decision making under Article 22 GDPR. SCHUFA was a private company under German law which provided its contractual partners with information on the creditworthiness of third parties, in particular, consumers. To that end, it established a prognosis on the probability of a future behaviour of a person ('score'), such as the repayment of a loan, based on certain characteristics of that person, on the basis of mathematical and statistical procedures. The establishment of scores ('scoring') was based on the assumption that, by assigning a person to a group of other persons with comparable characteristics who have behaved in a certain way, similar behaviour could be predicted.[36] OQ was refused the granting of a loan by a third party after having been the subject of negative information established by SCHUFA and transmitted to that third party. OQ applied for SCHUFA to send her information on the personal data registered and to erase some of the data which was allegedly incorrect.[37] In response to that request, SCHUFA

26 C-579/21 *Pankki S*.

27 Case C-307/22 *FT (Copies du dossier médical)* [2023] ECLI:EU:C:2023:811.

28 C-307/22 *FT (Copies du dossier médical)*.

29 C-307/22 *FT (Copies du dossier médical)*.

30 C-307/22 *FT (Copies du dossier médical)*.

31 Joined Cases C-26/22 and C-64/22 *SCHUFA Holding (Libération de reliquat de dette)* [2023] ECLI:EU:C:2023:958.

32 C-26/22 and C-64/22 *SCHUFA Holding (Libération de reliquat de dette)*.

33 C-26/22 and C-64/22 *SCHUFA Holding (Libération de reliquat de dette)*.

34 C-26/22 and C-64/22 *SCHUFA Holding (Libération de reliquat de dette)*.

35 Case C-634/21 *OQ v Land Hessen, SCHUFA Holding AG* [2023] ECLI:EU:C:2023:957.

36 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*, para 14.

37 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*, para 15.

informed OQ of her score and outlined, in broad terms, the methods for calculating the scores. However, referring to trade secrecy, it refused to disclose the various elements taken into account for the purposes of that calculation and their weighting. SCHUFA also noted that it limited itself to sending information to its contractual partners and it was those contractual partners which made the actual contractual decisions.[38]

The CJEU held that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning their ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of Article 22 GDPR, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.[39]

This is an important finding based on a broad interpretation of Article 22 GDPR. In fact, the Court noted that if a restrictive interpretation of that provision was retained according to which the establishment of the probability value must only be considered as a preparatory act and only the act adopted by the third party can be classified as a 'decision' under Article 22(1) GDPR, there would be a risk of circumventing Article 22 GDPR and, consequently, resulting in a lacuna in legal protection.[40] Indeed, in this case the data subject would not be able to assert, from the credit information agency which establishes the probability value concerning them, their right of access to the specific information according to Article 15(1)(h) GDPR, in the absence of automated decision-making by that company.[41]

In *Bundesrepublik Deutschland*,[42] the Court held that failure by the controller to comply with the obligations laid down in Articles 26 and 30 GDPR, which relate, respectively, to the conclusion of an arrangement determining joint responsibility for processing and to the maintenance of a record of processing activities, does not constitute unlawful processing under Articles 17(1)(d) and 18(1)(b) GDPR, conferring on the data subject a right to erasure or restriction of processing, where such a failure does not, as such, entail an infringement by the controller of the principle of 'accountability' (Article 5(2) GDPR read in conjunction with Article 5(1)(a) and Article 6(1) GDPR).[43]

In *X-FAB*,[44] the CJEU concluded that Article 38(3) GDPR does not preclude national legislation which provides that a controller or a processor may dismiss a data protection officer (DPO) who is a member of staff of that controller or processor 'solely where there is just cause, even if the dismissal is not related to the performance of that officer's tasks,' in so far as such legislation does not undermine the achievement of the objectives of the GDPR.[45]

In *KISA*,[46] the Court further clarified that Article 38(3) GDPR does not preclude national regulations providing that a controller processing or a subcontractor may only dismiss a data protection delegate who is a member of its staff for serious reasons, even if the dismissal is not linked to the exercise of the missions of this delegate, provided that such regulation does not compromise the achievement of the objectives of this regulation. However, the Court found that a 'conflict of interests' may exist under Article 38(6) GDPR, where a DPO is entrusted with other tasks or duties, which would result in them determining the objectives and methods of processing personal data on the part of the controller or its processor. The Court, however, left it to the national court to determine whether this is the case, on the basis of an assessment of all the relevant circumstances, in particular the organisational structure of the controller or its processor and in the light of all the applicable rules, including any policies of the controller or its processor.[47]

In *Budapesti Elektromos,*[48] the CJEU held that the remedies provided for in Article 77(1) GDPR (right to lodge a complaint with a supervisory authority) and Article 78(1) GDPR (right to an effective judicial remedy against a supervisory authority), on the one hand, and Article 79(1)GDPR (right to an effective judicial remedy against a controller or processor), on the oth-

38 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*, para 16.

39 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*.

40 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*, para 61.

41 C-634/21 *OQ v Land Hessen, SCHUFA Holding AG*, para 63.

42 Case C-60/22 *Bundesrepublik Deutschland* [2023] ECLI:EU:C:2023:373.

43 C-60/22 *Bundesrepublik Deutschland*.

44 Case C-453/21 *X-FAB Dresden GmbH & Co. KG v FC* [2023] ECLI:EU:C:2023:79.

45 C-453/21 *X-FAB Dresden GmbH & Co. KG v FC*.

46 Case C-560/21 *KISA* [2023] ECLI:EU:C:2023:81.

47 C-453/21 *X-FAB Dresden GmbH & Co. KG v FC*.

48 Case C-132/21 *Budapesti Elektromos* [2023] ECLI:EU:C:2023:2.

er can be exercised 'concurrently with and independently of each other'.[49] According to the Court, the protection granted pursuant to a decision in an action against a controller or a processor finding that the GDPR's provisions have been infringed, would not be consistent with a second judicial decision resulting from an action brought against a supervisory authority that has the opposite outcome.[50] Indeed, the result of these contradictory decisions would be 'a weakening of the protection of natural persons with regard to the processing of their personal data, since such an inconsistency would create a situation of legal uncertainty.'[51] The Court, nevertheless, left it to the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies 'in order to ensure the effective protection of the rights' guaranteed by GDPR and 'the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter of Fundamental Rights.'[52]

In the seminal case of *Österreichische Post (Préjudice moral lié au traitement de données personnelles)*,[53] the CJEU clarified that the concepts of 'material or non-material damage' and of 'compensation for the damage suffered' under Article 82 GDPR must be regarded as constituting 'autonomous concepts of EU law' which must be interpreted in a uniform manner in all of the Member States.[54]

It held that the mere infringement of the provisions of the GDPR is not sufficient to confer a right to compensation under Article 82(1) GDPR.[55] Indeed, three conditions must be satisfied to give rise to the right to compensation: i) the processing of personal data should infringe the provisions of the GDPR; ii) the data subject must have suffered damage; and, iii) there should be a causal link between the unlawful processing and the damage.[56]

Furthermore, the Court clarified that Article 82(1) GDPR precludes a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached 'a certain degree of seriousness'.[57] This is because making compensation for non-material damage subject to a certain threshold of seriousness would risk undermining

> the coherence of the rules established by the GDPR, since the graduation of such a threshold, on which the possibility or otherwise of obtaining that compensation would depend, would be liable to fluctuate according to the assessment of the courts seized.[58]

Finally, according to the Court, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with, when determining the amount of damages payable under the right to compensation enshrined in Article 82 GDPR.[59]

In *Deutsche Wohnen*,[60] the Grand Chamber ruled that Articles 58(2)(i) and 83(1) to (6) GDPR preclude national legislation under which an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement referred to in Article 83(4) to (6) only in so far as that infringement has previously been attributed to an identified natural person. The Court further added that an administrative fine may be imposed pursuant to Article 83 GDPR only where it is established that the controller, which is both a legal person and an undertaking, intentionally or negligently committed an infringement referred to in Article 83(4) to (6) thereof.[61]

VB v Natsionalna agentsia za prihodite[62] was another landmark judgment delivered in 2023 relating to the interpretation of several GDPR provisions and most importantly of the concept of 'non-material damage' under Article 82(1) GDPR. The case con-

49 C-132/21 *Budapesti Elektromos*, para 57.

50 C-132/21 *Budapesti Elektromos*, para 55.

51 C-132/21 *Budapesti Elektromos*, para 56.

52 C-132/21 *Budapesti Elektromos*, para 57.

53 Case C-300/21 *Österreichische Post (Préjudice moral lié au traitement de données personnelles)* [2023] ECLI:EU:C:2023:370.

54 C-300/21 *Österreichische Post*, para 30.

55 C-300/21 *Österreichische Post*.

56 C-300/21 *Österreichische Post*, para 32.

57 C-300/21 *Österreichische Post*.

58 C-300/21 *Österreichische Post*, para 49.

59 C-300/21 *Österreichische Post*.

60 Case C-807/21 *Deutsche Wohnen* (Grand Chamber) [2023] ECLI:EU:C:2023:950.

61 C-807/21 *Deutsche Wohnen*.

62 Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986.

cerned the unauthorised access to the Bulgarian National Revenue Agency (*Natsionalna agentsia za prihodite*, NAP) IT system, following a cyberattack, which resulted in the personal data contained in that system been published on the internet.[63] More than 6 million natural persons, of Bulgarian and foreign nationality, were affected by those events. Several hundred of them brought actions against the NAP for compensation for non-material damage allegedly resulting from the disclosure of their personal data.[64]

The CJEU noted that unauthorised disclosure of personal data or unauthorised access to those data by a 'third party', within the meaning of Article 4(10) GDPR, are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate', within the meaning of Articles 24 and 32 GDPR.[65] In this regard, the Court clarified that that the appropriateness of the technical and organisational measures implemented by the controller under Article 32 GDPR must be assessed by the national courts in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks.[66]

In light of this, the Court held that in an action for damages under Article 82 GDPR, the controller in question bears the burden of proving that the security measures implemented by it are appropriate pursuant to Article 32 GDPR and the principle of accountability of the controller (Article 5(2) GDPR).[67] Furthermore, it stated that the controller cannot be exempt from its obligation to pay compensation for the damage suffered by a data subject, under Article 82(1) and (2) GDPR, solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a 'third party', in which case that controller must then prove that it is in no way responsible for the event that gave rise to the damage concerned.

More importantly, the CJEU got the chance to clarify in *VB v Natsionalna agentsia za prihodite* the concept of 'non-material damage' under Article 82(1) GDPR. In this regard, it held that 'the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties' as a result of an infringement of the GDPR is capable, in itself, of constituting 'non-material damage' within the meaning of Article 82(1) GDPR.[68] The fear of misuse of personal data by third parties as a result of an infringement of the GDPR constitutes a broad interpretation of non-material damage that opens the door in the future for a multiplicity of actions on this basis both for individual and potentially also for collective interests.

In *Gemeinde Ummendorf*,[69] the Court helpfully reiterated that Article 82(1) GDPR precludes national legislation or a national practice which sets a 'de minimis threshold' in order to establish non-material damage caused by an infringement of that regulation. The data subject is required to show that the consequences of the infringement which they claim to have suffered constitute damage which differs from the mere infringement of the provisions of that regulation.[70]

Finally, in *Krankenversicherung Nordrhein*,[71] the CJEU held that processing of data concerning health must, in order to be lawful, not only comply with the requirements arising from these Article 9(2)(h) GDPR, but also fulfil at least one of the conditions of lawfulness set out in Article 6 (1) GDPR.[72]

The Court also clarified that the right to compensation provided for in Article 82(1) GDPR fulfils a 'compensatory function', in that financial compensation based on that provision must make it possible to fully compensate for the damage actually suffered as a result of the violation of that regulation, and not a dissuasive or punitive function.[73]

It found that under Article 82 GDPR the liability of the data controller is subject to the existence of a fault committed by the controller, which is presumed unless the latter proves that the damage cannot be attributed to them. Moreover, Article 82 GDPR does not require that the degree of seriousness of this fault be taken into account when fixing the amount of

63 C-340/21 *VB v Natsionalna agentsia za prihodite*, para 11.

64 C-340/21 *VB v Natsionalna agentsia za prihodite*, para 12.

65 C-340/21 *VB v Natsionalna agentsia za prihodite*.

66 C-340/21 *VB v Natsionalna agentsia za prihodite*.

67 C-340/21 *VB v Natsionalna agentsia za prihodite*.

68 C-340/21 *VB v Natsionalna agentsia za prihodite*.

69 Case C-456/22 *Gemeinde Ummendorf* [2023] ECLI:EU:C:2023:988.

70 C-456/22 *Gemeinde Ummendorf*.

71 Case C-667/21 *Krankenversicherung Nordrhein* [2023] ECLI:EU:C:2023:1022.

72 C-667/21 *Krankenversicherung Nordrhein*.

73 C-667/21 *Krankenversicherung Nordrhein*.

damages awarded in compensation for non-material damage on the basis of this provision.[74]

COVID-19 Pandemic

The Court issued three judgments in 2023 adjudicating questions that had arisen in the context of the COVID-19 pandemic.

Hauptpersonalrat der Lehrerinnen und Lehrer[75] concerned two measures adopted in 2020 by the Minister for Education and Culture of the Land Hessen establishing the legal and organisational framework for school education during the COVID-19 pandemic. That framework made it possible, among others, for pupils who could not be present in a classroom to attend classes live by videoconference. In order to safeguard pupils' rights in relation to the protection of personal data, it was established that connection to the videoconference service would be authorised only with the consent of the pupils themselves or, for those pupils who were minors, of their parents. However, no provision was made for the consent of the teachers concerned to their participation in that service.[76]

The Court held that the processing of teachers' personal data as part of the live streaming by videoconference of the public educational classes falls within the material scope of the GDPR[77] and within the material and personal scope of Article 88 GDPR (processing of employees' personal data in the employment context).[78] It noted that Article 88 GDPR constitutes an 'opening clause', as it gives Member States the option of adopting 'more specific rules' to ensure protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context,[79] but it ruled that that national legislation cannot constitute a 'more specific rule', within the meaning of Article 88(1) GDPR, where it does not satisfy the conditions laid down in paragraph 2 of Article 88 GDPR.[80] This is because, according to the Court, Article 88 GDPR -and, more generally opening clauses- have: i) a normative content specific to the area regulated, which is distinct from the general rules of the GDPR; ii) and, include suitable and specific measures to protect the data subjects' human dignity, legitimate interests and fundamental rights.[81]

The CJEU, thus, concluded that national provisions adopted to ensure the protection of employees' rights and freedoms in respect of the processing of their personal data in the employment context 'must be disregarded' where those provisions do not comply with the conditions and limits laid down in Article 88(1) and (2) GDPR, unless those provisions constitute a legal basis referred to in Article 6(3) GDPR, which complies with the requirements laid down by that Regulation.[82]

Ministerstvo zdravotnictví[83] concerned the adoption by the Ministry of Health of the Czech Republic (*Ministerstvo zdravotnictví*) of an 'extraordinary measure' regulating access of persons to certain places and events in order to protect the population in the context of the spread of the COVID-19 epidemic.[84] This measure obliged clients (spectators, participants) to provide proof of compliance with a number of conditions and required operators (organisers) to conduct compliance checks using the Ministry's mobile application 'čTečka'.[85]

The CJEU ruled that concept of 'processing' personal under Article 4(2) GDPR includes the verification, using a national mobile application, of the validity of interoperable COVID-19 vaccination, test and recovery certificates issued pursuant to the EU Digital COVID Certificate Regulation[86] to facilitate free movement during the COVID-19 pandemic, and used by a Member State for national purposes.[87] However, it left it to the national referring court to ascertain whether the processing introduced by the extraordinary measure, first, observed the principles relating to the processing of data laid down in Article 5 GDPR and, second, observed had a legal basis under Article 6 GDPR.[88]

74 C-667/21 *Krankenversicherung Nordrhein*.

75 Case C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer* [2023] ECLI:EU:C:2023:270.

76 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 14.

77 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 37.

78 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 56.

79 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 52.

80 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 75.

81 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*, para 75.

82 C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*.

83 Case C-659/22 *RK v Ministerstvo zdravotnictví* [2023] ECLI:EU:C:2023:745.

84 C-659/22 *RK v Ministerstvo zdravotnictví*, paras 2-3.

85 C-659/22 *RK v Ministerstvo zdravotnictví*, para 14.

86 Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate Regulation).

87 C-659/22 *RK v Ministerstvo zdravotnictví*.

88 C-659/22 *RK v Ministerstvo zdravotnictví*, para 32.

In *Nacionalinis visuomenės sveikatos centras*,[89] the CJEU addressed a number of interesting questions regarding the concept of controller. In the context of the COVID-19 pandemic, the Minister for Health of the Republic of Lithuania (*Lietuvos Respublikos sveikatos apsaugos ministras*, NVSC), requested the acquisition of an IT system for the registration and monitoring of the data of persons exposed to that virus, for the purposes of epidemiological follow-up. A private company was selected to create a mobile application for that purpose. The mobile application at issue became available for download in the Google Play Store (and it was downloaded by a number of individuals) before the NVSC informed that company that, due to a lack of funding for the acquisition of that application, it had, in accordance with the Law on Public Procurement, terminated the procedure relating to such acquisition.[90]

Interestingly, the Court ruled that

> an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application *may be regarded as a controller*, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data.[91]

The Court also held that the classification of two entities as joint controllers does not require that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question; nor does it require that there be an arrangement laying down the terms of the joint control.[92]

It clarified that that the use of personal data for the purposes of the IT testing of a mobile application constitutes 'processing', within the meaning of Article 4(2) GDPR, unless such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person.[93]

Finally, it held an administrative fine may be imposed pursuant to that Article 83 GDPR only where it is established that the controller has intentionally or negligently committed an infringement and such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing.[94]

ePrivacy Directive[95]

In *HYA and Others (Motivation des autorisations des écoutes téléphoniques)*,[96] the Court was asked to interpret Article 15(1) of the ePrivacy Directive in the context of targeted (rather than mass surveillance). It found that this provision read in the light of Article 47 of the Charter of Fundamental Rights of the European Union (EUCFR) does not preclude a national practice under which judicial decisions authorising the use of special investigative methods following a reasoned and detailed application from the criminal authorities, are drawn up by means of a predrafted text which does not contain individualised reasons.[97] This is provided that the precise reasons for such authorisation can be easily and unambiguously inferred from a cross-reading of the decision and the application for authorisation, the latter of

89 Case C-683/21 *Nacionalinis visuomenės sveikatos centras* [2023] ECLI:EU:C:2023:949.

90 C-683/21 *Nacionalinis visuomenės sveikatos centras*, para 19.

91 C-683/21 *Nacionalinis visuomenės sveikatos centras*. Emphasis added.

92 C-683/21 *Nacionalinis visuomenės sveikatos centras*.

93 C-683/21 *Nacionalinis visuomenės sveikatos centras*.

94 C-683/21 *Nacionalinis visuomenės sveikatos centras*.

95 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) [2002] OJ L201.

96 Case C-349/21 *HYA and Others (Motivation des autorisations des écoutes téléphoniques)* [2023] ECLI:EU:C:2023:102.

97 C-349/21 *HYA and Others*.

which must be made accessible to the person against whom the use of special investigative methods has been authorised.[98]

In *Lietuvos Respublikos generalinė prokuratūra*,[99] the CJEU stated that Article 15(1) of the ePrivacy Directive read in the light of Articles 7, 8 and 11 and Article 52(1) EUCFR precludes the use, in connection with investigations into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained, pursuant to a legislative measure adopted under that provision, by providers of electronic communications services and which have subsequently been made available, pursuant to that measure, to the competent authorities for the purpose of combating serious crime.[100]

LED[101]

In *Ministerstvo na vatreshnite raboti*,[102] the CJEU shed light on the interpretation of various provisions of the Law Enforcement Directive (LED). It found that Article 10(a) LED allows the processing of biometric and genetic data by the police authorities with a view to their investigative activities, for purposes of combating crime and maintaining law and order, provided that the relevant national law contains a sufficiently clear and precise legal basis to authorise such processing.

Furthermore, the Court found that Article 6(a) LED and Articles 47 and 48 EUCFR do not preclude national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise a measure enforcing their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.

Finally, the Court held that national legislation which provides for 'the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record', without laying down an obligation on the competent authority to verify whether and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned is prohibited under Article 10, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) LED.[103]

Ligue des droits humains, BA v Organe de contrôle de l'information policière[104] was another important judgment regarding the interpretation of the LED delivered by the CJEU in 2023. In this the Court held that Article 17 LED, interpreted in the light of the EUCFR -and in particular Articles 8(3) and 47 EUCFR- means that where the rights of a data subject have been exercised, pursuant to Article 17 LED, through the competent supervisory authority and that authority informs that data subject of the result of the verifications carried out, that data subject must have an effective judicial remedy against the decision of that authority to close the verification process.[105]

Conclusion

Overall, the above case-law has made a significant contribution to the CJEU's already rich jurisprudence on data protection matters. Particularly welcome are: i) the clarifications provided on the lawfulness of processing of personal data by operators of social networks; ii) the interpretation of the concepts of 'compensation for the damage suffered' under Article 82 GDPR and specifically on the meaning, scope and threshold of 'non-material damage'; iii) the clarification of what the right of access by the data sub-

98 C-349/21 *HYA and Others*.

99 Case C-162/22 *Lietuvos Respublikos generalinė prokuratūra* [2023] ECLI:EU:C:2023:631.

100 C-162/22 *Lietuvos Respublikos generalinė prokuratūra*.

101 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

102 Case C-205/21 *V.S.* [2023] ECLI:EU:C:2023:49.

103 C-205/21 *V.S.*.

104 Case C-333/22 *Ligue des droits humains, BA v Organe de contrôle de l'information policière* [2023] ECLI:EU:C:2023:874.

105 C-333/22 *Ligue des droits humains, BA v Organe de contrôle de l'information policière*.

ject under Article 15 GDPR entails; and, iv) the broad interpretation of Article 22 GDPR. The finding that an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a *controller* even if that entity has not itself performed any processing operations in respect of such data is significant as well and might have important repercussions in the future both in the area of data protection and more broadly AI systems development. The CJEU is, therefore, to be applauded for 'thinking ahead' when interpreting the GDPR and other EU data protection instruments. Indeed, the importance of some of the judgments rendered in 2023 and discussed above is here to stay.

II. Case Law of the European Court of Human Rights

by Bart van der Sloot

In 2023, there was a total number of 141 judgements (these are Court rulings on the substance of cases, thus excluding decisions, in which the Court determines the admissibility of cases) under Article 8 European Convention on Human Rights (ECHR). About a third of those cases were issued against Russia, which was temporarily suspended from the Council of Europe and then pulled out of the Convention mechanism, in the wake of the invasion in Ukraine.[106] The European Court of Human Rights (ECtHR) held that it could still assess the cases that were already pending when those events unfolded. It found that it had full authority to issue legal rulings and award compensation to victims of Russian human rights interferences, for which it referred to Article 58 ECHR, concerning denunciation, of which paragraphs 2 and 3 hold:

> 2. Such a denunciation shall not have the effect of releasing the High Contracting Party concerned from its obligations under this Convention in respect of any act which, being capable of constituting a violation of such obligations, may have been performed by it before the date at which the denunciation became effective.
> 3. Any High Contracting Party which shall cease to be a member of the Council of Europe shall cease to be a Party to this Convention under the same conditions.... It appears from the wording of Article 58, and more specifically the second and third paragraphs, that a State which ceases to be a Party to the Convention by virtue of the fact that it has ceased to be a member of the Council of Europe is not released from its obligations under the Convention in respect of any act performed by that State before the date on which it ceases to be a Party to the Convention.[107]

The only other two countries with more than 10 cases issued against them in 2023 were Turkey and Ukraine.

Arguably, the most important case under Article 8 ECHR was also issued against Russia. The right to privacy under the Convention is not limited to aspects over informational privacy, but is an umbrella right that provides protection to a number of distinct though related issues. The provision holds:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

From the four terms in Article 8 (private life, family life, home and correspondence), four classic privacy rights have been inferred, although they do not neatly map on those four terms, namely locational privacy (the protection of the home), informational privacy (protection of correspondence and private life), relational privacy (family life and, in so far as it does not concern relations with family members, private life) and bodily and psychological integrity (private life). Interpreting this provision in present daylight, Article 8 ECHR has become the broadest right in

106 <https://www.coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe>.

107 *Fedotova a.o. v Russia* App nos 40792/10, 30538/14 and 43439/14 (ECtHR, 17 January 2023), para 71.

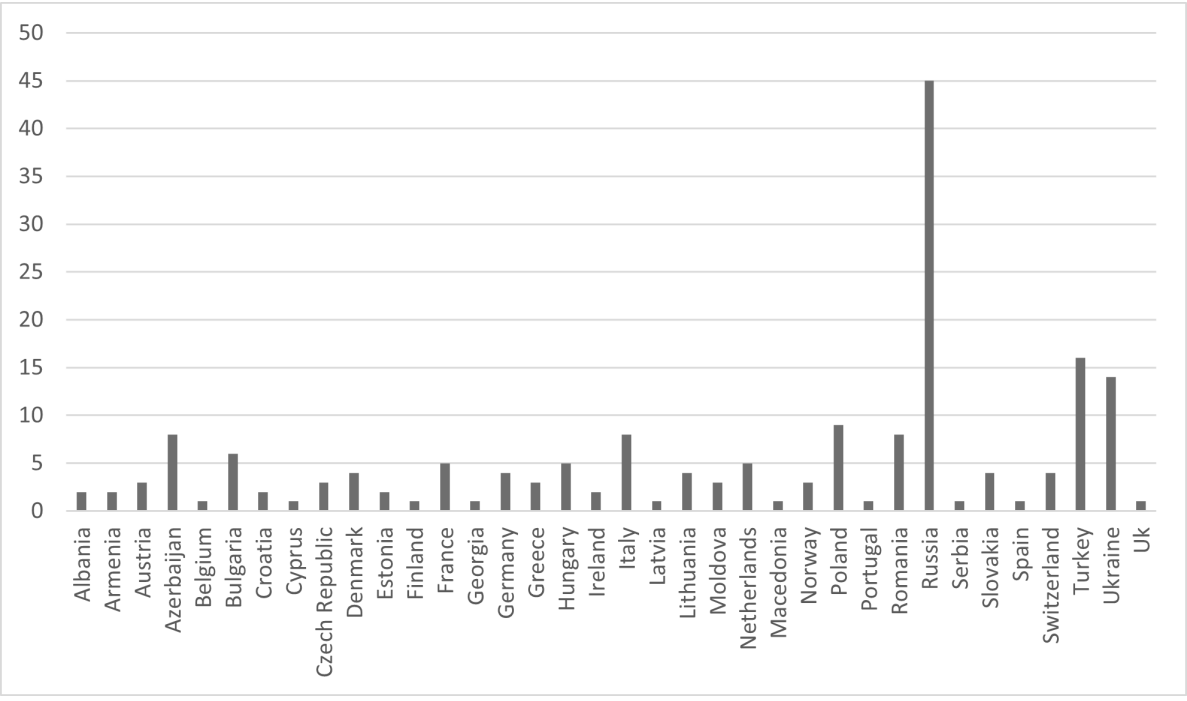


Figure 1. *Number of cases under Article 8 ECHR per country*

terms of material scope under the European Convention, providing protection to almost any interest that has a link to a natural person's integrity, personality or development, whether it be in private or in public, professional, social or personal life.[108] At the same time, other doctrines, such as the right to marry and found a family, have been interpreted restrictively, meaning that even issues that would intuitively fall under that right (Article 12 ECHR), are dealt with under Article 8 ECHR instead.

This also holds true for *Fedotova a.o. v Russia*. This case is important for two reasons, one concerns the substantive conclusion of the Court and the second the way in which it arrives at that conclusion. The conclusion of the Court is that, although countries are under no legal obligation to allow for or facilitate gay marriage, there is a positive obligation to legally recognize and protect same sex relationships. Although this approach had been written in the sky, as the Court step, by step, by step, has moved closer to this to this point by making small, incremental moves over the past decades, it is still evident how this judgment feeds into looming criticism from conservative circles. To their mind, the Court is a liberal entity that pushes a progressive agenda, an agenda that does not follow form the text of the Convention. As such, the criticism holds, the Court is ignoring both democratic rule of people and the national cultural and religious sentiments specific to countries, as those may vary from country to country. Not surprisingly, there were strong dissenting opinions from Eastern European judges, namely Pavli (Albania), Wojtyczek (Poland), Motoc (Romania), Polackova (Slovakia) and Lobov (Russia). This ties up to the second reason why this judgement is interesting, namely that until recently, the ECtHR was very hesitant to find a violation on the basis that an interference with a human right did not serve a public interest, because it believed that whether a measure should be said to be in the public interest was something that should be up to the government. Over the past years, the Court has been more and more willing to assess whether a policy or measure was actually in the public interest, also because it increasingly feels that countries are offering the Court what it calls ulterior motives -motives that serve as window dressing and that are used to disguise the real reasons for taking a certain action, which has led to a recent revival of jurispru-

108 Bart van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of Big Data' (2015) Utrecht J Int'l & Eur L, 31, 25.

dence on Article 18 ECHR.[109] In the case of *Fedetova*, the Court in detail discussed the reasons Russia provided for not legally recognising and protecting gay relationships, such as the aim of protecting the traditional family unit, the general sentiment among citizens that gay marriage is not to be approved of, let alone legally recognized, and the protection of minors from being corrupted. The Court rejects all of these and 'finds that none of the public-interest grounds put forward by the Government prevails over the applicants' interest in having their respective relationships adequately recognised and protected by law. The Court concludes that the respondent State has overstepped its margin of appreciation and has failed to comply with its positive obligation to secure the applicants' 'right to respect for their private and family life.'[110] For readers interested in these type of cases under Article 8 ECHR in 2023, there is a variety of interesting matters on gender reassignment surgery, gender assignment with athletes, abortion, the possibility to procreate through the gametes of a deceased partner and other aspects of private life.[111]

Normally, it would be possible to make a rough distinction between cases on one of the four types of privacy, although it is clear that there are borderline cases, such as with the *Fedotova* case which relates both to a person's bodily and psychological integrity and to their relational privacy. This distinction, however blurred it might have always been, is increasingly overshadowed, by a 'new' type of privacy, which can be called procedural privacy. In cases concerning procedural privacy, although in substance about one or more of the four categories of privacy, the Court does not assess the substantive question, but looks at procedural aspects. These concern, inter alia, the procedure followed by executive branches and national courts when making a decision, eg on custody cases or placing a child out of home. The ECtHR would then assess whether the parents have been adequately heard, whether exerts have been consulted, all relevant documents have been taken into account and whether the decision making process was speedy. All these elements, the Court has found, are not only protected through Articles 6 (right to a fair trial) and Article 13 (right to petition), but are also implicit in Article 8 ECHR itself.[112] Another example of procedural privacy is where the Court looks to the legal regime as such and what it calls the quality of law, mostly in cases revolving around mass surveillance. Sometimes it assesses the quality of a legal regime *in abstracto,* meaning that there is no applicant claiming to be affected in their legal interests, so that the Court is merely asked to scrutinise the legal regime as such and assess whether, inter alia, there are sufficient safeguards in place to prevent arbitrary use of power.[113] More recently, the Court has also assessed the quality of the legislative process, leading up to the adoption of a law or policy, inter alia by assessing whether all relevant arguments and counter arguments had been discussed in parliament with respect to a law which allowed to make public tax data of citizens.[114]

Of the 141 cases issued under Article 8 ECHR in 2023, the majority may be said to revolve around procedural issues, although the border between procedural and substantive issues is not always clear. This fits into what some have called the procedural turn of the Court, which was promoted to address the problem raised earlier, namely that some feel that the Court is too over-reaching, therewith substituting its opinion on moral and ethical issues for that of the national legislator. Under the procedural approach, the Court does not rule on that substantive issue, but 'merely' assesses whether the national authorities have taken all relevant steps when making a substantive decision.[115]

There is another turn the Court has made the past few years. Until about two decades ago, the Court worked strictly on a case-by-case basis, which it took almost to the extreme. This meant that it would judge

109 See also App no 54003/20. For the sake of brevity, references here will be mostly limited to the application number. Especially for the cases against Russia, dozens of application nos. are bundled per judgement; in those instances, reference is made merely to the first application no.

110 *Fedotova*, para 224.

111 10934/21; 53568/18 and 54741/18; 75135/14; 7246/20; 45373/99; 40119/21; 19475/20, 20149/20, 20153/20 and 20157/20; 1/16; 33085/12; 61860/15; 15798/20; 44810/20; 24225/19; 46412/21; 35648/10; 2022/18; 12482/21; 56513/17 and 56515/17; 22296/20 and 37138/20; 21424/16 and 45728/17; 54006/20; 76888/17; 65128/19; 20081/19; 11454/17; 40209/20; 3041/19.

112 Bart van der Sloot, 'Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling' (2017) 7(3) International Data Privacy Law, 190-201.

113 Bart van der Sloot, 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases'(2020) 11 J Intell Prop Info Tech & Elec Com L, 160.

114 *L.B. v Hungary* App no 36345/16 (ECtHR, 9 March 2023). See on the publication of tax data also: 15807/14.

115 OM Arnardóttir, 'The "procedural turn" under the European Convention on Human Rights and presumptions of Convention compliance' (2017) 15(1) International Journal of Constitutional Law, 9-35.

every case anew, on its own merits. This benefitted the Court's appreciation of any particular detail of every individual case, but it came at the price of legal certainty and foreseeability. Slowly, the Court changed this approach. For example, it made a division, the first part of its judgement consisting of a reiteration of the general principles laid out in previous jurisprudence and only then, in the second part, applying those principles to the case at hand. Now, especially in cases against Russia, it makes a next move; its judgements are basically no more than stating something in line of: 'It is clear that Member State A violated the general principles 1, 2 and 3 as set out in earlier case law, see inter alia cases X, Y and Z. That is why the Court awards compensation to the applicants, for which see the table.' The majority of cases against Russia, as well as occasionally against other Member States, concern this type of staccato judgements, through which the Court apparently makes it clear that the state is so abundantly in violation of the Convention that it does not want to waste many words on it. This means that these judgements do not contain a deliberation or legal reasoning of the Court, but rather are of a declaratory nature. These mostly regard surveillance of prisoners and detainees and suspects without a proper legal basis,[116] but also regard family visits not being allowed or made impossible for prisoners and detainees[117] and unlawful search of homes.[118] Like with Russia, most cases against Turkey concern the ill-treatment of prisoners and suspects, in particular in the wake of the attempted coup,[119] although these cases typically get a substantive, yet short, treatment by the ECtHR. Against other countries, there were quite a number of judgements with regard to the ill-treatment of prisoners as well.[120]

With respect to Ukraine, the Court emphasizes that it understands the complex situation the country is in and that it will therefore show some leniency in terms of length of legal procedures. At the same time, it points out, a swift legal and administrative procedure is required by the ECHR, in particular in cases where the length of the procedure as such affects the interests of the parties involved. Most cases against Ukraine regard family matters, in terms of family visits by a divorced parent, access rights by parents or custody cases where one parent takes the child to another country.[121] Also with respect to other countries, the protection of family life, both in terms of custody cases, child abduction and placing children out of home, and family reunification by immigrants or former immigrants, remains one of the largest categories in 2023.[122] To the contrary, the protection of locational privacy continues for years to be the category the Court issues the least cases on under Article 8 ECHR, also in 2023.[123]

Also consistent with previous years, by far most cases under Article 8 ECHR are brought by natural persons. There is only one interstate complaint, namely of Georgia against Russia,[124] and only a handful of claims accepted by the Court from legal persons.[125] There is one case in which the Court, which normally rejects claims by groups *qualitate qua*, seemed to allow for some room on this point.[126]

An important topic in the case law of 2023 under Article 8 ECHR concerns the protection of reputation, which the Court has found about a decade ago to also be protected under the right to privacy. Since then, the ECtHR has issued a substantial number of cases revolving around this aspect, in which the Court mostly balances the freedom of speech of one party

116 21514/18; 13567/13; 33236/18; 41090/18; 3219/19; 19753/18; 50837/18; 10881/21; 28628/21; 51892/19; 74497/17; 48796/18; 11590/17; 14228/18; 15304/19; 33771/16; 51678/15; 25056/14; 33803/19; 10142/19; 25692/19; 57747/10; 49321/18; 30389/19; 27284/17; 48041/16; 32695/14; 70387/16; 32706/15; 41090/18.

117 12205/18; 56247/15; 38521/16; 18369/18.

118 1570/18; 13079/17; 2829/18; 41761/20; 75231/17; 54714/17.

119 35614/19; 60846/19; 57407/19; 24074/19; 56578/11; 55569/19; 29218/20; 28377/11; 25820/18; 49535/18; 66763/17.

120 10753/21; 11148/18; 29908/20, 48734/20, 7171/21 and 12017/21; 39920/16; 35673/18; 38144/20.

121 51222/20; 5783/20; 14709/07; 27380/20; 53099/19; 28982/19; 56669/18.

122 28383/20; 51056/21; 57202/21; 66015/17; 44684/14; 16205/21; 31434/21; 27700/15; 30129/21; 64886/19; 18646/22; 35740/21; 37031/21; 48698/21; 19165/20; 26504/20; 8324/18; 32662/20; 82939/17 and 27166/19; 23851/20 and 24360/20; 48618/22; 10794/12; 48280/21; 44646/17; 19632/20; 12141/16; 17791/22; 47196/21; 25942/20; 10477/21; 55351/17; 6147/18; 15646/18; 12083/20; 57766/19; 8757/20; 63307/17 and 38105/19; 15784/19; 4065/21; 39769/17, 9167/18, 48372/18, 38097/19, 45985/19 and 58880/19; 13218/21; 37024/20; 19857/10; 57752/21; 8361/21; 21768/19; 13258/18, 15500/18, 57303/18 and 9078/20.

123 14301/14; 17414/11; 42419/04; 22619/14; 38228/12; 30782/16; 34734/13.

124 38263/08.

125 7668/15; 23503/15; 19162/19; 14139/21; 2799/16; 2800/16; 3124/16 and 3205/16. Bart van der Sloot, 'Data Protection Rights for Legal Persons' (2023) 9(2) EDPL.

126 31172/19. Bart van der Sloot, 'Data Protection and Door-to-Door Evangelising' (2023) 9(2) EDPL. Although individual applicants can also rely on Article 8 ECHR when their community or the group to which they belong is affected, see eg App nos 39954/09 and 3465/17. See also: 27094/20

(eg a newspaper) against the right to privacy of the other part (eg a politician).[127] This doctrine is becoming more and more important in countries were state owned, controlled or leaning media smear the reputation of rival politicians[128] or people working for them.[129] Article 8 ECHR is also an increasingly important tool for the Court in addressing judges and judicial personnel that are dismissed from office by regimes that want to dispose of a critical and independent judiciary.[130]

Turning to classic informational privacy related cases,[131] some cases stand out, such as, but not limited to, two cases against Russia issued in 2023 that concern the use of facial recognition techniques. In *Glukhin v Russia*, Russia allegedly used the technology to track down a sole protestor on the streets, and Court found a violation of Article 8 ECHR, inter alia pointing to the fact that:

> the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative offence proceedings – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as 'necessary in a democratic society'.[132]

In *N.F. a.o. v Russia*,[133] on various dates, criminal proceedings were instituted against the applicants. The Ministry of the Interior recorded the personal data relating to the criminal proceedings against the applicants in a special database. After a certain period, the applicants' convictions became spent or were lifted by a court. On various dates the local database centres of the Ministry delivered to the applicants, at their requests, certificates which contained information regarding the criminal proceedings against them, such as whether an amnesty had been granted, the dates of the respective convictions, the criminal offences for which they had been suspected or convicted, the sentences imposed and the names of the courts that had convicted them. The applicants complained to the heads of the database centres of the Ministry that the processing, including the storage, of data relating to discontinued criminal proceedings and spent and lifted convictions was unlawful and unnecessary and asked them to delete such data. Interestingly, while it sometimes appears that the ECtHR has accepted that any processing of personal data, as defined under the EU's General Data Protection Regulation,[134] also falls under the material scope of Article 8 ECHR, in this case, the Court makes clear that the processing of personal data only falls under that provision when it affects a person's private life. Because this case revolves around the processing of criminal data, the ECtHR concludes a person's private life has been affected. There was a law, the question of whether the legal regime met the quality of law requirements is directly related to the question of whether the interference is necessary in a democratic society, so it finds. The legitimate aim of the legal regime was the prevention of crime and the protection of the rights of others. With regard to the question of necessity, the Court notes that a substantial amount of data were gathered, that this was done irrespective of the gravity of the offence committed, that the storage period and the details of the ways in which the data were stored was not accessible to the public and that the domestic courts in one case held that the data could be stored until the subject reached the age of 80. The Russian legal system did not allow for an adequate proportionality test on a case-by-case basis, which is why the ECtHR found a violation of Article 8 ECHR.

The case of *Uckan v Turkey*[135] addresses a similar question. Police officers had come to the applicant's home to take him to the police station in the context of a complaint of theft of a cell phone after the complainant had erroneously been identified as the per-

127 4222/18; 6950/13; 70267/17; 14852/18.

128 50849/21; 45066/17.

129 55297/16.

130 25226/18, 25805/18, 8378/19 and 43949/19; 66292/14; 54588/13; 29943/18; 41047/19; 47052/18; 27276/15; 21181/19 and 51751/20. See also: 49647/14.

131 See also App nos 49922/16; 26476/14; 34467/15; 7286/16; 18593/19; 71522/17, 47646/19 and 61114/19; 44850/18.

132 11519/20.

133 3537/15.

134 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).

135 67657/17.

petrator of the crime during a search carried out by investigators in this database. Subsequently, taking into account the acquittal of the applicant, the photos concerning him were deleted and the remainder of the data appearing in the criminal file was rectified so as to place them in a register for identification purposes. The applicant sought to delete his data from that register, but to no avail. Although this interference had a legal basis and served a legitimate interest, the Court finds it is disproportional. The Court points to the risk of stigmatisation which resulted from the fact that people, after having benefited from an acquittal or a dismissal of proceedings, had been treated in the same way as convicted persons. The national law does not provide for the possibility of erasing the stored data and the duration of data retention – ten years after the death of the person concerned, and in any case eighty years after the date of recording – is in practice comparable to indefinite retention or, at least, to a standard rather than a maximum limit.

Building on its seminal case law on mass surveillance, the Court made an interesting new turn in *Wieder and Guarnieri v the United Kingdom.* The principal issue was whether a person residing outside a Member State falls within the state's territorial jurisdiction. The first applicant is a national of the United States of America and lives in Florida. The second applicant is an Italian who lives in Berlin, Germany. On the domestic level, the supervisory body (IPT) concluded that a Contracting State owed no obligation under Article 8 ECHR to persons both of whom were situated outside its territory in respect of electronic communications between them which passed through that State. The applicants complain that, as a result of their work and contacts, their communications might have been intercepted, extracted, filtered, stored, analysed and disseminated by the UK intelligence agencies pursuant to the Regulation of Investigatory Powers Act 2000 (RIPA). The government argues that any interference with the applicants' private lives could not be separated from their person and would therefore have produced effects only where they themselves were located – that is, outside the territory of the United Kingdom. But the Court disagrees, drawing several analogies, inter alia with searching a person's home:

> it could not seriously be suggested that the search of a person's home within a Contracting State would fall outside that State's territorial jurisdiction if the person was abroad when the search took place. ... Turning to the facts of the case at hand, the interception of communications and the subsequent searching, examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.[136]

In *Margar v Greece*,[137] the applicant was arrested in the context of a police investigation, along with six other persons. She was charged with various serious crimes. The applicant was released from detention pending trial on condition that she does not leave the country. The local department of public security asked the public prosecutor to publish the personal data and photographs of the accused, in order to protect society, and to investigate whether there were other cases in which the accused had participated. The prosecutor did so after the court approved of the conduct. At the end of the main investigation, the applicant was convicted and sentenced to eleven years and six months' imprisonment without suspensive effect. The ECtHR points out that the applicant was not informed officially of the publication of her photograph and personal data, either before the publication or afterwards, but was informed of it accidentally through her friends. Although this publication was in accordance with the law, was necessary in a democratic society and served a clear public interest, and although a court order had been obtained, the Court nevertheless considers that the applicant should at least have been notified prior to the dissemination of her photograph and the details of the pending criminal charges. It also points out that the applicant had no right to appeal against the prosecutor's order for the publication of her photograph and personal data, which meant that she had no opportunity either to be heard prior to the decision being taken or to apply for a review and put forward her arguments after the decision was taken.

136 64371/16 and 64407/16, paras 93-94.

137 36705/16.

In *Negru v Moldova,*[138] the applicant and her farther had a dispute over a house. The father issued criminal complaints against the her. An investigation followed. She was brought in for questioning, was released, and subsequently summoned at the police station again. The police could not find the applicant; her whereabouts were unknown. She was in Italy at the time. After her farther brought new criminal complaints, the applicant claims her lawyer, by chance, noticed on the public noticeboard of the police station that the applicant had been indicted and was wanted by the police. A subsequent request by the lawyer to have access to the criminal file and to have the investigation in respect of the applicant discontinued was rejected by the police. The domestic court also rejected applicant's claims as it concluded that she had failed to substantiate any violation of her rights under Article 8 ECHR. The ECtHR finds that the applicant was declared wanted in 2010, one day after charges had been brought against her in her absence. While the applicant did not dispute that in 2008, she had left Moldova for Italy, the Government failed to provide any evidence that the Moldovan authorities had genuinely tried to summon and find the applicant from 2008 to 2010 prior to that decision. Furthermore, the Government did not inform the Court of any measures taken by the domestic criminal investigating authorities to identify whether the applicant had crossed the border during the relevant time or to summon her through her lawyer, who had been retained the entire time. Consequently, the ECtHR finds, even if the prosecutor had the authority to declare the applicant wanted, the quality of law principles was not respected in this case. This conclusion is further supported by the fact that the applicant was unable to obtain any further information about the decision and, subsequently, to obtain a review of it.

Finally, in *D.H. a.o. v North Macedonia,*[139] a large group of sex workers was arrested on the grounds of suspicion of spreading transmissive diseases. Four of them suggest that they were subjected to medical (blood) testing, which they claim violated their bodily integrity. They also complain about both lacking medical treatment for, inter alia, the consequences of a heroin addiction, and of a lack of access to food, water and a toilet. Finally, they suggest that their photographs were taken and published on the Ministry of Interior's website, which they claim violated their right to privacy. This also holds true for alerting the press about their arrest, leading to media coverage. The ECtHR quickly establishes that there was a legal basis and that the interference served, inter alia, the legitimate interest of preventing crime. As to the proportionality of the measure, the Court points out that medical data is very sensitive, but that at the same time, there was a reasonable suspicion and a court order to take the samples. The ECtHR also notes that the taking of a blood sample is a very short medical procedure, which involves minor bodily harm, and that there was no reason to believe that applicants' personal data were retained or stored after they had fulfilled the purposes for which they were taken. Perhaps most interesting is that the Court does not conclude that consequently, the interference was in conformity with the conditions laid down in paragraph 2 of Article 8, but that the complaint was manifestly unfounded, a conclusion which it normally only reaches with respect to complaints that have a very weak factual or legal basis. As to the photographs, the applicants first contend that the police authorities had informed the media of their visit to the clinic, which had resulted in the taking and publication of the applicants' photographs in certain media outlets. The Court accepts that the applicants were photographed by journalists while they were being transferred to the clinic and that those photographs were subsequently published by certain media outlets, together with articles relating to that incident. However, it also finds that it has not been clearly established that the police authorities were directly responsible for the taking and the subsequent publication of the applicants' photographs. The distribution of the burden of proof and the level of persuasion necessary for reaching a particular conclusion are intrinsically linked to the specificity of the facts, the nature of the allegation made and the Convention right at stake, the Court reiterates. The applicants did not present *prima facie* evidence that the police officers had informed the media outlets of their transfer to the clinic and therefore the burden of proof had not been shifted to the Government, that is why no violation of Article 8 ECHR is established on this point. The applicants also argued that the Ministry had published their photographs, which had been taken while they were in police custody, on its website. On

138 7336/11.

139 44033/17.

this point, the Court finds that the court of appeal on the domestic level dismissed the applicants' complaint, which leads it to conclude that the national courts failed in their obligation to protect the applicants' right to respect for their private life against the infringement of that right by the publication of their photos on the Ministry's website. Consequently, there is a violation of Article 8 ECHR on this point.

III. Country Reports

by Christina Etteldorf

Frequent readers of our Reports section will be aware that we update on a wide range of developments at international, EU and national level. This includes legislative initiatives, decisions by national courts and authorities, activities of data protection boards, reports from and by practitioners in our respective 'corner' of the same name, and much more. It is therefore not easy to review an entire year, as so many exciting things have happened in 2023. It would be impossible to cover them all either by including reports in the regular editions of the EDPL or here in this glimpse back at what else happened that we could not cover in detail in the 2023 editions. We would therefore like to highlight below just a few of the key issues which we could not report on in detail during last year.

EDPB

Let us start with a look at the European Data Protection Board (EDPB) that has been, as usual and as we did actually report in several contributions in our reports section, very active in 2023. Actions that we could not address in more detail were, for example, the adoption of *Guidelines on Technical Scope of Art. 5(3) of ePrivacy Directive*[140] addressing 'new' tracking techniques under the 'old' ePrivacy Directive or the *Guidelines on Art. 37 of the Law Enforcement Directive*[141] concerning data transfers on international level, both published in autumn. Already in April 2023, the Board also launched a *Data Protection Guide for small businesses* containing various tools and practical tips to help such companies comply with the GDPR.[142] The *template forms for data protection complaints and responses* published by the Board in June 2023 should be similarly helpful for practitioners and data protection authorities alike.[143] In several task forces the EDPB has also been working throughout the year in-depth on specific subjects that are of supranational relevance to data subjects across the EU, such as the task forces on *TikTok, cookie banners, the 101 NOYB data transfers complaints, ChatGPT* and *age verification*. Some of these, as in the case of TikTok,[144] have already produced practical results. During its October 2023 plenary, the EDPB selected the topic for its third *coordinated enforcement action*, which will concern the implementation of the right of access by controllers and will be launched in 2024 – we surely will not miss out on that.

EDPS

The European Data Protection Supervisor (EDPS) was also active in 2023.[145] Key input was provided above all on current legislative initiatives at EU level, in which the EDPS reminded the legislators of the need for consistency with existing data protection law, made suggestions for improvement and, above all, pointed out risks to fundamental rights of data subjects. Among the 116 (!) legislative consultations in 2023 were the AI Act, which has meanwhile been agreed on, and the proposed CSAM Regulation (still under negotiation), as well as legislative proposals in the financial sector, notably on the Digital Euro and Financial and Payment Services. In the performance of his supervisory duties, the EDPS issued 15 Supervisory Opinions on various issues such as the envisaged processing of biometric data by European insti-

140 EDPB, 'Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive' (14 November 2023) <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en>. All internet links in this report were last accessed 29 April 2024.

141 EDPB, 'Guidelines 01/2023 on Article 37 Law Enforcement Directive' (19 September 2023) <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-012023-article-37-law-enforcement_en>.

142 EDPB, 'EDPB Launches Data Protection Guide for small businesses' (27 April 2023) <https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business_en>.

143 EDPB, 'Template Complaint form and Template Acknowledgement of receipt' (20 June 2023) <https://www.edpb.europa.eu/our-work-tools/our-documents/other/template-complaint-form-and-template-acknowledgement-receipt_de>.

144 E Lievens and V Verdoodt, 'A €345 Million Fine for TikTok for Violations of the GDPR Regarding the Processing of Children's Personal Data' (2023) 9(4) EDPL 472-481.

145 See on this and the following EDPS, 'Annual Report 2023: adaptability in a changing world' (2024) <https://www.edps.europa.eu/data-protection/our-work/publications/annual-reports/2024-04-09-annual-report-2023-adaptability-changing-world_en>.

tutions or their use of social media and the exchange of information on supranational level. As regards complaints received by individuals on the (unlawful) processing of their data by European institutions, the EDPS even created a dynamic tool on the EDPS website to provide easier and more understandable access to data subjects rights.[146] In addition, numerous investigations were carried out, whereby his findings on the processing of migrant data by the European Border and Coast Guard Agency (Frontex) were particularly relevant (and worrying), especially in their exchange with Europol, and raised serious doubts as regards GDPR compliance.[147]

DPAs

2023 was a year of *large fines* imposed by national data protection authorities for diverse violations of the GDPR vis-à-vis very different actors. We reported in-depth on major fines by the Irish DPC on the Meta company (regarding Facebook, Instagram and WhatsApp respectively €1.2 billion[148], €210 million[149], €180 million[150] and €5.5 million[151])[152] as well as TikTok[153] (€345 million[154]) which were conducted with involvement of the EDPB. But there were many other fines worth highlighting. For example, the DPC took action against TikTok also outside the EU, specifically the United Kingdom; the Chinese company was faced with a £12.7 (approximately €14.88) million fine for misusing children's data in April 2023.[155] The French CNIL in May 2023[156] fined Clearview AI €5.2 million due to incompliance with a previous order to not collect and process data on individuals located in France in the context of the company's facial recognition database. In June 2023[157] CNIL fined CRITEO, which provides a widespread online tracking tool in the context of behavioural advertising, €40 million due to violations of Articles 7(1) and (3), 12 and 13, 15(1), 17(1) and 26 GDPR. Other big penalties came from Italy – in April 2023[158] the GDPD ordered the telecommunications operator TIM S.p.A. to pay €7.6 million due to, inter alia, its unlawful telemarketing activities. In September 2023[159] GDPD also ordered the energy supplier Axpo Italia S.p.A. to pay €10 million for processing inaccurate and outdated customer data. Similar strict measures were taken in Spain (the AEPD fined in July 2023[160] Open Bank S.A. €2.5 million and in autumn 2023 both energy supplier ENDESA ENERGÍA S.A.U. €6.1 million[161] and CAIXABANK, S.A. €5 million[162], all for lacking security measures and failure to properly notify data breaches). In Sweden, the IMY fined music streaming service Spotify in June 2023[163] SEK 58 million (approximately €5.2 million) for not fully complying with data access and information requests from individuals and,

146 See the tool available at <https://www.edps.europa.eu/data-protection/our-role-supervisor/complaints_en>.

147 EDPS, 'Audit Report on the European Border and Coast Guard Agency (FRONTEX)', 2022-0749 (5. and 6.10.2022) <https://www.edps.europa.eu/system/files/2023-05/edps_-_23-05-24_audit_report_frontex_executive_summary_en.pdf>.

148 Data Protection Commission, DPC Inquiry Reference: IN-20-8-1 [12.5.2023] <https://www.edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf>.

149 Data Protection Commission, DPC Inquiry Reference: IN-18-5-5 [31.12.2022] <https://www.edpb.europa.eu/system/files/2023-01/facebook-18-5-5_final_decision_redacted_en.pdf>.

150 Data Protection Commission, DPC Inquiry Reference: IN-18-5-7 [31.12.2023] <https://www.edpb.europa.eu/system/files/2023-01/instagram_inquiry-18-5-7_final_decision_en.pdf>.

151 <https://www.edpb.europa.eu/system/files/2023-01/final_adoption_version_decision_wa_redacted_1.pdf>.

152 M Magierska, 'Three EDPB Binding Decisions in the Art. 65 GDPR Procedure and Two Major Questions for the Future' (2023) 9(1) EDPL 55-60.

153 Data Protection Commission, DPC Inquiry Reference: IN-18-5-6 [12.1.2023] <https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf>.

154 Lievens and Verdoodt (n 5).

155 Information Commissioner's Office, 'ICO fines TikTok £12.7 million for misusing children's data' (4 April 2023) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/>.

156 Commission Nationale de l'Informatique et des Libertés, 'Reconnaissance faciale : la CNIL liquide l'astreinte prononcée à l'encontre de CLEARVIEW AI' (10 May 2023) <https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-liquide-lastreinte-prononcee-lencontre-de-clearview-ai>.

157 Commission Nationale de l'Informatique et des Libertés, 'Personalised advertising: CRITEO fined EUR 40 million' (22.6.2023) <https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million>.

158 Garante per la protezione dei dati personali, case no. 9894662 [13 April 2023] <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9894662>.

159 Garante per la protezione dei dati personali, cas no. 9940988 [28 September 2023] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9940988>.

160 Agencia Española de Protección de Datos, case no. EXP202101565 [1 June 2023] <https://www.aepd.es/documento/ps-00331-2022.pdf>.

161 Agencia Española de Protección de Datos, case no. EXP202204846 [25 September 2023] <https://www.aepd.es/documento/ps-00002-2023.pdf>.

162 Agencia Española de Protección de Datos, case no. EXP202206311 [25 September 2023] <https://www.aepd.es/documento/ps-00020-2023.pdf>.

163 Integritetsskyddsmyndigheten, 'Sanktionsavgift mot Spotify' (13 June 2023) <https://www.imy.se/nyheter/sanktionsavgift-mot-spotify/>.

in August 2023[164] and Trygg-Hansa SEK 35 million (approximately €3 million) for the company's security flaws that led to data of around 650,000 customers being accessible to unauthorized persons via the internet. In Croatia, the AZOP took action against two debt collection agencies in the course of which the authority inter alia imposed fines in the amount of €2.26 million against B2 Kapital d.o.o. in May 2023[165] and of €5.47 million against EOS Matrix d.o.o. in October 2023[166] due to various violations of the GDPR, in particular in the context of information obligations and security measures. Noteworthy is also the Dutch APG's decision on Uber Technologies, Inc. and Uber B.V. from December 2023[167] resulting in a penalty of €10 million. The authority inter alia found the company failed to disclose the full details of its retention periods for data concerning European drivers, and to name the non-European countries in which it shares this data as well as obstructing its drivers' efforts to exercise their right to privacy. If one 'only' adds up the amounts of the aforementioned large fines, which of course do not reflect all fines incurred in 2023, the result is the staggering €2.04 billion, which have flowed or will flow into various state budgets in the Member States. Against this backdrop, it is somewhat ironic that the data protection authorities still do not appear to be adequately financed or resourced by their states for the tasks assigned to them. The EDPB once again highlighted this problem in its report of December 2023 on the application of the GDPR under Article 97. The EDPB pointed out that 'it is important to note that the resources of the SAs and EDPB are not increasing at the same pace as their responsibilities and tasks' also in the context of other evolving legislative initiatives such as the Digital Markets Act (DMA) or the AI Act.[168]

Of course, there were many other decisions by national authorities and courts which may seem not so exciting in view of the amount of the imposed fines, but which are just as important because of their substantive elements. As recent CJEU rulings also underline,[169] major issues concerned data processing by *national credit agencies*. In its decision of 2 February 2023, the Austrian DSB ruled that the retrieval of civil register data by credit agencies and the subsequent storage of this data in a 'business database' in response to a request for information from the data subject violates the right to confidentiality because the underlying data processing is unlawful.[170]

The topic of *AI* was omnipresent, including in its data protection dimension. While the Italian GPDP's ban on ChatGPT in April came like a 'big bang',[171] a decision from February 2023 received much less attention, but was no less interesting: the GPDP banned the web application 'My AI Friend' – essentially an interactive chatbot – due to violations in the processing of minors' data and, in particular, concerns about the protection of minors due to the bot's inappropriate (sexualised) responses to users (children's) questions.[172] The enforcement notice issued by the UK ICO against Snap's AI chatbot 'My AI' in October 2023 had a similar background in terms of minors' data and their further use, for example, for advertising purposes.[173] Some data protection authorities, eg the French CNIL, have also drawn up their roadmaps for the future handling of AI.[174] There were also some

164 Integritetsskyddsmyndigheten, 'Administrative fine of SEK 35 million against Trygg-Hansa' (5 September 2023) <https://www.imy.se/en/news/administrative-fine-of-sek-35-million-against-trygg-hansa/>.

165 Agencija za zaštitu osobnih podataka, 'An administrative fine in the amount of 2.26 million EUR imposed on the Debt Collection Agency' (4 May 2023) <https://azop.hr/an-administrative-fine-in-the-amount-of-2-26-million-eur-imposed-to-the-debt-collection-agency/>.

166 Agencija za zaštitu osobnih podataka, 'Debt Collection Agency EOS MATRIX D.O.O. imposed with administrative fine in the amount of 5.47 million EUR' (5 October 2023) <https://azop.hr/debt-collection-agency-eos-matrix-d-o-o-imposed-with-administrative-fine-in-the-amount-of-5-47-million-euros/>.

167 Autoriteitpersoonsgegevens [11 December 2023] <https://autoriteitpersoonsgegevens.nl/uploads/2024-01/Boetebesluit%20Uber%20.pdf>.

168 EDPB, 'Contribution of the EDPB to the report on the application of the GDPR under Article 97' (12 December 2023) <https://www.edpb.europa.eu/system/files/2023-12/edpb_contributiongdprevaluation_20231212_en.pdf>, para 4.4.

169 See the introduction to the Reports Section in (2023) 9(4) EDPL 444 et seq.

170 Datenschutzbehörde, case no. D124.3614/22 [2 February 2023] <https://noyb.eu/sites/default/files/2023-02/DSB_KSV1870_Redacted.pdf>.

171 PG Chiara, 'Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing' (2023) 9(1) EDPL 68-72.

172 Garante per la protezione dei dati personali, case no. 9852214 [2 February 2023] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214#english>.

173 Information Commissioner's Office, 'UK Information Commissioner issues preliminary enforcement notice against Snap' (6 October 2023) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap/>.

174 Commission Nationale de l'Informatique et des Libertés, 'Intelligence artificielle: le plan d'action de la CNIL' (16 May 2023) <https://www.cnil.fr/fr/intelligence-artificielle-le-plan-daction-de-la-cnil>.

decisions on a right that has so far rather been in the shadows within the GDPR: the *right to data portability under Article 20 GDPR*. The Federal Administrative Court of Austria decided that data from an outdated app no longer supported by the developer must not be provided in the former interactive format (ie raw data is sufficient)[175]; the Belgian DPA dismissed the right to data portability asserted vis-à-vis an insurance company when it comes to data processed due to a legal obligation to do so (ie not contract or consent as required by Article 20 GDPR)[176]; and the Finnish authority ruled that the possibility provided by an email service to users to export their emails one by one manually does not meet the criteria of a 'structured, commonly used, and machine-readable format'[177].

Furthermore, the Swedish IMY's fine of SEK 12 million (€1 million) against telecommunication provider Tele2 (as well as other providers) was already remarkable in its amount, but its content may have an even greater impact: the underlying reason was solely the provider's use of the *Google Analytics tool* on its website, as it is implemented on millions of other websites, too. In accordance with the clearly formulated judgement of the CJEU from 2020 on EU-US data transfers, this violates the obligations of data processors that must ensure an appropriate level of security for transfers to other countries outside the EU.[178]

As has become almost customary, many measures and fines imposed related also to *direct marketing* measures by companies which can be exemplified by the French CNIL's fine of €600,000 against Group Canal+[179] and the Swedish IMY's fine of SEK 350,000 (approximately €30,000) against the textile retailer H&M[180], both from October 2023.

Advertising in a different sense was also a major topic in 2023, namely *political advertising*. Not only was the Regulation on the transparency and targeting of political advertising proposed by the Commission, which has now been published in the Official Journal, intensively discussed on legislative level, but the utilisation of microtargeting for political advertising purposes in daily practice was also heavily criticised. In January 2023, the NGO noyb filed complaints against various German political parties that had used the microtargeting offered by Facebook for their political campaigns[181], as well as a complaint against the network X (formerly Twitter) in December 2023[182]. According to noyb's accusation in the latter case, which also took a sideway's glance at the behaviour of the European Commission, the company processed data on political views and religious beliefs to determine whether people should or should not see an ad campaign by the European Commission's Directorate General for Migration and Home Affairs, which tried to rally support for the 'chat control' in its proposed CSAM Regulation.[183]

In several contributions we also reported on another advertising topic in our Reports Section 2023: *targeted or behavioural advertising*. After the Norwegian DPA's initiative resulted in the EDPB pulling the plug on behavioural advertising for the Meta company, or rather instructing the Irish DPC to do so,[184] many Big Tech companies, whose financing is largely based on targeted advertising, are beginning to adopt methods that have been on the agenda for some time now. While the cookie pledge initiative which was developed and launched in 2023 by the European Commission still searches for new GDPR-compliant (voluntary) ways to respond to the so-called

175 Bundesverwaltungsgericht Republik Österreich, W211 2261980-1/7E [7 September 2023] <https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230907_W211_2261980_1_00/BVWGT_20230907_W211_2261980_1_00.pdf>.

176 Gegevensbeschermingsautoriteit, case no. DOS-2023-00609[27 April 2023] <https://www.gegevensbeschermingsautoriteit.be/publications/zonder-gevolg-nr.-45-2023.pdf>.

177 Tietosuojavaltuutetun toimisto, case no. 10048/182/20 [22 March 2023] <https://finlex.fi/fi/viranomaiset/tsv/2023/20231883>.

178 Integritetsskyddsmyndigheten, 'Four companies must stop using Google Analytics' (3 July 2023) <https://www.imy.se/en/news/four-companies-must-stop-using-google-analytics/>.

179 Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2023-015 [12 October 2023] <https://rb.gy/on7p3k>.

180 Integritetsskyddsmyndigheten, case no. DI-2020-10545 [17 October 2023] <https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-hm-klagomal.pdf>.

181 Noyb, 'Political microtargeting on Facebook: an election promise just for you!' (21 March 2023) <https://noyb.eu/en/political-microtargeting-facebook-election-promise-just-you>.

182 Noyb, 'GDPR complaint against X (Twitter) over illegal microtargeting for chat control ads' (14 December 2023) <https://noyb.eu/en/gdpr-complaint-against-x-twitter-over-illegal-micro-targeting-chat-control-ads>.

183 We reported intensely on the criticism the CSAM Regulation has faced, see T Quintel 'Renewed Concerns About Compliance of the Proposed 'Regulation to Prevent and Combat Child Sexual Abuse' with Essence of Right to Data Protection: The Council Legal Service Opinion' (2023) 9(2) EDPL 173-183.

184 MD Cole and K Kollmann, 'Norwegian DPA Blocks Personalised Advertising on Facebook and Instagram in Urgency Procedure: Another Step towards a Departure from Meta's Business Model?' (2023) 9(3) EDPL 363-370.

'cookie fatigue' phenomenon by simplifying the management of cookies and personalised advertising choices,[185] the industry seems to have already found the 'appropriate'(?) alternative. So called 'pay-or-okay' models present the user with a choice between actually paying (financially) for a service or paying with their data and being faced with personalised ads – a model which was recently introduced eg by Meta as subscription model for Facebook and Instagram. Various organisations, including the consumer protection organisation BEUC, have filed complaints against such models, particularly if they are applied on large platforms.[186] Meanwhile, on the initiative of several data protection authorities,[187] the EDPB has been called upon to comment on how to deal with the issue of 'paying or paying with data' in a consistent and harmonised approach in the future and did so at the beginning of April 2024[188]. For sure, the topic will therefore continue to stay with us also this year.

National Courts

As this issue seems to become relevant in 2024 as well, considering for example a recent judgement from Sweden which brought the IMY to rethink its practices concerning not to investigate complaints against media licence owners,[189] we want to close with pointing to some interesting decisions from national courts dealing with Article 85 GDPR, the so-called *media privilege*. The Polish Supreme Administrative Court ruled in February 2023 in a case concerning online archives of a website, that although they fall under the scope of Article 17 GDPR in principle a proper balance between freedom of expression and protection of personal data, in line with Article 85 GDPR, must be guaranteed and taken into account by the Polish DPA.[190] The Administrative Court of Hämeenlinna (Finland) in a judgement from December 2023 ruled even more extensively in favour of the media privilege: a media outlet that maintains a database on tax information about (private) persons may invoke the justification of journalistic processing purposes, even if the entries are not considered news articles in the traditional sense since they nevertheless serve public information interests.[191] On the other hand, the Austrian implementation of Article 85 GDPR in Section 9 of the Data Protection Act provides for a blanket exemption from the GDPR but only for media owners and other traditional media providers. The Austrian Federal Administrative Court ruled in August 2023 that this provision consequently only applies to such media and cannot be applied, even by analogy, to other persons, such as in this specific case to the operator of a website, even if they publish (ie process) 'journalistic' information (ie data). A direct application of Article 85 GDPR was also deemed out of question, as this was not a substantive provision of the Regulation, but an implementation mandate to the Member States.[192] The case is also interesting because the Supreme Court of Austria repealed the rule of Section 9 of the Data Protection Act at the end of 2022 due to incompatibility with EU law, but this will not apply until June 2024.[193]

With this review it becomes obvious that reporting on all relevant issue happening over the course of a year in data protection terms would necessitate a multiplication of the volume dedicated to reports. Instead, with the selection we do for every edition we hope to direct readers' attention to important but also diverse topics. The review as a supplementary look back at 2023 filled the puzzle of data protection developments with some additional pieces that we think also deserve your attention.

---

185 See for more information on the cookie pledge initiative <https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en>.

186 J Tar, 'Digital rights group files additional complaint against Meta's 'pay or okay' model' (Euractiv, 11 January 2024) <https://www.euractiv.com/section/platforms/news/digital-rights-group-files-additional-complaint-against-metas-pay-or-okay-model/>.

187 Datatilynet, 'Request for an EDPB opinion on "consent or pay"' (26 January 2024) <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/>.

188 EDPB, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' (17 April 2024) <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf>.

189 Integritetsskyddsmyndigheten, 'IMY ser över sin hantering av klagomål mot innehavare av utgivningsbevis' (15 March 2023) <https://www.imy.se/nyheter/imy-ser-over-sin-hantering-av-klagomal-mot-innehavare-av-utgivningsbevis/>.

190 Centralna Baza Orzeczeń Sądów Administracyjnych, case no. III OSK 6781/21 [9 February 2023] <https://orzeczenia.nsa.gov.pl/doc/6C317F6401>.

191 Hämeenlinnan hallinto-oikeus, case no. 2548/2023 [14 December 2023] <https://gdprhub.eu/index.php?title=H%C3%A4meenlinnan_hallinto-oikeus_(Finland)_-_2548/2023>.

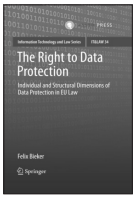
192 Bundesverwaltungsgericht Republik Österreich, case no. W2742243598-1/10E [24 August 2023] <https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230824_W274_2243598_1_00/BVWGT_20230824_W274_2243598_1_00.pdf>.

193 Verfassungsgerichtshof Österreich, case no. G 287/2022-16, G 288/2022-14 [14 December 2022] <https://www.vfgh.gv.at/downloads/VfGH-Erkenntnis_G_287_2022-_G_288_2022_vom_14._Dezember_2022.pdf>.

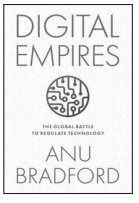
IV. Books of the Year

by Gloria González Fuster

Members of the EDPL editorial board have shared the titles that mattered to them this year, to prepare a special selection of recommended reads for EDPL readers. The books are listed in alphabetical order, and compiled by Gloria González Fuster:



Bieker, Felix, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (Asser Press/Springer 2022).

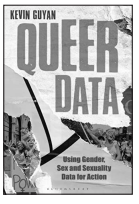


Bradford, Anu, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023).

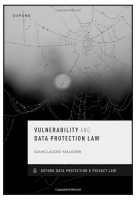
Collins, David, and Michael Geist (eds.), *Research Handbook on Digital Trade* (Edward Elgar 2023).

De Gregorio, Giovanni, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

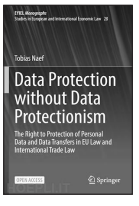
González Fuster, Gloria, Rosamunde Van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar 2022).



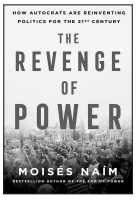
Guyan, Kevin, *Queer Data: Using Gender, Sex and Sexuality Data for Action* (Bloomsbury 2022).



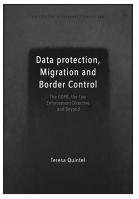
Malgieri, Gianclaudio, *Vulnerability and Data Protection Law* (Oxford University Press 2023).



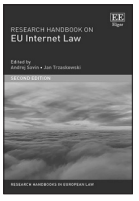
Naef, Tobias, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law* (Springer, 2022).



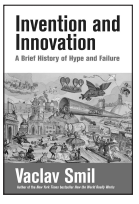
Naím, Moisés, *The Revenge of Power: How Autocrats Are Reinventing Politics for the 21st Century* (Macmillan Publishers 2022).



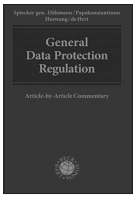
Quintel, Teresa, *Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond* (Bloomsbury, 2022).



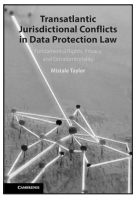
Savin, Andrej and Jan Trzaskowski (eds.), *Research Handbook on EU Internet Law* (2nd edn) (Edward Elgar 2023).



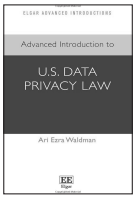
Smil, Vaclav, *Invention and Innovation: A Brief History of Hype and Failure* (The MIT Press 2023).



Spiecker gen. Döhmann, Indra, et al. (eds.), *General Data Protection Regulation: Article-by-Article Commentary* (Nomos 2023).



Taylor, Mistale, *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (Cambridge University Press 2023).



Waldman, Ari Ezra, *Advanced Introduction to U.S. Data Privacy Law* (Edward Elgar 2023).