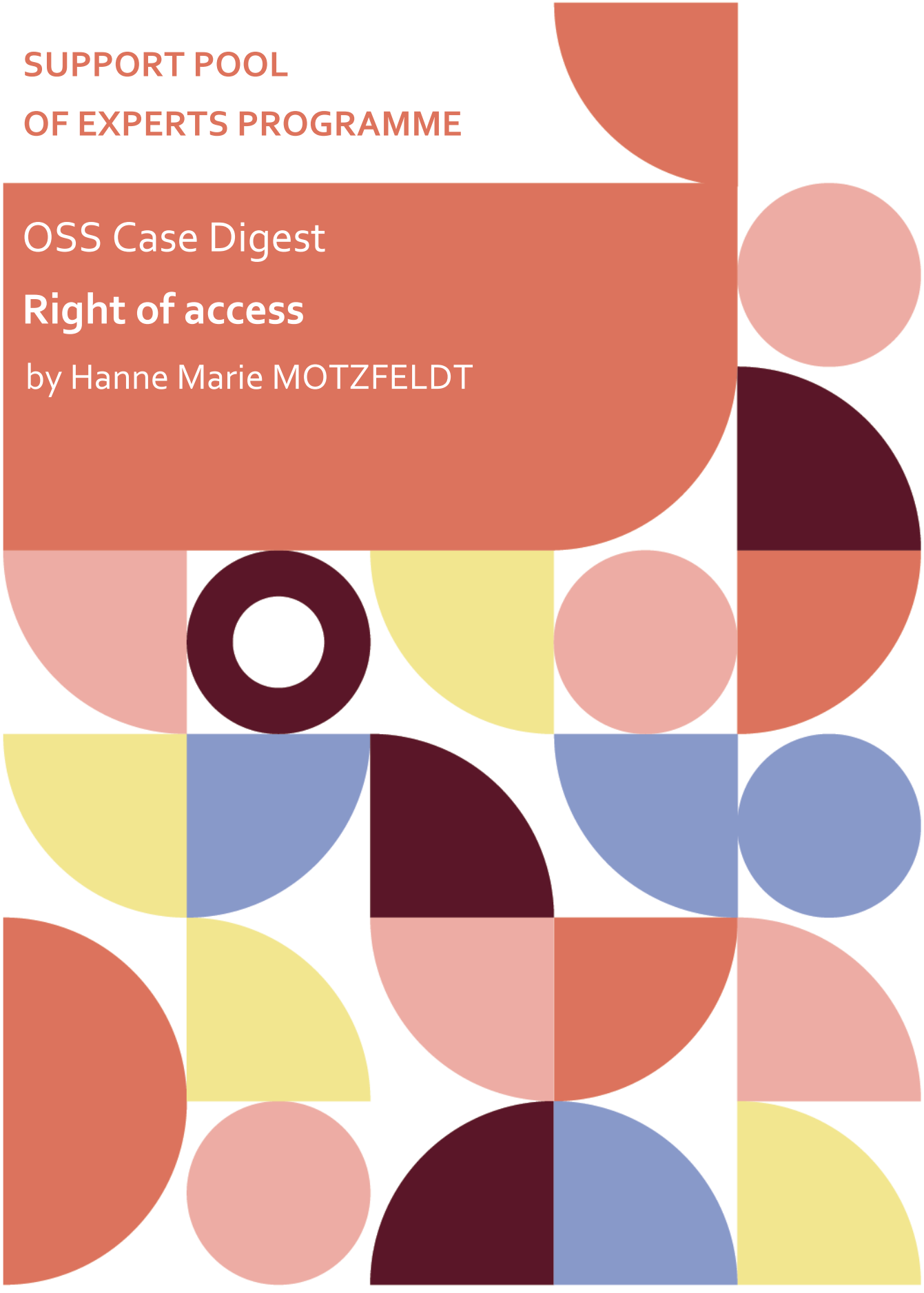
SUPPORT POOL
OF EXPERTS PROGRAMME

OSS Case Digest

Right of access

by Hanne Marie MOTZFELDT



Right of access by the data subject

Professor, Ph.D. in Law, Hanne Marie Motzfeldt

Contents

Document submitted in November 2024

1. Scope, methodology and structure

This report analyses decisions related to Article 15 of the General Data Protection Regulation (hereinafter GDPR) made by national Supervisory Authorities (hereinafter SAs) under the one-stop-shop mechanism (hereinafter OSS mechanism), as per Article 60 of the GDPR.[1] The dataset for the analyses is gathered from the OSS register established by the European Data Protection Board (hereinafter EDPB).[2] Using Article 15 of the GDPR as the primary legal reference to search the register, 185 final decisions were gathered between May 01, 2024, and August 01, 2024, and reviewed manually. The reviewed decisions span from a summary of a decision published on February 29, 2019 (OSS 2019:6) to a decision on April, 2, 2024 (OSS 2024:1246). As the majority of the decisions are relatively simple, legally uncomplicated and revolve around the same themes, only 52 decisions have been selected to be included in this report, see Annex 1.

The level of detail in describing the factual backgrounds and legal reasoning in *the dataset of gathered final decisions* varies significantly. In some instances, brief descriptions pose a challenge in understanding the exact nature of a stated violation or non-violation. Similar challenges arise when the decisions refer to or are based on previously exchanged documents, which are not cited in the final decisions or published and, therefore, cannot be examined. Such decisions have only been reviewed for background but not used as references in this report.

Further, some caution has been exercised in the use of amicable settlements.[3] These decisions focus on the elements of the cases that are of immediate importance for the data subjects. This means that not all statements, opinions and perceptions of the parties to the case can be seen as reflecting the views of the Leading Supervisory Authority (hereinafter LSA) and concerned SAs (hereinafter CSAs). An example is OSS 2023:828. The case revolved around the data subject´s email address being associated with an account on a social media platform which did not belong to the data subject. The data subject suspected that the account in question was a fake. The controller argued that as the account was "not associated with the Data Subject, it did not process any personal data relating to the Data Subject". The LSA did not contradict, adjust nor qualify the controller's argument as the substantive matter was admirably settled by disassociating the data subject's email addresses from the account.[4]

In the following, an overview of Article 15 is presented in Section 2, along with some general overall observations based on the results of the analyses of the gathered OSS final decisions. Section 3 roughly follows the structure of Article 15 and is, therefore, divided into six subsections.[5] Each subsection begins with a brief description of the themes to be reviewed, followed by a presentation of the relevant OSS decisions, which shed light on how the relevant components and elements of the right to access are applied in OSS decisions. Subsection 3.5 on limitations and exceptions to the right to access follows this structure. Therefore it includes an analysis of Article 12(5) on 'manifestly unfounded or excessive'

[1] 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).
[2] The OSS register is publicly available on the board's website, see https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en
[3] EDPB Guidelines 06/2022 on the practical implementation of amicable settlements, May 12, 2022.
[4] See further regarding fake profiles and impersonating in Section 3.1.
[5] Inspired by the structure of the EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023.

requests for access, as this provision is relevant in the context of a number of OSS decisions. The more detailed descriptions of selected OSS decisions in these subsections are not intended to review or analyse all aspects of the right of access but to present existing OSS decisions in an understandable context.[6] Finally, after Section 3, the importance of Article 12 of the GDPR is highlighted in Section 4 as a closing perspective before concluding remarks are given in short form in Section 5.

2. Introduction and overall observations

Natural persons' right to access personal data related to them is enshrined in Article 8 of the EU Charter of Fundamental Rights and is, therefore, to be considered the most essential data protection right.

Article 15 of the GDPR applies to requests for access submitted after the GDPR became applicable.[7] Article 15 specifies the right of access, which can be divided into three components:

- Confirmation as to whether personal data related to the data subject is processed or not.
- Access to personal data related to the data subject if such data is processed at the time of the data subject's access request.
- Information about the processing and the data subject´s other data protection rights.

The European Court of Justice (hereinafter ECJ) has repeatedly stated that the practical aim of the right to access, firstly, is to enable data subjects to verify that the personal data concerning them are correct and processed lawfully.[8] Further, the Court's view is that the: "right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing, conferred, respectively, by Articles 16 to 18 of the GDPR, as well as the data subject's right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage."[9]

In general, the OSS decisions reveal that the national SAs interpret the wording of Article 15 based on a similar understanding of the aim and interplay with other rights laid down in Chapter III of the GDPR, cf. OSS 2021:254, OSS 2022:407 and OSS 2022:367. Further, the relevant recitals of the GDPR (especially recital 63), the principle of transparency in Article 5(1)(a) of the GDPR and the recitals relevant for understanding this principle (especially recital 39) seem to influence the SAs' interpretations of Article 15. An example is the OSS decision mentioned above, OSS 2022:367, in which the Swedish SA as LSA, on May 11, 2022, applied almost word-to-word the interpretation later adopted by the ECJ in a ruling of January 12, 2023, in C-154/21, regarding information on recipients of personal data.[10] Another example is whether the data subject's intent to request access must correspond to the above-described purposes, which align with Recital 63 of the GDPR. Here, the supervisory authorities followed the reasoning of the Court in C-312/23 prior to this ruling.[11] Therefore,

[6] For an in-depth guide to Articles 15 and 12 of the GDPR, please refer to the EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023.
[7] C-579/21, J.M, ECLI:EU:C:2023:501.
[8] C-154/21, RW v Österreichische Post AG, ECLI:EU:C:2023:3, premise 38; Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081, premise 44, C-434/16, Peter Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994, premise 57, C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, ECLI:EU:C:2009:293, premise 49. See also recitals 7, 63, 68, 75 and 85 of the GDPR.
[9] C-487/21, F.F. mod Österreichische Datenschutzbehörde, ECLI:EU:C:2023:369, premise 58.
[10] C-154/21, RW v Österreichische Post AG, ECLI:EU:C:2023:3. See further on OSS 2022:367 in Section 3.4.
[11] C-312/23, Addiko Bank vs. Agencija za zaštitu osobnih podataka.

the underlying motives of the data subjects are of no significance unless misuse of law can be proven. See, for example, OSS 2021:218 and Section 3.5.3 below.

The above-described reasonably consistent approach and methodology are likely to prevent fragmentation in the implementation of the GDPR across the Member States.

However, another *overall tendency* in the examined OSS decisions is worth noticing, as it might, over time, pull in another direction and become an underlying cause of EU data protection regulation fragmentation and challenge the effective enforcement of Articles 15 and 12 of the GDPR. This potential challenge relates to the fact that almost all the OSS decisions reviewed originate from complaints, which revolve almost exclusively around private sector data controllers. The low representation of public authorities as controllers in OSS decisions is logical as the OSS mechanism will rarely apply in cases regarding the exercise of the right of access in the public sector, cf. Article 55(2) of the GDPR. In addition, the Member States have general and sectorial national legislation on access to public sector documents, which has a separate scope differing from the right of access to personal data under Article 15 of the GDPR. To enforce such national legislation, there are typically established administrative appeal boards within the national administrations (different from Chapter VI of the GDPR), Parliamentary ombudsman institutions, etc. The focus may be on national regulation applying to complaints processed within such national organisations and institutions. This focus may lead to overlooking data protection issues, especially if the cases also deal with substantive matters related to national administrative law. In comparison regarding the latter, plenty of the reviewed OSS decisions regarding access have arisen in a commercial context between consumers and businesses or in an employment or recruitment context. See OSS 2021:209, OSS 2021:218, OSS 2023:790, OSS 2023:864, OSS 2023:946 and OSS 2023:947 as examples.[12]

Besides the tendencies mentioned above, three overall observations are noteworthy even though there is no immediate basis to assume that they pose any risk of weakening the enforcement or harmonisation of data protection regulation within the EU.

First, it can be observed that in the majority of the OSS decisions, the complaints regarding the right of access involve other data protection issues, for example, the principles in Article 5 or other rights laid down in Chapter III of the GDPR.

Second, it can be observed that a significant percentage of the OSS decisions directly or indirectly touch upon designs, internal procedures, staff training, or roles in relation to and to the relation to data processors. See, for example, OSS 2020:167, OSS 2019:46, and OSS 2022:268.[13] The background for the latter, OSS 2022:268, was a data subject providing an email address to a controller in connection with an online purchase of an item from the controller on a marketplace. Later, the data subject received an email from a platform for online reviews with the (selling) controller presented as the sender. The data subject was asked to evaluate the buying experience in this email. The data subject contacted the platform for online reviews from another email address, stating their name and address, and requested access according to Article 15 of the GDPR. The platform for online reviews replied that it could not locate an active user for the (second) email address and did not process any information about the data subject. As the data subject later – again – received an email from the review platform on behalf of the controller (to the first email address), the data subject filed a complaint to the SA. Based on the information in the case, the LSA assumed that the platform for online reviews, when sending

[12] OSS 2024:1246 as an example of business and online platforms.
[13] Similarly and more recently OSS 2023:978.

notifications on behalf of the controller, processed the data subject's information as a data processor. As it is not the processor's - but the controller's - responsibility to handle and respond to requests for access, the platform for online reviews had not violated Article 12 nor 15 of the GDPR. The LSA did, however, find it regrettable that the platform did not have consistent procedures and designs for searching relevant information, including the name and address of data subjects, in order to exhaustively explore the possibility of uniquely identifying data subjects and thus, in its role as the processor, assist the controller as agreed in the data processing agreement.

Third, scenarios of parents acting on behalf of their children seem to challenge controllers due to insecurity regarding the interpretation of the GDPR, see OSS 2020:157 and OSS 2019:15. This might be an important theme as children are to be regarded as vulnerable in a data protection context, especially in online environments and particularly worthy of protection. Therefore, further guidance on parents' use of the rights in Chapter III of the GDPR on behalf of (and with the aim to protect) their children might be relevant.

The following section will focus on specific components and elements of Article 15 of the GDPR and the related OSS decisions, illustrating the effects of the components or elements in question and/or related interpretations.

3. Article 15 GDPR

3.1.The scope of Article 15 GDPR

Article 15 aims to provide access to the requested personal data as processed at the time of the access request. The concept of personal data refers to the definition in Article 4(1) of the GDPR, and the concept of processing to the definition in Article 4(2) of the GDPR.[14]

In the vast majority of the reviewed OSS decisions, there is no doubt whether the data processed is *personal data*, as the cases concern names, email addresses, financial transactions, phone numbers, etc.

Regarding the distinctions between personal data and business matters or legal assessments and documents, the OSS decisions are consistent and in line with the EJC rulings in C-141/12 and C-372/12, and these joined cases seem to have provided sufficient guidance.[15] An example referring to this EJC case law is OSS 2022:407. OSS 2022:407 arose from a complaint regarding water leak damages in a residence where the data subject lived. The data subject requested, among others, a copy of the documentation relating to the leak damages. The LSA stated that this part of the request could not be considered a request for access to personal data.[16]

Further, information with subjective elements does not seem to cause any significant interpretation issues either. OSS 2020:108 stated, for example, prior to the ECJ ruling in C-307/22, that medical assessments were personal data (following the reasoning of C-434/16 and recital 63 of the GDPR).[17]

[14] See further EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, page 31-
[15] Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081.
[16] See about OSS 2022:407 also Section 3.5.2.
[17] Case C-307/22, FT v DW, ECLI:EU:C:2023:811 and C-434/16, Peter Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994.

In cases regarding personal data relating to online behaviour, such as activity logs and search activities, where the data subject was identified via a username, a verified email address, an allocated/assigned ID or a similar piece of information, the ECJ case law has also been followed quite consistently, and the definition of personal data has been interpreted broadly. An example hereof is OSS 2023:809 regarding the collection of browsing data from Internet users via cookies stored on their terminals when they visited the controller's partners' websites. As a unique identifier was assigned to the data subject, enabling the controller to recognise them during subsequent visits to the partner's (and joint controllers) websites, the LSA found that, although the controller did not directly hold the identity of the data subjects using the devices on which the cookies were installed, the controller was able to re-identify individuals by reasonable means. Subsequently, the data was to be regarded as personal data within the meaning of Article 4(1) of the GDPR. [18]

In some areas, the OSS decisions provide more detailed insights than the case law from the ECJ, especially on the varying data protection issues arising in online environments. Notably, several questions regarding the definition of personal data have been examined in cases regarding fake online profiles and attempted identity thefts for financial gain.

Here, the OSS decisions suggest that personal data generated by impersonating or hacked profiles is to be considered as data related to the impersonated data subject, cf. OSS 2023:685 regarding social media and OSS 2023:962 regarding an online forum.[19] This also seems to apply to identity thefts in contexts other than social media, cf. OSS 2022:527. In the latter, OSS 2022:527, the data subject received a registration and shopping cart notification, a newsletter and a survey email. The data subject, therefore, contacted the controller by telephone and email and requested information as the data subject had not registered an account with the controller. It is implicit in this OSS decision that the data subject, as a concerned and impersonated natural person, had the right to access under Article 15 of the GDPR.

However, this decision includes a condition that the profile or identity must appear to the controller and third parties as a profile that actually pretends to be the data subject. Online parody profiles are therefore not regarded as impersonation, cf. OSS 2023:792. The legal significance hereof is not clearly stated in the amicable settlement in said OSS 2023:792 but points clearly towards the understanding that a data subject cannot gain access pursuant to Article 15 to the data generated during parody activities as these do not aim to pretend to be the data subject.

OSS 2023:784 illustrates the variety of scenarios regarding online profiles and access under Article 15 of the GDPR even more. In OSS 2023:784, the data subject set up a profile on a social network under an assumed (fake) name. Ten years later, he wanted to change the profile into a genuine profile in his own name. The account was disconnected as the social network's policies did not allow fake profiles. He, therefore, requested access pursuant to Article 15 of the GDPR, which he was granted.[20]

As mentioned initially in this subsection, Article 15 GDPR only applies if the personal data, at the time of the request, is *processed* by automated means (digitally) or is intended to form part of a filing system, cf. Article 2(1) of the GDPR. The interpretations of the processing definition in Article 4(2) of the GDPR do not seem to cause difficulties in any of the reviewed OSS decisions. However, in some cases,

[18] The LSA referred to the ECJ ruling of November, 24, 2011, C 70/10 and ruling of October, 19, 2016, C-582/14.
[19] Similarly, but not as clearly in 2023:1084.
[20] Regarding the definition of personal data in relation to online communications involving incoming and outgoing messages, see Section 3.5.2.

misunderstandings in communication lead to the controller erasing the personal data after receiving the request for access. This happened in the abovementioned OSS 2023:962, revolving around a personal data breach that affected an online forum (website). The data subject had requested access and inquired about whether personal data related to a specific profile had been affected by the personal data breach (a profile created via the email used by the data subject). However, he also claimed that someone else had created the account using his email address. The controller then informed the data subject *that* the account would be deleted as it had been created fraudulently, *that* the username and IP address were personal data of a third party, and explained *that* it was impossible to identify the exact data affected by the breach due to the nature of the incident.[21] The LSA stated, among others, that as the data subject's account – or the account registered via his email address – was active during the access request, the erasure of personal data had not been justified.

As briefly described above in Section 2, Article 15 of the GDPR contains three components. These are the subjects of the following three subsections: confirmation as to whether personal data related to the data subject is processed or not (Section 3.2), access to personal data related to the data subject if such data is processed at the time of the data subject´s access request (Section 3.3) and information about the processing and the data subject´s other data protection rights (Section 3.4).

3.2.Confirmation on whether personal data is processed

When a data subject makes a request for access to personal data, the controller is, as a first component of the response, obliged to inform whether or not the controller processes personal data concerning them, cf. Article 15(1) of the GDPR. If the controller does not process any personal data relating to the natural person requesting access, the controller is only to confirm this. If the controller, on the other hand, processes personal data relating to the data subject, the controller must confirm this activity unless limitations or restrictions apply under Articles 12(5) GDPR or 23 GDPR.[22] The latter can be confirmed separately or encompassed as part of providing a copy of the processed personal data and the required information on the processing.

A few of the OSS cases regarding confirmation bear the markings of the data subject's mistrust of the data controller's response that personal data is not processed at the time of the request for access. Others are related to untimely erasure of data; see sections 3.1 and 3.3. The majority of the OSS decisions on the "confirmation" aspect stem from a lack of response from the data controller, thereby violating Article 15(1) and Article 12(3) of the GDPR. These violations can be observed to happen due to staff forgetting to respond, unclear internal procedures and designation of roles in the controller's organisation to handle access requests, simple misunderstandings in the communication between the data subject and the data controller, or responses simply getting lost in spam filters or misplaced, see as examples OSS 2020:159, OSS:2019:58, OSS:2020:131 and OSS 2021:209.[23] In the latter, the data subject participated in a selection procedure for pilots and requested access after being notified that he had not passed the selection procedure. The data subject claimed before the LSA that the controller had not reacted to the request. The controller, on the other hand, claimed to have informed the data subject that all personal data had been deleted before the request. As it could not be proven whether the data subject had or had not received the

[21] The controller also referred the data subject to a notification on the website's blog post for information on the data breach.
[22] Article 15(3) of the GDPR do not apply in this context.
[23] Similarly and more recently 2024:1105, OSS 2024:1155 and 2024:1156.

controller's e-mail with the information, and the data subject received the confirmation during the proceedings, the LSA dismissed the case.

3.3.Access to and copy of the personal data

Data subjects are entitled to access all personal data relating to them, which are processed by the controller at the time of the request, cf. Article 12(1) and, Article 15(1) and (3) of the GDPR if no limitations or restrictions under Article 15(4) or Article 12(5) of the GDPR apply in the case. The personal data is to be complete, up to date and comprise the actual information or personal data held about the data subject, corresponding as closely as possible to the state of personal data processing when receiving the request, cf. C-487/21 and C-312/23.[24] According to Article 15(3) of the GDPR, the controller is to provide a copy of the personal data processed at the time of the request, and the first copy is to be free of charge. If the request for access is submitted electronically, the information shall be provided electronically if possible unless otherwise requested by the data subject, cf. Article 12(3) of the GDPR. According to Article 15(3) of the GDPR, the electronic means for access have to be commonly used unless otherwise requested by the data subject.

The majority of complaints regarding access to or copies of personal data at the time of the request in OSS decisions seem to occur because the personal data has been *erased*; for example, OSS 2020:152 and OSS 2020:159. OSS 2020:159 is an illustration. In OSS 2020:159, the data subject requested access to all personal data relating to a specific booking reference, including call recordings. The controller, a flight company, provided all personal data except a written copy of the call recording as the recording had been deleted in accordance with company policy, and they had been unable to retrieve it. The erasure did, however, happen after the request for access due to an unintended delay in processing the request in the controller's organisation (the agent who had initially handled the request had not finished the task at the end of his work day and forgot to re-assign the access request to another agent before departing). Consequently, the LSA stated that Article 15 of the GDPR had been violated as the controller failed to provide the data subject with a copy of the personal data that was undergoing processing at the time of the request.

Further, the reviewed OSS decisions indicate that it is not unusual for controllers to refuse specific *electronic means* requests from the data subjects due to the need for appropriate security measures. An example is OSS 2021:270, in which the data subject requested access to his personal data via e-mail. The controller refused as the controller assessed that it was impossible to ensure the proper protection of the personal data if it was sent by e-mail. Instead, the controller made the personal data in question available on the data subject's account at the controller. The LSA initially stated that a controller is responsible for and has to be able to demonstrate that personal data is being processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, cf. article 5(2)(f) of the GDPR. Further, the LSA stated that in accordance with Article 32 of the GDPR, the controller is to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. As the LSA found no grounds to question the controller’s statement regarding the appropriate security level, the LSA did not find a violation of the GDPR and had no grounds for ordering the controller to respond to the request by e-mail.

[24] C-487/21, F.F. mod Österreichische Datenschutzbehörde, ECLI:EU:C:2023:369 and C-312/23, Addiko Bank vs. Agencija za zaštitu osobnih podataka.

The above-described OSS 2021:270 is somewhat typical as these cases mainly revolve around difficulties in using self-service systems or data subjects asking for access to be provided via email. This tendency might be connected to an underlying problem of *varying levels of digital skills* within the European populations. This potential theme of some data subjects' lack of digital skills to effectively exercise their rights via electronic self-service systems is not touched upon in any of the reviewed OSS decisions.[25]

Finally, regarding the component of Article 15(1) in question in this subsection, it is notable and somewhat surprising that the reviewed OSS decisions do not suggest an inner friction between the requirements of providing, on the one hand understandable data, and, on the other hand, complete access to data. In other words, in the reviewed OSS decisions, dilemmas avoiding complexity to ensure that the personal data and information are understandable seem to be absent as the data subjects appear to be able to handle and understand the provided personal data.[26]

3.4.Contextual information

As described in overall terms in Section 2, the controller is not only obliged to provide access to the personal data, which is processed at the time of the request. Data subjects also have the right to be presented with additional information about the processing of the personal data and to be informed of other relevant rights in Chapter III of the GDPR, cf. Article 15(1). Further, data subjects must be informed of any appropriate safeguards if the personal data are transferred to third countries or to an international organisation, cf. Article 15(2). This information has to accurately, yet clearly and understandably, describe the ongoing processing, measures and applicable rights at the time of the request and reflect the processing operations carried out in relation to the specific data subject requesting access.

According to the first part of Article 15 of the GDPR, the controller has to describe the purposes of the processing, the categories of personal data and the recipients or categories of recipients to whom the personal data have been or will be disclosed (in particular recipients in third countries or international organisations), cf. Article 15(1)(a), (b), (c).

Describing the *purposes of the processing* seems, in particular, to be an issue if the controller pursues multiple purposes or/and engages in extensive personal data sharing. OSS 2019:42 illustrates this. In OSS 2019:42, the information from the controller pursuant to Article 13 stated that the personal data were processed (solely) for participating in a prize competition. However, the LSA stated that this information was incomplete because the personal data was to be transferred to sponsors for marketing purposes.

Regarding the *recipients or categories of recipients*, the controller is to inform of specific recipients when such detailed information is possible, cf. C-553/07 and C-154/21.[27] This is also stated in, among others, OSS 2022:367, in which the controller did not provide information about the recipients to whom the data subject's personal data had been disclosed. The controller was of the opinion that it was sufficient to

[25] See OSS 2023:739 as an example of what appears to be successful guidance of the data subject. See also recent examples of data subject having difficulties in using self-service systems OSS 2023:1020, OSS 2023:1055, OSS 2023:1086, OSS 2024:1246, OSS 2024:1235, and 2023:1090.

[26] Further regarding understandable information, see EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, page 16-17.

[27] C-154/21, RW v Österreichische Post AG, ECLI:EU:C:2023:3.

specify the categories of recipients. The LSA highlighted that storing information on the (actual) recipients is necessary to comply with the controller's obligations under Articles 5(2) and 19 of the GDPR. Therefore, Article 15(1)(c), read together with Article 19 and the principles of fairness and transparency in Article 5(1)(a), provides the data subject with a right to, especially when explicitly requested, obtain information about the actual recipients to whom the personal data have been or will be disclosed. This applies, the LSA stated, unless it proves impossible or involves a disproportionate effort for the controller to provide the information. As the data subject explicitly requested information about actual recipients, and the controller had not proven impossibility or disproportionate effort, the controller had violated Article 15 of the GDPR.[28]

Further, according to the following parts of Article 15(1), the envisaged *period for which the personal data will be stored*, or, if not possible, the criteria used to determine that period is to be described in the information to the data subject (Article 15(1)(d)). According to the reviewed decisions, this information has to be immediately understandable to the data subject. In OSS 2019:42, the controller informed the data subject that the period followed the national statutory retention periods. The LSA stated that such a reference to a retention period specification in legislation is insufficient to comply with Article 15(1). The storage deadlines or the criteria for determining this duration have to be explicitly described. The LSA added that it: "is not up to the data subject to check which specific statutory retention periods apply to the processing of his personal data."

The above-described information is to be given along with – if applicable and not restricted by EU law or national regulation in accordance with Article 23 of the GDPR – information on the right to request from the controller rectification or erasure of personal data, restriction of processing of personal data concerning the data subject and/or to object to the processing. Along with the information on these *rights in Chapter III of the GDPR*, the controller is to provide information on the right to lodge a complaint with an SA, and if the personal data are not collected from the data subject, any available information as to their source (Article 15(1)(e), (f), (g)).

Here, the OSS decisions provide some clarity regarding the specification of *the competent SA*. In OSS 2019:42, the LSA stated that "in principle, the complainant can judge by himself which shall be the Data Protection Authority for filing his complaint. In accordance with the legislator's requirement under Article 12(1) GDPR that the person responsible for data processing should facilitate the exercise of his rights in accordance with Articles 15 to 22 of the GDPR, the Liechtenstein SA pronounces the recommendation that the competent supervisory authority or at least the criteria for the designation of the supervisory authority shall be stated in the controllers' information pursuant to Art. 15 GDPR. However, there is no legal obligation to do so."

Finally, the mandatory minimum information required in Article 15(1) includes the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 15(1)(g). Here, the OSS register does not provide any decisions able to shed light on how detailed the description of the underlying logic has to be. C-203/22, currently pending before the ECJ, will hopefully bring some clarification of this part of Article 15(1) in the forthcoming years.[29]

[28] See also regarding OSS 2022:367 in Section 2.

[29] Case C-203/22, CK, ECLI 2024:745. Opinion of advocate general Richard de la Tour was delivered on 12 September 2024.

As briefly described above in Section 2, some limitations and restrictions to the data subject's right to access are set out in the GDPR. These limitations and restrictions are the theme of the following subsection (subsection 3.5), divided into a short introduction, followed by sections on Article 15(4) and Article 12(5), respectively.

3.5.Limitations and exceptions to the right to personal data and contextual information

3.5.1. Introduction

As mentioned in Section 2 and indicated in Section 3, OSS decisions also provide some insights into the application of the limitations and exceptions of the right to access in Articles 15(4) and 12(5) of the GDPR. Further limitations may potentially be laid down in EU law or national legislation pursuant to Article 23 of the GDPR. The latter is, however, only briefly mentioned in very few OSS decisions, and the reliance on Article 23 of the GDPR is not questioned in these cases.

Article 15(4) and Article 12(5) may only *apply to some of the information* under Article 15(1) and (2).[30] If this is the case, the data subject is to be provided with the information to which the exception in question do not apply. A couple of OSS decisions are related to the theme of providing the remaining information when some information are exempt from access. OSS 2022:517 is an example of this in relation to Article 15(4). In this case, the data subject's social network account was disabled due to an alleged serious violation of the Terms of Service. During the investigation, the controller shared the reasons for the data subject's account suspension with the LSA and argued that providing the data subject with access to the data may be a security risk for others and, as such, could adversely affect the rights and freedoms of other users according to Article 15(4) of the GDPR. The complaint was amicably settled by holding back the potential damaging data but providing the data subject with access to the remaining personal data to which Article 15(4) did not apply as these personal data was unrelated to the reason for the disablement, and the parties agreed that access hereto would not infringe on any person's rights and freedoms.

3.5.2. Article 15(4) GDPR

It follows from Article 15(4) of the GDPR that the right to obtain a copy of one's personal data shall not adversely affect the rights and freedoms of others. The wording of the provision may suggest that this limitation only applies when access is provided as a copy of personal data pursuant to Article 15(1). The EDPB guidelines on access do, however, suggest a broad interpretation, implying that the restriction also applies when access to personal data is provided by other means, for example, on-site access.[31]

The *rights and freedoms of others* are probably to be interpreted broadly as recital 63 of the GDPR preamble only exemplifies by mentioning trade secrets, intellectual property and copyright. OSS 2022:457 takes positions in relation to the protection of business secrets and the protection of communications. The background for the case was that the data subject was excluded from online gaming at the controller's platform due to alleged cheating. The person in question was informed of the reasons for the exclusion and the time of the alleged cheating. He requested access under Article 15 of the GDPR. The controller did, among others, exclude the anti-cheat-related information and in-game chat messages from access.

[30] As opposed to Article 12(5) of the GDPR and – depending on the chosen design of national legislation – Article 23.
[31] EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, page 52.

The information on anti-cheat information was withheld as the controller did not consider this personal data and, at the same time, assessed that revealing this information could reveal how to cheat and thereby harm the company and other players. The in-game chat messages were not provided as this, in the view of the controller, would involve the disclosure of third-party personal data. The data subject filed a complaint to the LSA as the provided information, in his view, was incomplete. The LSA initially stated that a data controller may refuse to comply with an access request from a data subject if one of the exceptions to the right of access under Article 15(4) of the GDPR or if Section 22 of the national legislation (the Danish Data Protection Act: DDPA) can be invoked. Therefore, in this case under Danish law, Article 15(1) of the GDPR does not apply if the data subject's interest in the personal data relating to him or her and the information on the processing is found to be overridden by essential private or public interests. These can, among other things, be business secrets or the interests and rights of people involved other than the data subject. However, Section 22(1) of the DDPA can only be applied if there are decisive interests at stake and an obvious danger that the said interests will be adversely (negatively) affected. In OSS 2022:457, the LSA found that the controller had been entitled not to provide further information about anti-cheat measures, cf. Section 22(1) of DDPA. There was, however, no legal basis for not providing a copy of chat messages sent directly to and from the complainant regarding the in-game chat messages. Messages sent between others in the forum chat could maybe, on the other hand, be withheld according to Article 15(4) of the GDPR. A relevant element in the controller's assessment hereof was, according to the LSA, that such chats may be in different languages and in a jargon that may justify an exception from access in conjunction with the fact that other participants in the conversions may expect a certain degree of confidentiality regarding messages 'sent in the heat of the moment'.

Connected to the above-mentioned interest in the protection of communications are the OSS decisions on recorded phone calls. These decisions are well suited to shed light on the application of Article 15(4). In OSS 2021:254, which is also mentioned in Section 3.1, the data subject had contacted the data controller several times in writing and via telephone regarding a purchased car. On November 12, 2018, the data subject requested access under Article 15 of the GDPR to, among others, recorded telephone calls. The controller did not provide copies of these recordings as the controller argued that the voices of the controller's employees were also on the recording. As an alternative, the controller offered the data subject the opportunity to visit the controller's premises and listen to the recordings. The LSA stated that Article 15(4) of the GDPR was not applicable as the recording of a person doing a job for the controller cannot be considered to adversely affect the rights and freedoms of the employee[32]. Further, the LSA interpreted Article 12(1) in conjunction with Article 15(3) and concluded that the data subject had the right to a copy of the recordings, and the offer to listen to the recordings was insufficient to comply with said articles in the GDPR. Here, the LSA also referred to Article 8(2) of the European Charter of Fundamental Rights and stated that any restrictions on the right to access must be narrowly interpreted.[33] OSS 2022:407, as mentioned in Section 3.1, goes along the same lines. OSS 2022:407 arose from the previously described case regarding water leak damages in a residence where the data subject lived. As the data subject, among others, requested access to a recorded telephone call between the data subject and the company employees, a similar theme as in OSS 2021:254 was a part of this case as well. With reference to ECJ case law, the LSA simply stated in OSS 2022:407 that the right of access provided for in Article 15 aims to ensure that a data subject has access to information about the

[32] In that regard, please see Example 35 of EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, for similar facts.
[33] C-579/21, J.M, ECLI:EU:C:2023:501 focuses on consultation operations carried out on a data subject's personal data and the dates and purposes of those operations and is therefore not fully comparable to OSS 2022:407.

processing of and a copy of the personal data processed in order to be able to verify the accuracy of the personal data and whether they are processed in accordance with the provisions of the GDPR.[34]

3.5.3. Article 12(5) GDPR

According to Article 12(5) of the GDPR, when a controller receives a manifestly unfounded or excessive request, the controller may either reject the request or charge a reasonable fee for accommodating it. Here, OSS decisions provide some examples able to guide the interpretations of the concepts of "manifestly unfounded" and "excessive", respectively.

Manifestly unfounded requests mean that the requirements of Article 15 of the GDPR are clearly and obviously not met. As there are few prerequisites for requests for the right of access, this has a somewhat limited scope. One of the reviewed OSS decisions does, however, point in the direction that the concept of "manifestly unfounded" may include data subjects' abuse of the law. In OSS 2021:218, the data subject and his family had claimed reimbursement of more than EUR 280 in connection to a booking. In a request for access to personal data under Article 15 of the GDPR, the data subject requested payment data in connection with his payment card, e-mail correspondence and other data relating to the disputed booking. He also stated that he was willing to refrain from the access request if the controller concluded that it would be more economically beneficial to comply with the claim for reimbursement. On the one hand, the LSA highlighted that the right to access in Article 15 of the GDPR is not forfeited by the fact that information is sought for a purpose other than the purposes mentioned in Recital 63 of the GDPR. On the other hand, abuse of rights can be assumed if it is apparent from special circumstances. As the data subject openly expressed that he would be willing to refrain from requesting the information if his substantial demand for a refund was met, such circumstances were present in the case.

Whether a request may be regarded as *excessive* depends on all relevant circumstances and does not only apply to repetitive requests. If the controller has designed a possibility to access personal data by electronic means or by remote access to a secure system (self-service systems), repetitive use hereof is not likely to be regarded as excessive as it doesn't strain the controller. According to the reviewed OSS decisions, electronic self-service systems are frequently used, especially if personal data is continuously collected, processed or disclosed on a large scale. This, of course, means that the exception on excessive requests is rarely applied.

The above tendency and the reviewed OSS decisions do, however, point in the direction of a potentially overlooked challenge. Complications arise when data subjects lose or forget their account passwords, lack the digital skills to use self-service systems, or their accounts are hacked. This might indicate an increasing need for the user-friendly and inclusive design of electronic self-service systems along with procedures and organisational design that are able to handle atypical scenarios if all data subjects are to be supported in the effective exercise of their data protection rights.

In the following, the focus will not be on the specific elements of Article 15 of the GDPR and the connected OSS decisions. Instead, some short comments on the importance of Article 12 are offered as a perspective element.

[34] See about OSS 2022:407 also Section 3.1.

4. Perspectives on Article 12 GDPR

To ensure the effective exercise of data subjects' rights, Article 12 of the GDPR sets out a series of requirements with the common denominator that the requirements specify and detail the broad obligation of controllers to facilitate the exercise of the data subjects' rights. Therefore, it is logical that most of the reviewed OSS decisions related to Article 15 are also concerned with Article 12 of the GDPR.

According to the first sentence in Article 12(1) of the GDPR, the controller shall take appropriate measures to communicate to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for information addressed specifically to a child. Further, the controller is to facilitate the exercise of data subject rights, cf. Article 12(2) of the GDPR. In other words, controllers are to provide appropriate and user-friendly communication channels that the data subjects can easily use. However, the data subject is not obliged to use these specific channels and may instead send the request to the controller's official contact point. [35]There are no specific requirements on the request format either, and data subjects do not need to mention GDPR or otherwise argue or justify their need for insight; see, for example, OSS 2020:120.

Further, Article 12(3) states that requests under Articles 15-22 shall be answered without undue delay and, as a general rule, within one month. The exception to the general rule of one month maximum processing time is that it may be extended by two months if this is necessary due to the complexity and/or number of requests. If the controller postpones with reference to such complexity or amount of requests, the postponement must be justified to the data subject before the expiration of the one-month rule. The aggregated three months constitute an absolute time limit. According to the EDPB guidelines on access and OSS 2022:359, reasonable grounds to doubt the data subject's identity will, however, suspend the countdown as long as the controller requests adequate information without delay.[36]

Based on the reviewed cases, human errors or lack of adequate procedures and policies can lead to controllers exceeding the *time frames* in Article 12 of the GDPR, see OSS 2019:6, OSS 2019:70, OSS 2020:81, OSS 2020:104 and OSS 2019:61.[37] Misunderstandings in communication between controllers and data subject or confusion with substantive matters in the relationship between the parties also seem to matter. See, for example, OSS 2019:15, OSS 2019:33 and OSS 2023 816. In the latter, OSS 2023 816, the problem was (simply) different spelling of the data subjects' names in Gaelic and English, respectively.

The *means for identifying the data subject* according to Article 12(6) and the broader requirement of data security, cf. Article 5(1)(f) and 32 of the GDPR proportionally seem to cause some difficulties in the daily application of the GDPR.[38] For example, requests for official documents are not uncommon, even when other means of verification or identification are available to the controllers; see, for example, OSS 2022:341 and OSS 2022:334.[39] In the latter, the controller required the data subject to prove her identity before access could be granted. This was, according to the controller, to be done by providing two of the following documents: passport, identity card or driving license showing the date of birth; social security or national insurance card; utility bill not older than three months. These credentials were, however, not required to create or log in to the online profile, which the request for access revolved around.[40] The LSA

[35] EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, pages 3 and 23-24.
[36] EDPB Guidelines 01/2022 on data subject rights - Right of access, April 17, 2023, page 50.
[37] Recent example in OSS 2024:1242.
[38] Recent example in OSS 2024:1236.
[39] Probably similar in 2023:1044 (amicable settlement).
[40] See Recital 57 of the GDPR.

stated that additional information can only be gathered if there is reasonable doubt about the data subject's identity. See similar OSS 2020:166.

5. Concluding remarks

The above analysis, combined with general observations during the review of the gathered OSS decisions, can be summarised in short form:

- After reviewing the OSS decisions, the general impression is that the enforcement of Article 12 significantly supports data subjects in effectively invoking their right to access under Article 15 in their everyday lives in the EU member states.
- Almost all the OSS decisions reviewed originate from complaints and revolve almost exclusively around private sector data controllers and processors.
- The majority of the reviewed OSS decisions regarding access revolves around social media and online environments, often combined with commercial elements.
- The OSS decisions regarding Article 15 of the GDPR touch upon all the three components of the right of access, and the number of OSS decisions relating to the right of access is high, which indicates that SAs are familiar with cooperating on this issue.
- In many OSS decisions on the right of access, SAs do not automatically impose corrective measures. On the contrary, they often dismiss or settle the case if the matter has been resolved during the course of the proceedings.
- OSS decisions often rely on the (growing) case law of the CJEU in the field of the right of access and have recently started to refer to the EDPB Guidelines on the right of access.
- OSS decisions can provide guidance on interpretation issues related to Article 15 of the GDPR, especially regarding themes that arise in online environments, such as how to handle impersonation in varying contexts and for different purposes.

Annex 1 - List of OSS decisions included in the Case Digest

2024 (5)
OSS 2024:1246
OSS 2024:1242
OSS 2024:1235
OSS 2024:1155
OSS 2024:1236

2023 (16)
OSS 2023:1090
OSS 2023:1086
OSS 2023:1084
OSS 2023:1055
OSS 2023:1044
OSS 2023:1020
OSS 2023:978
OSS 2023:947
OSS 2023:946
OSS 2023:864
OSS 2023:962
OSS 2023:828
OSS 2023 816
OSS 2023:790
OSS 2023:739
OSS 2023:685

2022 (9)
OSS 2022:1105
OSS 2022:527
OSS 2022:517
OSS 2022:457
OSS 2022:407
OSS 2022:341
OSS 2022:334
OSS 2022:268
OSS 2022:367

2021 (4)
OSS 2021:270
OSS 2021:254
OSS 2021:218
OSS 2021:209

2020 (10)
OSS 2020:167
OSS 2020:166
OSS 2020:159

OSS 2020:157
OSS 2020:152
OSS:2020:131
OSS 2020:120
OSS 2020:108
OSS 2020:104
OSS 2020:81

2019 (8)
OSS 2019:70
OSS 2019:61
OSS:2019:58
OSS 2019:46
OSS 2019:42
OSS 2019:33
OSS 2019:15
OSS 2019:6


edpb
European Data Protection Board