FEDMA position paper

November 2019

FEDMA contribution to the EDPB workshop on Data Subject Rights

In line with FEDMA priorities, FEDMA is reaching out to the EDPB to provide some input on data subject rights (A) and legitimate interest (B). FEDMA defends a thriving environment for marketers powered by user's trust. For this reason, FEDMA and its DMA members are available to further discuss this paper with the EDPB and national data protection authorities so we can continue to find the right balance between consumer and industry interests.

A) Data Subject Rights

General Comments

i) **Guidelines on data subject rights are an opportunity for the EDPB to put forward a balanced approach to the interpretation of these rights within the wording of the GDPR. Some issues will be solved by Courts.**

ii) **Data Subject Rights (DSR) serve, in essence, as a way of data subjects exercising control over and checking the processing of their personal data by controllers.** For example, the right to have inaccurate personal data corrected and/or completed under Article 16 means that data subjects can ensure that controllers are using up to date personal information in their processing.

iii) **Data subject rights are not always absolute rights.** For example, the controller can refuse the right to erasure if the controller is required to keep the personal data for a legal obligation such as the need to keep information for a tax authority.

iv) **We would like to share in particular the situations here below where a balanced approach between the interests of the controller and the rights of the data subject (DS) must be found.**

Data Subject access requests (DSAR)

Relation article 12 and 15

Our industry sees **layered information as an indispensable tool**, also for the offline world, to provide data subjects with the relevant information at the right place and time.

The information provided in an answer to a DSAR is very different from the information provided under article 13 and 14 of the GDPR. Article 13 and 14 will provide categories of the data (e.g. name, address) and in a layered manner. The data provided under article 15 is specific and can be more technical. For example[1]:

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

"An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to your key or index to explain this information, it would be impossible for anyone outside your organisation to understand. In this case, you are required to explain the meaning of the coded information. However, although it is good practice to do so, you are not required to decipher the poorly written notes, as the GDPR does not require you to make information legible."

Individualization of information

Please find here example from ICO:

"You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. You are not required to do this even if the person who receives it cannot understand all of it because it can be understood by the average person. However, it is good practice for you to help individuals understand the information you hold about them."

Third party services

Controllers/processors should respect three steps:

1) check the identity of the data subject (DS),

2) check if the intermediary is fully enabled to exercise rights on behalf of DS and if DS conferred necessary powers to intermediary

3) assess DS full awareness of data transfer to intermediary and purpose of transfer (on basis article 13 GDPR).

In Germany, mandates were not substantiated enough for the intermediaries to exercise the mandate. However, the debate over the possibility for a data subject to provide a mandate to an intermediary is still open.

Please refer to data portability for on in this document.

Need for controllers to be able to check identity of data subject making DSAR

There should be the possibility for the controller to check the identity of the data subject. Controllers could be at risk of personal data security breaches if, depending on the nature and quantity of data, they do not assess the risk and check the identity of the data subject, in one way or another. If Controllers do not do this then they could inadvertently disclose a large volume of personal data subject by sending the response to the DSAR to the wrong data subject. The Dutch data protection authority's interpretation is that in most cases asking for a copy of a passport or identity card is not permissible. However, in other countries, it is. FEDMA supports the position taken by the UK data protection authority. Their view is that the controller should only ask for the data subject making the DSAR to prove their identity if it has doubts about whether or not the individual making the data subject access request is the data subject. The key is proportionality to the risks of disclosing the personal information to another individual.

Identity can be checked in many ways. For example, by asking for data subject to log into an account, provide postal address or ID paper, responding to an email sent to the email account linked to the data subject request, or answering a secrete question.

Possibility to request data subject further information: scope of DSAR

The controller/processor can ask the data subject (DS) to specify the data which he/she is really interested in accessing. The purpose of the DSAR is important to determine the scope of the personal data to be provided to the data subject. The controller can always ask the data subject making the DSAR if they want all the personal information which the organisation holds about them or just a particular document. **In many cases, the data subject may be happy just to get a copy of one document rather than all the personal information the organization holds about them. This request also helps process the request and provide the relevant information faster to the data subject.**

The first SAR response may be a summary or a standard SAR response. Recital 63 also says „Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates". **That way, it does not have to be the case that whenever a SAR is raised, say by a disgruntled employee, that the HR department has to go on an endeavor of going through non-structured data. Going through non-structured data is hugely time consuming.**

The connection between DSARs and 1) right to rectify 2) right to erasure and 3) right object to processing is essential.

DSARS should not become a gateway for all data subject's rights regarding their relationship with a controller. Controllers may need to remind data subjects that they have other rights under the GDPR namely 1) right to be informed 2) right to request rectification 3) Right to erasure and 4) right to object to processing of their personal information.

Data subjects may think that DSARs are the only right they have because of all the publicity surrounding such requests, it is quite possible that the data subject may by exercising one of their other rights under the GDPR achieve what they wanted to do through the DSAR in a quicker and more effective way.

Asking the data subject (or the intermediary) for more information is particularly recommended in the following situations:

- **blanket access request e.g. templated requests**
- **blanket requests from intermediaries**
- **blanket access from a non-regular customer.**

Conflict DSAR and other data subjects' rights:

Other data subject's rights must be respected. **This can be hugely time consuming**. Indeed, not all data are stored in a structured database or a particular directory on a server. A DSAR implies potentially going through all the unstructured data, for instance emails also those that are in the email inbox/archive of colleagues, data in the backup file, etc.), which is hugely time consuming, **especially in the context of HR requests** for long serving employees.

Examples where other data subject's right must be taken into account:

- unstructured data (references in internal chats/emails. Mention in meeting minutes, Mention on internal newsletter (Ms. Xyz (ex-employee) has ran a marathon for a charity), Appearance of the person in old outlook calendars of her colleagues, Pictures from company events and parties, sales call log ("today I (Ms. Xyz) visited prospect X. Prospect X runs an annual campaign for their summer collection in May. Contact him again in February to follow up").

- video surveillance (other faces have to be blurred),

- in a client's account some of them have their address book stored in it as well (data has to be removed)

DSARs and archived and back- up data

- Archived data

Controllers need to be reminded that if they archive data and the data subject cannot be identified from the archived data then there is no need to disclose it in response to a DSAR (article 11). For example: pseudonymized data without the key.

Also if the archived data is simply a copy of personal data which is already stored elsewhere then the Controller will not have to provide the data subject with a further copy of that information in response to a DSAR but simply a note that the same information is held on the archived system.

- Back up data

If the back-up data is simply a copy of personal data which is already stored elsewhere then the Controller will not have to provide the data subject with a further copy of that information in response to a DSAR but simply a note that the same information is held on the back-up system.

DSARs and technical, automatic data:

The challenge with this data is that:

- It needs to be explained to the data subject (see previous example from ICO). Hence, the importance of being able to ask the data subject which document or information they are requesting.
- Even if the data is pseudonymised and the organisation does not have the key, the data is considered as personal data (recital 26 GDPR).
- The technical or automatic data may not be personal data (e.g. if the data subject is not a registered customer and no cookies were dropped, the data will not be personal). Article 11 applies.
- There is a risk that the technical or automatic data may identify another data subject (e.g. if the data identifies a PC rather than an individual. If the customer is registered with the controller, then the controller may be able to provide access to the personal data. If the customer is not registered with the controller, then article 11 will likely apply).

Use of article 11

Article 11 helps drive the principles of data minimisation and anonymisation.

DSARS and fees

Controllers need to be reminded that they can charge an administrative fee for responding to a DSAR if it 1) manifestly unfounded or excessive or 2) a data subject request further copies of the same information which the Controller has already provided in response to a DSAR.

DSARS and future technologies

Controllers need to be reminded to think carefully about DSARs when considering using new technologies such as Artificial Intelligence (AI) which are data rich and rely on combining data from a number of sources. Much of the data used in AI technologies is likely to be copies of personal information held in other systems of the Controller. What counts is not so much the access to all the data but the logic involved, the significance and envisaged consequences for the data subject and the possibility of human intervention to review the decisions made by the AI system to protect the interests and rights of the data subject (article 13, 14, 22). Article 22 applies to AI only in cases where AI leads to a decision with legal effect or similarly significant effect.

Data erasure

Data erasure is a **qualified right**. **It may be in the interest of the data subject to have the data suppressed rather than erased. The controller must inform the data subject that a permanent erasure cannot be achieved by deletion, as deletion of the personal data would lead to the removal from the in-house or national suppression lists and consequently would not achieve the DS' goal. Blocking the data is advisable. The controller can request that the DS contacts them once more to confirm whether they wish for all the personal data to be deleted, including the personal data in the controller's in-house suppression system. Holding personal data for the purpose of blocking Direct Marketing communication is lawful on the basis of legal obligation under the GDPR.**

Data subjects may request for data erasure where in fact, they simply wish to opt out of direct marketing.

Data erasure must be balanced with article 17.3.b.

For example: a consumer does not pay an item and then requests for the provider of the item to erase the personal data relating to him/her. This is a case of tentative fraud.

For example: a court order is sent to an organization, specifying that a data subject has dementia and that the organisation should engage in contracts with this data subject, and then the data subject asks for the data to be erased.

Data Portability

A balance should be found between the data subject's right to port personal data to benefit from a different provider's items and the enrichment of that personal data by the receiving controller. **FEDMA considers that individuals can mandate organisations to exercise their right portability on their behalf, but only for their individual interest. Large scale data portability requests exercised by a business should not be used for the purpose to monetize individual's personal data and build up a competitive dataset with monopolistic dimensions.** There is a fine balance to reach here between (a) individuals porting their data to a new market provider for their own individual benefits (cheaper or more appropriate service/item), which drives market fairness, and (b) a controller orchestrating massive portability requests to become an intermediary between the consumer and the provider. The Italian DPA referred to the EDPB a case which is still under consideration by the EDPB (the Weople App). As explained in the Garante request to the EDPB, the case concerns the applicability of the right

to data portability: an Italian company has indeed proposed itself as an intermediary in the relationship between controllers and data subjects. The company is requesting, on behalf of the data subjects, the personal data held by important business entities, in particular in the large retail sector, in order to bring them together in their own database for data enrichment process. Weople has made numerous data portability requests on behalf of Weople members to retail companies in Italy asking for the transfer of personal data of loyalty card customers of the retail companies from them to Weople if such customers are also members of Weople. The Weople App provides members with money in exchange for their personal data. In FEDMA view, this could lead to new forms of monopolies, new forms of data chains (traditional retailers may end up being in third party situations, without direct access to their customers' data, and not being able to provide better items to their customers).

Right to be informed

Interpretation of article 13 and 14 must also be balanced[2]. As provided in recital 4 of the GDPR, "the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality". The balance provided for in recital 4 of the GDPR, and quoted above, must be reflected in article 13 and 14 and their exceptions. This is why, FEDMA published a position paper to contribute to the discussion on information requirements and reach a balanced approach within the spirit of the GDPR.

B) Legitimate interest

FEDMA encourages the EDPB to organize such workshops in the future and we look very much forward to receiving an invitation to the potential workshop on legitimate interest. We consider this important as discussions at national level challenge the use of legitimate interest as a legal basis for processing of personal data for direct marketing (e.g. profiling, data validation, enrichment). A structured dialogue between civil society, on the one hand, and on the other, key institutions such as national Data Protection Authorities, the European Data Protection Board, the European Data Protection Supervisor, and the European Commission is needed to resolve the issue of whether legitimate interest can be used for profiling where the profiling does not produce legal effects on or similarly significantly affect the data subject.

The legitimate interest legal ground can be used in a wide variety of circumstances, which fall outside the other legal grounds. Most of the other legal grounds have quite narrow and precise instances where they can be used (e.g. necessity for the performance of a contract). However, if an organisation wants to use the legitimate interest legal ground then it 1) must identify a legitimate interest 2) show that its processing of personal data is necessary to achieve its legitimate interest and 3) balance its interests against the individual data subject's rights, freedoms and interests. It is important to note that a third party whom the data subject has not been in contact with (and the data subject may not have any relation with to the party who is processing their personal data) can use the legitimate interest legal ground. However, any third party in such circumstances will need to carefully weigh up such factors in connection with the balancing test in point 3) above.

In our view, the **GDPR allows the use of legitimate interest for profiling on the basis of recital 47, provided the profiling does not have a legal effect or similarly have a significant effect on the**

[2] https://www.fedma.org/wp-content/uploads/2019/05/20190509-FEDMA-position-paper-on-transparency-under-article-14-of-the-GDPR-FINAL.pdf

individual[3]. The organisation would have to factor in the risks to the individual rights caused by the profiling. For example, the second last paragraph of page 17 under section 3.3 « Non-special category data » of the ICO Real Time Bidding report provides that "in any case, reliance on legitimate interest as a lawful basis for processing means that organisations take on extra responsibility for ensuring that the interests, rights and freedoms of individuals are fully considered and protected".

The EDPB has an opportunity when drafting its guidelines on legitimate interests to include a principle based checklist for organisations wanting to use this legal ground for processing personal data under the GDPR. As an example, we would like to refer you to this checklist developed by the ICO. The legitimate interest legal ground is also linked to the accountability principle in that organisations must carry out a balancing exercise between their legitimate interests and individual rights. Organisations must be able to demonstrate the reasons why they believe that they can use the legitimate interest legal ground. A checklist will be more future proof against technological developments than an exhaustive list of situations where legitimate interest should apply. Also, the legitimate interest assessment (LIA) needs to reflect the risk of the processing of the data to the individual rights of data subjects. A principle-based checklist will enable organisations, especially SMEs to adapt their LIA to the level of risk to the individual rights of data subjects posed by their processing of personal data. Finally, a principle-based approach will also leave sufficient grounds for Codes of Conduct wit industry best practices (e.g. Our FAQ which will support our Code of Conduct refers to a more specific LIA questionnaire developed by the Data Protection Network).

Unlike what some guides to the GDPR provide[4], **legal requirements in other legislation than the GDPR should not impact the use of legitimate interest under the GDPR**. **The risk is to jeopardize harmonisation and an EU data protection culture.** For example, processing of personal data for profiling for telemarketing purposes can be done, on the basis of legitimate interest, under the GPDR, if the result of the assessment is positive for the controller. Therefore, the fact that, under the ePrivacy rules prior consent is required in some countries, must not impact the lawfulness of the processing of personal data for profiling on the basis of legitimate interests as provided under the GDPR. A B2C telemarketing theoretical example: Company A wants to promote its products to prospects in 3 countries via telemarketing (Sweden, Germany and UK). All three countries enable processing of data under legitimate interests of company A. However, in Germany, this processing would be forbidden because national marketing law requires prior consumer consent for telemarketing. The processing would be lawful in UK and Sweden where telemarketing is opt-out. A distinction needs to be made between processing of personal data under the GDPR and processing of personal information under the ePrivacy regime. In the example above the profiling of personal data for telemarketing should be allowed under legitimate interests under the GDPR. The fact that Germany has an opt-in system for telemarketing only affects the making of the telemarketing calls under the national implementation of the e Privacy rules, not the processing of personal data under the GDPR used prior to the making of the telemarketing call.

[3] EDPB Guidance on automated decision and profiling p14: the EDPB acknowledges that profiling is possible on legitimate interest, if the risks and interests are properly balanced.

[4] ICO, Legitimate Interest P. 29 (*https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf*); German DPAs (Guide on use of personal data for promotional purpose: P. 5) and Austrian DPA (case: DSB-D130.033_0003-DSB-2019, No. 5).