PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

THE GDPR – DATA SUBJECTS' RIGHTS

4 Data Subjects' Rights

Carlotta Rigotti, Andrés Chomczyk Penedo, Alessandro Ortalda, Paul De Hert (all VUB)

Acknowledgements: The authors thankfully acknowledge the review and suggestions by Rosario Duaso Cales and Saverio Carusso.

This part of the Guidelines has been validated by Willem Debeuckelaere, former President of the Belgian Data Protection Authority & Deputy Chair of the European Data Protection Board

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Chapter III of the GDPR provides for a set of rights that the data subjects can exercise to safeguard their personal data. Although each right has specific details and issues that could affect and be affected by ICT research[1], they all share some general features concerning their transparent information, communication, and modalities of exercise (Article 12 GDPR). In this respect, before jumping into the analysis of each specific right (Article 13-22 GDPR), it is appropriate to briefly mention some issues that each researcher and research institution should take into consideration when complying with the exercise of one of the data subject's rights.

Article 12.1 GDPR begins by providing how information must be given to the data subjects, so that they can exercise their rights effectively. In brief, the **controller must provide information that is correct and comprehensive**, thereby avoiding unnecessary information. Additionally, **the language used must be understandable to the average data subject concerned and provided in writing** (unless the data subject requests otherwise). In this regard, more details will be provided in Section 6.1.

When it comes to the time frame, the controller must provide information on action taken on a request to exercise the data subject's right without undue or excessive delay and, in any case, within one month after receiving the request, on grounds of Article 12.3 GDPR. This span can be extended by two further months, when necessary and on the condition that the controller informs the data subject of the extension and justifies it within one month of the receipt of the request.

Article 12.5 GDPR enables the controller to refuse a data subject's request, if the latter is manifestly unfounded or excessive. In this respect, some **examples** would be: the data subjects have no intention to exercise their rights (and require, for instance, benefits in exchange for the withdrawal of the request), seek to harass the controller, submit identical requests in the same timeframe, and so on. Simultaneously, Article 12.5 GDPR also lays down that the exercise of each data subject's right must be **free of charge**, unless the controller is able to prove that the request was manifestly unfounded or excessive. In this case, the controller can charge reasonable fee, considering the administrative cost of the procedure.

Where the controller has reasonable doubts concerning the identity of the individual making a request, the controller may request the provision of additional information in order to confirm the identity of the data subject, on grounds of Article 12.6 GDPR.

The Exercise of the Data Subject's Rights: Transparency, Communication and

[1] As shown by Ducato, indeed, processing for research purposes enjoys a favorable regime within the GDPR, as it seeks to balance amongst the data subject's rights, the freedom to conduct a business and the legitimate expectations of society for an increase of knowledge. On such premises, Article 89 GDPR allows to derogate from Articles 14,15, 16, 18 and 21 GDPR, on the sole condition that adequate safeguards are provided. Particularly, the provision requires the use of technical and organizational measures to fulfil data minimization, as well as anonymization and pseudonymization techniques. In R. Ducato, 'Data Protection, Scientific Research and the Role of Information', *Computer Law & Security Review,* 2020, Vol. 37, pp. 4-5

Modalities:

- ☐ The provided information must be:
  - Correct and comprehensive, thereby avoiding the unnecessary ones;
  - Understandable to the average data subject concerned;
  - Easily accessible, be it in writing or by any other means;
  - In a language that the specific data subject quite masters.
- ☐ The information must be provided:
  - Without undue or excessive delay and, in any case, within one month after the data subject's request;
  - Within two months after the data subject's request, when necessary and upon communication and justification within one month after the data subject's request;
- ☐ The data subject's request can be refused, whenever it is:
  - Manifestly unfounded;
  - Excessive;
- ☐ The exercise of each data subject's right must be free of charge. If the request is manifestly unfounded or excessive, a reasonable fee can be charged.
- ☐ Additional information can be requested to confirm the data subject's identity.

4.1 Right to Information

On grounds of Article 12 GDPR, controllers are obliged to inform data subjects about their intended processing. The right to information is therefore intertwined with the transparency principle described in Recital 39 GDPR (see also "Lawfulness, fairness and transparency" in the section "Principles" within Part II of these Guidelines)

The right to information **does not require any action from the data subject; instead, it must be proactively fulfilled by the controller.** What should this information look like? In this respect, as already mentioned, any information must be *concise, transparent, intelligible and easily accessible, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including electronically where appropriate, and it may even be provided orally at the data subject's request and if his or her identity is proven beyond doubt. The information shall be provided without excessive delay or expense* (Article 12, GDPR).

Information should be provided **efficiently and shortly**, so that the data subject is not overwhelmed with it and can foresee the scope and the consequences of the processing.[2] To reach such goals, certain aspects need to be considered. First, the information should be first **tailor-made for 'the average member of the intended audience'**[3], which in the case of a research would be the average participant. When in doubt about what the average individual looks like, Data Protection Authorities or other relevant stakeholders *(e.g.,* advocacy groups) could provide feedback. Alternatively, draft informative texts

[2]

[3] Article 29 Data Protection Working Party (ed.), 'Guidelines on Transparency under Regulation no. 2016/679', 2018, WP260 rev.01, p. 7

can be validated before test subjects prior to launching a research project and data collection activities take place[4].

Second, as no active effort is required from the data subject, the information should be **immediately available for the data subject.** The controller can thus provide them as it best suits the context: directly, through a link or a signpost or as a response to a natural language question.

Third, **the language used by the controller should be as simple as possible**. To this end, the EU Commission's publication Claire's Clear Writing Tips and How to Write Clearly[5] could provide tools to simplify the message to be conveyed. Among the things to avoid when drafting any information notice are:

- complex sentences,
- the passive forms,
- any technical jargon,
- modal verbs, and
- abstract notions that could all lead to divergent interpretations.

Children and other vulnerable groups require additional consideration. Here again, much have been written to address this thorny issue[6]. Article 12 states that the information due to the data subject has to be particularly tailored for children – as an example of a vulnerable group – if the data processing activities are targeted towards them. Language is fundamental when it comes to vulnerable individuals, as the Spanish supervisory authority points out[7], since the vulnerability could be exacerbated if the individual lacks the knowledge to understand the information.

Fourth, in order to be more accessible, any written information should be provided in **one single place or one complete document** (whether in digital or paper format). In addition to the paper format, the data controller can make use of other electronic and non-electronic means that will be addressed below, such as a layered data protection statement, pop-up notices, infographics, flowcharts, videos, voice alerts, animations and so on. By contrast, information might be also provided orally, either person-to-person basis and through automated means, on the condition that the data subject's identity is proven through other means.

Articles 13 and 14 GDPR specify the information to be provided, depending on whether personal data were collected directly from the data subject or not.

---

[4] *Ibid.*

[5] As the title suggests, both documents provide the reader with some tips to write more clearly. They are available at: https://ec.europa.eu/info/sites/info/files/clear_writing_tips_en.pdf; https://op.europa.eu/en/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1/language-en [last access: 30.10.2020]

[6] See for instance, I. Milkaite & E. Lievens, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies', *Journal of Children and Media*, 2020, Vol. 14, No. 1, pp. 5-21.

[7] Agencia Española de Protección de Datos Personales, El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles, p. 2. At: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf (accessed Nov. 6, 2020)

When **personal data are directly collected from the data subject** (Article 13, GDPR), the controller must provide at the time they are collected the following information:

- The controller's identity and contact details (namely, the research institution) and the contacts of its data protection officer;
- The purposes and the legal basis for the processing, including the legitimate interest if applicable;
- The identity of recipients (or categories of recipients) of personal data, if any;
- Whether the data will be transferred outside the EU, as well as the details about the legal basis and the safeguards for the processing abroad;
- The data retention period. If establishing such period is not feasible, the criteria used to determine it must be laid down;
- All the data subject's rights, including the right to lodge a complaint with a supervisory authority. Additionally, if the processing is based on the data subject's consent, the right to withdraw consent must be included;
- Whether the provision of personal data is provided by law or contract and whether the data subject must provide the personal data, together with the potential consequences arising from the failure not to provide them;
- The existence of automated decision-making; namely, decisions taken using personal data processed solely by automatic means without human intervention.

Additionally, in its Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR focusing on health research (2021), the European Data Protection Board recommends that *if a controller intends to use data obtained from data subjects also for other purposes, this controller should at the time of collection of the data take appropriate measures in order to be able to meet the information obligations pertaining to such further processing*.[8]

Article 13 GDPR **exempts the controllers** from their obligation when the data subject has already this information. Whilst the data controller must prove these circumstances (relating, for instance, to how and when such information was provided, as well as to what extent they have not changed in the meanwhile), there is still an obligation to potentially complete the data subject's knowledge.

When **personal data are not directly collected from the data subject** (Article 14, GDPR), the controller must also **inform the individual about the source of the personal data and the specific categories of data it plans to process.** All the information must be provided *within a reasonable period [of time] after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.*

[8] European Data Protection Board, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR focusing on health research, adopted on 2 February 2021, p. 9, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf [last access: 28.06.2021]

Ultimately, Article 14.5(b) GDPR lays down three **exemptions for research institutions from the controller's obligation to inform the data subjects** about the processing of personal data that were not collected from them:

- such provision *proves impossible;*
- *or would involve a disproportionate effort;*
- *[…] or insofar as the obligation […] is likely to render impossible or seriously impair the achievement of the objectives of that processing*.

This first means that the controllers must show what has prevented them from providing the information, considering also that, whenever any obstacle is temporary, the provision of information must be done as soon as possible[9]. For example, researchers obtain data from a social network through an application programming interface and, before they can comply with Article 14 GDPR, the social network suffers a denial of service that renders impossible any communication with data subjects.

As regards the **disproportionate effort**, Recital 62 GDPR refers to the amount of data subjects, the age of the data, and the existence of safeguards measures. Here again, the disproportionate effort must be evaluated and proved, by **balancing the costs and benefits** at stake. In any event, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. Public availability can stem, for instance, from the upload of the information on a website and/or its publication on a newspaper. Other appropriate measures range over the performance of an impact assessment, the pseudonymization and anonymization of the personal data (see the see "Identification, Pseudonymization and Anonymization" within Part II section "Main concepts" of these Guidelines), the adoption of organizational and technical measures able to improve the level of security and so on.

Ultimately, **the serious impairment of the objectives of such processing requires the proof that the provision of information enshrined in Article 14.1 GDPR would nullify these objectives.** For example, a research conducted regarding how human interaction in social networks is affected during a lockdown scenario resulting from a global pandemic may demand that researchers perform their analysis as secretly as possible in order not to disturb those interactions. In such cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available according to Article 14.5 (b) GDPR.

Notwithstanding the source of personal data, the data controllers must inform the data subject about their intention of further processing the personal data for a purpose other than the one for which they were collected, prior to that further processing. All in all, the principle of purpose limitation (see "Purpose limitation principle" within Part II section "Principles" of these Guidelines) provides that **personal data must be processed for specified, explicit and legitimate purposes, so that any further processing which is incompatible with them must be prohibited**. Yet, according to Article 5.1(b) GDPR, any further processing for archiving purposes in the public

[9] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation no. 2016/679', *op. cit.,* p. 29

interest, scientific or historical research purposes or for statistical purposes shall not be regarded as incompatible with the original purpose. In any case, the controller's obligation to inform the data subject about the further processing involves the compatibility (see the "Data protection and scientific research" within Part II section "Main concepts" of these Guidelines) test carried out on grounds of Article 6.4 GDPR, in order to explain why the processing for additional purposes is consistent with the original ones. As stressed by the Article 29 Working Party (2013), the performance of the compatibility test is of the utmost importance to ensure transparency and purpose limitation. [10] But, when relying on the presumption of compatibility enshrined in Article 5(1)(b) GDPR for further processing personal data for scientific research purposes, it should be taken into account that this presumption can only be used under the condition that the further processing respects adequate safeguards as required by Article 89(1) GDPR.[11]

Building on such provisions, research institutions can adopt all the measures they consider appropriate to comply with this obligation. The GDPR, indeed, does not prescribe any form as to how information shall be given. Generally, the right to information is fulfilled by adopting a data protection policy, a privacy statement or a fair processing notice; their effectiveness, however, have led to a polarized debate amongst scholars and policy makers[12]. Accordingly, new methods have been developed and could be used to provide information to data subjects in a clear and accessible way, such as:

- A **layered approach**: rather than showing all the required information in a single notice and so risking overwhelming the data subject, a first privacy notice can link to the other categories of information, so that the level of details increases progressively. In this context, the first layer should include the identity of the controller, the purpose of the processing and the data subject's rights[13], together with the potential consequences arising from the processing[14]. It is important to stress that the layered approach can be adopted both in the online and offline scenarios. As regards the latter, the first layer could be provided orally, while later sending a copy of the data protection policy and/or sharing a link to the layered online privacy statement[15].

[10] For further details on the compatibility test, see Article 29 Data Protection Working Party (ed.), 'Opinion 03/2013 on Purpose Limitation', 2013, p. 13 WP 203 00569/13/EN

[11] European Data Protection Board, *op. cit.,* p. 6

[12] M. Arcand, J. Nantel, M. Arles□Dufour & A. Vincent, 'The Impact of Reading a Web Site's Privacy Statement on Perceived Control over Privacy and Perceived Trust, *Online Information Review*, 2007, Vol. 31, No. 5, pp. 661–681; J. A. Obar & A. Oeldorf-Hirsch, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media', *Social Media + Society*, 2018, Vol. 4, No. 3, pp. 1-14; Y. Pan & G. M. Zinkhan, 'Exploring the Impact of Online Privacy Disclosures on Consumer Trust, *Journal of Retailing*, 2006, Vol. 82, No. 4, pp. 331–338; B. Custers, S. van der Hof & B. Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users', *Policy & Internet*, 2014, Vol. 6, No. 3, pp. 268–295

[13] Recital 39, GDPR

[14] Article 29 Data Protection Working Party (ed.), 'Guidelines on Transparency under Regulation no. 2016/679', *op. cit.*, p. 19

[15] *Ibid.,* p. 20

- A **privacy dashboard**: this user interface allows data subjects to manually manage their preferences for the processing of the personal data;
- Icons, pop-ups, QR codes and voice alerts, indicating the existence of a particular kind of personal data processing;
- Information sheets, infographics, flowcharts, information embedded in contracts.

In addition to the Guidelines on transparency under Regulation no. 2016/679 adopted by the Article 29 Working Party, several research projects are currently exploring how to make information more accessible to the data subjects, such as the GDPR by Legal Design Project[16] and the PROTECT ITN[17].

Last but not least, in its 2020 Preliminary Opinion, the European Data Protection Supervisor examines the intersection amongst deception, informed consent and the right to information. Generally speaking, *deception may include withholding information in the instructions to research participants, providing only limited information as to the purpose of the research or even misleading participants by providing a 'cover story' for the study to mask the actual topic of the study. In some psychology experiments known as covered research, subjects are misled about what is being tested, and this is cited as a key success factor because awareness of the exact nature of the research would alter people's behavior. […] [D]ebriefing of the research participants and retrospective informed consent along with specific ethics approval before the start of the research are among the measures to ensure ethics compliance*. It is nonetheless the case that such practices apparently clash with the right to information, whenever the data are collected directly from the data subject pursuant to Article 13 GDPR[18].

Checklist for complying with the right to information

What to provide:

- ❑ If the personal data were directly provided by the data subject, provide all the information enlisted in Article 13.1 GDPR;
- ❑ If the personal data were <u>not</u> provided by the data subject, provide all the information enlisted in Article 14.1 – 2 GDPR;
- ❑ If the information was already fully provided to the data subject, no need to comply with this obligation anymore.

When to provide:

- ❑ At the time the information was collected from the data subject;
- ❑ When the data are <u>not</u> collected from the data subject:
  - ▫ within a reasonable period after obtaining the personal data, but at the latest within one month;
  - ▫ if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data

[16] For further information: http://gdprbydesign.cirsfid.unibo.it/

[17] For further information: https://protect-network.eu/research/

[18] European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research', 2020 available at: <u>https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf</u> [last access: 30.10.2020]

subject;
    - if a disclosure to someone else is envisaged, at the latest when the personal data are first disclosed.

How to provide:

- Concisely;
- ❑ Transparently;
- ❑ Intelligibly;
- ❑ Easily accessible;
- ❑ In a clear and plain language.

Exemptions:

- ❑ When the data subject already has all the relevant information;
- ❑ If the personal data were not provided by the data subject:
    - When the provision of information is impossible or disproportionate.

4.2 Right of Access

According to Article 15 GDPR and in compliance with Article 8.2 of the Charter of Fundamental Rights of the European Union, each data subject has the right to *obtain from the controller confirmations as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and to* ***the following information:***

- The purpose of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- The data retention period. If establishing such period is not feasible, the criteria used to determine it must be laid down;
- All the data subject's rights, including the right to lodge a complaint with a supervisory authority;
- The origin of personal data, if they are not collected from the data subject directly;
- The existence of automated decision-making; namely, decisions taken using personal data processed solely by automatic means without human intervention.
- The existence of all the safeguards taken to eventually transfer personal data outside the EU.

Upon the data subjects' request, the data controller must provide them with a copy of the personal data being processed, without charge. For any additional copies requested by the data subjects, Article 15.3 GDPR allows the controller to potentially charge *a reasonable fee based on administrative costs.* In this scenario, the controller should get in contact with the data subjects promptly, in order to make them aware of the cost.

The data subjects are just entitled to their personal data, unless the latter information is intertwined with the one from other individuals. If the personal data includes information about other people, the following disclosure **will depend on the balancing between the data subjects' right of access and the third party's fundamental rights** pursuant to Article 15.4 GDPR. For example, any duty of professional secrecy, the nature of personal data, and so on should be taken into consideration when carry out research. In this scenario, the controller might conceal data that could adversely affect others, such as blackening selected information[19].

The GDPR does not prevent a person from potentially acting on behalf of the data subjects, while proving it, for example, through a power of attorney[20]. In case of any doubt, the controller can ask the data subjects to identify themselves. As already said, though, such process should be proportionate. Furthermore, the data controller can ask the data subjects to specify their request, by offering further details that will contribute to identifying the requested information. Nevertheless, the controller's request for further clarification does not affect the one-month term.

The GDPR does not establish a **procedure to exercise the right of access**. Accordingly, the controller could provide a specific form that the data subjects could easily fill in and submit. The establishment of any procedure, however, does not allow the controller to refrain from accepting requests that have been submitted through other means.

Likewise, the GDPR says nothing about **how the controller should provide the information to the data subjects.** Generally, the provision of any information should be done in a commonly used electronic format (e.g. e-mail where a PDF fill is attached), if the request was made electronically and the data subjects did not request otherwise. Yet, Recital 63 GDPR suggests the controller to provide the data subjects with a remote access to a self-secure system, so that they are able to accede to their personal data directly; for example, accessing the controller's database through a VPN.

Checklist for complying with an access request:

Is the exercise of the right of access compliant with the GDPR?

- Did you receive an access request from a legal entity? If yes, please indicate that the request was not lodged by an individual and deny the request;
- Have the data subjects correctly identified themselves? If not, please ask for further information to confirm the identity;
- Can the request be fulfilled within one month? If not, please inform why and how long it will it take to process the request (without exceeding the time limits provided in the GDPR, see Section 6);
- The request needs to be fulfilled.

[19] P. Voigt & A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide,* Cham: Springer, 2017, p. 153

[20] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, 2019, p. 108, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [last access: 30.10.2020]

How to further comply with all the GDPR obligations:

- ☐ Provide all the information listed in Article 15.1-2 GDPR;
- ☐ If the information intertwines with the one from other individuals, please carry out a balancing test as to whether the disclosure to the individual that has filed the request does not affect the personal data of the other individual;
- ☐ Provide the data subject with a copy of the personal data being processed. For any additional copies requested by the data subject, the controller can charge a reasonable fee.

Best practices:

- ☐ Provide a specific form that the data subject could easily fill in and submit;
- ☐ Provide all the information in a commonly used electronic format, unless the data subject requests otherwise.

4.3 Right to Rectification

As laid down in Article 16 GDPR, data subjects hold the right to have their personal data rectified. Such right derives from the need to ensure the accuracy of personal data and, consequently, a higher level of protection for data subjects[21]. **Personal data are inaccurate, insofar as they are incorrect, incomplete and/or misleading**[22]. In other words, they misrepresent the reality. Accordingly, the right to rectification only deals with objective and factual data, including the spelling of the research participant's name.

When it comes to value judgements that are fact-related (*e.g.,* the personal evaluation of research participants based on their life conditions), **controllers must perform a balancing test** between their freedom of expression and the data subjects' right under scrutiny. **The aim of the balancing is to understand whether a rectification is reasonable for the controller and necessary for the data subjects.** For example, whenever the value judgement results in an incorrect impression of the data subjects that can be proven, the interest of the data subjects will prevail[23].

The **request can be made in writing or orally**. As regards its essence, it will sometimes be sufficient for the data subject to simply request rectification, such as in the case of misspelling. It is nonetheless the case that the controller might request proof of the inaccuracy, without placing an unreasonable burden of proof on the data subjects and thereby refraining their from exercising the right under scrutiny[24]. Moreover, it is important to emphasize that any addition of information must be necessary for the purpose(s) of the processing and the controller's effort must be proportionate in the

[21] Recital 65, GDPR and Article 5.1 (d) GDPR

[22] Information Commissioner's Office (ed.), *op. cit.*, pp. 115-116

[23] P. Voigt & A. von dem Bussche, *op. cit.*, p. 155

[24] Fundamental Rights Agency (ed.), *op. cit.*, p. 220

specific context situation[25]. As a matter of good practice, **the controller should restrict the data processing, while verifying the accuracy of the information**[26].
A data subject can only exercise the right to rectification for its own information, given that Article 16 GDPR **does not grant a right relating to the rectification of personal data of a third party.** This means that the scope of the data subject's right is constrained, whenever personal data also related to other individuals (e.g. relationship with another person)[27].

Checklist for complying with a rectification request: Is the exercise of the right to rectification compliant with the GDPR?

- Did you receive a rectification request from a legal entity? If yes, please indicate that the request was not lodged by an individual;
- Have the data subjects correctly identified themselves? If not, please ask for further information to confirm identity;
- Can the request be fulfilled within one month? If no, please inform why and how long will it take to process the request?
- Do you need a proof of inaccuracy or additional information to rectify the data? If yes, please ask for further information to the data subject. Remember not to place an unreasonable burden of proof on the data subject
- The request needs to be fulfilled.

How to further comply with all the GDPR obligations:

- Communicate the data to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

4.4 Right to Erasure ('Right to be forgotten')

Article 17 GDPR grants the right to the data subject to have its personal data erased without undue delay. This right reflects the data minimization principle (see "Data minimization principle" within Part II section "Principles" of these Guidelines) and the accuracy principle (see "Accuracy principle" within Part II section "Principles" of these Guidelines), according to which personal data must be limited to what is necessary for the purposes for which those data are processed, as well as must be accurate and updated (Article 5.1(c) and (d)).

Pursuant to Article 17.1 GDPR, the right to erasure **applies in the following scenarios:**

a) The personal data are no longer necessary regarding the purposes for which they were processed;
b) The data subject withdraws the consent on which the processing is based and there is no other applicable legal ground;

[25] P. Voigt & A. von dem Bussche, *op. cit*., p. 156
[26] Information Commissioner's Office (ed.), *op. cit.*, p. 115
[27] P. Voigt & A. von dem Bussche, *op. cit*., p. 155

c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) The personal data have been unlawfully processed;
e) The personal data have to be erased, in order to comply with a legal obligation laid down in the EU or Member State's law to which the controller is bound;
f) The personal data have been collected concerning the offer of information society services to children according to Article 8.1 GDPR.

From a practical perspective, the right to erasure involves **making data unusable in any way,** that prevents the controller and any other party from (re-)accessing and (re-)processing the data[28]. Be it either by destructing the physical support (e.g. paper documents) or by deleting the data from IT systems. The erasure process is successful, **insofar as it is no longer possible to restore the data without excessive effort**. Voigt and von dem Bussche, for instance, consider the theoretical possibility of restoring the data through a specialized software as reasonable[29].

On the one hand, there are **international standards** specifically created to state how information on paper has to be destroyed. In particular, the paper has to be destroyed by an appropriate shredder. One example of a standard on this matter is the DIN 66399 Standard[30], which offers guidance on the adequacy of shredders and their configuration. Destruction of information can be performed either internally by the controller or by an external company**. If outsourced, the external company must be considered a data processor** since Article 4.2 GDPR considers also "erasure or destruction" to be a processing operation. According to Article 28.3 GDPR, the controller must write a **contract** that imposes all necessary obligations on the processor to implement appropriate safeguards (see Article 28 GDPR for detail).

On the other hand, it is the case that erasure from live systems may not occur immediately. Moving data to the computer bin is not sufficient. For instance, the data could be stored in a different location, and in back-up repositories as well. In such cases act upon the data subject's request could be more complicated and longer due to technical mechanisms in force. Accordingly, the controller shall put the back-up data beyond use (namely, so that no one can process the data in the back-up repository for any purpose), until the repository is updated upon schedule and the data can finally be erased permanently. A recent example of standards applicable to this process can be found in the ISO 27701.

Moreover, when personal data are public and must be erased, **the controller must take reasonable steps to inform other controllers who process the same data about the subject's request to erase them**. Such reasonableness derives from the available technologies and the cost of implementation, as explained in Recital 66 GDPR. Similarly, Article 19 GDPR requires the controller to communicate the erasure to each recipient to whom the data have been disclosed, unless this proves impossible or

[28] P. Voigt & A. von dem Bussche, *op. cit*., p. 161

[29] *Ibid.*, p. 161

[30] This standard was developed by the DIN, which is the abbreviation for the German Institute for Standardization. For further information, see: https://din66399.de

involves disproportionate effort (see "Accuracy principle" within Part II section "Principles" of these Guidelines).

A much debated question concerns the burden of proof. On the one hand, according to Voigt and von dem Bussche (2017), the data subjects have to demonstrate the existence of their right to erasure; the controller will nonetheless be obliged to prove favorable circumstances for it, such as a producing counterevidence to negate unlawful processing under Article 17.1 (d) GDPR. The same also goes for proving exceptions from the right to erasure laid down in Article 17. 3 GDPR (see below)[31]. On the other hand, the Fundamental Rights Agency states that, upon the data subject's request for erasure, it is just the responsibility of the controller to indicate the lawfulness of the processing.[32]

Against this background, indeed, Article 17.3 GDPR provides several **exemptions** to the right to the erasure, including when the processing for personal data is necessary for:

- Exercising the right of freedom of expression and information;
- Compliance with a legal obligation which requires processing by the EU or Member States' law to which the controller is bound, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Reasons of public interest in the area of public health;
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- The establishment exercise or defence of legal claims.

Focusing on the limitation set to the right to erasure when its exercise would render impossible or impair achievement of research purposes, Ducato outlines that *such a limitation […] is justified in the light of the specific needs of the research context: erasure of whole or part of the data used for a study, even where technically possible, would risk undermining the scientific validity of research by preventing verification of its results and the peer review process*[33]. The restriction, the author reports, is thus apparently limited to studies that are already concluded, given that the failure to commence the research and the following exercise of the right to erasure would not affect the research objectives[34].

Checklist for complying with an erasure request:

Is the exercise of the right to erasure compliant with the GDPR?

- Did you receive an erasure request from a legal entity? If yes, please indicate that the request was not lodged by an individual;
- Have the individuals correctly identified themselves? If not, please ask for further information to confirm identity;

[31] P. Voigt & A. von dem Bussche, *op. cit*., p. 159

[32] Fundamental Rights Agency (ed.), *op. cit.*, p. 223

[33] R. Ducato, *op. cit.*, p. 6

[34] *Ibid.*

- Does the request fall within one of the scenarios laid down in Article 17.1 GDPR? If not, please inform and explain to the data subject that the request shall be denied;
- Does the request satisfy one of the exemptions provided by Article 17.3 GDPR? If yes, please inform and explain to the data subject that the request shall be denied;
- Can the request be fulfilled within one month? If not, please inform why and how long will it take to process the request.
- The request needs to be fulfilled.

How to further comply with all the GDPR obligations:

- ☐ Make data unusable in a way that prevents you and any other party from (re-) accessing and (re-)processing the data;
- ☐ Communicate the erasure to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

4.5 Right to Restriction of Processing

Article 18 GDPR enables the data subjects to temporarily restrict a controller from processing their personal data. Such right enshrines a reconciliation of interests between the data subjects' in a rectification or erasure of their information and the controller's interest in continuing the data processing[35]. The GDPR **does not define how the request should be done: it is nonetheless a matter of good practice that it is made in a sufficiently clear way.**

Pursuant to Article 18.1 GDPR, the data subject's request **can be made, when:**

a) The accuracy of the personal data is contested (See Section 6.3);
b) The processing is unlawful, and the data subject opts for the restriction of the processing, rather than the erasure of the personal data;
c) The data must be kept for the exercise or defence of legal claims;
d) A decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject.

As provided by Recital 67 GDPR, the **methods** in which the controller can restrict personal data processing can include, for example, temporary movement of the selected data to another processing system, making the data unavailable to users or the removal of personal data on a temporary basis. Overall, the aim is to prevent data from being processed, with the exception of the storage (Article 18.2 GDPR).

While the restriction is pending, personal data can still be processed:

- on grounds of the data subject's consent;
- for the establishment, exercise or defence of legal claims;
- for the protection of the rights of another individual or legal person;

[35] *Ibid.*, p. 164

- for reasons of important public interest of the EU/an EU Member State.

On grounds of Article 19 GDPR, the controller must **communicate** the restriction of the processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The **disproportionate effort** depends on the specific circumstances and could involve, for example, the vast number of recipients and following notifications, or the difficulty in identifying the recipient.

Finally, the controller **must notify the data subject before the restriction on processing is lifted.** In fact, the restriction could be temporary, especially when the data subjects exercise their rights to rectification and to object.

Turning now to the data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, Article 89 GDPR and Recital 156 GDPR allows *Member States to provide, under specific conditions and subject to appropriate safeguards for data subjects specifications and derogations with regard to the right […] to object*. In this respect, the European Data Protection Supervisor (2020) recognizes that the objection of a large number of individuals to all or part of the project could negatively affect the representativeness and reliability of the research data. According to the EU authority, the scope of this derogation should therefore remain limited to cases where the integrity of research would be compromised by the exercise of data subjects' rights.[36]

Checklist for complying with a restriction of processing request

Is the exercise of the right to restriction of processing compliant with the GDPR?

- Did you receive a request to restrict data the processing from a legal entity? If yes, please indicate that the request was not lodged by an individual;
- Have the individuals correctly identified themselves? If not, please ask for further information to confirm identity;
- Does the request fall within one of the scenarios laid down in Article 18.1 GDPR? If not, please inform the data subject that the request shall be denied;
- Can the request be fulfilled within one month? If not, please inform why and how long will it take to process the request?
- The request needs to be fulfilled.

How to further comply with all the GDPR obligations:

- ☐ Remember that the restriction does not encompass the data storage;
- ☐ When restriction is pending, personal data can still be processed under the circumstances laid down in Article 18.2 GDPR;
- ☐ Communicate the restriction of the processing to each recipient to whom the personal data has been disclosed in compliance with Article 19 GDPR, unless this proves impossible or involves disproportionate effort.

[36] EDPS, "A Preliminary Opinion on data protection and scientific research", January 2020, p. 21-22

4.6 Right to Data Portability

On the basis of Article 20 GDPR, the data subject has *the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.* In providing so, the data subjects are empowered, as they have better control over their personal data and so move, copy, or transfer them as desired. According to Article 20.1 GDPR the right to data portability, however, can be exercised only **when personal data are processed by automated means, on grounds of consent or for the performance of a contract.**

As stressed in the Guidelines on the right to data portability developed by the Article 29 Data Protection Working Party (2017), the right to data portability is **not limited to the possibility to transmit the data subject's personal data to one controller to another, but it also encompasses the data subject's right to receive a subset of the processed personal data and store them for personal use.** To put it differently, the data transmission to another controller is not a mandatory constitutive element of the right to data portability, given that one of its specificities lies in the fact that *it offers an easy way for the data subject to manage and reuse personal data themselves*[37]. All in all, data portability deals with personal data concerning the sole data subject, either be they actively provided by the data subject or be they provided by virtue of the use of the service of the device. In the latter case, the Article 29 Data Protection Working Party highlights that the controller should not take an overly restrictive interpretation of what counts as 'personal data concerning the data subject'[38].

The right to portability is satisfied, insofar as the controllers directly transmits the requested information to the data subjects or provides access to an automated tool, allowing them to extract the requested information on their own. The latter method does not involve that the controllers must provide a more general and routine access to their own system; rather, it must be limited to the extraction of the information following the portability request[39].

The transferal of the personal data from a controller to another depends on its legal, technical and financial feasibility. Amongst potential obstacles, the Article 29 Data Protection Working Party identifies: *fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demand*[40]. To this end, Recital 68 GDPR provides that the controller should develop interoperable formats; namely, the information's system ability to exchange data and to enable

[37] Article 29 Data Protection Working Party (ed.), 'Guidelines on the Right to Data Portability', 2017, WP 242 rev.01, pp. 4-5. At: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

[38] For further example see: *ibid*., p. 9

[39] Information Commissioner's Office (ed.), *op. cit.*, p. 140

[40] Article 29 Data Protection Working Party (ed.), 'Guidelines on the Right to Data Portability', *op. cit.,* p. 15

information sharing. Yet, there is no obligation on the controller to support these formats, with the consequence that the direct transmission can occur, insofar as the communication between the two systems is possible and safe. Examples of interoperable formats are: an SFTP server, a secured WebAPI or WebPortal.

In addition, the data should be *in a structured, commonly used and machine-readable format.* So as to understand this feature, the Open Data Handbook published by Open Knowledge International can be a useful source[41]. Specifically, structured data can be defined as *data where the structural relation between elements is explicit in the way the data is stored on a computer disk.* This means that the software can extract specific elements of the data. An example of a structured format is a spreadsheet file, where the data is organised into rows and columns. Instead, machine-readable data are those data that can be automatically read and processed by a computer. Machine-readable data can be made directly available to applications that request that data over the web[42]. This is undertaken by means of an application programming interface ("API"). Finally, it is important to stress that, although 'the commonly used' requirement could be satisfied by using common software applications, such applications must also meet the structured and machine-readable standards to comply with the right to portability. In any event, open formats such as CSV, XML, JSON and RDF are a good illustration of ways to answer a portability request.

Considering that data portability involves the transferral of personal data, such act could become a potential source of **risk** for the personal data as such. Consequently, the controller is required to **take all the necessary measures to guarantee a safe transferal** to the right recipient. This objective could be reached through data encryption, one-time passwords, and so on.

It is also noted that when a controller responds to a data portability request, it acts on the data subject's instructions and, consequently, is not responsible for the recipient's compliance with the data protection framework. Besides, the controller who transfers the data is not required to check the accuracy of the personal data[43]; nevertheless, **data portability neither automatically involve the erasure of the personal data from the system, nor affect the original retention period**[44].

If the data subject's request involves **information about other individuals,** the controller must consider whether there will be an adverse effect on their rights and

[41] The handbook is available at: https://opendatahandbook.org/ [last access: 30.10.2020]

[42] The term is defined in Recital 21 of the Directive 2013/37/EU17 as (…) *a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats*.

[43] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability', *op. cit.*, p. 6

[44] *Ibid.*, p. 7

freedoms. By contrast, if the portability request is made by several data subjects, the controller must make sure that all of them agree on the request[45].

Finally, it must be highlighted that there is not a right to access to inferred data, since these are NOT provided by the data subjects. Nevertheless, the data subjects can still use their "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" as well as information about "the existence of automated decision-making, including profiling, 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", according to Article 15 of the GDPR (which refers to the right of access)[46].

Moving to the realm of research, data portability could allow the development of "more and more user-centric platforms for the management of personal data"[47], while also providing data subjects with effective control over their personal information. Particularly, data portability could be useful for the establishment of a broad research network, the facilitation of secondary use, and the fulfilment of citizen science (namely, that individuals should be able to transfer their data from various resources to research institutions)[48].

Checklist for complying with a portability request

Is the exercise of the right to data portability compliant with GDPR?

- ☐ Did you receive a request for data portability from an individual? If not, please indicate that the request was not lodged by an individual and indicate that the request should be made following the relevant legislation;
- ☐ Is the portability request made by several data subjects? If yes, make sure that all of them agree on the request;
- ☐ Have the data subjects correctly identified themselves? If not, please ask for further information to confirm identity;
- ☐ Are data processed on one of the lawful bases provided in Article 20.1 GDPR? If not, please inform the data subject that the request shall be denied;
- ☐ Is the data processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller? If yes, please inform the data subject that the request shall be denied;
- ☐ Can the request be fulfilled within one month? If no, please inform why and how long will it take to process the request?
- ☐ The request needs to be fulfilled.

[45] Information Commissioner's Office (ed.), *op. cit*., p. 139

[46] Article 29 Data Protection Working Party (ed.), 'Guidelines on the Right to Data Portability', *op. cit.,* p. 15.

[47] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*", Computer Law and Security Review*, Vol. 34, No. 2, 2018, p. 203.

[48] P. Quinn P., "Is the GDPR and its Right to Data Portability a Major Enabler of Citizen Science?", *Global Jurist*, June 2018, pp. 8-9

How to further comply with all the GDPR obligations:

- ☐ If the information intertwines with the one from other individuals, please carry out a balancing test;
- ☐ Transmit data in structured, commonly used and machine-readable formats;
- ☐ Transmit data in a secure way.

4.7 Right to Object

Article 21 GDPR attributes to the data subject *the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her*. Blocking cookies on a web page, for instance, is an example of objection.

This provision and its reference to the data subject's particular situation aim at balancing its rights with the legitimate ones of others in processing their data. This is exemplified in the data subject's professional interest in confidentiality. It is important to emphasize that the right to object is **applicable where the legal basis for the processing is the controller's performance of a task carried out in the public interest, or where the processing is based on the controller's legitimate interests.** In any event, **the burden of proof lies with the controller**, who must demonstrate compelling grounds for continuing the processing.

The successful objection, in fact, leads to the impossibility of processing the data at stake, whereas, according to the Fundamental Rights Agency (2018) processing operations performed prior to the objection remain legitimate[49]. Voigt and von dem Bussche, instead, argue that it is unclear whether the successful objection results in the compulsory erasure of the data[50]. In any event, a successful objection allows the data subject to exercise the right to erasure pursuant to Article 17.1(c) GDPR.

At the latest at the time of the first communication with the data subject, the right to object must be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

It is nonetheless the case that Article 21.6 GDPR prevents the data subject from objecting the data processing, on the condition that the latter is performed for scientific or historical research purposes and statistical purposes and is necessary for the performance of a task carried out for reasons of public interest. The burden of proof concerning the necessity falls on the controller, who, however, does not have to demonstrate the existence of compelling legitimate grounds, such as in the case of the first paragraph of Article 21 GDPR.[51] In this regard, it is important to remind that,

[49] Fundamental Rights Agency (ed.), *op. cit.*, p. 231

[50] P. Voigt & von dem Bussche, *op. cit.,* p. 179

[51] G. Zanfir-Fortuna, 'Article 21. Right to Object', in C. Kuner, L. A. Bygrave & C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford: Oxford University Press, 2020, p. 519

according to the EDPB (2020), the scope of this derogation should be restricted to cases where the integrity of the research would be compromised by the exercise of data subject's rights.[52] As a matter of fact, the objection to all or part of a scientific research by several data subjects may negatively influence the representativeness and reliability of the research data,.

Albeit unrelated to research purposes, the GDPR provides other two nuances relating to the right to object. First, Article 21.2 GDPR also includes a specific right to object relating to the use of personal data for **direct marketing**. This right can be exercised at any time and free of charge and the data subject must be informed about its existence in a clear way, separate from any other information.
Second, Article 21.5 of the GDPR regulates the right to object, when the processing is carried out by information society services through **automated means.** In this context, which is particularly relevant in terms of ICT research, the data controller must develop appropriate technical arrangements and procedures to guarantee that the right to object can be exercised effectively, such as in the case of blocking cookies on the web page and turning off the tracking of internet browsing.

Checklist for complying with an objection request

Is the exercise of the right to object compliant with GDPR?

- Did you receive an objection request from a legal entity? If not, please indicate that the request was not lodged by an individual.
- Does the request fall within one of the exceptions laid down in Article 21.2-6 GDPR? If yes, please inform the data subject that the request shall be denied.
- Have the data subjects correctly identified themselves? If not, please ask for further information to confirm identity.
- Can the request be fulfilled within one month? If not, please inform why and how long will it take to process the request.
- The request needs to be fulfilled.

How to further comply with all the GDPR obligations:

- ☐ Check the data subjects' particular situation aims at balancing their rights with the legitimate ones of others in processing their data.

4.8 Right not to be Subject to Automated Decision-Making

Pursuant to Article 22 GDPR, *the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*. As explained by Bygrave (2021), the rationale behind this provision lies in the potentially serious repercussions that profiling and other automated processing operations might

[52] EDPB, *op. cit.,* pp. 21-22

have on the decision-making process of the data subject.[53] Researchers, for instance, could develop software to process a large amount of personal data, classify data subjects according to them, make predictions, and determine outcomes that could cause data discrimination, when later applied in the context of public administration (*e.g.*, provision of welfare and health services) or the private sector (*e.g.*, target advertisement and e-recruitment)

A much-debated question is the nature of Article 22 GDPR. The Article 29 Working Party, on the one hand, interprets this provision as a general prohibition and mostly justifies its reading based on Recital 71, which makes it clear that processing under Article 22 GDPR is not allowed generally.[54] On the other hand, Bygrave and other authors argue that this interpretation runs counter the actual wording of Article 22 GDPR, as well as its placement in the structure of the Regulation (namely, Chapter III on data subject's rights) and its special consideration in Articles 13.2(f), 14.2(g), 15.1(h), and 35.3(a).[55] Whereas the interpretation of Article 22 GDPR as a prohibition requires the data controller to apply it regardless of the data subject's action for this purpose, its interpretation as a right involves its exercise following the aforementioned requirements enshrined in Article 12 GDPR that will also be mentioned below.

The **automated decision-making** is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example, data provided directly by the individuals concerned (such as responses to a questionnaire); data observed about the individuals (such as location data collected via an application); derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score)[56].

Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements (see Article 4 GDPR).

Although the GDPR **does not define the 'legal' and 'similar effects'** arising from the automated decision-making, the Article 29 Working Party clarifies that *a legal effect requires that the decision, which is based on solely automated processing, affects someone's legal rights, such as the freedom to associate with others, vote in election or take a legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract*[57]. Examples of legal effects encompass the

[53] L. A. Bygrave, 'Article 22. Automated individual decision-making, including profiling, in C. Kuner, L. A. Bygrave & C. Docksey *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford: Oxford University Press, 2020, p. 526

[54] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2018, WP251rev.01, pp. 19-20

[55] L. A. Bygrave, *op. cit.,* pp. 531-532

[56] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', *op. cit.*, p. 8

[57] Article 29 Data Protection Working Party, 'Guidelines on Automated Individuals Decision-Making and Profiling for the Purpose of Regulation no. 2016/679', *op. cit.,* p. 21

termination of a contract, the denial of a social benefit granted by law, the denial of citizenship or resident permits. As regards the similar effects, the Article 29 Working Party considers them as the consequence of *decisions that must have the potential to significantly affect the circumstances, behaviors or choices of the individual concerned: have prolonged or permanent impact on the data subject or; lead to the exclusion or discrimination of the individual*[58]. This is evident in a e-recruitment practice that favor white men over women or people pertaining to minority or vulnerable groups.

Pursuant to Article 22.4 GDPR, where special categories of personal data are involved, automated decision-making can occur, **on the condition that the data subject has explicitly consented to it or where it is necessary for reasons of substantial public interest** provided for by EU or EU Member State Law. In this context, the controller must take all the appropriate measures to safeguard the data subject's rights and freedoms.

As already mentioned, Article 12 GDPR provides the controller's obligation to inform the data subject about the existence of the automated decision-making. In addition, the information should not be limited to the fact that such decision-making occurs, but it should also explain **the logic involved and the potential consequences** for the data subject[59].

Article 22.2 GDPR provides three exceptions from the prohibition of automated decision-making, namely:

- The decision is necessary for entering into, or performance of, a contract between the data subject and a controller;
- The decision is authorized by EU or EU Member State law to which the controller is subject;
- The decision is based on the data subject's explicit consent.

In cases one of these exceptions applies, the data controller shall implement specific safeguards other than the ones generally provided in Article 12 GDPR. Based on Article 22.3 GDPR, in the cases of derogations for contract and consent, data subjects will still have the right to demand human review of the fully automated decision, in addition to the general safeguards that the data controller should implement to protect their fundamental rights and freedoms, as well as legitimate interests. Additionally, in order to guarantee a fair and transparent data processing, Recital 71 requires the data controller to *use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect.* For

[58] *Ibid.*

[59] Fundamental Rights Agency (ed.), *op. cit.,* p. 234

these purposes, the implementation of the principle of data protection by design and by default are of the utmost importance. Furthermore, Recital 91 clarifies that a data protection impact assessment should be made in the context of automated decision-making processes, whenever the data processing results in *decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures*. The provision continues by saying that *[a] data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic- electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale.*

Checklist for complying with a request not to be subject to automated decision-making

How to comply with all the GDPR obligations:

- ☐ Does the automated decision-making fall within one of the exemptions laid down in Articles 22.2 and 22.4? If yes, you can proceed with the data processing;
- ☐ Inform the data subject about the existence of the automated decision-making, including also an explanation of the logic involved and the potential consequences for the data subject.

4.9 Restrictions to the Data Subjects' Rights

Pursuant to Article 23 GDPR, EU or Member State law may restrict the scope of certain data subject rights in order to safeguard certain objectives, namely:

a) National security;
b) Defence;
c) Public security
d) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
e) Other important objectives of general public interest of the EU or of a Member State;
f) The protection of judicial independence and proceedings;
g) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the aforementioned cases (except for the protection of judicial independence and proceedings);
i) The protection of the data subject or the rights and freedoms of others; or
j) The enforcement of civil law claims

For any restriction to be lawful, Article 23(1) GDPR clarifies that it must be provided for in a legislative measure, concern the sole data subject's rights and the corresponding obligations enshrined in Articles 5, 12-22, and 34 GDPR, respect the essence of fundamental rights and freedoms, and be a necessary and proportionate measure in a democratic society.

As explained by the EDPB, the condition to respect the essence of fundamental rights and freedoms means that the restrictions cannot be so extensive and intrusive that will void these rights and freedoms of their basic content.[60] When it comes to the necessity and proportionality requirements, the EDPS outlines, the former is satisfied insofar as the objective of general interest is sufficiently identified in detail. In this way, it will be possible to evaluate whether the restrictive measure is necessary. As regards its proportional nature, it means that the legislative measure must be appropriate for achieving the legitimate objectives.[61]

Later, Article 23(2) GDPR provides that the legislative measures restricting the data subject's rights and the controller's obligations must include, where relevant:

(a) The purposes of the processing or categories of processing;
(b) The categories of personal data;
(c) The scope of the restrictions introduced;
(d) The safeguards to prevent abuse or unlawful access or transfer;
(e) The specification of the controller or categories of controllers;
(f) The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) The risks to the rights and freedoms of data subjects; and
(h) The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

In its Guidelines, the EDPB also clarifies, "the controller should document the application of restrictions on concrete cases by keeping a record of their application",[62] in compliance with the accountability principle (see "Accuracy principle" within Part II section "Principles" of these Guidelines). This record should contain the applicable reasons for the restrictions, which grounds among those listed in Article 23(1) GDPR apply, its timing, as well as the outcome of the necessity and proportionality test.

[60] European Data Protection Board, Guidelines 10/2020 on Restrictions under Article 23 GDPR, adopted on 15 December 2020, p. 10, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-102020-restrictions-under-article-23_en [last access: 15.09.2021]
[61] *Ivi.*
[62] *Ibidem,* p. 14

4.10 **Final Remarks on the Data Subject's Rights**

Before concluding, it is important to note that this document just provided a brief overview of the data subject's rights included in Chapter III of the GDPR. Nevertheless, as these rights simultaneously impose a reciprocal obligation for the controller and the processor, Chapter IV of the GDPR regulating obligations on the controller and the processor also attribute further rights to the data subject.

More generally, data subject's rights can be found all over the GDPR. The basic principles enshrined in Chapter II, Articles 5-10, for instance, likewise provide additional protection for the data subject. The reason behind this widespread safeguard lies in one of the rationales of the GDPR, that is to say, the need to guarantee a consistent and high level of protection of natural persons in the digital era, where continuous processing and cross-border flows of personal data are the order of the day.

For the sake of completeness, the reader should thus be aware that the GDPR includes, *inter alia,* the following data subject's rights[63]:

- The right to withdraw consent (Article 7.3 GDPR); the data subjects shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a supervisory authority (Article 78 GDPR); namely, data subjects can lodge requests and/or complaints to the competent supervisory authority, if they believe that the processing of their personal data has not been carried out in accordance with the law;
- The right to an effective judicial remedy (Article 79 GDPR); namely, the data subjects can bring a complaint before a court;
- The right to compensation (Article 82 GDPR); namely, the data subjects can claim compensation for any damage suffered due to the processing of personal data in breach of the GDPR.

[63] For further detail, see, for instance: Fundamental Rights Agency (ed.), *Handbook on European Data Protection Law,* Luxembourg: Publications Office of the European Union, 2018, pp. 236-248