

Recommendations on IMI transparency obligations

The EU internal market rules give people and businesses the right to move freely within the European Economic Area (EEA) for work, study, or other purposes. Since your authority is involved in the cooperation procedures for applying these rules, via the Internal Market Information System (IMI), you are required to exchange information with competent authorities in other countries, and therefore to process personal data.

This means that, as data controller, you have to comply with the General Data Protection Regulation (GDPR)¹, which is directly applicable throughout the EEA. Under the GDPR, transparency obligations play a key role in ensuring the rights of data subjects in relation to the processing of their personal data.

The following recommendations are intended to assist you, as a data controller, in complying with the GDPR's data protection provisions on the information to be provided to data subjects, in relation to the data processing carried out by your authority when using the IMI.

The recommendations briefly describe what information must be given to data subjects and when and how this information must be provided under the GDPR in combination with the IMI Regulation².

Your obligations as an actor within the IMI are laid down in the IMI Regulation.

This regulation determines³ that an IMI actor, being a data controller, shall ensure that data subjects are informed *as soon as possible* about the processing of their personal data in the IMI, and of the identity and contact details of the controller and of the controller's representative, if any. They must also be informed of their individual rights⁴ and how they can exercise them. These information duties must be complied with in accordance with the GDPR⁵.

¹ Regulation (EU) 2016/679 (GDPR).

² Regulation (EU) No 1024/2012 (IMI Regulation).

³ Article 18 IMI Regulation.

⁴ Article 191MI Regulation.

⁵ The reference in Regulation 1024/2012 to Directive 95/46/EC shall be construed as a reference to the GDPR, pursuant to Article 94 (2) GDPR.

Therefore, the provisions of the GDPR on transparency and information obligations⁶ also apply to the processing of personal data in the IMI and must be complied with to ensure the principle of transparency⁷ is respected. This requires that that personal data is processed in a fair and transparent manner in relation to the data subject. As an IMI actor and data controller, you must be able to demonstrate compliance with this principle⁸. In addition, the GDPR ensures the protection of data subject rights by the national data protection authorities⁹, also when their data are processed in the IMI.

I. What information should be provided?

When providing information to the data subject under the GDPR, it is important to establish whether the data is obtained directly from the data subject or from another source. This distinction determines the scope of the information obligations and possible exceptions. Please note that the requirements of applicable national legislation must also be observed in this regard.¹⁰

You are obliged to act appropriately to provide data subjects with the relevant information in accordance with Articles 13 and 14 GDPR.

1. Information obligation in case of direct collection from the data subject

According to Article 13 GDPR, you must provide the data subject with certain information on your own initiative, where the personal data was collected directly from the data subject. The data subject should, at least, be informed of the following:

- Name and contact details of the controller, i.e. the public body processing the data;
- Contact details of the Data Protection Officer (DPO);
- Purposes and legal basis for the processing of personal data, matching each purpose with the corresponding legal basis; in case the data processing is based on the compliance with a legal obligation to which you are subject¹¹, you may indicate the legal reference;
- Recipients or categories of recipients of personal data;
- Data retention period or, if not possible to provide a specific deadline, the criteria used to determine that period;
- Reference to the data subject rights, explaining what these rights are and how to exercise them;
- The right to lodge a complaint with the data protection supervisory authority;

If relevant: the performance of automated decision-making, including profiling, together with information about the logic involved, as well as the scope and intended effects of the processing for the data subject.

⁶ Articles 12 to 14 GDPR.

⁷ Article 5 (1) (a) GDPR.

⁸ Pursuant to Article 5(2) GDPR.

⁹ Article 21(1) of IMI Regulation.

 $^{^{10}}$ Article 20 of IMI Regulation.

 $^{^{\}rm 11}$ Pursuant to Article 6 (1) (c) or Article 9 (2) GDPR

Please note:

This list is not exhaustive. Further information must be provided to the data subject in accordance with Article 13 (2) GDPR and Article 13 (3) GDPR, if certain conditions are met.

2. Information obligation in case of collection from third parties

Where personal data have not been obtained directly from the data subject, but from other sources, Article 14 GDPR prescribes which information is to be provided. In this situation, in addition to all the information required by Article 13 GDPR as set out above, the data subject must also be informed of the categories of personal data that are processed about them. This is because, in circumstance where the data subject did not provide their data themselves, they will not already know this. Additionally, when collecting data from third parties, you must also inform the data subject of the source from which you obtained their personal data.

This information must be communicated to data subjects within a reasonable period¹² of obtaining the data, but at the latest within one month. If the personal data is used for communication with the data subject, this information shall be communicated at the latest at the time of the first contact. If disclosure to another recipient is intended, the information shall be made available at the latest at the time of the first disclosure.

3. Information in case of change of purpose

Both direct collection and indirect collection require data subjects to be informed prior to the change of purpose in accordance with Article 13 (3) and Article 14 (4) GDPR. A change of purpose may occur, for example, if personal data is made available to third parties.

4. Exceptions to the obligation to provide information

If the data subject already has the information, the information obligations under Articles 13 and 14 GDPR do not apply. In the case of third-party collection, the obligation to provide information does not apply if it proves impossible or would require disproportionate effort, if the means of obtaining the data is expressly regulated by law, or in case that the data is subject to an obligation of professional secrecy regulated by law.

In addition, the GDPR and some national regulations regulate further exceptions.

II. How the information should be provided

Not only the content of the information is important, but also how the information is provided to individuals. Special attention should be given to the intended addressees to ensure the language is clear and appropriate, and that the message is easily understood.

On the other hand, the accessibility of the information largely depends on the format in which it is provided. Please take into consideration that individuals may prefer to use alternatives to online

¹² For more information, Article 14 (3) GDPR

services when interacting with public authorities, including in-person attendance and physical correspondence. Be prepared to facilitate this where appropriate.

5. Implementation of the information requirements in accordance with Article 12 GDPR

According to Article 12 GDPR, information needs to be provided in clear and simple language and in a concise, transparent, comprehensible and easily accessible form.

The information referred to in Articles 13 and 14 GDPR shall be provided in writing, or where appropriate, by other means, including electronic means. Controllers should take into account that data subjects increasingly prefer to interact with public authorities remotely where possible. Transparency information should therefore take account of this reality and be adjusted accordingly to ensure that it is always adequate and intelligible to the reader.

Organisations using the IMI should have processes in place to ensure that the information is made available to data subjects in an appropriate form. In addition to the procedural rules, the definition of responsibilities must be laid down in the process design. The provision of the information should be documented.¹³

In addition to the information provided directly to the data subject, it is recommended, as a rule, to make transparent information publicly available using other media, such as providing general information about data processing in the IMI on your website.¹⁴

6. Implementation of processes to guarantee data subject rights under Article 12 GDPR

Technical and organisational measures should be implemented to guarantee the rights of the data subject. In addition to the determination of responsibilities and procedural safeguards (e.g. identity checks where necessary) this may also include logging obligations to the extent necessary. It is strongly recommended that these technical and organisational measures are implemented in a binding and transparent manner and by means of in-house procedures.

Modalities must be laid down to facilitate the exercise of data subject rights.¹⁵ An organisation using the IMI should for example ensure that requests can be submitted electronically. In addition, the controllers shall reply to requests from the data subjects exercising their rights without delay, and in principle, at the latest, within one month of receipt of the request, and, if this is not the case, explain the reasons for the delay, for not taking action or for the refusal of the request.

III. Data Subject Rights under the GDPR

Transparency obligations enable data subjects to exercise their rights. Individuals whose personal data are collected, retained or otherwise processed by public sector bodies, when using the IMI, have rights

¹³ Article 5 (1) (a) and (2) GDPR

 $^{^{\}rm 14}$ link website Commission and the National IMI Coordinators

 $^{^{\}rm 15}$ Article 12 and Recital 59 GDPR

with respect to their personal data¹⁶. You, as data controller, shall facilitate the exercise of those rights, under Articles 15 to 22 GDPR.

7. Catalogue of Data Subject Rights

This means that data subjects have at least the following rights in relation to the IMI, depending also on the legal basis of the data processing and on any national derogations:

- Right of access (Article 15 GDPR)
- Right to rectification (Article 16 GDPR)
- Right to erasure (Article 17 (1) GDPR) and the right to be forgotten (Article 17 (2) GDPR)
- Right to restriction of processing (Article 18 GDPR)
- Right to object (Article 21 GDPR).

When receiving a request from a data subject, you must ensure that it is handled in full compliance with the GDPR.

The data subject shall receive an answer without undue delay and in any event within one month upon receipt of the request. That period may be extended by two further months if necessary. In that case, you shall inform the data subject of the reasons for the delay, within one month upon receipt of the request.

If you do not take action on the request, the data subject shall be informed without delay, and in any case within one month, on the reasons for such refusal together with the possibility to lodge a complaint with the supervisory authority and to seek a judicial remedy.

Any information given to data subjects shall be provided free of charge, unless requests from a data subject are manifestly unfounded or excessive; in such cases, a reasonable fee may be charged to the data subject, taking into account the administrative costs involved in handling the request. The burden of proof of that situation lies with you, as the data controller.

In the event that there are doubts about the data subject's identity, additional information may be requested to ascertain that the person requesting the information is the data subject concerned.

7.1 Right of access pursuant to Article 15 GDPR

Article 15 GDPR provides for a right of access for data subjects. The right of access is expressly recognised by the EU Charter of Fundamental Rights¹⁷ and, consequently, it is one of the most important data subject rights under the GDPR. It often lays the foundation for exercising other data subject rights, such as rectification and erasure requests.

A data subject must be informed upon request whether his or her personal data is being processed, and if so, what these data are. This means that a data subject must also be informed if no personal data is processed. This right includes three different components¹⁸:

 Confirmation as to whether personal data of the person requesting access are processed or not

 $^{^{\}rm 16}$ Article 19 of the IMI Regulation in conjunction with Chapter III GDPR

¹⁷ Article 8 (2) of the Charter.

¹⁸ <u>Guidelines 1/2022 on data subject rights – Right of access</u>, version 2.0, of the EDPB

- Access to the personal data, the data subject must be able to download their data in a commonly used electronic form or receive a (paper) copy of these data
- Access to information about the processing.

A data subject must be provided with a copy of the personal data being processed.

In addition, the data subject has the right to obtain the following information:

- The processing purposes;
- The categories of personal data that are being processed;
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- The period of storage, or, if this is not possible, the criteria for determining that period;
- The existence of data subject rights to rectification, erasure, restriction of processing; objection based on the particular situation of a data subject;
- The right to lodge a complaint with a supervisory authority;
- In the case of third-party collection, information on the origin of the data;

If relevant: the existence of automated decision-making, including profiling, as well as, information about the logic involved, as well as the scope and intended effects of the processing for the data subject;

If relevant: where data is transferred to a third country, information on the appropriate safeguards to protect the data.

When the request is made by electronic means, the data and any other information must be provided in a commonly-used electronic form, unless otherwise requested by the data subject.¹⁹

You must ensure an appropriate level of security while sending the data to the data subject, in particular when dealing with special categories of personal data. Therefore, a controller must take into account data security requirements when choosing the means of transmitting the electronic file to the data subject. This may include applying encryption, password protection, and so forth.

Please note:

This right shall not affect the rights and freedoms of others, especially third-party personal data.²⁰

7.2 Right to rectification pursuant to Article 16 GDPR

According to Article 16 GDPR, data subjects have the right to obtain from the controller the rectification of inaccurate personal data or, taking into account the purposes of the processing, the completion of incomplete personal data.

This concerns for example information that is objectively inconsistent with reality, e.g. an incorrect name or date of birth, or incomplete data or data that has become obsolete for not being kept up-to-date The correction of inaccurate personal data must be carried out without undue delay.

¹⁹ Article 12(1) GDPR

²⁰ Article 15(4) GDPR

7.3 Right to erasure ("right to be forgotten") pursuant to Article 17 GDPR

In accordance with Article 17 (1) GDPR, data subjects have the right, under certain conditions, to order the erasure of their personal data without undue delay. According to Article 17 (1) (a) GDPR, the data must be erased if they are no longer necessary for the purposes for which they were collected or otherwise processed. In addition, the personal data must be erased if there is no (longer) a legal basis for the processing. This is the case, for example, when the consent on which the processing was based is withdrawn, if the data were processed unlawfully, or the data must be erased under a legal provision. Further storage of the data is inadmissible, unless one of the exceptions set out in Article 17 (3) GDPR applies.

According to the IMI Regulation, the correction or erasure of data must be carried out as soon as possible, and at the latest 30 days after the request from the data subject is received.²¹ This deadline is aligned with the one-month period provided by the GDPR. Where the accuracy or lawfulness of data blocked in the IMI, according to the IMI Regulation, is contested by the data subject, it must be recorded, together with the accurate, corrected information.²²

7.4 Right to restriction of processing pursuant to Article 18 GDPR

According to Article 4 (3) GDPR, the restriction of processing is the marking of stored personal data with the aim of limiting their processing in the future. In accordance with Article 18 (1) GDPR, the restriction of processing must be carried out upon request by the data subject:

- if the accuracy of the personal data is disputed by the data subject, for a period of time enabling the controller to verify the accuracy of the personal data;
- if the processing is unlawful and the data subject opposes the erasure of the personal data and instead requested the restriction of the use of the data;
- if the controller no longer needs the personal data for the purposes of processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims²³. In this case, the interests of the data subject must be weighed against the interest of deletion;
- if the data subject has objected to the processing pursuant to Article 21 (1) GDPR.

7.5 Right to object pursuant to Article 21 GDPR

In principle, Article 21 (1) GDPR grants the data subject a general right to object to data processing that might be in itself lawful. Following receipt of an objection, the controller may no longer process that personal data, unless they can provide a compelling legitimate ground that outweighs the interests of the data subject, or if the processing serves to assert, exercise or defend legal claims.

The right to object pursuant to Article 21 (1) GDPR can be invoked if the processing of personal data is necessary:

²¹ Article 19(1) IMI Regulation

²² Article 19(2) IMI Regulation

²³ Article 18(1) (c) GDPR

- for the performance of a task entrusted to the controller which is in the public interest, or is carried out in the exercise of official authority²⁴;
- to safeguard the legitimate interests of the controller or a third party and where the interests or fundamental rights and freedoms of the data subject do not outweigh that interest.²⁵ It should be highlighted, however, that this legal basis must not apply to data processing carried out by public authorities in the performance of their tasks.

The objection needs, in principle, to be justified. This means that the grounds for objection should not arise from the processing circumstances as such, but must be based on the particular situation of the data subject. Following receipt of an objection, the controller must undertake a balancing of interests. Unless the controller can prove that any of the above reasons apply, the personal data in question must no longer be processed and must in principle be deleted.²⁶

Please note: Article 21 GDPR cannot be invoked if the processing by the controller is necessary to comply with a legal obligation as provided for in Article 6 (1) (c) GDPR.

Further information on transparency obligations can also be found in the <u>Guidelines on</u> <u>transparency under Regulation 2016/679</u>, of the Article 29 Working Party and endorsed by the EDPB in 25 May 2018 (WP 260, rev.01)

You may also contact your national Data Protection Authority.

²⁴ Article 6 (1) sub (e) GDPR

²⁵ Article 6 (1) sub (f) GDPR

 $^{^{26}}$ Article 17 (1) (c) GDPR