Data protection rules implementing Regulation (EU) 2018/1725

November 2022

European Investment Bank

The EU bank

Data protection rules implementing Regulation (EU) 2018/1725

November 2022

Data protection rules implementing Regulation (EU) 2018/1725

© European Investment Bank, 2022.
All rights reserved.
All questions on rights and licensing should be addressed to publications@eib.org

For further information on the EIB's activities, please consult our website, www.eib.org.
You can also contact our info Desk, info@eib.org.

European Investment Bank
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
+352 4379-1
info@eib.org
www.eib.org
twitter.com/eib
facebook.com/europeaninvestmentbank
youtube.com/eibtheeubank

Published by the European Investment Bank.

Printed on FSC® Paper.

Data protection rules implementing Regulation (EU) 2018/1725

Adopted on 9 November 2020

Reviewed on 10 November 2022

The Management Committee of the European Investment Bank,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 (2) thereof,

Having regard to Regulation (EU) 2018/1725 ("Regulation") of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, and in particular Article 45 (3) thereof,

Whereas:

1. The Regulation lays down the principles and rules applicable to all Union institutions and bodies and provides for a Data Protection Officer (DPO) to be appointed by each Union institution and body.

2. Pursuant to Article 45 (3) of the Regulation, each Union institution or body must adopt further implementing rules concerning the DPO in accordance with the provisions in Articles 44 and 45 of that Regulation.

Has adopted the following rules.

SECTION 1
General provisions

Article 1
Subject matter and scope

These internal provisions lay down the rules implementing the Regulation as regards the Bank.

For the purposes of these internal rules, the definitions set out in Article 3 of the Regulation shall apply.

SECTION 2
The Data Protection Officer (DPO)

Article 2
Designation and status of the DPO and organisational measures

1. The President of the Bank, after consultation of the Bank's Management Committee ("Management Committee"), shall designate the DPO from among members of the Bank's staff who are sufficiently senior to meet the requirements of Article 43 of the Regulation.

   The DPO shall be designated for a term of three to five years and shall be eligible for reappointment. The President of the Bank shall decide on the reappointment of the DPO, following consultation of the Bank's Management Committee. The President shall decide on the length of the term of the DPO.

   The DPO shall be designated on the basis of his or her personal and professional qualities as they relate to the DPO functions and, in particular, his or her expert knowledge of data protection law and practices, including the ability to fulfil the tasks referred to in Article 45 of the Regulation.

   The Secretary General of the Bank shall register the DPO with the European Data Protection Supervisor (EDPS).

   The selection of the DPO shall not result in a conflict of interest between his or her duty as DPO and any other duties that the DPO might exercise within or outside the Bank, in particular in relation to the application of the provisions of the Regulation.

2. The DPO may be dismissed from his or her post if he or she no longer fulfils the conditions required for the performance of his or her duties. Dismissal can only occur following the consent of the EDPS. The DPO shall not be dismissed or otherwise penalised by the Bank for performing the tasks relating to the role of DPO.

3. The DPO shall be duly involved in a timely manner in all issues that relate to the protection of personal data.

4. Data subjects may directly contact the DPO with regard to all issues related to the processing of their personal data and to the exercise of their rights under the Regulation.

5. In exercising his or her duties, the DPO shall act in an independent manner and in cooperation with the EDPS and shall not receive any instructions regarding the exercise of his or her tasks, or regarding his or her cooperation and consultation with the EDPS.

   The DPO shall directly report to the highest management level of the Bank. The DPO shall have a yearly session with the Management Committee to present his or her annual activity report, including any encountered DPO issues and monitoring results.

   Without prejudice to the independence of his or her role, the DPO shall be subject to the provisions applicable to members of the Bank's staff. For administrative purposes, the office of the DPO shall form part of one of the Bank's organisational areas without prejudice to his or her independence, in particular with regard to his or her duties as DPO.

   The Bank shall ensure that any other responsibilities entrusted to the DPO shall be compatible with the DPO's duties.

6. The DPO and his or her staff shall be bound by professional secrecy and/or confidentiality concerning the performance of their tasks, in accordance with EU law and the applicable internal rules of the Bank.

7. The persons assisting the DPO on data protection matters shall be appointed after consultation with the DPO. When working on matters relating to data protection, such persons shall act solely on the DPO's instructions.

8. Directorates may designate a DPO coordinator to liaise with the DPO. The coordinator shall act as the contact point for the DPO and refer to the DPO for any matter related to data protection.

9. The Secretary General of the Bank shall determine the deputising arrangements for occasions when the replacing DPO is prevented from acting in such a capacity in line with the "Memorandum of Understanding between the EIB and the EIF regarding the replacement of the Data Protection Officers of the EIB and the EIF".

Article 3
Tasks

When carrying out the tasks specified in Article 45 of the Regulation, the DPO shall:

a) inform and advise the Bank and its staff members who carry out data processing of their obligations pursuant to this Regulation and/or other data protection provisions of EU law;

b) ensure in an independent manner the internal application of the Regulation and monitor compliance with the Regulation, as well as all other relevant provisions of EU law and policies of the Bank in relation to the protection of personal data. This includes the assignment of responsibilities (e.g. for data controllers, data processors), the raising of awareness and training of staff involved in processing operations, and conducting audits;

c) ensure that data subjects are informed of their rights and obligations pursuant to the Regulation; in carrying out this task, the DPO shall make information available to the data subjects, consult with the parties concerned and take steps to raise awareness of data protection issues;

d) provide advice as regards the necessity for the notification or communication of a personal data breach pursuant to Articles 34 and 35 of the Regulation; and propose policy and procedural measures, including the creation of an incident response team in relation to personal data breaches;

e) provide advice where requested as regards the data protection impact assessment pursuant to Article 39 of the Regulation, as well monitoring its performance and consulting the EDPS in case of doubt as to the need for a data protection impact assessment, in particular in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- processing on a large scale of special categories of data referred to in Article 10 of the Regulation, or of personal data relating to criminal convictions and offences referred to in Article 11 of the Regulation; or

- a systematic monitoring of a publicly accessible area on a large scale.

f) provide advice where requested as regards the need for prior consultation of the EDPS pursuant to Article 40 of the Regulation and to consult the EDPS in case of doubt as to the need for a prior consultation;

g) act as the EIB's contact point for the EDPS for all data protection related matters;

h) respond to requests from the EDPS and, within the sphere of his or her competence, cooperate and consult with the EDPS at the latter's request or on his or her own initiative;

i) ensure that the rights and freedoms of data subjects are not adversely affected by processing operations; and

j) on his or her own initiative, upon a request made by the President, by any controller or processor, by the Bank's organisational areas, by the College of the Staff Representatives or by any other individual, the DPO shall investigate matters and occurrences that directly relate to his or her responsibilities and have been brought to his or her attention. Following his or her investigation, the DPO shall make a report addressed to the President, the entity or person initiating the request. All other parties who may be concerned by the investigation shall be informed accordingly. If the requester is an individual or acting on behalf of an individual, the DPO must, to the extent possible, ensure that the request remains confidential unless the data subject gives unambiguous consent for the request to be treated otherwise.

Article 4
Other activities

1. The DPO may fulfil other tasks and duties that are not linked with matters relating to data protection. The Bank shall ensure that any such tasks and duties do not result in a conflict of interest with the responsibilities of the DPO.

2. In addition to the general tasks assigned to him or her, the DPO shall:

   a) advise the Bank's services, as well as the controllers and/or the processors, on matters concerning data protection law. The DPO may be consulted directly, without going through official channels, on any issue concerning the interpretation or application of the Regulation, by the Bank's services, by the relevant controllers and/or processors, by the College of Staff Representatives or by any other individual;

   b) in carrying out his or her duties, cooperate with the DPOs of the other EU institutions, bodies, offices and agencies, in particular by exchanging experience and best practices;

   c) represent the Bank with regard to all data protection issues, except for matters referred to a competent court or the European Ombudsman;

   d) submit to the Management Committee and the EDPS an annual report on the DPO's activities and make it accessible to staff members;

   e) propose policy and/or procedural measures, including guidance notes or other documents, related to the implementation of the Regulation.

3. No one shall suffer prejudice on account of bringing a matter to the DPO's attention alleging a breach of the provisions of the Regulation.

4. In accordance with the Memorandum between the EIB and EIF regarding the replacement of the Data Protection Officers of the EIB and the EIF, the DPO of the EIB and the DPO of the EIF will replace each other whenever either of them is absent or otherwise unable to fulfil his or her tasks.

Article 5
Powers

In carrying out his or her tasks and duties, the DPO:

a) shall have at all times physical access to all premises of the Bank, and physical and/or electronic access to data being processed, all data processing installations and all information media;

b) may, without prejudice to the duties and powers of the EDPS, propose administrative measures to the Bank's Secretary General;

c) may make general recommendations on the appropriate application of the Regulation;

d) may, in particular circumstances, make any other recommendation to the Bank's Secretary General and/or all the other parties concerned for the concrete improvement of the Bank's data protection processing operations;

e) may bring to the attention of the Bank's Secretary General and the Director General of Personnel any failure by a staff member to comply with the obligations pursuant to the Regulation and propose an initiation of disciplinary proceedings as specified in article 69 of the Regulation, in accordance with the Bank's Staff Regulations and Staff Rules;

f) may request an opinion from the relevant services of the Bank on any issue associated with his or her tasks and duties.

Article 6
Resources

The DPO shall be allocated the resources necessary to appropriately perform his or her duties, to enable access to personal data and processing operations, and to maintain his or her expert knowledge.

SECTION 3
Controller

Article 7
Tasks and duties of the Bank as a controller

1. Controllers shall ensure and be able to demonstrate that all processing operations involving personal data that are performed within the controllers' sphere of responsibility comply with the Regulation. The following provisions mainly cover interactions between the controller and the DPO and are without prejudice to the (remaining) obligations of the EIB as controller as mandated by the Regulation.

2. Where one or more EIB controllers jointly determine the purposes and means of the processing, they shall be joint controllers. Where an EIB controller jointly determines the purposes and means of the processing with one or more external controllers, they shall also be joint controllers.

   By means of a written arrangement between the joint controllers upon consultation with the DPO, they shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations referred to in the Regulation. Such an arrangement shall be without prejudice to their respective responsibilities as determined by EU or national law to which the controllers are subject. The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis data subjects. The essence of the arrangement shall be made available to all data subjects, who may exercise their rights under the Regulation in respect of and against each of the controllers, taking into account their roles as determined in the terms of the arrangement.

3. Where a type of processing (in particular, one using new technologies) is likely to result in a high risk to the rights and freedoms of natural persons, the relevant controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. In doing so, the controller shall describe the envisaged processing operation and its purpose, assess its necessity and proportionality vis-à-vis its purpose and assess the risks to the rights and freedoms of the data subjects. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the DPO when carrying out a data protection impact assessment.

4. When fulfilling his or her obligation to assist the DPO and/or the EDPS in the performance of their duties, the relevant controller shall provide them with all relevant information, grant them access to personal data and respond to their questions. As regards the DPO, the controller shall respond to such requests for information within a period not exceeding thirty working days from receipt of the request.

5. The relevant controller shall ensure that the DPO is informed without undue delay:

   a) when an issue arises that has or could have data protection implications; and

   b) of all contacts established with third parties relating to the application of the Regulation, in particular with regard to interaction with the EDPS.

6. In case of a personal data breach, the relevant controller shall notify and involve the DPO in its evaluation without undue delay after becoming aware of the personal data breach or any incident that could be considered as constituting a personal data breach.

7. The relevant controller shall implement appropriate technical and organisational measures to ensure a level of security adequate to the processing risks and the nature of the personal data to be protected. The controller shall consult the DPO when setting up relevant policies having personal data security implications. In instances where a controller requests the DPO to advise on the appropriateness of technical and organisational measures ensuring the security of a given operation involving personal data processing, CS-IT, upon the DPO's request, shall provide its expert advice on security matters.

8. The relevant controller shall maintain a record of processing activities under his or her responsibility including all information referred to in Article 31 of the Regulation. This obligation of the controller shall be fulfilled by submitting the record to the central register kept by the DPO, as provided for by Article 8.

9. The relevant controller shall validate the accuracy of the information included in the records of processing activities under his or her responsibility on a biennial basis. The DPO must be notified without delay by the controller of any change affecting this information.

10. Whenever drafting data protection contractual clauses with processors (Chapter IV of the Regulation) or data protection clauses related to the transfer of personal data to third countries or international organisations (Chapter V of the Regulation) the relevant controller shall consult the DPO.

Article 8
Records of processing activities

1. The relevant controller shall transmit the records of processing activities to the DPO, who shall publish them upon receipt in a central register. The DPO shall further determine the means by which the register is kept. Following the guidance of the DPO, controllers shall review the records of their processing activities on a biennial basis.

2. The Bank shall make the central register publicly accessible according to Article 31 (5) of the Regulation. The register shall be made available to the EDPS upon request.

Article 9
Tasks and obligations of the Bank as a processor

1. Where the Bank or a service of the Bank acts as a processor, it shall ensure that the Bank's obligations under the Regulation are respected. In particular, the processor shall ensure that it:

   a) implements appropriate technical and organisational measures to ensure a level of security appropriate to the processing risks and the nature of the personal data to be protected;

   b) takes into account the nature of the processing and assists the relevant controller by adopting appropriate technical and organisational measures (insofar as this is possible) for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the Regulation;

   c) assists the relevant controller in ensuring compliance with the obligations pursuant to Articles 33 to 40 of the Regulation taking into account the nature of processing and the information available;

   d) at the request of the relevant controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless EU or national law requires the continued storage of the personal data in question;

   e) makes available to the relevant controller all information necessary to demonstrate compliance with the obligations laid down in Article 7 of these implementing Rules and duly cooperates in and contributes to audits of the DPO and/or the EDPS, including inspections conducted by the controller or another auditor mandated by the controller;

   f) keeps a record of all categories of processing activities carried out on behalf of the relevant controller;

   g) shall consult the DPO on the drafting of data protection contractual clauses with controllers or sub-processors (Chapter IV of the Regulation) or of data protection clauses related to the transfer of personal data to third countries or international organisations (Chapter V of the Regulation).

SECTION 4
Data subjects' rights

Article 10
Access to the register

The register kept by the DPO pursuant to Article 31 of the Regulation shall serve as an index of all processing operations relating to personal data conducted by the Bank. Data subjects may make use of the information contained in the register to exercise their rights under Articles 14 to 24 of the Regulation. Any person may consult the register directly or indirectly through the EDPS.

Article 11
Exercise of data subjects' rights

1. In accordance with their right to be appropriately informed about any processing of their personal data, data subjects may contact the relevant controller to exercise their rights pursuant to Articles 14 to 24 of the Regulation as specified below.

    a) These rights may only be exercised by the data subject or his or her duly authorised representative. Such persons may exercise any of these rights free of charge.

    b) Requests to exercise their rights under the Regulation shall be addressed in writing to the relevant controller. The controller shall respond to the request provided that the requester's identity or, in the case of a duly authorised representative, his or her entitlement to represent the data subject, have been appropriately verified. Upon receiving a request from a data subject, the relevant controller shall send an acknowledgment of receipt to the data subject within five working days, provide him or her with the contact details of the DPO and inform him or her of the possibility of lodging a complaint with the EDPS and of seeking judicial redress. The controller shall without delay and in any event within one month of receipt of the request inform the data subject in writing of whether or not the request has been accepted. If the request has been rejected, the controller's response shall include the grounds for the rejection.

    c) If the data subject's request has been accepted, the relevant controller shall, without undue delay and in any event within one month of receipt of the request, grant the data subject access to his or her personal data by enabling them to consult his or her personal data by electronic means where possible, unless otherwise requested by the data subject. In case of rectification, erasure, objection or data portability request the data controller shall inform the data subject on his or her decision and the follow-up action taken in response. That period may be extended by two additional months where necessary, taking into account the complexity and the number of requests received by the controller. The controller shall inform the data subject accordingly.

d) Data subjects may contact the DPO if the controller does not comply with the time requirement specified in paragraphs (b) or (c) of this article. In the event of an evident abuse by a data subject in the course of exercising his or her rights under Articles 14 to 24 of the Regulation, the relevant controller may refer the case to the DPO, who can determine the merits of the request and advise on the appropriate follow-up. In the event of disagreement between the data subject and the controller, both parties shall have the right to consult the DPO.

2. Members of the Bank's staff and any other individual may consult the DPO before addressing the EDPS or lodging a complaint with the EDPS pursuant to Article 63 of the Regulation, whenever they consider that the processing of their personal data infringes the Regulation.

Article 12
Exemptions and restrictions

1. The relevant controller may restrict the rights referred to in Articles 14 to 22, 35, and 36, as well as Article 4 of the Regulation (in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22), if legitimate reasons specified in Article 25 of the Regulation clearly so justify and when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society. The controller may proceed with such a restriction provided that the DPO has been consulted in advance. Any restriction shall be based on the implementing rules adopted in accordance with Article 25 of the Regulation.

2. Pursuant to Article 58 (2) (d) of the Regulation, any data subject may request the EDPS to order the Bank to comply with the data subject's request to exercise his or her rights under the Regulation.

Article 13
Investigation procedure by the DPO

1. Any request for an investigation shall be addressed to the DPO in writing.

2. The DPO shall send an acknowledgement of receipt to the requester within fifteen working days of receipt of the request.

3. The DPO may investigate the matter in the way he or she sees fit and in line with the provisions included in these implementing Rules. The DPO may conduct an on-site investigation and/or request a written statement from the relevant controller, the processor and/or other person he or she considers relevant to his or her investigation. The controller shall respond to the DPO within a period not exceeding thirty working days from receipt of the DPO's request. The DPO may ask for additional information or assistance from any other of the Bank's services. The requested service shall provide such additional information or assistance within a period not exceeding thirty working days from receipt of the DPO's request.

4. The DPO shall report back to the requester within three calendar months from receipt of the request.

SECTION 5
Final provisions

Article 14
Implementing measures

In line with these rules, the DPO may issue further guidance related to their implementation.

Article 15
Publication

These internal provisions shall be accessible to the public by being displayed on the Bank's website (http://www.eib.org).

Article 16
Entry into force

These rules shall enter into force on the twentieth day following the date of their adoption[1].

[1] These rules were adopted on 20 October 2020 and reviewed on 10 November 2022.

Data protection rules implementing Regulation (EU) 2018/1725

November 2022

European Investment Bank
98 -100, boulevard Konrad Adenauer
L-2950 Luxembourg
+352 4379-22000
www.eib.org – info@eib.org

© European Investment Bank, 11/2022 EN