



CHAFEA Procedure for Handling Data Subject Access Requests (DSAR) and requests for other Rights

Contents

1. Background	2
2. What is a 'Data Subject Access Request'?	3
3. Procedure for handling a Data subject's Rights	3
(1) Identifying a Request of a Data subject to exercise a right	3
(2) Notifying the Data Controller and DPO	4
(3) Verifying identity	4
(4) Reviewing information on the Data Subject request	4
4. Timeframe for handing of requests from Data subject to exercise their rights	5
5. Responding to requests from Data subject to exercise their Rights	5
6. Registry of Data Subjects Requests	6
7. ARES Workflow	6
8. Procedure for handling Data Subject Access Requests	8

1. Background

Regulation (EU) 2018/1725¹ gives individuals ('data subject') several explicit rights.

Individuals have the **right to know** what personal data is held by Data Controllers about themselves, the **right to access** their information and to exercise **other related rights** related to the processing of their personal data by the Data Controller.

What are Data Subjects Rights?

CHAFEA must process personal data *fairly, lawfully* and only for *legitimate purposes*.

This general right is complemented by several specific rights:

Right to transparency (Art.14)

The Data Controller must use clear and plain language when informing data subjects about how their personal data will be processed. The information must be clear, concise and transparent, and it must be provided to them in an easily accessible format.

NEW

Right to access (Art. 17)

Data Subjects have the right to receive information from Data Controllers on whether their personal data is processed by the Agency, the purpose of this processing, the categories of data concerned and the recipients to whom their data are disclosed, the storage period, as well as the right to access this personal data, processed by CHAFEA.

Right to erasure / *

Right to be forgotten (Art.19)

Data subjects have the right to erase their data for example if their personal data is no longer needed by the Data Controller, if they withdraw their consent or if the processing operation is unlawful.

NEW

Right to data portability (Art.22)

Data subjects have the right to obtain the data that the controller holds on them and to transfer it from one controller to another. Where technically possible, the controller has to do this directly.

NEW

Right to be informed (Art.15 & 16)

Data subjects have the right to be informed, for example, about the fact that their data has been processed, the purpose for which it was processed and the identity of the controller. This is usually provided through a Data Protection Notice.

Right to rectification* (Art. 18)

Data subjects have the right to rectify their data if it is inaccurate or incomplete.

Right to restrict the processing* (Art.20)

Data subjects can ask the controller to restrict the data processing under certain circumstances, such as if they contest the accuracy of the processed data or if they are not sure if their data is lawfully processed.

Right to object (Art.23)

Data subjects can object, on compelling legitimate grounds, to the processing of data relating to them.

Rights not to be subject to automated decision making and profiling (Art.24)

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which results in legal consequences for them or significantly affects them in a similar way.

NEW

* The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort (Art. 21).

The following defines the procedure for **requests to access** to personal data received by CHAFEA and requests to exercise **other data subject rights**.

¹ [Regulation \(EU\) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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 \(OJ L 295/39 of 21.11.2018\).](#)

In cases of doubt, please contact your CHAFEA Data Protection Officer (CHAFEA-DATA-PROTECTION@ec.europa.eu).

2. What is a ‘Data Subject Access Request’?

A ‘Data Subject Access Request’ is any request made by an individual (or an individual’s legal representative) to obtain:

- (a) confirmation whether or not personal data concerning him or her is processed (i.e. stored, used, held etc.) by the Data Controller.
- (b) Through the right of access, individuals may as well obtain a copy of their personal data and
- (c) other supplementary information, which largely corresponds to the information that should be provided in a Data Protection Notice ².

3. Procedure for handling a Data subject’s access request and other data subject Rights

(1) Identifying a Request of a Data subject to exercise a right

A data subject can make a request by any means (verbally or in writing) as long as it is clear that the individual is asking to exercise any rights related to his or her own personal data, or of individuals he/she is the legal representative (i.e. minors).

The Data Controller should ‘provide means for requests to be made electronically, especially where personal data are processed by electronic means’³. This is usually done by informing the data subject in the ‘Data Protection Notice’ about a functional mailbox through which they can contact the Data Controller to exercise this right.

Requests of Data subjects should be acknowledged and registered in a specific Ares file by the competent unit.

² Article 17 Regulation (EU) 2018/1725:

- (1) The data subject shall have the 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 and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with the European Data Protection Supervisor; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 24(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.

- (2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 48 relating to the transfer.

(3) Recital 34 Regulation (EU) 2018/1725.

(2) Notifying the Data Controller and DPO

Upon receipt of a Request of a Data Subject, the competent Data Controller shall be promptly informed and the DPO notified via ares.

(3) Verifying identity

Only where the Data Controller has **reasonable doubts** on the identity of the individual requesting to exercise rights referred to in Articles 17 to 23, the Data Controller may request additional information necessary to confirm the identity of the Data subject⁴.

This information must be proportional and limited to only the information that is necessary to confirm the identity of the requester⁵.

In line with the principle of data minimisation, requestors can be invited to provide a copy of an identification document for confirmation of their identity. Only a limited number of personal (identity document number, country of issue, first and last name, address, date and place of birth and document expiration date) needs to be visible on the copy of the identification document. In principle, all other data on the copy of the identification document (eg the photo, any personal characteristics) can be blanked out on the copy.

As the above mentioned personal data is obtained only to be used to verify the identity of the requestor's identity, they cannot become part of the data inventory of the agency.

The retention period for the copy of an identification document is limited to the period required to establish the identity of the requestor.

Any such requests for verification should be done as soon as possible after the receipt of the request. The delay for responding to the request begins when you receive the additional information.

(4) Reviewing information on the Data Subject request

For Access Requests, the Data Controller should provide the relevant and required information as requested and may review this with the Data Protection Officer.

The Data Controller may wish to check with the requester that the access request is correctly understood. Also in case a large amount of personal data of an individual is concerned, clarification from the Data subject's can be requested.

Consideration should be given to whether responding to this access request would adversely affect the rights or freedoms of other individuals⁶, including trade secrets or intellectual property and in particular the copyright protecting the software.

However, the result of those considerations should not be a refusal to provide all information to the data subject⁷. Where possible, the Data Controller should consider whether some of the information can be disclosed or whether the non-relevant information can be anonymised redacted.

⁴ Article 14(6) Regulation (EU) 2018/1725.

⁵ See Data Protection Notice for identifying data subject (data subject rights Regulation (EU) 2018/1725)

⁶ Art.14(4) Regulation (EU) 2018/1725.

⁷ Recital 37 Regulation (EU) 2018/1725.

Where an individual refuses to provide any additional information, the Data Controller should still endeavour to comply with the access request, for example by making reasonable searches for the information covered by the request.

Similarly to point 3), any such requests for clarification should be done as soon as possible after the receipt of the access request. The delay for responding to the access request begins when you receive the additional information.

4. Timeframe for handing of requests from Data subject to exercise their rights

The controller shall reply to the data subject for requests under Articles 17 to 24 without undue delay and in any event **within one month** of receipt of the request⁸.

This delay may be extended by two further months where necessary, taking into account the complexity and number of the requests. In this case, the Data Controller shall inform the Data subject within one month of receipt of the request, together with the reasons for the delay.

5. Responding to requests from Data subject to exercise their Rights

Where the data subject makes the request by electronic form means, the reply shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(1) positive reply – the Data Controller confirms the exercise of the data subjects rights.

- For Access Requests: the Data Controller confirms the processing of personal data, provides the individual with full access to the requested personal data about him/her (or individuals he/she is the legal representative) and the supplementary information about the processing. The data controller can provide a summary of the information relating to the personal data of the individual rather than the whole document. In case the whole document is provided, Regulation 1049/2001 on access to public documents should be considered.

– For other Data subject's Rights: the Controller confirms that the request to exercise of the data subjects rights is well founded and proceeds with the request, e.g. corrects, blocks or deletes the personal data.

(2) partial reply – the Data Controller confirms partially the exercise of the data subjects rights

- For Access requests: the Data Controller provides the individual with some personal data about him/her and responds with some relevant information, justifying why the remaining personal data about him/her cannot be provided.

– For other Data subject's Rights: the Controller confirms that the request to exercise of the data subjects rights is partially founded and proceeds partially with the request, justifying why not the request cannot be entirely justified eg. corrects, blocks or deletes only certain personal data.

⁸ Art.14(3) Regulation (EU) 2018/1725.

(3) negative reply - the Data Controller refuses the exercise of the data subjects rights

- For Access Requests: after carefully checking all available data bases and files, the Data Controller responds to the data subject confirming that no personal data is held or processed concerning him/her and therefore no access can be provided

OR

the Data Controller responds to the data subject with suitable and justifiable reasons for not responding to the request. This can be due to the fact that a request from a data subject is manifestly unfounded or excessive, in particular because of its repetitive character. In this case, the data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request⁹.

– For other Data subject's Rights: after carefully checking all available information, the Data Controller responds to the data subject that he/she refuses the exercise of the data subjects rights based on duly justified reasons. This could be the case e.g. if a restriction decision based on Article 25 applies, if the information is still correct, necessary or lawful.

If the data controller **does not take action** on the request of the data subject, the controller shall inform the data subject without delay and at the latest **within one month** of receipt of the request¹⁰

- a) of the reasons for not taking action,
- b) on the possibility of lodging a complaint with the European Data Protection Supervisor,
- c) on the possibility of seeking a judicial remedy.

6. Registry of Data Subjects Requests

The Data Protection Officer shall keep a register of all requests from data subjects to exercise their rights and document the measures taken. Records of communications relating to a data subject access request shall be registered in ares.

7. ARES Workflow

Request of data subjects should be registered in Ares, with INFO to DPO.

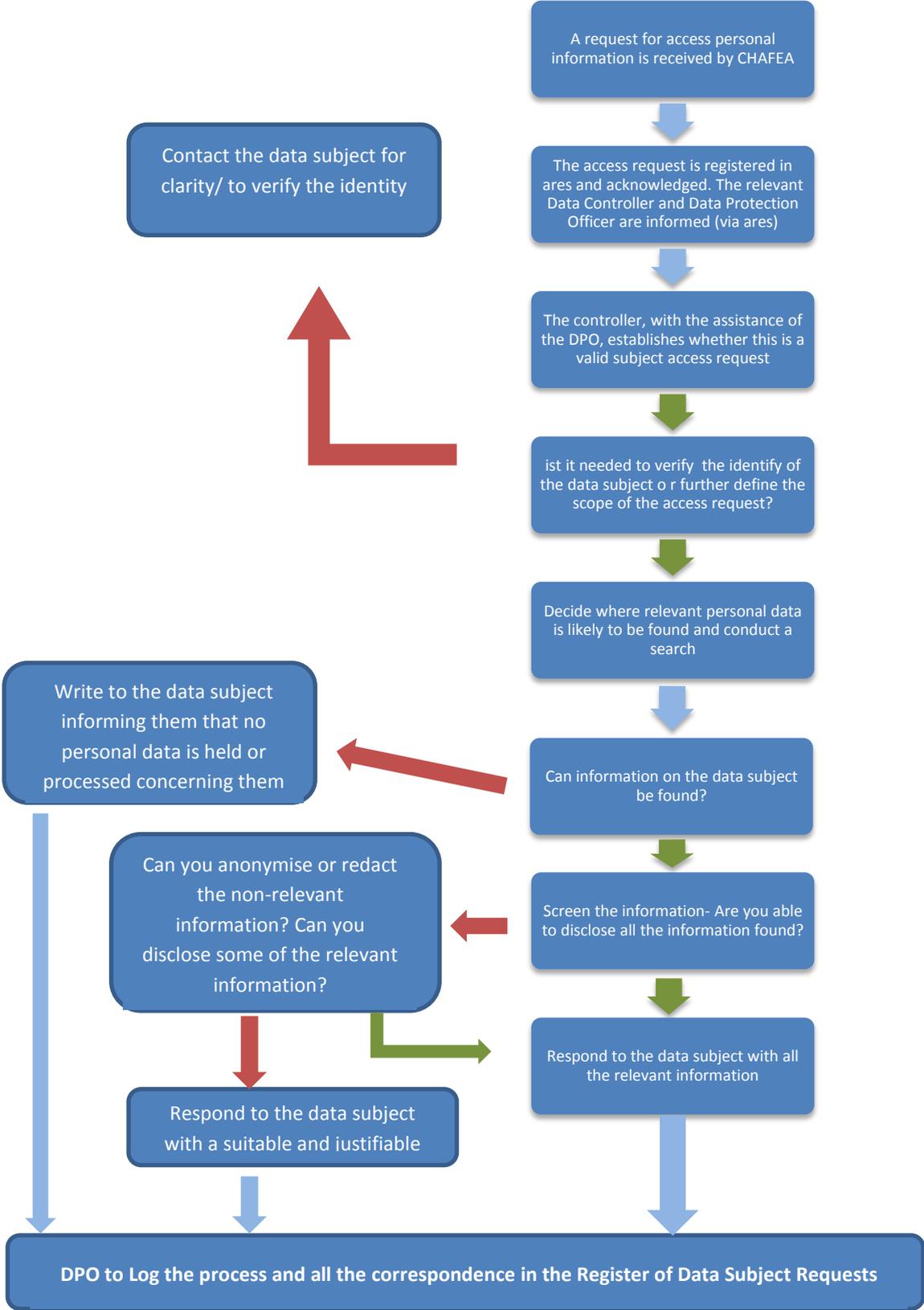
Replies to requests of data subjects to exercise a right should follow the ARES workflow below:

RED	Data Controller
CON	DPO (ve_CHAFEA.legal-advisor)
SIGN	Director
EXP	Data Controller
INFO	DPO (ve_CHAFEA.legal-advisor)

⁹ Art.14(5) Regulation (EU) 2018/1725.

¹⁰ Art.14(4) Regulation (EU) 2018/1725.

8. Procedure for handling Data Subject Access Requests¹¹



¹¹ Can be used also for other data subject rights.