Procedure for Data Subjects Requests

BISS

Contents

1. Purpose *3*
2. Applicability *3*
3. Preliminary information on Data Subject requests handling *3*
1.1 Types of Data Subjects in BISS **3**
1.2 Receiving channels **4**
1.3 Handling of Data Subject requests **5**
1.3.1 Types of data requests 5
1.3.2 Workflows and roles within BISS 5
1.3.2.1 High impact requests 6
1.3.2.2 Low impact requests 6
1.3.2.3 Roles 6
At glance 6
Step 1 – New request 8
Step 2 – Identity verification 8
Step 3 – Check on the request type 8
Step 4 - Involvement of relevant stakeholders 9
Step 5 – Feedback to the Data Subject 9
1.3.2.4 Other relevant information 9
Deadlines 9
Costs 9
Exceptions 9
4. Non-compliance notifications and disciplinary measures *10*
5. Updates and changes to the policy *10*
6. Appendices *10*
1.4 Appendix I – Templates **10**
1.5 Appendix II – Record of exercised data rights **10**

1. Purpose

The purpose of this policy is to define how BISS shall respond to data protection requests and complaints that come from Data Subjects.

2. Applicability

All Authorized Persons working for BISS must be familiar with and apply the provisions described herein as from the Effective Date.

3. Preliminary information on Data Subject requests handling

1.1 Types of Data Subjects in BISS

BISS may face a request to exercise a data right by the following types of Data Subjects:

	Description	Relevant Information Notice	Covered by this policy
Students	Any natural person who is/was a student. It might be the case that, in certain circumstances, "Guardian/Parents (meaning person who has the legal representation of students) may be involved.	Privacy Notice for students	✓
Website users	Any natural person who has used BISS website (e.g., a person who submitted a request for information, who created a parental account, etc.)	Website privacy policy	✓
Suppliers	Any natural or legal person providing services who entails the processing of BISS Personal Data	Information notice for suppliers	✓
Job Applicants	Any natural personal who applies for a job at BISS	Information notice for recruitment	✓
Employees	Any person framed as BISS workforce.	Information notice for employees/collaborators	✓
Supervisory Authorities /governmental bodies	Any Supervisory Authority or other authority, who acts in the performance of their public duties, asking for information Personal Data Processed by BISS	N/A	✗

1.2 Receiving channels

The Admin of BISS shall define, with the support of the IT Department, the specific electronic contact details to receive Data Subjects' requests. Such contact details shall be indicated in each and all information notices to Data Subjects.

Notwithstanding the above, the Data Subject may contact the Data Controller by writing to the BISS Schools/ Preschool postal address:. Below a summary of the possible options (the "stars" indicate the preferred channel) and the instructions that the Management must follow to manage requests:

	Description	Allowed	Management (To do)	Timeline
☆☆☆ **Privacy dedicated channel**		✅	Follow the Workflows (section 1.3.2 below)	See Workflows
Contact us channels (e-mails)		⚠️	Forward to the privacy dedicated channel and follow the Workflows (section 1.3.2 below)	As soon as possible
Paper mail	Request received at BISS postal address	✅	Follow the Workflows (section 1.3.2 below)	See Workflows
Phone/Oral channels	Request received via phone or via oral channels	⚠️	Ask the Data Subject to use the privacy dedicated channel	As soon as possible
Social Media	(e.g., Facebook Messenger, SMS, instant messaging)	⚠️	Ask the Data Subject to use/forward the request to the to privacy dedicate channel	As soon as possible
Other platforms	(e.g., Mine, Privacy Bee etc.)	✅	Follow the Workflows (no need to reply on platforms)	See Workflows
Automatic Unsubscribe	(e.g., e-mail links)	✅	Nothing	N/A

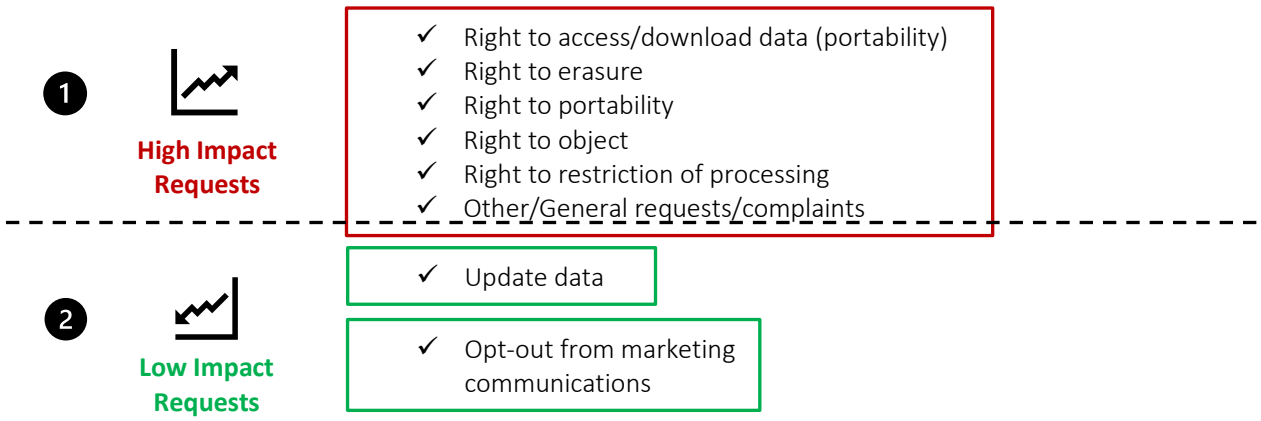
1.3 Handling of Data Subject requests

1.3.1 Types of data requests

The following data subject rights shall be taken into account by BISS:

- Right of access: right to obtain from BISS confirmation if Personal Data related to the Data Subject are processed and, in case, have access to them;
- Right to rectification: right to obtain from BISS, without undue delay, the correction of inaccurate Personal Data concerning the Data Subject;
- Right to erasure ("right to be forgotten"): right to obtain from BISS the erasure of Personal Data concerning the Data Subject without undue delay;
- Right to restriction of processing: right to obtain from BISS a limitation on the Processing activities on Data Subject' Personal Data;
- Right to data portability: right to receive from BISS the Personal Data concerning the Data Subject, in a structured, commonly used and machine-readable format and/or transmit those data to another Data Controller, if the Processing is carried out by automated means;
- Right to object: right to object at any time to Processing of Personal Data concerning the Data Subject.

BISS has divided these rights into the following two categories:

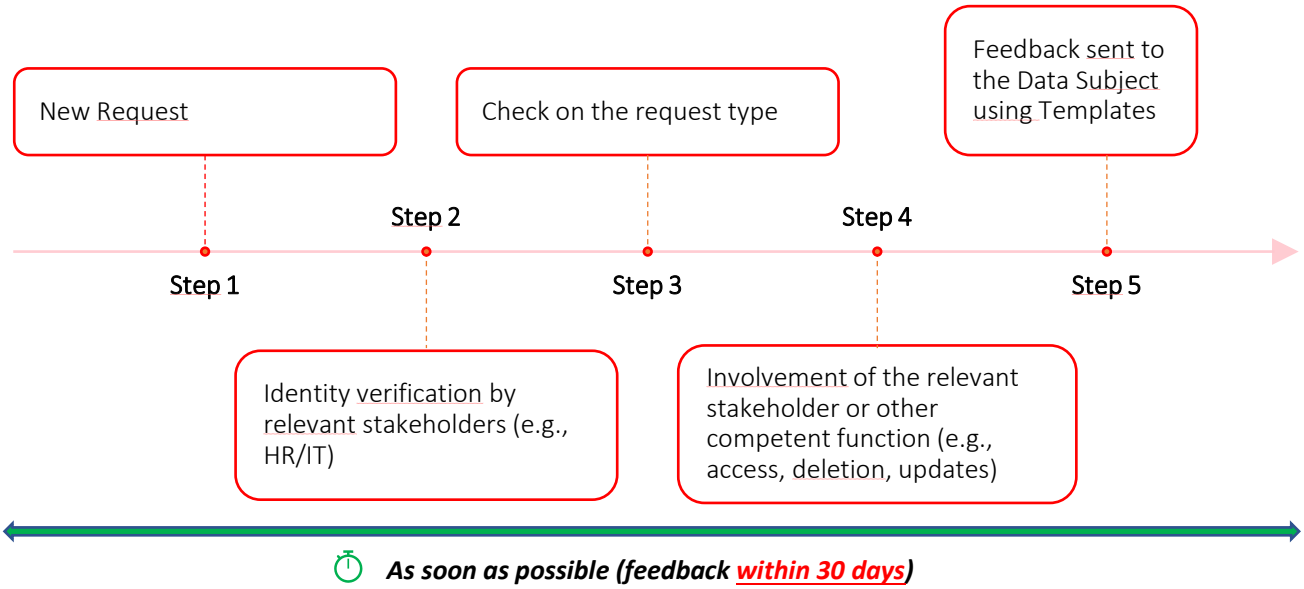


1.3.2 Workflows and roles within BISS

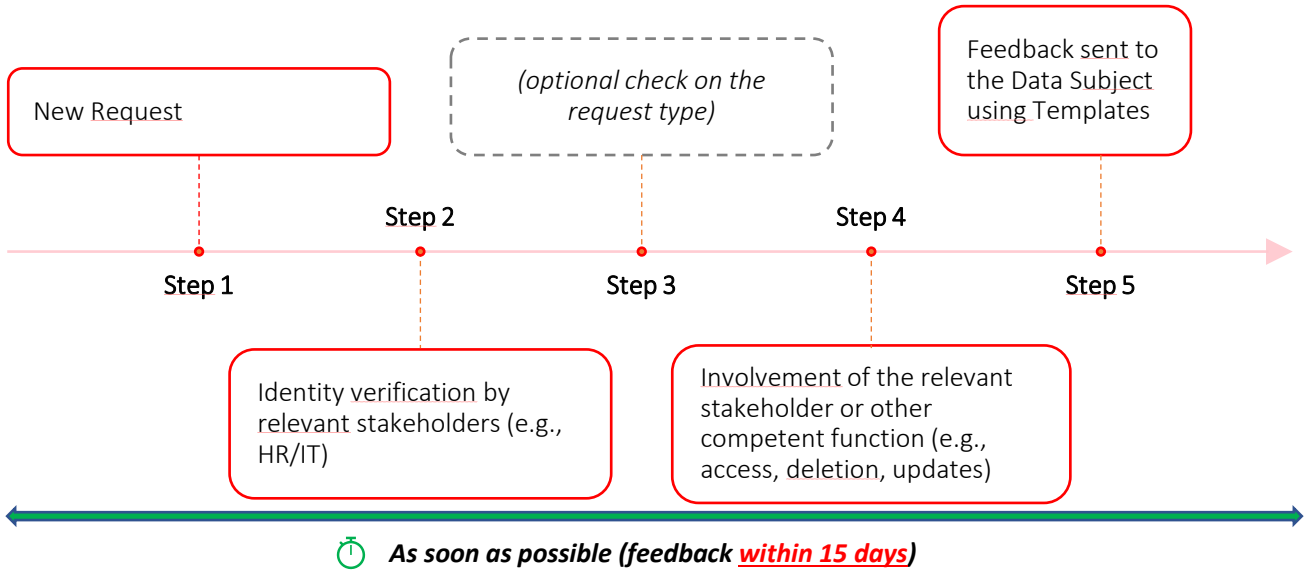
Depending on the type of request, BISS has different workflows and steps to follow regardless of receiving (allowed) channels (see section "Receiving channels" above).

The Admin may, with the cooperation of the Management, conduct inspection/assessments on the respect of any of the following steps.

1.3.2.1 High impact requests



1.3.2.2 Low impact requests



1.3.2.3 Roles

For each step described in the workflows, BISS has assigned specific roles and tasks to accomplish.

At glance

Admin	Management	Department(s)	IT Department

			holding data	
Monitoring requests and start the workflows	✓	✓		
Identity verification on BISS databases	✓	✓	✓	
Doubts on identity verification (e.g., e-mail, phone, need of IDs; proxies)	✓		✓	
Data recovery from databases (e.g., personal data, user history, etc.)	✓		✓	✓
Identifying the privacy request (e.g., access, deletion, opt-out, etc.)	✓			
Doubts on the privacy request (e.g., opt-out or deletion?)	✓			
Updating BISS databases (e.g., granting right of access, deletion, updating preferences, etc.)			✓	✓
Feedback to Data Subjects	✓			

Step 1 – New request

The Admin and Management must monitor and forward to the pertinent receiving channels (see "Receiving channels" section above) the data protection requests.

Step 2 – Identity verification

Once received a data request, the Admin is in charge of involving the relevant Management and Departments (likely) holding/Processing the Personal Data of the inquirer (e.g., HR Department if the data request comes from an employee). These stakeholders must cooperate in confirming the competence on the request or finding the right one.

If the request comes from a Data Subject in his/her own name, the Admin, with the support of the relevant Departments, must:

- verify the identity of the Data Subject based on the request itself (e.g., e-mail address, name, surname) or on a comparison of the request's elements with other suitable elements regarding the Data Subject which the competent Department may access within BISS (e.g., if the e-mail address who sent the request is the same recorded in BISS IT systems, the identity is likely verified);
- verify the identity of the Data Subject, based on any suitable elements available, such as, for example, the competent Department's personal knowledge of the Data Subject, or any statements made by others regarding the person submitting the request (e.g., when it comes to colleagues/employees sending a data request);
- not ask for additional information (especially national IDs, tax codes) unless such information are strictly necessary in order to identify the inquirer (before doing so, it is advisable – if applicable - to ask support of the privacy/legal consultants) ;
- bear in mind that additional information must be Processed only to confirm the identity and then deleted.

If the request comes from a natural or legal person (e.g., a law firm, an online platform etc.) allegedly acting in the name and on behalf of a Data Subject, the Admin, with the support of the relevant Departments, must:

- ensure that the person making the request encloses a copy of the signed proxy / power of attorney / mandate which grants that person powers to make the request on behalf of the Data Subject;
- ensure that the person making the request is to enclose a copy of a valid identity document for the Data Subject;
- if applicable, consult the privacy/legal consultants in case of doubts on the validity of the attached proxies and IDs.

In case further information to verify the identity of the Data Subject is deemed as necessary or if the request is not pertinent, the Admin is meant to address the person making the request with the relevant template (Annex I to this policy).

Step 3 – Check on the request type

Once the identity verification phase is completed, the Admin must identify the type of request (e.g., access vs. deletion vs. portability etc.).

The Admin is responsible of providing the Management with all the practical instructions and adequate template (Annex I to this policy) on how to proceed further. Particular attention shall be given to vague requests (that shall be interpreted extensively); exceptions that may not allow the fulfillment of data requests; cases where access may entail portability, deletion may mean opt-out from a specific purpose and opt-outs may lead to data erasure.

The check on the request type is mandatory for high impact requests and optional for low impact requests.

Step 4 - Involvement of relevant stakeholders

Once the request type is identified, the Admin sends back the request to the relevant Management(s) and Departments holding/Processing the Personal Data of the Data Subject. The latter, with the support of the IT Department, are in charge of:

- collecting the information and Personal Data necessary to fulfill the template to the Data Subject; and
- updating the IT systems (e.g., updating preferences, erasing data etc.) according to the Data Subject request.

The Admin shall proceed as soon as possible.

Step 5 – Feedback to the Data Subject

The Admin is in charge of double checking the content of the drafted template and send it over to the Data Subject using the same means employed by the person making the request. Requests received via online platforms (e.g., Mine, Privacy Bee etc.) may be replied using the contact details inserted into the request (e.g., e-mail address).

The delivery of the template to the Data Subject may be delegated to the Management, who is also in charge of keeping the Record of data subject requests up to date.

The templates are drafted by the Admin (supported - if applicable - by the privacy/legal consultants) and may be amended or updated by the former on a case-by-case basis.

1.3.2.4 Other relevant information

Deadlines

According to the GDPR, a Data Subject must receive feedback as soon as possible and no later than 30 days from receipt of the request.

In some exceptional cases (to be assessed and approved by the Admin, supported - if applicable - by the privacy/legal consultants), the deadline may be extended by two further months. In these cases, the Admin will immediately use the relevant template to inform the Data Subject about the reasons of the delay.

Costs

Feedbacks to Data Subjects requests are normally free of charge.

In some exceptional cases (to be assessed and approved by the Admin, supported - if applicable - by the privacy/legal consultants), BISS may charge the Data Subject a reasonable fee, based on administrative costs of the response.

Exceptions

BISS is not obliged to satisfy Data Subject rights as specified in their requests. There might be cases in which, for instance, a request of deletion may not be accomplished due to a fiscal obligation to retain data or to preserve BISS's right of defense.

The applicability of an exception is assessed by the Admin (supported - if applicable - by the privacy/legal consultants) during Step 3 above.

4. Non-compliance notifications and disciplinary measures

All legal and natural persons listed in this document are expected to fully comply with the present document and other data protection documentation released from time to time. Failure to comply with this policy may result in disciplinary action up to and including termination of employment or service contract.

5. Updates and changes to the policy

The Admin, with the support of Management, is responsible for maintaining and updating the present document.

6. Appendices

1.4 Appendix I – Templates

See "Templates"

1.5 Appendix II – Record of exercised data rights

See "Record of data subjects requests.xls"