GDPR and Student Mobility

GDPR Meets Student Mobility:

Use Cases for Students Taking Part in Erasmus+ Mobility for Studies and Traineeships

The following section elaborates on different stages, actors and documents related to student mobility for studies and traineeships and use cases relevant to the Higher Education Institutions for an internal self-reflection on compliance questions.

A. Stages of Mobility:

There are different aspects to take into consideration at different stages of mobility and in this document we will look into the following:

1. Pre-Mobility
2. During Mobility
3. Post-Mobility

Questions to keep into consideration:

- When do you collect the consent to process each student’s personal data at your institution? Upon admission? How are any updates communicated?
- What is the scope of such consent? Multiple purposes and mobility included in the documentation?
- Should you have additional Terms and Conditions and Privacy Policy documentation in place to process the student’s data for the mobility management?

B. Mobility Actors (potentially involved in the data processing):

1. Student
2. Sending HEI
    a. IT Department/Central Database manager
    b. Departmental/Institutional Coordinators
    c. International relations/Exchange programmes manager
    d. ...
3. Intermediary Organisation
    a. Third Party Service providers for processing data
    b. National registry/Statistics office
    c. ...
4. Receiving HEI/Organisation or Enterprise (for traineeships)
    a. IT Department/Central Database manager
    b. Departmental/Institutional Coordinators
    c. Responsible Person, Supervisor, Mentor (for traineeships)
    d. ...

Questions to keep into consideration:

- Are you aware of all the actors that are processing your student’s data?
- Are students informed about all the actors processing their data?
- How are you keeping track on updates in the process?

C. Mobility Documents:

There are several key documents that are exchanged throughout the mobility management process and each contains different items of personal or sensitive data.

1. Inter-Institutional Agreement between the HEIs
2. Application for Studies/Traineeship abroad (e.g. CV)

3. Student Nomination
4. Access credentials to OLS
5. Learning Agreement for Studies
6. Learning Agreement for Traineeships
7. Grant Application (annexed by Transcript, Traineeship/Study Offer)
8. Grant Agreement (The Grant Agreement comes under the purview of national laws of each individual member states9
9. Potentially confirmation of having special needs/coming from disadvantaged backgrounds/proof of financial situation.
10. Any additional data that might be necessary for Visa or acceptance at the host institution.
    a. ID or Passport
    b. Proof of not having criminal record
    c. ...
11. Certificate of Arrival/confirmation of the length of the mobility period
12. Transcript of Record/Traineeship Certificate (After completion of the agreed study/training period)
13. Participant’s report/Feedback surveys
14. Other: (e.g. grade distribution data or other specifics as per needs of different HEIs etc.)

Questions to keep into consideration:

- Is the difference between personal and sensitive data clear in all the cases at your institution?
- Are there appropriate practices for handling and storing personal and sensitive data?
- Are you ready for situations when students want to exercise their rights under GDPR to retract, delete, edit etc. their data?

Stages of Mobility:
Important aspects to keep into consideration

There are many aspects to keep into consideration when handling student data at different stages that will be analysed in detail.

Pre-Mobility:

Questions to keep into consideration:

- How is student data handled if the student cancels the mobility application at your institution? What if the student data is already transferred to the host institution/organisation?
- How is student data processed, if the student lands in the waiting/pending list?
- Are you fully aware how is sensitive data (e.g information regarding health condition/special needs) handled by the receiving/host organisation?
- Are students made aware of their name to be published after being nominated and signing Erasmus+ Grant Agreement?
- How are students informed about their data rights: Are students receiving the information through the HEI’s website, seminars, workshops and other platforms?

B. During Mobility:

Questions to keep into consideration:

- In case the mobility is cancelled due to the force majeure: Does the HEI have internal guidelines for handling data in such cases?
- Mobility cancelled due to other reasons: How is data handled on such occasions?
- Access to services: How is student data used to provide services (e.g library, canteen, sports services, student union, housing etc.) at the home /host HEI?

C. Post-Mobility:

Questions to keep into consideration:

- ToR/TC issued by Receiving Institution within 5 weeks (means of report: post, email, or other?) and Acceptance by the Sending HEI: What are the means of communicating such documents and are those GDPR compliant?
- ‘Participant’s Report’ to be submitted by the student. How is the information handled and anonymity ensured? Especially in cases of small numbers of participants?
- How is the data processed from any other feedback mechanisms on Erasmus mobility (should those be in place) and how is it communicated to the student?

Mapping Good Practices and Avoiding Bad Ones:

Some Must-Do’s to ensure the compliance.

- Standard Operating Procedures (SOPs) for data breach: The HEI has SOPs in case of data breach in compliance with the national legislation and GDPR. Responsible person/s appointed. Staff handling sensitive data have sufficient and ongoing training.
- Data handling procedures in place and security ensured for different data types (public, internal, sensitive, highly confidential). Data encryption, password protection and access only given to authorised persons. Passwords not shared with others.

- Only relevant persons having access to data, and respective data rights to amend and view it.
- Data Storage strategies are well-through through and risks mitigated: Internal Servers (Intranet), 3rd Party Servers (EU, non-EU with appropriate legal background), Offline Data storage, Manual storage in hard copy form etc. Full awareness of such a system and practices to keep trail of storage of individuals data.
- HEI don’t collect any additional data on students that is not relevant for the processes to be carried out.
- Mobility Software used by the HEI is GDPR compliant and so are other HEI’s software used in parallel.
- Software and hardware regularly upgraded. Have appropriate and sufficient security solutions.
- When assessing feedback post-mobility and notifying the National Agency and Commission appropriate levels of anonymity are ensured.
- If student selected on mobility on pending list, the list contains only the information that student has consented to display publicly. Pending list circulated or stored respecting student’s consent communicated.
- Student data shared/disclosure by HEI with 3rd parties only in exceptions under GDPR. e.g emergency, crime.
- Students with special needs are provided with additional information and encouraged to go on Erasmus+ mobility, yet their health status handled with appropriate levels of confidentiality.
- ...

Related articles

Content by label

There is no content with the specified labels