Part A. UPEX Privacy Policy

as of 05 November 2020

This privacy policy applies to the use of the User Portal to the European XFEL (UPEX) provided by European X-Ray Free-Electron Laser Facility GmbH (European XFEL GmbH, we or us) and is intended to inform the users about the processing of their personal data.

Table of contents

1. Who is the controller of your personal data?

The controller in the sense of the European data protection laws is European XFEL GmbH, Holzkoppel 4, 22869 Schenefeld, Germany. For further contact details as well as the **contact details of our data protection officer** see section "Contact Information".

2. What personal data do we collect and are you required to provide this information?

Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The use of UPEX requires the user to accept the UPEX T&Cs and to register and create a user account unless the user is accessing UPEX only for administrative or technical reasons. The amount of personal data we collect during the registration process and afterwards during your use of UPEX depends on the purposes you are using UPEX for and whether you are an employee of European XFEL GmbH or of Deutsches Elektronen-Synchrotron DESY (DESY). We mark mandatory information with an asterisk *. If you decide not to provide us with this information, unfortunately you will not be able to register respectively use UPEX.

a. Simplified log in for certain user groups

Some users are able to use the simplified log in offered by UPEX. The simplified log in is available to employees of European XFEL GmbH who need to use UPEX for administrative or technical reasons and to users who use the European XFEL facility themselves as a member of an experiment team and are employees of European XFEL GmbH or DESY. The simplified log in is also available for members of the proposal review panels which are employed by DESY.

Users eligible for the simplified log in only have to enter their username and password provided to them by European XFEL GmbH or by DESY to log in. All other information required for the registration will be collected from DESY.

b. Data collected via the registration process

Users which are not eligible for the simplified login described above need to register first. During the registration process they will be asked to provide mandatory information which includes username, password, workplace email, position, first name, last name, gender, birth date, birth place, nationality, institute and workplace phone number. Title and middle initials are optional information. In the event a registration has not been completed, the collected data will be deleted.

In addition, the user will be asked for consent to the processing of his/her first and last name, date and place of birth including country, gender, nationality, name and address of his/her current institute by us for the purpose of matching these data with embargo lists. Information on these lists is available here.

Please note that without this consent a registration cannot be completed respectively we might have to terminate the contractual relationship regarding the user account.

c. Data collected via the proposal process

If you submit a proposal for beam time via UPEX as a main proposer, you will be asked to provide additional information about the project and the involved persons (e.g. principal investigator, co-proposers).

This data will be used to process the proposal and might be made available to third parties (e.g. members of the proposal review panels) for review of the proposal. For further information, please refer to section "Recipients of your personal data".

d. Data collected from users receiving travel funding

If you receive travel funding from us we collect certain information via the “Visitor Allowance Form” which includes information on your bank account.

e. Data collected from users requesting a visa invitation letter

If you are going to request a visa invitation letter via UPEX and in order to participate in an experiment, we will collect information about your passport number, arrival and departure dates, and the organization to which your visa application will be submitted (mandatory fields). Your first and last name as shown on the passport (mandatory), title (optional), date of birth (mandatory), nationality (mandatory), your institute (mandatory), will be pre-filled from your UPEX user account but they are editable as required for this purpose.

f. Data collected from users coming to our site

If you are going to participate in an experiment in person, we will collect information about your arrival and departure dates on site via UPEX, and, if you are a funded user, information about whether accommodation assistance is needed and your wished travel data.

g. Data collected from users taking part in European XFEL User Organization Executive Committee

If you want to become or if you are a member of the European XFEL User Organization Executive Committee (UOEC), you will be asked to provide the

following information: your first name, last name, affiliation, address, affiliation country, business email address, business telephone number, expertise area, professional experience, role in the UOEC and – if you consent to this – your photograph will furthermore be published on the Organization's web pages on European XFEL GmbH's website.

If you use the feedback tool of the UOEC in UPEX, you will be requested to give your consent for us to contact you per email in this respect.

h. Data automatically collected from users

Every time you use the internet, your internet browser will automatically transfer certain information that we will store in so-called log-files.

The log-files will solely be stored for the detection of malfunctions and for security reasons (e.g. attack detection) for between seven and ten days. Log-files will be stored for a longer period of time and might be transferred to investigating authorities if they are needed as evidence if an incident took place. They will be subject to restriction of processing upon the final clearance of the matter.

In particular, log-files include the following information:

- IP address of the terminal from which the online service is accessed;
- Internet address of the website from which the online service is accessed (referrer URL);
- Name of the accessed data respectively information;
- Date and time as well as duration of access;
- Transferred amount of data;
- Operating system and information regarding the internet browser used, including add-ons (e.g. flash player); and
- http-Status-Code (e.g. "request successful").

In addition to the above, UPEX log-files contain debugging messages and are used for software debugging purposes.

These log-files contain only data that are already stored in UPEX database e.g. username, UPEX user ID, email address, and are stored for maximum 30 days.

i. Data we collect from third parties

In some cases, we collect your personal data from third parties. This is namely the case if you are eligible for the simplified log in or if you are named as principal investigator or co-proposer (please see section "Sources of your personal data" for further scenarios).

In the context of the simplified log in we receive information from DESY user repositories which are required to integrate your UPEX account with existing DESY/XFEL IT infrastructure.

If the main proposer of a proposal names you as principal investigator or co-proposer, we will collect from the main proposer your role in the experiment and link your UPEX registration information to the respective proposal.

If you are named as a team member who will actually visit the European XFEL facility and/or access our IT infrastructure remotely, the main proposer will additionally provide us with the following categories of personal data via the so-called A-form (experiment team registration): whether you will attend the experiment remotely or in person, and in the latter case whether you will receive travel funding (Experiment Team Data).

Please see section "Sources of your personal data" for further information, in particular on the sources of your personal data.

3. Purposes and legal bases of data processing

We process your personal data for the purposes and based on the legal bases listed in the table below. Where the processing is based on legitimate interests (of us or a third party) we have also included a description of the respective interests:

No.	Purpose for processing	Legal basis for processing	Description of legitimate interest for processing if applicable

1	To provide UPEX for our users in accordance with our Terms and Conditions (available here)	Performance of contract	n/a
2	To provide the services requested by our users via UPEX	Performance of contract or taking steps at the request of the data subject prior to entering into a contract	n/a
3	To match user information with international embargo lists in order to determine your eligibility to participate in UPEX	Consent	n/a
4	To match the name and date of birth provided by you in UPEX with your national identity card respectively your passport in order to determine your eligibility to participate in UPEX respectively to access restricted areas of our facility	Legitimate interest (for German nationals in addition section 20 of the Act on Identity Cards and Electronic Identification respectively section 18 of the Act on Passports)	We have a legitimate interest in ensuring that the information provided by you in UPEX is correct and in ensuring that only persons entitled to do so and properly identified access restricted areas of our facility in order to ensure the safety of other users and our employees as well as the security of our facility and assets stored within.
5	To determine disruptions and to ensure the security of our systems, including the detection and tracing of (the attempt of) unauthorised access to our web servers	Compliance with our legal obligations regarding data security as well	We have a legitimate interest in resolving disruptions, ensuring the security of our systems and the

		as legitimate interest	detection and tracing of (the attempt of) unauthorised access.
6	To contact you about proposals you have submitted, e.g. to inform you about a decision that has been made regarding your proposal	Performance of contract	n/a
7	To engage in communication you send to us relating to the registration and use of UPEX and to deal with any matters deriving from this communication	Performance of contract	n/a
8	To engage our funding agencies who are competent for the country in which your institute is located or if you are a citizen of the country for which the respective funding agency is competent in order to assess whether you are entitled to receive any (additional) funding or support; these agencies will receive first and last name, title, the institute you are working for, your role in a proposal (e.g. proposer or member of experiment team), whether the proposal was successful or not and in some cases your nationality	Legitimate Interest	We have a legitimate interest in securing the costs of operating our facility by means of funds from funding agencies and the funding agencies have a legitimate interest in being able to fulfil their duty of providing funds for scientific purposes to those who are eligible.
9	To provide our funding agencies with the information necessary for them to calculate the repartition they have to pay for the operation of the facility, which is partly based on the success of proposals from the respective institutes; for this purpose all funding agencies will receive the necessary information	Legitimate Interest	We have a legitimate interest in securing the costs of operating our facility by means of funds from funding agencies and the funding agencies have a legitimate interest in being able

	with regard to successful proposals, in particular your first and last name, the institute you are working for and your role in a proposal (e.g. proposer or member of experiment team)		to calculate and fulfil their duty of providing funds to the facility.
10	To publish a list of successful publicly funded proposals (proposal IDs and proposal titles) (e.g. on our website, in our annual report) that includes the certain information about the principal investigator and main proposer (first and last name, the institute the principal investigator/main proposer is working for and the time schedule for the related experiment)	Legitimate Interest	We have a legitimate interest in publishing a list of successful proposals to draw attention to the experiments that are being carried out in our facility in order to further promote our scientific research activities.
11	To send periodic emails to the email address you provide to inform about technical news relating to UPEX and the European XFEL facility and to send automated service emails	Performance of contract	n/a
12	To be able to provide travel funding (either from our own budget or from external funding) to users who are eligible to this	Performance of a contract	n/a
13	To be able to provide visa invitation letters to users requesting this in order to enable them to participate in an experiment	Performance of a contract	n/a
14	To manage your participation in an experiment on site	Performance of a contract	n/a
15	To manage your membership in European XFEL User Organization respectively in the UOEC, e.g. to carry out elections for the UOEC or	Performance of a contract	n/a

	to communicate with you in your position as a member of the European XFEL User Organization or the UOEC		
16	To upload basic information about you (first name, last name, affiliation, address, affiliation country, business email address, business telephone number, expertise area, professional experience and role in the UOEC onto the User Organization's web pages on the European XFEL GmbH's website if you are a member of the UOEC	Performance of a contract	n/a
17	To upload your photograph onto the User Organization's web pages on the European XFEL GmbH's website if you are a member of the UOEC	Consent	n/a
18	To provide related support services to our users (information services only)	Performance of contract	n/a
19	To create statistics about user activities including use of the European XFEL facility	Legitimate interest	We have a legitimate interest in creating anonymous user statistics about user activities and potentially sharing these with third parties.
20	To safeguard and defend our rights	Legitimate interest	We have a legitimate interest in exercising and defending our rights.

21	To comply with relevant legal obligations such as keeping accounting records and complying with safety and health regulations	Compliance with legal obligations	n/a
22	To contact you with regard to feedback you provided through the feedback tool of the UOEC in order to improve our services	Consent	n/a

4. Sources of your personal data

We collect most information we process directly from you. However, additionally we may collect personal data from third parties, namely:

- The main proposer of a proposal who may name you as the principal investigator, as co-proposer, as a member of an experiment team of a particular proposal or as a person with a possible conflict of interest in relation to a particular proposal if engaged in a review; and

- Embargo lists: refer to https://in.xfel.eu/upex/docs/Information_on_Embargo_lists.pdf

5. Recipients of your personal data

Your personal data may be transferred to the following categories of recipients:

a. Service Providers (processors)

We reserve the right to appoint external service providers for the processing of personal data. These service providers will only have access to data they need for the performance of their service. Service providers will be appointed as so-called data processors which are only allowed to process the personal data on our behalf and according to our documented instructions. We disclose your data to the following categories of processors:

- IT service provider, in particular (but not limited to) for storage services, data analysis services, curation services (e. g. Deutsches Elektronen-Synchrotron DESY, for accounts and hosting service, data analysis and curation service, computing infrastructure, Germany; National Centre

for Nuclear Research, Poland, for storage, data analysis and curation services),

- Provider of a controlled access system (Deutsches Elektronen-Synchrotron DESY), Germany,
- Provider of security services (security and gate reception staff), Germany,
- Provider of technical emergency services, Germany,
- Provider of an embargo list database system for antiterrorism checks, Germany.

b. Other recipients

We may disclose your personal data to the following categories of third parties:

Members of the proposal review panel engaged in the review of a proposal you are associated with (Reviewer) will receive the proposal and certain personal information about all members of the proposal team (i.e., their names, the name of the institute they are working for and their role in the team.

- The main proposer, the principal investigator, all co-proposers and all team members of the proposals you are associated with have access to the respective proposals and to the names of main proposer, principal investigator, all co-proposers and all members of the experiment team.

- Registered users of UPEX while preparing a proposal submission in their role as main proposer have access to information about other registered UPEX users (first and last name, title, UPEX-ID no. and the institute the user is working for).

- Funding Agencies will be provided with information about registered UPEX users associated with a proposal (first and last name, the institute the user is working for, the user's role in a proposal (e.g. proposer or member of experiment team), whether the proposal was successful or not and in some cases the user's nationality) with the purpose of the provision of funding or support and/or calculating the repartition costs.

- The public will be informed (e.g. on our website, in our annual report) about publicly funded successful proposals and its principal investigator / main proposer (first and last name, the institute the principal investigator is working for and the time schedule for the related experiment).

- The public will be informed on our website about the following basic details of members of European XFEL's user organization's executive committee (UOEC): first name, last name, affiliation, address, affiliation country, business telephone number, business email address, professional experience, role in the UOEC as well as the members' photograph if they chose to consent to this.

- The User Organization Executive Committee (UOEC) may be informed about your first name, last name, affiliation (in addition to the title and ID of the proposal of reference) if these personal data are required for carrying out their representation and mediation activity within our user community.

- If you are funded by a transnational access program of the European Union, we transfer your personal data (e.g. first name, last name, institute, gender, nationality, title, travel dates, scientific area) to the respective program coordinator and the European Commission.

- If you take our offer to conclude a travel, health and accident insurance, we transfer your personal data (e.g. salutation –(Mr./Mrs.) following the gender/sex field in UPEX, title, first name, last name, date of birth, business address, email, travel start date, travel end date, travel country, language) to the insurance company that provides the insurance.

- If you are being assisted by us in your search for suitable accommodation (e.g. guest houses, hotels, apartments) and we book such for you, we transfer your personal data (e.g. first name, last name, arrival date, departure date, email, salutation (Mr./Mrs.) following the gender/sex field in UPEX, in some cases your institute address or billing address) to the provider of the accommodation; for stays at the

European XFEL Guest House due to open in 2021, please refer in addition to the specific privacy policy.

- If we book travels to our facilities for you, we transfer your personal data (e.g. salutation (Mr./Mrs.) following the gender/sex field in UPEX, academic title, first name , last name, date of birth, email address) to the corresponding travel agency, transportation companies and/or airlines; If you decide to provide information on your frequent flyer or any bonus program respectively the membership number in the correspondence with our Travel Office before a reservation, we will transfer these data to the corresponding travel agency, transportation companies and/or airlines for booking/ticketing purposes. The information will not be stored in UPEX or in any other system at European XFEL.

- Bank services, lawyers, tax advisors, consultants, external auditors for administrative purposes.

Additionally, personal data might be transferred to third parties if we are obliged to transfer the data by statutory provisions or by an enforceable order of a court or an administrative authority. We may also release your data when we believe this is appropriate to comply with the law or one of our policies (e.g. our Scientific Data Policy), or to protect our or others' rights. Furthermore, we may transfer data which has been rendered anonymous to third parties for statistical purposes.

The parties mentioned above can be located in the European Economic Area (EEA) as well as in other countries. For transfers of personal data to countries outside the EEA see next section.

6. Transfers of personal data to countries outside the EU/EEA

We might transfer personal data to service providers or third parties located outside the European Union (EU) respectively outside the European Economic Area (EEA) in so-called third countries (e. g. reports to funding agencies located outside the EU).

In such cases typically the transfer will be necessary for the performance of the contract we have concluded with you when registering for UPEX (e.g. information required for the peer-review of the proposal will be sent to a reviewer in the U.S.). If

neither this nor any other exception for transfers of personal data to third countries applies (under Art. 49 (1) of the General Data Protection Regulation – GDPR), we ensure prior to the transfer that

- The European Commission has decided that the third country ensures an adequate level of protection (Art. 45 GDPR, e.g. Switzerland); or

- That the transfer is subject to appropriate safeguards (Art. 46 GDPR), for example by entering into so-called standard data protection clauses of the European Union with the recipient of the data .

In specific situations we might also ask for your explicit consent to the transfer or base the transfer on another exception provided for in Art. 49 (1) GDPR.

You are entitled to receive an overview of third country recipients and a copy of appropriate or suitable safeguards in place. For your request please use the details provided in section "Contact Information".

7. Duration of storage

We will store your personal data as long as it is necessary for the performance of the contract respectively as long as we have a legitimate interest in the storage. In all other cases we will delete your personal data with the exception of those data that we need to store further in order to comply with contractual or statutory retention periods. We keep your personal data for the following periods:

- Data from registered UPEX users and travel data:
  - ➔ Data collected via the registration process will be stored for ten years from the end of the calendar year in which your last login in UPEX took place or for a maximum period of three months after your user account was terminated by you or European XFEL GmbH, whichever storage period is shorter.
  - ➔ Travel data contained in Personal Arrival Forms (e. g. passport number, travel dates) will be deleted three years from the end of the calendar year in which respective travel has taken place.

- Data in relation to proposals you are associated with as Main Proposer, Principal Investigator, Co-proposer, experiment team member and/or reviewer:

➔ Data in relation to proposals will be stored for ten years from the end of the calendar year in which your last login in UPEX took place or for a maximum period of three months after your user account was terminated by you or European XFEL GmbH, whichever storage period is shorter.

- Data we collect from embargo lists:
  ➔ Data will be kept for ten years from end of the calendar year in which the last embargo list verification was made.

- Data collected from users only for the purpose to become or to be a member of the UOEC (e. g. professional experience, expertise area, photograph):
  ➔ Data will be kept for three years from the end of the calendar year in which the membership has ended.

As regards the storage of scientific data see our Scientific Data Policy.

8. Cookies

UPEX makes use of so-called cookies. Cookies are small text files that your internet browser downloads and stores on your computer. If a website is accessed again the internet browser sends the information stored in the cookie back and enables the recognition of the user. Some cookies will be deleted at the end of the browser session (so-called session cookies), other cookies will be deleted after a stated term (so-called persistent cookies).

You can prevent cookies from being installed by changing the settings on your browser software accordingly. However, UPEX only uses cookies which are mandatory for the provision of UPEX (so-called strictly necessary cookies). These cookies are strictly necessary for the safe provision of UPEX. They include, for example, cookies which serve the purpose of identifying or authenticating our users and cookies that temporarily store certain user entries (e. g. a prior log in so that our users do not have to log back into UPEX after every click or information our users have previously entered to complete a form). Therefore, you will not be able to use UPEX if you do not accept these cookies.

Please find a list of the cookies we use, their purpose and retention periods below.

Purpose	**Name of cookie**	**Retention period**
Strictly necessary	Laravel_session (keeps user session)	1 day

Strictly necessary	XSRF-TOKEN (protects against Cross-Site Request attacks)	1 day
Strictly necessary	Remember_web_* ("Stay signed in" functionality)	Applies if user checks "Stay signed in" flag. Erased on logout.

9. No web analytics and no advertising by means of tracking technologies

UPEX does not use web analytics tools or tracking tools for interest based advertising.

10. No social Plugins

UPEX does not use social plugins.

11. Data Security

Your personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. Please note that, regarding any communication via email, confidentiality cannot be guaranteed as third parties may be able to access the information during the transmission process. Therefore, please refrain from using emails for confidential information.

12. Your rights as data subject and how to exercise them

You have the following rights:

a. Right of access and rectification:

You have the right to obtain confirmation from us as to whether or not your personal data is being processed and a right to access your personal data that is being processed by us.

You also have the right to obtain without undue delay the rectification of any inaccurate personal data relating to you and to have any of your personal data that is incomplete completed. Please note that you might also be able to correct your data in UPEX yourself.

In case we have transferred your personal data to third parties, we will inform them about this rectification and completion if required by law.

b. Right to erasure ('right to be forgotten'):

You have the right to obtain the erasure of your personal data from us without undue delay and we have the obligation to erase your personal data without undue delay if one of the following grounds applies:

- your personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the processing of your personal data is based solely on your consent and you have withdrawn your consent;
- you have objected to direct marketing;
- you have objected to the processing that is based on our legitimate interest on grounds that relate to your particular situation and there are no overriding legitimate grounds for the processing;
- your personal data have been unlawfully processed; or
- your personal data have to be erased for compliance with a legal obligation.

In case we have transferred your personal data to third parties, we will inform them about this erasure if required by law.

Please keep in mind that there are limitations to your right to erasure. We are for example not allowed to erase data that we are legally obliged to store. Also, your right to erasure does not apply if we need to store the data for the establishment, exercise or defence of legal claims.

c. Right to restriction of processing:

You have the right to restrict our processing of your personal data where

- you contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy;
- the processing is unlawful but you do not want us to erase the data;

- we no longer need your personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or
- you have objected to processing based on our legitimate interest (see below) pending verification as to whether we have compelling legitimate grounds to continue processing.

Where personal data is subjected to restriction in this way, we will only process it with your consent or to a very limited extent, e. g. for the establishment, exercise or defence of legal claims.

d. Right to object:

You have the right to object to the processing of your personal data that is based on our legitimate interest, on grounds relating to your particular situation, at any time. You also have the right to object to the processing of your personal data for marketing purposes at any time. Please also refer to section "Information on your rights to object".

e. Right to data portability:

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to us in a structured, commonly used and machine readable format, and also to require us to transmit it to another controller where this is technically feasible.

f. Right to withdraw consent:

In case you gave us your consent for the processing of data you may withdraw your consent at any time. The withdrawal of your consent does not affect the lawfulness of processing based on consent before its withdrawal.

You may exercise your rights by contacting us via the contact details provided in section "Contact Information". Please ensure for this purpose that we are able to verify your identity.

13. Right to lodge a complaint with a supervisory authority

You may lodge a complaint with a supervisory authority. You may file your complaint at your local supervisory authority or at the data protection authority competent for us. This is:

Unabhaengiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel
Germany

Telephone: +49 (0) 431 988-1200
Fax: +49 (0) 431 988-1223
Email: mail@datenschutzzentrum.de

14. Contact information

If you have comments or questions, any concerns or a complaint regarding the processing of your personal data, please feel free to contact us at:

European X-Ray Free-Electron Laser Facility GmbH
Holzkoppel 4
22869 Schenefeld
Germany
Email: useroffice@xfel.eu
Telephone: +49 8998 6767

You may also contact our **data protection officer** Carsten Porthun at the following email address: carsten.porthun@desy.de

Part B. UPEX

Information on your rights to object

Right to object to processing based on legitimate interest

You may have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on the legal basis legitimate interests.

Right to object to direct marketing

You may at all times object to the processing of your personal data for direct marketing purposes. Please take into account that, due to logistical reasons, there might be an overlap between your objection and the usage of your data within the scope of a campaign which is already running.

You may address your objections to:

European X-Ray Free-Electron Laser Facility GmbH
Holzkoppel 4
22869 Schenefeld
Germany
Email: useroffice@xfel.eu
Telephone: +49 8998 6767