Directive on the Use of EPFL Electronic Infrastructure

LEX 6.1.4

13th November 2014, status as at 15th March 2021

The Direction of the Ecole polytechnique fédérale de Lausanne,

based on the Federal Act on the Federal Institutes of Technology (FIT Act);

based on Art. 57i ss of the Government and Administration Organisation Act (GAOA);

based on the Ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération;

based on Art. 3, para. 1, letter a, of the Ordonnance du Conseil des EPF sur les écoles polytechniques fédérales de Zurich et de Lausanne (ETH Board Ordinance on ETHZ and EPFL);

based on the Ordinance on the organisation of the Ecole polytechnique fédérale de Lausanne, in particular its Art. 4;

based on the Loi fédérale du 24 mars 2000 sur le personnel de la confédération (LPers);

based on the Ordonnance du Conseil des EPF sur le personnel du domaine des écoles polytechniques fédérales (OPers-EPF);

based on the Disciplinary Rules and Regulations of 15 December 2008 concerning Students of the EPFL,

based on the Ordinance for the Use of Software Subject to a License Agreement (LEX 6.1.5)

hereby adopts the following:

Section 1 General Provisions

Article 1 Purpose

The purpose of this Directive is to ensure that the use of the EPFL electronic infrastructure is in line with its mission and to prevent any misuse in this respect.

Article 2 Definitions

For the purposes of this Directive the following meanings shall apply:

1. **user**: any person using the EPFL electronic infrastructure;
2. **employee**: any EPFL member in the sense of Art. 13 para. 1 let. a, b and d of the FIT Act (faculty members, assistants, PhD candidates, as well as scientific, administrative staff and technical staff);
3. **electronic infrastructure**: all fixed and mobile equipment able to record or transmit data - including personal data -, especially computers, network components, software, data carriers, telephones, printers, scanners, fax machines, photocopiers, facility control systems at the entrance to and inside the premises and location-based services;
4. **subcontractor**: any natural or legal person entrusted by the EPFL with providing services related to the mission or operation of the EPFL;
5. **managed data**: the data, including personal data, stored while using EPFL electronic infrastructure, which are regularly used, analysed or deleted automatically or intentionally;
6. **unmanaged data**: data, including personal data, recorded while using the EPFL electronic infrastructure, but not regularly used, analysed or deleted intentionally.
7. **Personal data**: any information relating to an identified or identifiable natural person in the sense of art. 3 let. a Federal Act on Data Protection (FADP);

8. **Official secrecy**: obligation for a person to keep secret an information that has been confided to him or which has come to his knowledge in the execution of his official duties (art. 320 Criminal Code, art. 22 LPers and art. 57 OPers-EPF). This concerns the information that cannot be disclosed according to the Federal Freedom of Information Act (FoIA).

Article 3 Personal scope

[1] This Directive shall apply to any person using the EPFL electronic infrastructure (users).

[2] It applies in particular to:

1. EPFL members in the sense of Art. 13 of the FIT Act;
2. all other users of the EPFL electronic infrastructure (including in case of temporary use).

Article 4 Material scope

This Directive shall apply to any use of the EPFL electronic infrastructure, including remote use or through terminals not provided by the EPFL.

Article 5 Terms of use of the electronic infrastructure

[1] Use of the EPFL electronic infrastructure is permitted to the extent that it is consistent with the institution's mission, with the provisions of this Directive and, where applicable, with the specific terms of subcontractors as indicated to the user.

[2] Users are prohibited from using the EPFL electronic infrastructure in a manner that:

1. is contrary to EPFL's mission;
2. violates the law or this Directive, in particular through misuse of the infrastructure;
3. violates the terms of a third-party license agreement;
4. is harmful to EPFL's interests;
5. compromises the security of EPFL's IT systems;
6. seeks to alter software or facilities in a manner contrary to their intended use; or
7. seeks to circumvent or remove security restrictions.

[3] The Director of the Information Systems Management department jointly with the Director of Legal Affairs may authorise use contrary to Art. 5, para. 2, items 6 and 7. Such authorisation shall be given in advance in writing based on valid reasons.

[4] Use of the EPFL electronic infrastructure for private purposes is permitted to the extent that it:

1. only generates minimal costs to the EPFL and does not consume computing resources excessively;
2. furthermore, such use shall not interfere with the professional obligations of employees vis-à-vis the EPFL.
3. EPFL assumes no responsibility for the private use of its electronic infrastructure, in particular for the availability and integrity of private data stored on EPFL-owned equipment.

[5] Use of the EPFL electronic infrastructure for private purposes shall be reported by users using the tools provided to them (directory in the mailbox or storage system clearly identified as private through its name).

[6] If any EPFL hardware or software is lost or stolen, Information Security or the head of IT for the corresponding school will immediately delete all data – both personal and professional – stored on the hardware or software, insofar as it is possible to do so remotely. Private and professional data will not be treated differently.

[7] EPFL email addresses are professional or student email addresses used by people for their work or studies at EPFL. They allow users to communicate using the EPFL name. EPFL's professors emeritus are given an EPFL email address as part of their privileges. Third-party

users who are not members of EPFL under Article 13 of the ETH Act are only permitted to have an EPFL email address if they need to communicate using the EPFL name in order to properly carry out their work assignment at EPFL. In summary, the following categories of people may have an EPFL email address:

1. EPFL students, for the duration of their studies;
2. EPFL staff, for the duration of their contract;
3. EPFL's professors emeritus; and
4. third-party users who are not members of EPFL under Article 13 of the ETH Act, for the duration of their work assignment and only if required by their assignment.

[8] A third party who is not an EPFL member within the meaning of Article 13 of the ETH Act is required to sign an undertaking to comply with the provisions of this Directive and appropriate additional provisions taking into account its status as a third party user; the text of the undertaking will be made available by the Information Systems Management department. This para. does not apply to users, who have no administrator rights, of open access systems.

Section 2 Powers

Article 6 Head of Unit

Heads of Unit are responsible for implementing this Directive. They are in charge of:

1. informing the users;
2. ensuring that all third parties not Article 13 of the ETH Law accredited in its unit have signed the document cited in accordance with Article 5 para. 8 before their accreditation;
3. enforcing the measures set out in Art. 11;
4. issuing additional rules pursuant to Art. 29;
5. receiving notifications from users about security issues (Art. 11 para. 4) and ensuring that Information Security has been alerted accordingly;
6. taking the measures provided for in Art. 23.

In addition, he has the possibility to order evaluation of non person-related data (Art. 14) and data evaluation not relating to named individuals (Art. 15).

Article 7 Information Security

Information Security is competent to:

1. delete all data stored on EPFL hardware or software that has been reported as lost or stolen (Art. 5 para. 6);
2. issue instructions (Art 11 para. 2);
3. require additional security measures or restrict or delete a user's access to EPFL electronic infrastructure without warning (Art. 12);
4. receive notifications from users about security issues (Art. 11 para. 4) and misuse (Art. 21 para. 4);
5. take provisional measures (art. 23);
6. take emergency measures (art. 24);
7. carry out authorised analyses or mandate a third party to do so (Art. 14 to 17).

Article 8 Director of the Information Systems Management department

The Director of the Information Systems Management department is competent to:

1. order data evaluation relating to named individuals and notify the persons concerned (art. 17);
2. decide on emergency measures pursuant to Art. 24 para. 3;
3. issue authorisations (Art. 5 para. 3 and Art. 21 para. 2 item 7);

4. supervise implementation of this Directive by Heads of Unit;
5. appoint a substitute.

Article 9 EPFL Direction

The EPFL Direction is competent to:

1. take the measures provided for in Art. 22 para. 2;
2. take emergency measures as provided for in Art. 24;
3. order access to the professional documents and e-mails of users whose relationship with the EPFL has ceased (Art. 25 para. 5);
4. order an evaluation of data relating to named deceased users (Art. 25 para. 1);
5. order access to the documents and e-mails of deceased users (Art. 26 paras. 2 to 4).

Article 10 Exclusive powers

[1] Human Resources department shall have exclusive jurisdiction to order an evaluation of compliance with professional obligations, in particular to monitor working time, or in the context of an administrative investigation (Art. 58 OPers-EPF and Art. 27j ss OGAOA) or disciplinary investigation (Art. 58a OPers-EPF). HR shall nevertheless inform the Information Systems Management department. If this Directive provides that the evaluation is the responsibility of the EPFL Direction, the latter's prior agreement must be obtained.

[2] Only EPFL faculty members in charge of evaluating the progress and the skills of student applicants, students, PhD candidates and course auditors shall have the jurisdiction to order data evaluations for such purposes, after having notified the student applicants, students, PhD candidates and course auditors of the evaluation process. This analysis must not take sensitive data or personality profiles into account.

[3] An analysis pursuant to para. 2 may also be ordered by the disciplinary authority as part of a disciplinary procedure pursuant to Art. 9 of the Disciplinary Rules and Regulations concerning Students of the EPFL.

Section 3 Liability and security measures

Article 11 Liability

[1] Individual users shall be responsible for their use and management of access to the electronic infrastructure. In particular, each user shall take care not to breach the provisions of this Directive or of the law, not to infringe third party rights or EPFL interests and not to endanger the EPFL electronic infrastructure.

[2] Users shall fully comply with the instructions of Information Security. They shall be notified by the latter of any specific security measures applicable to certain parts of the EPFL electronic infrastructure.

[3] Private terminals connected to the EPFL network on site or remotely shall have an up-to-date anti-virus. The software and operating systems which they contain shall be subject to security-related updates. In all other respects, LEX 6.1.3 shall apply to the use of private hardware.

[4] Should they become aware of security issues, users shall immediately inform the Head of Unit and Information Security.

[5] EPFL provides a professional data backup service. Users must make sure that all professional data they use are backed up adequately and regularly, or that equivalent safeguards are in place.

[6] Users must inform as soon as possible their supervisor, Information Security and the Response and Safety Service if any EPFL hardware or software they use is lost or stolen.

[7] Users must inform immediately their supervisor and Information Security if any personal data

or any professional data subject to confidentiality requirements (official or business secrecy) are lost or stolen.

[8] Users who unlawfully breach the provisions of this Directive, of the law or related instructions shall be personally liable and shall compensate the EPFL for any damages suffered.

Article 12 Security of EPFL electronic infrastructure

[1] Information Security can require that users implement additional security measures, or can restrict or block, without warning, the access to EPFL electronic infrastructure of any hardware or software that it deems to be insufficiently secure.

[2] Information Security can require users to implement specific security measures before using certain components of EPFL electronic infrastructure.

Article 13 Paid services

Faculty members, assistants, PhD candidates and scientific, administrative and technical staff (non-exhaustive list of staff categories) who privately use paid services billed to EPFL (e.g. premium-rate calls) without the approval of their immediate superior shall personally bear the costs.

Section 4 Data collection

Article 14 Data which may be collected

[1] The EPFL may collect and record personal data related to the use of its electronic infrastructure for the following purposes:

1. to ensure the security of EPFL data and premises, as well as the security and proper operation of the EPFL electronic infrastructure;
2. to ensure technical maintenance of the EPFL electronic infrastructure;
3. to trace file access;
4. to monitor compliance with this Directive;
5. to bill costs to individual cost centres and users (Art. 13);
6. to manage staff working time and improve the functioning of the EPFL;
7. to perform backups and ensure archiving.

[2] The EPFL may also collect and record data in order to evaluate student applicants, students, PhD candidates and course auditors, pursuant to Art. 10 para. 2.

[3] The EPFL and subcontractors may collect and store personal data as needed for the provision of their services.

Section 5 Evaluation of collected data

Article 15 Evaluation of non person-related data

[1] Evaluation of non person-related data is permitted for the purposes stated in Art.13.

[2] The Head of Unit is competent to order the evaluation and may entrust a third party with performing this.

[3] Such evaluations may be carried out with no limitations on time or content.

Article 16 Data evaluation not relating to named individuals

[1] Evaluation of person-related data is permitted by random sampling provided the persons remain unnamed (using pseudonyms) for the following purposes:

1. to monitor the use of electronic infrastructure;
2. to monitor staff working hours.

[2] The Head of Unit is competent to order the evaluation and may entrust a third party with performing this. Information Security shall take the necessary measures to ensure that individuals are not identifiable.

Article 17 Data evaluation relating to named individuals

[1] Evaluation of person-related data which relates to named individuals is permitted for the following purposes:

1. to investigate specific suspicion documented in writing regarding misuse;
2. to take action against or document proven misuse;
3. to analyse and eliminate disruptions to electronic infrastructure and protect against clear threats to this infrastructure;
4. to provide required services;
5. to record and invoice services rendered;
6. to monitor individual working hours;
7. to determine the services to be re-billed (Art. 13);
8. to access professional data in cases provided for in Art. 25 and 26.

[2] The Director of the Information Systems Management department is competent to order data evaluation relating to named individuals.

[3] Unless the results of the evaluation may be compromised or the person concerned cannot be contacted, the competent HR manager shall inform the person concerned in writing prior to the evaluation.

[4] As far as possible, the person concerned is informed of the results of the evaluation.

[5] If the evaluation relates to a Vice President, the EPFL Direction is competent to order it.

[6] If the evaluation relates to someone working in the Information Systems Management department or in Information Security, the EPFL Direction is competent to order it and to entrust it to a third party.

Article 18 Users' rights to data evaluation

Users do not have the right to carry out evaluations of their data within the meaning of this Directive.

Section 6 Duration of storage and destruction of data

Article 19 Duration of storage and destruction of managed data

[1] When processing objectives so require, managed data may be stored

1. for data referred to in Art. 14, para. 1, items 1, 2, 5 and 6: for maximum two years;
2. for data referred to in Art. 14, para. 1, item 3: for maximum five years;
3. for data referred to in Art. 14, para. 1, items 4 and 7: for maximum ten years;

[2] As for evaluation data, these must be destroyed within three months of completion of the evaluation or within 30 days following entry into force of the ruling concluding the proceedings in which they are used. An anonymous summary of evaluation results may be retained.

[3] Longer statutory periods or other legal obligations may apply.

Article 20 Duration of storage and destruction of unmanaged data

[1] The duration of storage of unmanaged data depends on the storage capacity of the device in question.

[2] Unmanaged data shall be destroyed latest when the device on which they are stored is transferred or eliminated.

Section 7 Misuse

Article 21 Definition

[1] Any conduct in breach of the provisions of this Directive, higher-ranking legislation, instructions by the Head of Unit pursuant to Art. 6 or infringement of the rights of third parties constitutes misuse.

[2] In particular, the following constitute misuse:

1. the downloading, consultation, retention or transmission of pornographic images;
2. private use of the EPFL electronic infrastructure in breach of the rules of Art. 5;
3. committing or incitement to commit criminal offenses;
4. use of the EPFL infrastructure in breach of third party rights, including copyright;
5. the downloading, consultation, retention or transmission of films or pieces of music without the prior approval of the copyright owner, unless done so for strictly academic or personal purposes, pursuant to Art. 19 of the Federal Act on Copyright and Related Rights (CopA);
6. harassment or spreading false, misleading or unnecessarily offensive information;
7. setting up access to the EPFL electronic infrastructure without the prior written consent of the Director of the Information Systems Management department.

[3] Misuse pursuant to para. 2 (art. 21) shall be considered serious when committed intentionally or repeatedly.

[4] The immediate superiors of persons with professional obligations vis-à-vis the EPFL, as well as the Heads of Unit, shall report any misuse of which they are aware to Information Security.

Article 22 Consequences

[1] Any misuse will be sanctioned in accordance with the Disciplinary Rules and Regulations concerning Students of the EPFL and with Opers-EPF.

[2] If such a measure appears necessary to prevent further misuse, the EPFL Direction may order the denial or restriction of access to the EPFL electronic infrastructure, for a limited time where applicable. Whenever possible, the person concerned is heard previously.

[3] Such rulings by the EPFL Direction may be appealed to the FIT Appeals Commission (Art. 37 of the FIT Act).

[4] The costs arising from misuse, including the costs of evaluation and subsequent investigations, court costs and legal fees, may be charged to the offender.

Section 8 Provisional and emergency measures

Article 23 Provisional measures in case of misuse or suspected misuse

[1] In the event of misuse or suspected misuse pursuant to Art. 21, Information Security may, at the request of the Head of Unit:

1. preventively block user access to the EPFL electronic infrastructure to prevent further misuse, for a period of maximum three months;

2. prevent the transmission of abusive content and delete abusive content for security purposes or in compliance with this Directive;
3. take whatever measures necessary to keep a copy of abusive content as evidence.

[2] Whenever measures provided for under para. 1 are decided, Information Security shall promptly notify the Director of the Information Systems Management department, who shall rule whether to authorise the measure. To the extent possible this ruling shall be notified to the person concerned. Should the ruling find that the measure should not have been ordered, the latter shall be immediately lifted.

Article 24 Emergency measures

[1] When data security so requires, particularly to deal with specific threats or to investigate the cause of disruption of the electronic infrastructure, Information Security may order, to the extent necessary, an evaluation of data relating to named individuals without informing the persons concerned.

[2] In case of emergency and in the event of suspected misuse, Information Security may order, to the extent necessary, an evaluation of data relating to named individuals without informing the persons concerned and without requiring a written justification of the suspected misuse.

[3] Should the measures foreseen under paras 1 and 2 (Art. 24) be decided, Information Security shall promptly notify the Director of the Information Systems Management department, who shall rule whether to authorise the measure. To the extent possible this ruling shall be notified to the person concerned. Should the ruling find that the measure should not have been ordered, the results of the evaluation may not be used to the disadvantage of the persons concerned.

Section 9 Departure and death

Article 25 Departure

[1] Before the end of their relationship with the EPFL, users must transfer all their professional data (including documents and emails), as well as any EPFL hardware or software, to the person designated by the Head of Unit or, for users who are students, by the teacher who supervised their work.

[2] Before the end of their relationship with the EPFL, users shall be responsible for deleting any data relating to their private use from the EPFL electronic infrastructure.

[3] Access rights to EPFL electronic infrastructure, including to cloud-based programs, will be removed automatically upon termination of the user's relationship with EPFL, except for:

a. recent PhD graduates who are no longer registered with EPFL. Their email addresses will remain active for six months after they graduate, but they will not be included in the EPFL directory or mailing lists. The recent graduates will also be able to store data and use the internet during this period. However, they must delete all private data from EPFL electronic infrastructure before the period ends.
b. recent Bachelor's and Master's graduates who are no longer registered with EPFL. Their email addresses will remain active for one month after they graduate, but they will not be included in the EPFL directory or mailing lists. The recent graduates will also be able to store data and use the internet during this period. However, they must delete all private data from EPFL electronic infrastructure before the period ends.

[4] Employees, recent PhD graduates, or recent Bachelor's and Master's graduates who leave EPFL can have their new email address appear in the automatic reply that will be sent from their former EPFL address for one year after they leave. To do this, they should send their new email address to 1234@epfl.ch before they leave. The automatic reply will also include the name of a contact person at EPFL. Messages to the email addresses of former employees will be deleted automatically and not forwarded.

[5] To the extent that the mission of the EPFL so requires, the EPFL Direction may order access to the professional data (including documents and emails) of users whose relationship with the EPFL has ceased.

Article 26 Death

[1] In case of death of a user, the user's email address and access to EPFL's IT system will be blocked immediately and the user's data will be saved on a back-up system in compliance with the laws and provisions in force.

[2] In case of death of a user and if circumstances so require, the EPFL Direction may order an evaluation of data relating to named individuals.

[3] To the extent that the mission of the EPFL so requires, the EPFL Direction may order access to the professional data (including documents and emails) of the deceased user.

[4] The EPFL Direction may only deliver private documents and emails to the heirs subject to a valid court order or to a request by the user prior to their death. Information Security will prepare the documents and emails to be delivered.

[5] Messages sent to the deceased user's email address will receive an automatic reply stating that the email address is no longer valid and giving the name of a contact person at EPFL. Messages to the deceased user's email address will be deleted automatically and not forwarded. This automatic reply will remain in place for four weeks, unless required otherwise for security reasons.

Section 10 Requests by the authorities

Article 27 Response to requests by the authorities

The EPFL is expressly authorised to act upon requests by the authorities pertaining to the data it collects under this Directive, including by conducting evaluations of data relating to named individuals and transmitting the information to these authorities.

Section 11 Final provisions

Article 28 Appeals

[1] Rulings by Heads of Unit, the Director of the Information Systems Management department and Information Security may be appealed to the EPFL Direction.

[2] The rights of appeal against rulings by the EPFL Direction are governed by Art. 37 of the FIT Act (FIT Appeals Commission). Information Security must be consulted in appeal procedures concerning issues related to EPFL's electronic infrastructure.

Article 29 Additional rules

To the extent of their powers, Heads of Unit may issue additional rules. In case of discrepancy, the order of precedence is as follows:

1. this Directive;
2. instructions by Information Security;
3. additional rules.

Article 30 Repeal of previous Directives and entry into force

[1] The following directives are hereby repealed:

1. Directive of 10th September 2007 concerning student use of IT resources (LEX 6.1.1);
2. Directive of 21st January 2002 concerning employee use of IT resources (LEX 6.1.2).

[2] This directive entered into force on 13th November 2014 and was revised on 15th March 2021.

On behalf of the EPFL Direction:

Martin Vetterli
President

Françoise Chardonnens
Director of Legal Affairs