Directive on the Use of EPFL Electronic Infrastructure

LEX 6.1.4

13 November 2014, status as at 1 January 2017

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. 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,

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. **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;
3. **subcontractor**: any natural or legal person entrusted by the EPFL with providing services related to the mission or operation of the EPFL;
4. **managed data**: the data, including personal data, stored while using EPFL electronic infrastructure, which are regularly used, analysed or deleted automatically or intentionally;
5. **unmanaged data**: data, including personal data, recorded while using the EPFL electronic infrastructure, but not regularly used, analysed or deleted intentionally.

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 contrary to its purpose and in particular:

1. seeking to alter software or facilities in a manner contrary to their intended use;
2. seeking to circumvent or remove security restrictions;
3. breaching third party licence agreements.

[3] The Vice President for Information Systems may authorise use contrary to Art. 5, para. 2, items 1 and 2. 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. does not endanger EPFL IT security;
3. complies with the law and with this Directive;
4. is not detrimental to the interests of the EPFL;
5. furthermore, such use shall not interfere with the professional obligations of users (in particular faculty members, assistants, PhD candidates, as well as scientific, administrative and technical staff) vis-à-vis the EPFL.

[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).

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. enforcing the measures set out in Art. 11;
3. issuing additional rules pursuant to Art. 27;
4. receiving notifications from users about security issues (Art. 11 para. 4) and ensuring that Information Security has been alerted accordingly;
5. taking the measures provided for in Art. 21;
6. ordering 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. issue instructions (Art 11 para. 2);
2. receive notifications from users about security issues (Art. 11 para. 4) and misuse (Art. 19 para. 4);
3. take provisional measures (art. 21);
4. take emergency measures (art. 22).

Article 8 Vice President for Information Systems (VPSI)

The Vice President for Information Systems is competent to:

1. order data evaluation relating to named individuals and notify the persons concerned (art. 16);
2. decide on emergency measures pursuant to Art. 22 para. 3;
3. issue authorisations (Art. 5 para. 3 and Art. 19 para. 2 item 6);
4. supervise implementation of this Directive by Heads of Unit;
5. appoint a substitute in his/her absence.

Article 9 EPFL Direction

The EPFL Direction is competent to:

1. take the measures provided for in Art. 20 para. 1;
2. take emergency measures as provided for in Art. 22;
3. order access to the professional documents and e-mails of users whose relationship with the EPFL has ceased (Art. 23 para. 3);
4. order an evaluation of data relating to named deceased users (Art. 24 para. 1);
5. order access to the documents and e-mails of deceased users (Art. 24 paras. 2 and 3).

Article 10 Exclusive powers

[1] Human Resources shall have exclusive jurisdiction to order an evaluation of compliance with professional obligations, in particular to monitor working time. HR shall nevertheless inform the Vice President for Information Systems accordingly.

[2] If this Directive provides that the evaluation is the responsibility of the EPFL Direction, the latter's prior agreement must be obtained.

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.

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

[5] 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.

[6] Unless expressly warranted, the EPFL assumes no responsibility for the use of its electronic infrastructure.

Article 12 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 13 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. 12);
6. to manage staff working time and improve the functioning of the EPFL;
7. to perform backups and ensure archiving.

[2] 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 14 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.

Article 15 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. He/she shall take the necessary measures to ensure that individuals are not identifiable.

Article 16 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 or to take action against proven misuse;
2. to analyse and eliminate disruptions to electronic infrastructure and protect against clear threats to this infrastructure;
3. to provide required services;
4. to record and invoice services rendered;
5. to monitor individual working hours;
6. to determine the services to be re-billed (Art. 12);
7. to access professional data in cases provided for in Arts 23 and 24.

[2] The Vice President for Information Systems 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.

Section 6 Duration of storage and destruction of data

Article 17 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. 13, para. 1, items 1, 2, 5 and 6: for maximum two years;
2. for data referred to in Art. 13, para. 1, item 3: for maximum five years;
3. for data referred to in Art. 13, 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 18 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 19 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. 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. harassment or spreading false, misleading or unnecessarily offensive information;
6. setting up access to the EPFL electronic infrastructure without the prior written consent of the Vice President for Information Systems.

[3] Misuse pursuant to para. 2 (art. 19) 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 20 Consequences

[1] 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.

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

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

[4] The provisions of the Disciplinary Rules and Regulations concerning Students of the EPFL and of Opers-EPF shall remain applicable.

Section 8 Provisional and emergency measures

Article 21 Provisional measures in case of misuse or suspected misuse

[1] In the event of misuse or suspected misuse pursuant to Art. 19, 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 transmission of abusive content and keep a copy thereof as evidence;
3. delete abusive content for security purposes or in compliance with this Directive.

[2] Whenever measures provided for under para. 1 are decided, Information Security shall promptly notify the Vice President for Information Systems, 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 22 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. 22) be decided, Information Security shall promptly notify the Vice President for Information Systems, 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 23 Departure

[1] 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.

[2] Access rights to EPFL electronic infrastructure are removed automatically upon termination of the user's relationship with EPFL. If justified, access to the user's e-mail may be exceptionally maintained beyond that date.

[3] To the extent that the mission of the EPFL so requires, the EPFL Direction may order access to the professional documents and e-mails of users whose relationship with the EPFL has ceased.

Article 24 Death

[1] 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.

[2] To the extent that the mission of the EPFL so requires, the EPFL Direction may order access to the documents and e-mails of the deceased user.

[3] The EPFL Direction may only deliver private documents and e-mails to the heirs subject to a valid court order or to a request by the user prior to their death.

Section 10 Requests by the authorities

Article 25 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 26 Appeals

[1] Rulings by Heads of Unit, the Vice President for Information Systems 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).

Article 27 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 28 Repeal of previous Directives and entry into force

[1] The following Directives are hereby repealed:

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

[2] This Directive enters into force on 13 November 2014, status as at 1 January 2017.

On behalf of the EPFL Direction:

Patrick Aebischer
President

Susan Killias
General Counsel

Comment: this Directive has been reviewed as part of the 2017 reorganisation. No modifications were made to this directive as a result of the review.