Directive pour l'utilisation de l'infrastructure électronique de l'EPFL

LEX 6.1.4

13 novembre 2014, état au 15 mars 2021

La Direction de l'Ecole polytechnique fédérale de Lausanne,

vu la Loi fédérale sur les écoles polytechniques fédérales (Loi sur les EPF) ;

vu les art. 57i ss, de Loi sur l'organisation du gouvernement et de l'administration (LOGA) ;

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

vu l'art. 3 al. 1, let. a, de l'Ordonnance du Conseil des EPF sur les écoles polytechniques fédérales de Zurich et de Lausanne (Ordonnance sur l'EPFZ et l'EPFL) ;

vu l'Ordonnance sur l'organisation de l'Ecole polytechnique fédérale de Lausanne, en particulier son art. 4 ;

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

vu l'Ordonnance du Conseil des EPF sur le personnel du domaine des écoles polytechniques fédérales (OPers-EPF) ;

vu l'Ordonnance de l'EPFL sur les mesures disciplinaires ;

vu l'Ordonnance pour l'utilisation des logiciels soumis à contrat de licence (LEX 6.1.5)

arrête :

Section 1 Dispositions générales

Article 1 But

La présente directive a pour but de garantir une utilisation de l'infrastructure électronique de l'EPFL conforme à sa mission et de prévenir les abus à cet égard.

Article 2 Définitions[1]

Au sens de la présente directive on entend par :

1. **utilisateur** : toute personne utilisant l'infrastructure électronique de l'EPFL ;
2. **collaborateur :** toute personne relevant de l'EPFL au sens de l'art. 13 al. 1, let. a, b et d de la Loi sur les EPF (corps enseignant, assistants, collaborateurs scientifiques, candidats au doctorat, collaborateurs administratifs et collaborateurs techniques) ;
3. **infrastructure électronique** : ensemble des équipements fixes ou mobiles qui peuvent enregistrer ou transmettre des données, y compris des données personnelles, en particulier les ordinateurs, composants de réseau, logiciels, supports de données, appareils téléphoniques, imprimantes, scanneurs, télécopieurs, photocopieurs, systèmes de contrôle des installations à l'entrée et à l'intérieur des locaux, ainsi que les systèmes de géolocalisation ;
4. **sous-traitant** : toute personne physique ou morale chargée par l'EPFL de fournir des services liés à la mission ou au fonctionnement de l'EPFL ;
5. **données administrées** : les données, y compris des données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de l'EPFL et qui sont régulièrement utilisées, analysées ou effacées automatiquement ou volontairement ;
6. **données non administrées** : les données, y compris des données personnelles, qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de l'EPFL, mais qui ne sont pas régulièrement utilisées, analysées ou effacées volontairement.

[1] Tous les termes représentant des fonctions désignent des personnes des deux sexes.

7. **donnée personnelle :** toute information se rapportant à une personne physique identifiée ou identifiable au sens de l'art. 3 let. a de la Loi sur la protection des données (LPD).
8. **secret de fonction :** obligation d'une personne à garder le secret sur une information qui lui a été confiée ou qui est venue à sa connaissance dans le cadre de son travail (art. 320 CP, l'art. 22 LPers et l'art. 57 OPers-EPF). Cela concerne tous les documents officiels qui ne peuvent pas être rendus accessibles en vertu de la Loi fédérale sur le principe de la transparence dans l'administration (LTrans).

Article 3 Champ d'application personnel

[1] La présente directive s'applique à toute personne qui utilise l'infrastructure électronique de l'EPFL (utilisateurs).

[2] Elle s'applique en particulier :

1. aux personnes relevant de l'EPFL au sens de l'art. 13 de la Loi sur les EPF ;
2. à tous les autres utilisateurs de l'infrastructure électronique de l'EPFL (y compris lorsqu'il s'agit d'une utilisation temporaire).

Article 4 Champ d'application matériel

La présente directive s'applique à toute utilisation de l'infrastructure électronique de l'EPFL, y compris lorsqu'il en est fait une utilisation à distance ou au moyen de terminaux qui n'ont pas été mis à disposition par l'EPFL.

Article 5 Conditions générales d'utilisation de l'infrastructure électronique

[1] L'utilisation de l'infrastructure électronique de l'EPFL est permise dans la mesure où elle est conforme à la mission de l'EPFL, aux dispositions de la présente directive et, le cas échéant, aux conditions particulières des sous-traitants qui ont été transmises à l'utilisateur.

[2] Toute utilisation de l'infrastructure électronique de l'EPFL est strictement interdite lorsqu'elle :

1. est contraire à la mission de l'EPFL ;
2. viole le droit applicable ou la présente directive, notamment en constituant un abus ;
3. viole les contrats de licence de tiers (notamment les licences logicielles)
4. porte atteinte aux intérêts de l'EPFL ;
5. met en danger la sécurité informatique de l'EPFL ;
6. cherche à modifier des logiciels ou des installations d'une façon contraire à leur usage prévu ; ou
7. cherche à contourner ou à supprimer des restrictions de sécurité.

[3] Le Directeur du domaine des systèmes d'information conjointement avec la Directrice des Affaires juridiques peuvent autoriser des exceptions à l'art. 5, al. 2, points 6 et 7. L'autorisation sera donnée préalablement et par écrit en présence de motifs valables.

[4] L'utilisation à des fins privées de l'infrastructure électronique de l'EPFL est permise dans la mesure où :

1. elle n'entraîne que des coûts minimes pour l'EPFL et ne consomme pas exagérément des ressources informatiques ;
2. elle ne devra en outre pas nuire aux obligations professionnelles des collaborateurs vis-à-vis de l'EPFL ;
3. l'EPFL n'assume aucune responsabilité pour l'utilisation privée de son infrastructure électronique, notamment pour la disponibilité et l'intégrité des données privées stockées sur du matériel appartenant à l'EPFL.

[5] L'utilisation à des fins privées de l'infrastructure électronique de l'EPFL est signalée par les utilisateurs au moyen des outils qui leur sont fournis (répertoire dans la messagerie électronique ou dans le système de stockage, clairement identifié dans son nom comme privé).

[6] En cas de vol ou perte de matériel informatique appartenant à l'EPFL, toutes les données stockées sur ledit matériel seront effacées à distance sans délai par la Sécurité de l'information ou par le responsable IT de faculté en charge, pour autant que ce soit techniquement possible. Les données privées et professionnelles ne seront pas traitées différemment.

[7] L'adresse de courrier électronique EPFL est une adresse professionnelle ou d'étude, utilisée par son détenteur dans le cadre de sa mission ou de ses études à l'EPFL. Elle lui permet de communiquer avec le nom de l'EPFL. A titre honorifique, les professeurs honoraires de l'EPFL peuvent détenir une adresse email EPFL. Un utilisateur tiers ne relevant pas de l'EPFL au sens de l'art. 13 de la Loi sur les EPF peut disposer d'une adresse de courrier électronique EPFL uniquement si sa mission à l'EPFL exige qu'il communique avec le nom de l'EPFL, afin de remplir correctement sa mission. En conséquence, les détenteurs d'une adresse de courrier électronique EPFL sont :

1. les étudiants de l'EPFL pour la durée de leurs études ;
2. les collaborateurs de l'EPFL pour la durée de leur contrat ;
3. les professeurs honoraires de l'EPFL ; et
4. les utilisateurs tiers ne relevant pas de l'EPFL au sens de l'art. 13 de la Loi sur les EPF pour la durée de leur mission et pour autant que leur mission l'exige.

[8] Pour pouvoir utiliser l'infrastructure électronique de l'EPFL, un tiers ne relevant pas de l'EPFL au sens de l'art. 13 de la Loi sur les EPF est tenu de signer un engagement à respecter les dispositions de la présente directive ainsi que des dispositions additionnelles appropriées tenant compte de son statut d'utilisateur tiers ; le texte de l'engagement sera mis à disposition par le Domaine des systèmes d'information. Cet alinéa ne s'applique pas aux utilisateurs non administrateurs des systèmes en libre accès.

Section 2 Compétences

Article 6 Du responsable de l'unité

Le responsable de l'unité est responsable de la mise en œuvre de la présente directive. Il a pour mission :

1. d'informer les utilisateurs ;
2. de s'assurer que tous les tiers ne relevant pas de l'EPFL au sens de l'art. 13 de la Loi sur les EPF accrédités dans son unité aient signé au préalable à leur accréditation le document cité selon l'art. 5 al. 8.
3. de mettre en œuvre les mesures décrites à l'art. 11 ;
4. d'édicter des règles supplémentaires au sens de l'art. 29 ;
5. de recevoir les notifications des utilisateurs relatives à des problèmes de sécurité (art. 11, al. 4) et s'assurer que la Sécurité de l'information ait été prévenue ;
6. de prendre les mesures prévues à l'art. 23.

Il a de plus la possibilité d'ordonner les analyses ne se rapportant pas aux personnes (art. 14) et les analyses non nominales se rapportant aux personnes (art. 15).

Article 7 De la Sécurité de l'information

La Sécurité de l'information a la compétence :

1. d'effacer toutes les données stockées sur du matériel appartenant à l'EPFL déclaré volé ou perdu (art. 5 al. 6) ;
2. d'édicter des instructions (art. 11, al. 2) ;
3. d'imposer la mise en place de mesures de sécurité supplémentaires, restreindre ou interdire sans préavis l'accès à l'infrastructure électronique (art. 12) ;
4. de recevoir les notifications des utilisateurs relatives à des problèmes de sécurité (art. 11, al. 4) et des abus (art. 21, al. 4);
5. de prendre des mesures provisionnelles (art. 23) ;

6. de prendre des mesures urgentes (art. 24) ;
7. de procéder aux analyses ordonnées ou de charger un tiers d'y procéder (art. 14 à 17).

Article 8 Du Directeur du domaine des systèmes d'information

Le Directeur du domaine des systèmes d'information a la compétence :

1. d'ordonner les analyses nominales se rapportant aux personnes et d'informer les personnes concernées (art. 17) ;
2. de statuer concernant les mesures d'urgence au sens de l'art 24, al. 3 ;
3. de délivrer des autorisations (art. 5, al. 3 et art. 21, al. 2, point 7) ;
4. de superviser les responsables d'unité dans la mise en œuvre de la présente directive ;
5. de nommer un suppléant.

Article 9 De la Direction de l'EPFL

La Direction de l'EPFL a la compétence :

1. de prendre les mesures prévues à l'art. 22, al. 2 ;
2. de prendre des mesures d'urgence prévues à l'art. 24 ;
3. d'ordonner l'accès aux documents et courriels professionnels d'utilisateurs dont les rapports avec l'EPFL ont pris fin (art. 25, al. 5) ;
4. d'ordonner l'analyse nominale, se rapportant aux personnes, de données qui concernent des utilisateurs décédés (art. 25, al. 1) ;
5. d'ordonner l'accès aux documents et courriels d'utilisateurs décédés (art. 26, al. 2 à 4).

Article 10 Compétences réservées

[1] Une analyse portant sur le respect des obligations professionnelles, en particulier le contrôle du temps de travail, ne peut être ordonnée que par le Domaine des ressources humaines ou dans le cadre d'une enquête administrative (Art. 58 OPers-EPF et Art. 27j ss OLOGA) ou disciplinaire (Art. 58a OPers-EPF). Les RH en informeront néanmoins le Domaine des systèmes d'information.Dans le cas d'une enquête administrative ou disciplinaire, l'accord de la Direction de l'EPFL devra être obtenu préalablement.

[2] Une analyse des données dans le but d'évaluer la progression des études et les compétences des candidats aux études, des étudiants, des candidats au doctorat et des auditeurs, ne peut être ordonnée que par l'enseignant responsable de cette évaluation, après avoir préalablement informé les candidats aux études, les étudiants, les candidats au doctorat et les auditeurs des modalités de l'évaluation. Cette analyse ne doit pas porter sur des données sensibles ou des profils de personnalité.

[3] Une analyse au sens de l'al. 2 peut également être ordonnée par l'autorité disciplinaire dans le cadre d'une procédure disciplinaire au sens de l'art. 12 de l'Ordonnance de l'EPFL sur les mesures disciplinaires.

Section 3 Responsabilité et mesures de sécurité

Article 11 Responsabilité

[1] Chaque utilisateur est responsable de l'utilisation et de la gestion de ses accès à l'infrastructure électronique. En particulier, chaque utilisateur veille à ne pas violer les dispositions de la présente directive et de la loi, à ne pas porter atteinte aux droits de tiers ou aux intérêts de l'EPFL et à ne pas mettre en danger l'infrastructure électronique de l'EPFL.

[2] Les utilisateurs respectent scrupuleusement les instructions de la Sécurité de l'information. Ils sont rendus attentifs par celle-ci aux mesures de sécurité particulières s'appliquant à certaines parties de l'infrastructure électronique de l'EPFL.

[3] Les terminaux privés connectés au réseau de l'EPFL sur site ou à distance doivent être munis d'un anti-virus à jour. Les logiciels et systèmes d'exploitation qu'ils contiennent doivent faire l'objet

des mises à jour relatives à la sécurité. Pour le surplus, la LEX 6.1.3 s'applique en cas d'utilisation de matériel privé.

[4] S'ils ont connaissance de problèmes de sécurité, les utilisateurs en informent immédiatement le responsable de l'unité et la Sécurité de l'information.

[5] L'EPFL met à disposition un service de sauvegarde de données professionnelles. Chaque utilisateur est tenu de s'assurer que les données professionnelles sur lesquelles il travaille font l'objet de sauvegardes adéquates et régulières ou bénéficient d'un mécanisme équivalent.

[6] En cas de vol ou de perte du matériel informatique mis à sa disposition par l'EPFL, chaque utilisateur est tenu de prévenir au plus vite le service Sécurité, interventions et sûreté, son responsable hiérarchique et la Sécurité de l'information.

[7] En cas de vol ou de perte de données personnelles ou de données soumises au secret de fonction ou au secret d'affaires, traitées dans le cadre professionnel, chaque utilisateur est tenu de prévenir immédiatement son responsable hiérarchique et la Sécurité de l'information.

[8] Les utilisateurs qui, sans droit, contreviennent aux dispositions de la présente directive, de la loi ou à des instructions y relatives en sont personnellement responsables et indemnisent l'EPFL pour tout dommage subi.

Article 12 Sécurité de l'infrastructure électronique de l'EPFL

[1] La Sécurité de l'information peut imposer la mise en place de mesures de sécurité supplémentaires, restreindre ou interdire sans préavis l'accès à l'infrastructure électronique de l'EPFL à certains matériels dont le niveau de sécurité est jugé insuffisant.

[2] La Sécurité de l'information peut imposer la mise en place de mesures de sécurité pour accéder à certaines ressources de l'infrastructure électronique de l'EPFL.

Article 13 Services payants

Les membres du corps enseignant, des assistants, candidats au doctorat, ainsi que des collaborateurs scientifiques, administratifs et techniques (mention de catégories de personnel non exhaustive) qui font usage à titre privé de services payants facturés à l'EPFL (par exemple des appels surtaxés) sans l'accord de leur supérieur direct en assument personnellement les coûts.

Section 4 Données récoltées

Article 14 Données personnelles pouvant être récoltées

[1] L'EPFL peut récolter et enregistrer des données personnelles liées à l'utilisation de son infrastructure électronique dans les buts suivants :

1. garantir la sécurité des données et des locaux de l'EPFL, ainsi que la sécurité et le bon fonctionnement de l'infrastructure électronique de l'EPFL ;
2. assurer l'entretien technique de l'infrastructure électronique de l'EPFL ;
3. retracer l'accès aux fichiers ;
4. surveiller le respect de la présente directive ;
5. facturer les coûts à chaque unité d'imputation, ainsi qu'aux utilisateurs (art. 13) ;
6. gérer le temps de travail du personnel et améliorer le fonctionnement de l'EPFL ;
7. effectuer des copies de sauvegarde et assurer l'archivage.

[2] L'EPFL peut également récolter et enregistrer des données dans le but d'évaluer les candidats aux études, les étudiants, les candidats au doctorat et les auditeurs au sens de l'art. 10 al. 2.

[3] L'EPFL et les sous-traitants peuvent récolter et enregistrer des données personnelles indispensables à la fourniture de leurs services.

Section 5 Analyse des données récoltées

Article 15 Analyse ne se rapportant pas aux personnes

[1] Les données peuvent être analysées sans rapport avec des personnes dans les buts mentionnés à l'art. 14.

[2] Le responsable de l'unité est compétent pour ordonner l'analyse.

[3] Ces analyses peuvent être effectuées sans limite de temps ni de contenu.

Article 16 Analyse non nominale se rapportant aux personnes

[1] Les données peuvent être analysées en rapport avec des personnes, mais de manière non nominale (utilisation de pseudonymes), lorsque l'analyse a lieu par sondage et dans les buts suivants :

1. contrôler l'utilisation de l'infrastructure électronique ;
2. contrôler le temps de travail du personnel.

[2] Le responsable de l'unité est compétent pour ordonner l'analyse. La Sécurité de l'information prend les mesures nécessaires pour que les personnes ne soient pas identifiables.

Article 17 Analyse nominale se rapportant aux personnes

[1] Les données peuvent être analysées en rapport avec des personnes et de manière nominale dans les buts suivants :

1. élucider un soupçon concret et documenté par écrit d'abus ;
2. poursuivre ou documenter un cas avéré d'abus ;
3. analyser les perturbations de l'infrastructure électronique, y remédier ou parer aux menaces concrètes qu'elle subit ;
4. fournir des prestations indispensables ;
5. contrôler le temps de travail de personnes déterminées ;
6. déterminer les prestations à refacturer (art. 13) ;
7. accéder à des données professionnelles dans les cas prévus par les art. 25 et 26.

[2] Le Directeur du domaine des systèmes d'information est compétent pour ordonner l'analyse nominale se rapportant aux personnes.

[3] A moins que les résultats de l'analyse ne risquent d'être compromis ou que la personne concernée ne puisse pas être contactée, le chef de personnel compétent informe la personne concernée par écrit avant de procéder à l'analyse.

[4] Dans la mesure du possible, la personne concernée est également informée des résultats de l'analyse.

[5] Si l'analyse concerne un Vice-président, la Direction de l'EPFL est compétente pour l'ordonner.

[6] Si l'analyse concerne un membre du Domaine des systèmes d'information ou de la Sécurité de l'information, la Direction de l'EPFL est compétente pour l'ordonner et confier son exécution à un tiers.

Article 18 Droit des utilisateurs à une analyse

Les utilisateurs n'ont aucun droit à une analyse de leurs données au sens de la présente Directive.

Section 6 Durée de conservation et destruction des données

Article 19 Durée de conservation et destruction des données administrées

[1] Lorsque les finalités de traitement l'exigent, les données administrées peuvent être conservées :

1. pour les données visées à l'art. 14, al. 1, points 1, 2, 5 et 6 : deux ans au plus ;
2. pour les données visées à l'art. 14, al. 1, point 3 : cinq ans au plus ;
3. pour les données visées à l'art. 14, al. 1, points 4 et 7 : dix ans au plus.

[2] Lorsqu'il s'agit de données d'analyse, elles doivent être détruites au plus tard trois mois après la fin de l'analyse ou dans les 30 jours suivant l'entrée en force de la décision mettant fin à la procédure dans laquelle elles sont utilisées. Un résumé anonyme du résultat d'analyse peut être conservé.

[3] Des délais légaux plus longs ou d'autres obligations légales sont réservés.

Article 20 Durée de conservation et destruction des données non administrées

[1] La durée de conservation des données non administrées dépend de la capacité de mémoire de l'appareil considéré.

[2] Les données non administrées sont détruites au plus tard lorsque l'appareil sur lequel elles sont enregistrées est cédé ou éliminé.

Section 7 Abus

Article 21 Définition

[1] Tout comportement violant les dispositions de la présente directive, de règlements de rang supérieur, d'instructions du responsable de l'unité au sens de l'art. 6 ou violant les droits de tiers constitue un abus.

[2] Constituent en particulier des abus :

1. Le téléchargement, la consultation, la conservation ou la transmission d'images pornographiques ;
2. l'utilisation de l'infrastructure électronique de l'EPFL à titre privé en violation des règles de l'art. 5 ;
3. la commission ou l'incitation à la commission d'infractions pénales ;
4. l'utilisation de l'infrastructure de l'EPFL en violation des droits de tiers, y compris les droits d'auteurs ;
5. le téléchargement, la consultation, la conservation ou la transmission de films ou de morceaux musicaux sans l'autorisation de l'ayant-droit, sauf dans le cadre pédagogique d'enseignement ou à des fins personnelles au sens de l'art. 19 LDA ;
6. le harcèlement ou la propagation d'informations fausses, trompeuses ou inutilement blessantes ;
7. la mise en place d'accès à l'infrastructure électronique de l'EPFL sans le consentement préalable écrit du Directeur du domaine des systèmes d'information.

[3] Constituent des abus graves, les abus au sens de l'al. 2 (art. 21) lorsqu'ils sont commis intentionnellement ou de manière répétée.

[4] Les supérieurs directs des personnes ayant des obligations professionnelles vis-à-vis de l'EPFL, ainsi que le responsable de l'unité ont l'obligation de signaler à la Sécurité de l'information les abus dont ils ont connaissance.

Article 22 Conséquences

[1] Un abus peut être sanctionné par une mesure disciplinaire conformément à l'Ordonnance de l'EPFL sur les mesures disciplinaires et à l'Opers-EPF.

[2] Si la mesure paraît nécessaire pour prévenir de nouveaux abus, la Direction de l'EPFL peut ordonner la privation ou la restriction de l'accès à l'infrastructure électronique de l'EPFL, le cas échéant en limitant la mesure à une durée déterminée. Dans la mesure du possible, la personne concernée sera entendue préalablement.

[3] La décision de la Direction de l'EPFL peut faire l'objet d'un recours à la Commission de recours des EPF (art. 37 de la Loi sur les EPF).

[4] Les coûts engendrés par les abus, y compris les frais relatifs aux analyses et investigations subséquentes, les frais judiciaires et d'avocats peuvent être mis à la charge de l'auteur des abus.

Section 8 Mesures provisionnelles et d'urgence

Article 23 Mesures provisionnelles en cas d'abus ou de soupçon d'abus

[1] En présence d'un abus ou d'un soupçon d'abus au sens de l'art. 21, la Sécurité de l'information peut notamment sur demande du responsable de l'unité :

1. bloquer préventivement l'accès de l'utilisateur à l'infrastructure électronique de l'EPFL, afin d'empêcher que de nouveaux abus ne soient commis pour une durée de trois mois au plus ;
2. empêcher la transmission du contenu abusif et supprimer le contenu abusif lorsque la sécurité ou le respect de la présente directive l'exige ;
3. prendre toutes mesures nécessaires à la sauvegarde de preuves.

[2] Lorsque les mesures prévues à l'al. 1 sont décidées, la Sécurité de l'information informe dans les meilleurs délais le Directeur du domaine des systèmes d'information, qui rend une décision autorisant la mesure. Cette décision est, dans la mesure du possible, communiquée à la personne concernée. Lorsque la décision constate que la mesure n'aurait pas dû être ordonnée, elle est immédiatement levée.

Article 24 Mesures d'urgence

[1] Lorsque la sécurité des données l'exige, et notamment afin de parer à des menaces concrètes ou pour rechercher la cause de perturbations de l'infrastructure électronique, la Sécurité de l'information peut ordonner, dans la mesure nécessaire, l'analyse de données nominales se rapportant aux personnes sans en informer les personnes concernées.

[2] En cas d'urgence et en présence d'un soupçon d'abus, la Sécurité de l'information peut ordonner, dans la mesure nécessaire, l'analyse de données nominales se rapportant aux personnes sans en informer les personnes concernées et sans qu'une motivation écrite du soupçon d'abus ne soit nécessaire.

[3] Lorsque les mesures prévues aux al. 1 et 2 (art. 24) sont décidées, la Sécurité de l'information informe dans les meilleurs délais le Directeur du domaine des systèmes d'information, qui rend une décision autorisant la mesure. Cette décision est dans la mesure du possible, communiquée à la personne concernée. Lorsque la décision constate que la mesure n'aurait pas dû être ordonnée, les résultats de l'analyse ne peuvent pas être utilisés au détriment des personnes concernées.

Section 9 Départ et décès

Article 25 Départ

[1] Avant la fin des rapports qu'ils entretiennent avec l'EPFL, les utilisateurs sont responsables de transmettre, toutes leurs données professionnelles (y compris les documents et courriers électroniques) à la personne désignée par le responsable de l'unité ou, pour les étudiants, par l'enseignant qui a encadré leur travail, ainsi que le matériel informatique mis à leur disposition par l'EPFL.

[2] Avant la fin des rapports qu'ils entretiennent avec l'EPFL, les utilisateurs sont responsables d'effacer les données relatives à leur utilisation privée de l'infrastructure électronique de l'EPFL.

[3] Les droits d'accès à l'infrastructure électronique de l'EPFL, y compris aux ressources externalisées de type cloud, sont retirés automatiquement lorsque les rapports de l'utilisateur avec l'EPFL prennent fin, à l'exception :

a. des doctorants qui restent accrédités comme étudiants exmatriculés pendant les six mois suivant leur exmatriculation. La boîte aux lettres électronique desdits doctorants reste active durant cette période, mais ils n'apparaissent ni dans l'annuaire ni dans les mailing-lists. L'accès au stockage individuel et l'accès à Internet restent actifs durant cette période. Les utilisateurs sont responsables d'effacer les données relatives à leur utilisation privée de l'infrastructure électronique de l'EPFL avant la fin de cette période.

b. des étudiants nouvellement diplômés en Bachelor et Master, qui restent accrédités comme étudiants exmatriculés pendant un mois suivant leur exmatriculation. La boîte aux lettres électronique desdits étudiants reste active durant cette période, mais ils n'apparaissent ni dans l'annuaire ni dans les mailing-lists. L'accès au stockage individuel et l'accès à Internet restent actifs durant cette période. Les utilisateurs sont responsables d'effacer les données relatives à leur utilisation privée de l'infrastructure électronique de l'EPFL avant la fin de cette période.

[4] Chaque collaborateur, doctorant, ou étudiant nouvellement diplômé en Bachelor et Master, quittant l'EPFL peut fournir, préalablement à son départ, à 1234@epfl.ch une adresse de courrier électronique, qui figurera pendant une année dans un message de réponse automatique de départ définitif de l'EPFL incluant aussi une adresse de contact à l'EPFL. Le message de l'expéditeur n'est pas dévié, mais il est automatiquement supprimé.

[5] Dans la mesure où la mission de l'EPFL l'exige, la Direction de l'EPFL peut ordonner l'accès aux données professionnelles (y compris les documents et courriers électroniques) des utilisateurs lorsque les rapports qu'ils entretenaient avec l'EPFL ont pris fin.

Article 26 Cas de décès

[1] En cas de décès de l'utilisateur, les accès informatiques et le compte de messagerie électronique du défunt sont bloqués immédiatement, et ses données sont conservées dans le respect des lois et dispositions en vigueur.

[2] En cas de décès d'un utilisateur et si les circonstances l'exigent, la Direction de l'EPFL peut ordonner l'analyse de données nominales se rapportant aux personnes.

[3] Dans la mesure où la mission de l'EPFL l'exige, la Direction de l'EPFL peut ordonner l'accès aux données professionnelles (y compris les documents et courriers électroniques) du défunt.

[4] La Direction de l'EPFL ne peut transmettre des documents et courriers électroniques privés aux héritiers qu'en présence d'une décision judiciaire valable ou d'une demande anticipée adressée par le défunt à l'EPFL. La Sécurité de l'information est responsable de préparer les documents et courriers électroniques à transmettre.

[5] Les personnes envoyant des courriers électroniques à l'adresse bloquée reçoivent une réponse automatique indiquant que l'adresse du destinataire n'est plus valable et une adresse de contact à l'EPFL. Le message de l'expéditeur est supprimé sans être dévié. Le système de réponse automatique est maintenu en place quatre semaines, sauf motif de sécurité.

Section 10 Demandes émanant d'autorités

Article 27 Réponse aux demandes d'autorités

L'EPFL est expressément autorisée à donner suite aux demandes d'autorités relatives aux données qu'elle collecte en vertu de la présente directive, y compris procéder à des analyses nominales se rapportant aux personnes et transmettre les informations auxdites autorités.

Section 11 Dispositions finales

Article 28 Recours

[1] Les décisions du responsable de l'unité, du Directeur du domaine des systèmes d'information et de la Sécurité de l'information sont sujettes à recours devant la Direction de l'EPFL.

[2] Le droit de recours contre les décisions de la Direction de l'EPFL est régi par l'art. 37 de la Loi sur les EPF (Commission de recours interne des EPF). La Sécurité de l'information doit être consultée dans les procédures de recours ayant pour objet des questions liées à l'infrastructure électronique de l'EPFL.

Article 29 Règles additionnelles

Dans la mesure de ses compétences, le responsable de l'unité peut édicter des règles additionnelles. En cas de divergence, l'ordre de primauté est le suivant :

1. la présente directive ;
2. les instructions de la Sécurité de l'information ;
3. les règles additionnelles.

Article 30 Abrogation des directives préexistantes et entrée en vigueur

[1] Les directives suivantes sont abrogées :

1. celle du 10 septembre 2007 pour l'utilisation des moyens informatiques par les étudiants (LEX 6.1.1) ;
2. celle du 21 janvier 2002 pour l'utilisation des moyens informatiques mis à disposition des collaborateurs (LEX 6.1.2).

[2] La présente directive, entrée en vigueur le 13 novembre 2014, a été révisée le 15 mars 2021 (version 2.1).

Au nom de la Direction de l'EPFL:

Le Président :
Martin Vetterli

La Directrice des Affaires juridiques :
Françoise Chardonnens