PROTECTION DES DONNÉES À L'UNINE
Guide pour le traitement des données personnelles

Sommaire

Préambule

La protection des données suscite de multiples interrogations au sein de la communauté universitaire et dans le public, autant parmi celles et ceux qui traitent des données que parmi celles et ceux dont les données sont traitées.

Ce guide s'adresse aux membres du personnel académique et du PATB de l'Université qui traitent de données personnelles institutionnelles concernant des étudiantes et des étudiants, concernant des collaboratrices et des collaborateurs de l'UniNE ou concernant des personnes externes à l'UniNE dont les données doivent être conservées. Il a l'objectif de donner des clés pour :

- Définir les données et la façon dont elles doivent être protégées
- Distinguer les données entre elles
- Déterminer les traitements possibles
- Désigner les personnes qui les traitent
- Décider où elles peuvent être stockées

- Donner une réponse appropriée à certaines questions récurrentes

Ce guide ne s'adresse pas spécifiquement aux personnes qui traitent de données de recherche soumises à protection, même si les informations et conseils qu'il renferme peuvent s'appliquer par analogie, sous réserve de dispositions spécifiques exigées par les projets de recherche.

A. Définitions et principes généraux (partie théorique)

I. Introduction

Dans un premier temps, il paraît nécessaire de faire le tour de certaines généralités en matière de protection des données, de revoir quelques fondamentaux.

Qu'est-ce que la protection des données ?

La protection des données est un pan de la protection de la personnalité. Ce que protège la législation en la matière, c'est la personnalité de celle ou celui dont les données sont traitées. Autrement dit, la législation sur la protection des données ne protège pas les données elles-mêmes, mais plutôt les atteintes à la personnalité des personnes concernées par un traitement de données. Il est donc nécessaire que lesdites données se rapportent à une personne identifiée ou identifiable pour qu'elles puissent bénéficier d'une protection au sens de la législation présentée ci-dessous. Les données ne se rapportant pas à des personnes et/ou qui jouissent d'une protection contre leur diffusion (par exemple une clause de confidentialité dans un contrat ou un extrait de procès-verbal) ne sont pas concernées par ce guide.

Quelle est la législation qui s'applique à l'Université ?

L'UniNE, en tant qu'établissement de droit public cantonal neuchâtelois, fait partie des entités soumises à la Convention intercantonale des 8 et 9 mai 2012 relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE). C'est dans ce texte qu'il faut aller chercher en premier les réponses aux questions qui se posent au quotidien en matière de protection des données. Cette convention se retrouve in extenso sur le site du Préposé à la protection des données et à la transparence Jura Neuchâtel (PPDT-JUNE), qui est l'autorité compétente s'agissant de l'application à l'Université. Le site contient également des outils pour aider les personnes qui sont confrontées à des questions relatives à la communication ou à l'utilisation de données.

Quelques définitions

Selon la CPDT-JUNE (art. 14) :

a) Données personnelles : toutes les informations qui se rapportent à une personne identifiée ou identifiable.

   Une personne est « identifiée » lorsqu'il ressort directement des informations détenues (par exemple une pièce d'identité) qu'il s'agit d'une personne déterminée et d'elle seule.

En revanche, une personne est « identifiable » à partir du moment où, par corrélation indirecte d'informations tirées des circonstances ou du contexte, il est possible de l'identifier avec les moyens technologiques disponibles. Ainsi, un numéro d'immatriculation ne permet pas d'identifier directement une étudiante ou un étudiant, mais la ou le rend identifiable pour les personnes qui ont accès à son dossier.

Ainsi, les données statistiques ou anonymisées ne sont pas soumises aux règles de la protection des données. Attention toutefois : l'anonymisation doit empêcher toute identification, même par recoupement. Par exemple, un tableau contenant l'origine et la nationalité des étudiantes et étudiants d'une faculté (sans les noms, évidemment) ne pose en principe pas de problème ; il en va autrement du même tableau concernant les doctorantes et doctorants d'un institut.

La notion de « données personnelles » est très large : un numéro de téléphone, une empreinte digitale, une adresse de courrier électronique, une adresse IP en font en principe partie.

b) Données sensibles :

Certaines données, qualifiées de « données sensibles » de par leur nature, sont soumises à des règles de protection plus strictes que des données « normales ». Parmi les données sensibles on trouve :

- données concernant les opinions ou les activités religieuses, philosophiques, politiques ou syndicales ;
- données concernant la santé, la sphère intime, l'origine ou l'ethnie ;
- données génétiques ;
- données biométriques identifiant une personne de façon unique ;
- données concernant les mesures d'aide sociale ;
- données concernant les poursuites ou sanctions pénales et administratives.

c) Profilage, toute forme de traitement automatisé de données consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

c^{bis}) Profilage à risque élevé, tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

d) Fichier, tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

e) Personne concernée, la personne physique au sujet de laquelle des données sont traitées.

f) Responsable du traitement, l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données.

g) Traitement, toute opération relative à des données – quels que soient les moyens et les procédés utilisés – notamment

- la collecte,
- la conservation,
- l'exploitation,
- la modification,
- la communication,
- l'archivage,
- l'effacement,
- la destruction.

h) Communication, le fait de rendre des données accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant.

i) Communication en ligne, procédure automatisée permettant à un tiers de disposer de données sans l'intervention de celui qui les communique.

j) Loi au sens formel, les textes législatifs soumis au référendum obligatoire ou facultatif, ainsi que les règlements adoptés en assemblée communale.

k) Sous-traitant, la personne privée ou l'entité qui traite des données pour le compte du responsable du traitement.

l) Destinataire, la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles.

m) Décision individuelle automatisée, toute décision prise exclusivement sur la base d'un traitement de données automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

   Lorsqu'il y a une décision individuelle automatisée, la personne concernée doit être informée de ce type de traitement (cf. art. 31 CPDT-JUNE).

n) Violation de la sécurité des données, toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.

Ce guide ne revient pas sur tous les éléments définis ci-dessus. Si un membre du personnel ou une entité réalise une tâche usuelle, ou doit réaliser une nouvelle tâche, qui relève de l'une de

ces définitions, et si ce guide ainsi que les autres outils à disposition ne permettent pas de trouver une réponse quant à la licéité de ladite tâche, il est indiqué de se renseigner auprès des Affaires juridiques.

II. Les principes généraux

Il s'agit ici de principes qui doivent guider toute décision ou action en matière de données. C'est en visant au respect de ces principes que l'on pourra trouver des réponses aux questions listées en préambule. On les retrouve, eux aussi, dans les textes légaux et conventionnels déjà cités (LPD et CPDT-JUNE).

a) Légalité (art. 16 CPDT-JUNE)

Des données peuvent être traitées uniquement si une base légale le prévoit ou si leur traitement sert à l'accomplissement d'une tâche légale. Autrement dit, une récolte de données doit être prévue dans une base légale, comme toutes les activités de l'Etat, conformément à l'art. 5 de la Constitution fédérale (RS 101).

La base légale du traitement de données par l'Université est l'art. 95 LUNE. L'Université peut traiter de données personnelles si c'est nécessaire à l'accomplissement de ses tâches et en veillant à leur protection. Il faut donc toujours se demander si le traitement est nécessaire à l'accomplissement des tâches légales, lesquelles découlent essentiellement des articles 2 et 3 LUNE, mais aussi du droit fédéral et international (LEHE, accords de Bologne, principalement).

L'art. 2 LUNE dit que l'Université a pour missions fondamentales d'assurer l'enseignement supérieur et la recherche. L'art. 3 confie également à l'Université d'autres missions, notamment de vulgarisation, de formation continue, d'encouragement de l'innovation, de promotion de la mobilité ainsi que de contribution au débat public et au développement culturel, social, scientifique et économique.

Il en découle que les tâches de l'Université justifiant le traitement de données consistent principalement à permettre aux personnes qui remplissent les conditions légales et réglementaires de suivre des cursus et de recevoir des titres. Le traitement de données personnelles peut aussi intervenir dans le cadre de la recherche et concerner d'autres personnes que les étudiantes et étudiants, ou le personnel pour ce qui est des données nécessaires au fonctionnement de l'institution. Les activités de communication de l'Université, dans le cadre du recrutement d'étudiantes et d'étudiants, de diffusion de la recherche, mais aussi pour la réalisation des missions de l'art. 3 permettent le traitement de données personnelles.

b) Proportionnalité (art. 17 CPDT-JUNE)

Principe essentiel en droit public, il signifie en matière de protection des données que *seules peuvent être traitées les données nécessaires et propres à atteindre le but visé*.

Principe Général : si, en examinant une information relative à une personne, on ne peut pas répondre par l'affirmative à la question de savoir si le traitement de cette information/donnée est nécessaire et propre à atteindre l'un des buts de l'Université, alors il ne faut pas traiter cette donnée/information, donc ni la recueillir, ni la conserver, ni la communiquer.

De plus, des données personnelles ne doivent être conservées que pendant la durée nécessaire au regard des finalités pour lesquelles elles sont traitées. Le meilleur moyen de protéger contre sa divulgation une donnée recueillie pour exécuter une tâche donnée est de l'effacer lorsqu'elle n'est plus utile pour cette tâche. Attention : certaines données sont utiles pour plusieurs tâches et si l'une de ces tâches disparaît, la donnée peut devoir rester accessible pour les tâches restantes.

c) Bonne foi et finalité (art. 18 CPDT-JUNE)

Le traitement des données doit être effectué conformément au principe de la bonne foi. Les données ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités.

Les principes de bonne foi et de finalité sont très importants en droit de la protection des données. De ces principes découle le fait que, par exemple, les données concernant les étudiantes et les étudiants collectées par les Immatriculations ou les Facultés, ou les données de personnes participant à des événements universitaires, ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées. En effet, la personne qui fournit ses données personnelles au moment de son immatriculation doit pouvoir se fier au fait qu'elles sont récoltées pour les besoins de son propre cursus et dans aucun autre but.

d) Exactitude (art. 19 CPDT-JUNE)

Toute personne qui traite des données doit s'assurer que les données sont exactes et complètes.

Cela oblige à prendre les mesures appropriées afin de pouvoir rectifier, effacer ou détruire les données inexactes ou incomplètes. Une attention particulière doit être apportée à l'exactitude des données qui présentent un risque pour la personnalité ou les droits fondamentaux des personnes concernées.

e) Sécurité des données (art. 20 CPDT-JUNE)

Les entités doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données par rapport au risque encouru.

Les mesures doivent permettre d'éviter toute violation de la sécurité des données. Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.

B. La protection des données au quotidien par les collaboratrices et collaborateurs de l'UniNE (questions pratiques)

Qu'implique la protection des données dans l'accomplissement des tâches des autorités universitaires et dans le travail quotidien des collaboratrices et collaborateurs ?

I. Secret de fonction et accès aux données

Pour commencer, il faut rappeler que tous les membres du personnel de l'Université, quel que soit leur statut contractuel, sont soumis au secret de fonction dont la violation est susceptible de poursuites pénales. Avant de transmettre des informations à quelqu'un, il faut se demander si elles ne sont pas couvertes par ledit secret[1].

Ensuite, le fait de savoir qui, au sein d'une entité, doit disposer de connaissances spécifiques sur les questions en matière de protection des données dépend fortement de l'organisation des facultés ou des services, ainsi que de la répartition des tâches entre les personnes.

Enfin, il faut se demander dans tous les cas si une entité ou une personne qui a accès à des informations ou souhaite y avoir accès en a réellement besoin dans le cadre de l'accomplissement de ses tâches. L'absence de connaissance de ces informations empêche-t-elle cette entité ou cette personne de remplir sa mission, notamment à l'égard d'étudiantes, d'étudiants ou de tiers ? En cas de réponse négative à cette question, il n'est pas nécessaire que l'entité ou la personne accède à ces informations.

II. Quelques questions fréquemment posées

Quelles sont les données protégées ?

- Coordonnées privées (adresse du domicile et courriel(s) privée(s), téléphone, n° AVS,…)
- Etat civil
- Photographies
- Notes et évaluations
- Certificats médicaux
- Décisions des décanats, du SACAD et du Rectorat, voire de la commission de recours
- Contrats pédagogiques
- Relevés de notes

[1] Explications sommaires sur le secret de fonction sur le site du PPDT-JUNE : https://www.ppdt-june.ch/fr/Documentation/Index/Secret-de-fonction-et-professionnel/Guichet-social-romand/Explications-du-Guichet-social-romand.html

- Dossiers du personnel conservés par les RH
- Dossiers de postulation
- Autres données en fonction des circonstances

Quelles données peuvent être collectées et traitées ?

- Les données qui sont par exemple nécessaires au bon déroulement du cursus d'une étudiante ou d'un étudiant et à l'obtention du titre visé ainsi que les données nécessaires pour que le personnel puisse accomplir son travail.
- Le moins de données personnelles possible, respectivement seulement les données nécessaires à l'accomplissement des tâches d'une personne ou d'une entité, ce qui implique notamment la destruction dès que les données ne sont plus utiles.

Où les données protégées peuvent-elles être stockées ?

- Données numériques : sur les serveurs sécurisés (se renseigner au SITEL pour savoir si des solutions externes de type cloud sont sécurisées). Des mesures de protections supplémentaires tels que la protection d'un document par un mot de passe ou un cryptage peuvent être utiles pour les données sensibles.
- Données papier et périphériques externes tels qu'une clé USB : dans des armoires ou tiroirs fermés à clés (pas sur les bureaux).

Quelles personnes sont autorisées à traiter des données protégées et/ou à y accéder ?

- Les personnes dont le cahier des charges ou le règlement organique de la faculté, ou une autre base règlementaire ou légale, prévoit qu'elles doivent traiter des données personnelles.

  Exemples :

  - Si une étudiante ou un étudiant souhaite obtenir un congé ou un retrait d'une session d'examen, l'autorité compétente doit, pour pouvoir se prononcer, connaître le motif à l'appui de la demande. Cela implique que la personne chargée d'enregistrer les demandes de ce type doit les soumettre à l'autorité compétente et l'informer du motif. D'autres personnes au sein de la faculté peuvent savoir qu'une étudiante ou un étudiant est en congé ou s'est retiré-e de la session, mais elles n'ont pas à connaître le motif de ce congé ou de ce retrait, ni à avoir connaissance des congés ou retraits précédents de l'étudiante ou de l'étudiant si ça n'est pas nécessaire à leurs activités.
  - Le Service académique statue, sauf exceptions prévues par des règlements ad hoc, sur les demandes d'admission à un cursus. Le Décanat, son secrétariat et les personnes en charge du cursus connaissent la liste des personnes

admises. Un secrétariat d'institut peut recevoir des informations limitées. Par exemple s'il s'agit d'organiser une sortie annuelle de l'institut, il faut les noms et adresses électroniques, mais pas l'ensemble du dossier académique des personnes suivant un cursus. Une faculté ou un institut peuvent se voir remettre des statistiques sur le nombre de demandes rejetées ou en attente, mais pas sur l'identité des personnes dont la demande a été rejetée ou est en cours de traitement.

- Dans la gestion des cas limites, notamment en vue de statuer sur un repêchage, les membres du Décanat doivent disposer du relevé de notes d'une étudiante ou d'un étudiant. Par contre, s'il faut demander l'avis d'autres personnes, par exemple de l'enseignante ou l'enseignant dont l'évaluation négative implique l'élimination du cursus, cette personne ne pourra pas accéder au relevé de toutes les notes.
- Si un service doit fournir des statistiques à un autre service et utilise pour cela une extraction d'une base contenant des données personnelles (par exemple une liste de noms accompagnés de données protégées), il ne faut pas transmettre l'extraction avec les éléments d'identité, mais uniquement les statistiques anonymisées. Idem si un service doit réaliser un rapport sur la base d'une extraction contenant des données personnelles et tirée d'une base de données, il faut supprimer l'extraction une fois que le rapport est terminé. Par exemple un rapport sur les cantons et pays de provenance des étudiantes et des étudiants : c'est la répartition par lieu de provenance qui est la finalité de la tâche, pas la liste des personnes individuelles avec l'adresse de leur domicile au moment de l'inscription.
- Attention également à ne transmettre d'un service à un autre que ce dont le service demandeur a besoin. Par exemple une liste des membres du corps professoral engagés à 100% qu'il faut contacter dans le cadre d'une procédure ne doit contenir que le nom, le prénom et l'adresse électronique de la personne, mais pas d'autres informations personnelles qui seraient détenues par le service émetteur.
- Une ambassade veut contacter les étudiantes et les étudiants de son pays. Dans ce cas, il est possible de servir d'intermédiaire en transmettant une invitation aux personnes concerné-e-s, mais pas de transmettre une liste des noms avec des adresses postales ou électroniques. Idem si une ancienne étudiante ou un ancien étudiant veut contacter des personnes qui ont eu leur diplôme la même année et demande une liste. De manière générale, des listes de personnes ne doivent pas être transmises à des tiers en l'absence de base légale y autorisant. Toutefois, si le travail administratif pour contacter des personnes en servant d'intermédiaire est trop important, notamment si quelqu'un demande une liste de personnes qui ne sont plus à l'Université, la

demande doit être faite au moyen d'un formulaire ad hoc, transmis au Secrétariat général, afin de statuer sur une éventuelle exception à la règle de non-transmission.

- Les parents d'une étudiante majeure ou d'un étudiant majeur demandent des informations sur le relevé de notes ou les crédits obtenus par leur enfant, ou interviennent dans une procédure concernant leur enfant en demandant des explications. Il n'est pas permis de leur communiquer des informations sur la personne concernée. Idem si la police ou un autre service de l'Etat demande des renseignements sur un membre de la communauté universitaire. Il n'est pas possible de répondre : même une demande policière doit être validée du Ministère public pour avoir accès à des données personnelles.

Quelles personnes n'ont aucun droit d'accéder aux données personnelles ?

- Les collaboratrices ou les collaborateurs qui n'en ont pas besoin pour accomplir leurs missions directement ou indirectement. L'accès aux données personnelles doit être limité aux personnes auxquelles elles sont nécessaires pour fournir leurs prestations. Si elles ne sont pas nécessaires à une collaboratrice ou à un collaborateur, celle-ci ou celui-ci ne doit pas y avoir accès.
- Les parents d'étudiantes et étudiants majeur-e-s.
- Les autorités externes sauf en cas de décision judiciaire (y compris si la police demande des informations, il faut que la demande soit accompagnée d'une décision du Ministère public) ou de consentement de la personne concernée.
- En général toutes les personnes tierces qui n'y ont pas été expressément autorisées par la personne concernée, sauf si une base légale justifie expressément la transmission des données.

C. Références et annexes

I. Références

- PHILIPPE MEIER, *Protection des données – Fondements, principes généraux et droit privé*, Berne 2011.
- CHRISTIAN FLUECKIGER, *Principes généraux de la protection des données et communications transfrontalières dans le cadre des relations de travail*, in : JEAN-PHILIPPE DUNAND/PASCAL MAHON (édit.), *La protection des données dans les relations de travail*, Zurich/Bâle/Genève 2017.

- Site du préposé Jura Neuchâtel à la protection des données et à la transparence : https://www.ppdt-june.ch/
- Site de PRIVATIM, l'association des préposé-e-s suisses à la protection des données : https://www.privatim.ch/fr/
- Site du préposé fédéral à la protection des données et à la transparence : https://www.edoeb.admin.ch/edoeb/fr/home.html
- Think Data !, Service de sensibilisation à la protection des données et à la transparence : http://www.thinkdata.ch/

II. Annexes

- Annexe 1 : Liens utiles
- Annexe 2 : Bases, contexte et droit applicable
- Annexe 3 : formulaire de requête pour liste d'adresse