UNIVERSITE DE LILLE
POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION ET PROTECTION DES DONNEES PERSONNELLES

ACCÈS AUX DONNÉES PROFESSIONNELLES D'UN PERSONNEL INDISPONIBLE V20190606-SSI/EC-DAJI/LB

Les données professionnelles d'une entité (composante, service, laboratoire), sont celles nécessaires à ses missions, quel que soit le lieu de stockage (espace disque local, serveur de fichiers, boite aux lettres individuelle ou partagée, site WEB, …).

Ces données professionnelles doivent être sécurisées, c'est-à-dire protégées suffisamment en termes de confidentialité, intégrité et disponibilité.

Le Directeur de l'entité doit mettre en œuvre tous les moyens nécessaires pour assurer cette sécurité, en particulier par une gestion des droits d'accès (pour la confidentialité), et par la mise en place de mécanismes permettant d'assurer la continuité de service (pour la disponibilité).

Bien que les mesures préventives soient préférables, le Directeur a le droit d'effectuer ou de faire effectuer toute correction de droits d'accès aux données professionnelles de son entité au cas où ces données deviendraient inaccessibles pour diverses raisons, y compris l'indisponibilité d'un personnel.

Pour les besoins de l'entité et afin d'assurer la continuité du service, il est donc légitime d'accorder à d'autres personnels des droits d'accès aux données professionnelles d'un personnel indisponible, même sans l'accord de celui-ci.

Cependant, afin d'éviter tout risque juridique majeur, il faudra s'assurer que l'accès par des tiers aux espaces de stockage d'un personnel indisponible ne provoque ni divulgation de ses données privées (cf. définition dans le Règlement de l'Université : https://ssi.univ-lille.fr/sites/ssi.univ-lille.fr/files/ssi/Reglement_inte__rieur_Universite_de_Lille.pdf**)**, ni communication de données professionnelles confidentielles à des personnes n'ayant pas le besoin d'en connaître (y compris à l'intérieur de la même entité).

Pour limiter les risques précités, il est vivement recommandé de suivre la procédure détaillée ci-dessous.

À effectuer par le Directeur de l'entité :

1) Par respect pour la personne indisponible, essayer d'obtenir communication des données manquantes par celle-ci, puis poursuivre la procédure en cas d'échec de cette tentative.

2) Par courriel à son adresse personnelle**,** ou par courrier postal, signaler à la personne indisponible qu'il sera procédé à une extraction de ses données professionnelles, et que cet accès se fera dans le respect le plus strict de la confidentialité de ses données privées.

Mettre en copie la Direction des Affaire Juridiques et Institutionnelles (affaires-juridiques@univ-lille.fr), les Responsables de la Sécurité des Systèmes d'Information et le Délégué à la Protection des Données Personnelles (adresse commune = ssi@univ-lille.fr)

3) Déterminer les bénéficiaires des données professionnelles qui seront récupérées, en tenant compte du niveau de confidentialité de ces données.

4) Déterminer les personnels qui seront chargés d'effectuer concrètement la récupération. De préférence, on confiera cette tâche à l'administrateur des systèmes informatiques de l'entité s'il existe.

5a) Lui-même, ou par l'intermédiaire des personnels désignés au point 4), extraire les données professionnelles de l'espace de stockage du personnel indisponible, réduire si possible au nécessaire (un fichier plutôt qu'un dossier, un mail plutôt qu'une boite aux lettres, etc...), puis communiquer les données à chaque bénéficiaire (rappel : en tenant compte du fait que chaque bénéficiaire n'a pas nécessairement les mêmes autorisations à connaître telle ou telle information).

Si des données privées venaient malgré tout à être connues pas un des "opérateurs" ou bénéficiaires, ces personnes seraient bien évidemment tenues, par le secret professionnel, à respecter la confidentialité de ces données (rappel : sauf si elles s'avéraient illégales, cf. article 40 du code de procédure pénale, obligation du fonctionnaire de signaler un crime ou un délit).

5b) Si l'intervention de la DSI est nécessaire pour accéder aux espaces de stockage de la personne indisponible, le Directeur de l'entité effectuera la demande par courriel ou courrier aux Responsables de la Sécurité des Systèmes d'Information et au Délégué à la Protection des Données Personnelles (adresse commune = ssi@univ-lille.fr).

Ceux-ci s'assureront du statut hiérarchique du demandeur, puis transmettront la requête à la DSI qui se mettra alors directement en contact avec les personnels désignés au point 4) pour la suite des opérations. La Direction de l'entité, la direction de la DSI et les RSSI+DPO seront mis en copie des échanges éventuels (mais pas des données récupérées !).

PREVENTION

Le droit résiduel à la vie privée, reconnu aux utilisateurs du Système d'Information de l'Université, implique un risque juridique important lors de l’accès par un tiers aux données d’un personnel indisponible .

Ce risque est réduit, mais pas totalement éliminé, quand on respecte la procédure décrite dans ce document.

Pour cette raison, cette procédure devrait rester **exceptionnelle.**

Il est donc préférable d'anticiper la situation en mettant en œuvre des mesures préventives permettant d'accéder en toute sécurité (juridique) aux données professionnelles d'un personnel indisponible. Liste non exhaustive de mesures préventives :

- mettre en œuvre des mécanismes de partage de données professionnelles (gestion des droits d'accès par le mécanisme de « Groupes », partages réseau, liste de diffusion ou partage sécurisé de boites aux lettres),
- concernant la configuration de l'outil de courrier électronique, préconiser ou imposer aux personnels de définir un message d'absence contenant une adresse alternative de contact,
- rappeler régulièrement le caractère professionnel des données et des postes de travail et la nécessité de réduire au minimum les données privées, dont le stockage dans le SI de l'Université n'est qu'un droit "résiduel",

- interdire aux personnels de mettre en œuvre des techniques supplémentaires de sécurisation de leurs données si elles ne sont pas associées à une communication à leur hiérarchie des moyens de débloquer ces protections (mots de passe, clefs de déchiffrement, clefs physiques, ...).

A EVITER

Omettre d'informer la personne concernée,

Accéder aux documents manifestement étiquetés « privé »,

Utiliser les identifiants/mots de passe de la personne indisponible pour accéder à sa place à ses données ou à ses services numériques (usurpation d'identité),

Rediriger automatiquement l'adresse de messagerie nominative d'un personnel indisponible vers un autre destinataire.