Trois recommandations aux étudiants

pour les aider à protéger leurs données (et celles des autres…)

Synthèse :

Étudiants de l'enseignement supérieur, le réseau SupDPO vous propose **trois recommandations simples** pour vous sensibiliser au Règlement général sur la protection des données (RGPD)[1], et ainsi **mettre en place de bonnes pratiques** de sécurité et de protection des données personnelles.

Le recours aux technologies de l'information **exige que chacun de nous respecte les principes du droit à la protection des données personnelles**[2] dans ses deux volets : droits et obligations de respecter la vie privée et les libertés des personnes.

Vous êtes concernés à double titre : vos données sont traitées[3] (par l'établissement dans lequel vous êtes inscrit, et par des tiers), et vous traitez les données d'autrui. Il est donc important de pouvoir :

- vous former pour connaître les risques et la réglementation ;
- protéger vos propres données lorsqu'elles sont transmises pour bénéficier d'un service ;
- protéger les données des autres lorsque vous les utilisez dans un but déterminé.

L'utilisation des données personnelles s'effectue en effet dans le respect de mesures de confidentialité et de sécurité pour ne pas porter atteinte à la vie privée des personnes auxquelles elles appartiennent (divulgation, vol ou détournement d'informations, usurpation d'identité, falsification,…). **Ces risques ne sont pas théoriques : ils existent et ont des conséquences.**

• Recommandation n°1 : Formez-vous pour maîtriser l'utilisation des données personnelles

Formez-vous, informez-vous, et valorisez-le

En complément de votre cursus, initiez-vous au RGPD : le MOOC de la CNIL (atelier-rgpd.cnil.fr/) est complet et délivre une attestation de suivi. Il peut également être valorisé dans votre CV.

Lisez les mentions légales et politiques de confidentialité des applications et réseaux sociaux.

Exercez vos droits

En tant qu'étudiant, vous avez des droits sur l'utilisation de vos données durant votre cursus, et après : vous devez être informé sur l'usage de vos données, y avoir accès et pouvoir rectifier les données erronées, vous opposer à l'utilisation de vos données ou revenir sur votre consentement.

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[2] Donnée à caractère personnel : donnée qui identifie directement ou indirectement une personne physique (nom, note, adresses postale et électronique, @IP, identifiant de connexion informatique, coordonnées bancaires, photographie, voix, certificat médical, n° de sécurité sociale…)

[3] Traitement de données : toute opération portant sur des données personnelles (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...)

Comment exercer ces droits ? Auprès du Délégué.e à la protection des données (DPO) de l'établissement[4]. Sans réponse, vous pouvez saisir la Commission nationale de l'informatique et des libertés (CNIL).

Vous avez des obligations : respectez-les !
En tant qu'utilisateur de données (par exemple si vous menez des travaux de recherche), une réflexion sur la protection des données que vous souhaitez utiliser est à engager **avant de mettre en œuvre votre recherche,** en collaboration avec votre responsable d'études et le DPO de votre établissement.

Suivez la méthodologie de recherche pour respecter la réglementation adéquate.

5 règles de protection des données à respecter :

- Utilisez des données personnelles uniquement si votre recherche le justifie ;
- Utilisez les seules informations nécessaires pour votre recherche (**proportionnalité** des données) ;
- **Informez** les personnes qui vous confient leurs données sur l'utilisation que vous en faites ;
- **Garantissez la confidentialité et la sécurité** des données que vous détenez ;
- **Supprimez** les données à la fin de la recherche.

• Recommandation n°2 : Protégez-vous !

Respectez les précautions élémentaires de sécurité :

- ✓ Protégez l'accès à vos comptes (messagerie, applications…) par des mots de passe complexes, uniques et secrets. Au besoin, utilisez un gestionnaire de mots de passe (par ex. Keepass, Zenyway, Passwordsafe,…)
- ✓ **Ne prêtez pas vos codes** (ENT, réseaux sociaux, wifi,…) ;
- ✓ Soyez prudent vis-à-vis des contenus extérieurs, notamment les courriels (contact inconnu, tournures employées inhabituelles, etc.), un document reçu, un lien de téléchargement sur un site web, etc. En cas de doute, n'ouvrez pas le document et mettez-le dans la corbeille.
- ✓ Pensez l'organisation de vos dossiers :
  - séparez les usages personnels et les usages universitaires,
  - nettoyez et récupérez régulièrement vos données sur les serveurs institutionnels.
- ✓ Ne laissez pas votre poste de travail sans surveillance, verrouillez-le lorsque vous le quittez.
- ✓ Nettoyez vos traces après utilisation d'un poste en libre accès (corbeille, historique,...) et **déconnectez-vous !**

Allez -un tout petit peu- plus loin :

- ✓ Utilisez prioritairement des environnements sécurisés institutionnels :
  - Enregistrez vos travaux pour éviter toute perte de données sur des espaces sécurisés institutionnels ;
  - Privilégiez les canaux sécurisés et outils institutionnels : réseau, serveurs pédagogiques, messagerie… ;
  - Chiffrez votre matériel de stockage des données (disque dur et matériels amovibles).
- ✓ Paramétrez les options de confidentialité en ligne (*cookies*) ;
- ✓ Utilisez des antivirus mis à jour et installez un « pare-feu » (*firewall*) logiciel ;
- ✓ Alertez votre responsable d'études en cas d'anomalie constatée (accès non autorisé, accidentel ou volontaire, hameçonnage, divulgation de données personnelles, etc.).

• Recommandation n°3 : Adoptez les bonnes pratiques numériques pour la sécurité de tous !

- ✓ Préservez votre identité numérique et celle des autres (le harcèlement numérique est un délit) ;
- ✓ Ne connectez pas vos équipements sur des réseaux non maîtrisés ;
- ✓ Respectez la charte informatique de l'établissement ;
- ✓ Respectez les données d'autrui en toutes circonstances (réseaux sociaux, formulaires de collecte…) !
  - pas de collecte de données sans information préalable et recueil de consentement !
  - les résultats d'enquêtes et sondages diffusés sont toujours anonymes et non-identifiants !
- ✓ Si vous pensez être victime d'un piratage, procédez immédiatement au renouvellement des identifiants compromis et signalez l'incident aux personnes ou organisations concernées (votre établissement, banque, impôts, fournisseur d'accès à internet, etc.).

[4] https://www.cnil.fr/fr/retrouver-les-coordonnees-dun-organisme-pour-exercer-vos-droits