PANTHÉON SORBONNE
UNIVERSITÉ PARIS 1

FICHE PRATIQUE RGPD
Sécurité des données

Table des matières

Dans les fiches précédentes, nous avons souvent évoqué l'importance de mettre en place des « mesures techniques et organisationnelles appropriées » pour protéger les données traitées.

Sécuriser les données de la recherche : une obligation ?

La sécurité des données de recherche est une **exigence** incontournable du RGPD, et elle est spécifiquement encadrée par l'article 32, qui énumère plusieurs mesures techniques et organisationnelles pour protéger les données. Bien que cette liste ne soit pas exhaustive, elle souligne que les mesures doivent être **adaptées en fonction des caractéristiques du traitement** : type de données sensibles, risques particuliers, présence de personnes vulnérables, etc.

En plus de cet article général, le RGPD renforce cette obligation pour les acteurs de la recherche à travers l'article 89-1, rappelant que le chercheur doit garantir la sécurité des données par des mesures techniques et organisationnelles appropriées. Cette obligation est même une condition essentielle pour bénéficier des libertés spécifiques prévues pour la recherche, comme le traitement de données sensibles ou l'allongement des durées de conservation.
En somme, vous ne pouvez pas faire l'impasse sur cette étape : assurer la sécurité des données est un élément central de votre conformité !

Dernière modification : 16-10-2025
Rebecca Rousseau, adjointe DPO-RSSI Université Paris 1 Panthéon-Sorbonne

Que signifie « sécuriser les données » ? Contre quels risques se prémunir ?

La mise en place de mesures de sécurité vise à protéger contre trois principaux risques liés à l'utilisation et au traitement des données personnelles :
- Risque de **perte de disponibilité des données** : cela concerne l'incapacité à accéder ou récupérer des données, les rendant ainsi inaccessibles.
- Risque de **perte d'intégrité des données** : cela implique la protection contre toute modification non autorisée des données personnelles.
- Risque de **perte de confidentialité des données** : il s'agit de prévenir tout partage ou accès non autorisé aux données personnelles.

Il n'existe pas de référentiel clé en main rassemblant toutes les exigences de sécurité que vous devez suivre car les bonnes pratiques et mesures de sécurité techniques mises en œuvre doivent se faire en fonction de chaque projet. Ces mesures doivent être **proportionnées en fonction de la sensibilité des données traitées** : plus les données sont sensibles, plus la sécurité et la confidentialité doit être importante. Il ne s'agit pas d'appliquer toutes les mesures listées à chaque actif, mais de sélectionner celles qui sont les plus pertinentes pour votre projet de recherche.

La suite de ce document va présenter les deux grandes catégories de mesures de sécurité à mettre en œuvre dans le cadre d'un projet de recherche pour prévenir ces risques : les mesures « **techniques** » et les mesures « **logiques** » ou organisationnelles. Ces deux types de mesures sont complémentaires et doivent être soigneusement réfléchis et combinés.

Quelles mesures de sécurité technique mettre en œuvre ?

Les mesures techniques désignent tous les **dispositifs et solutions informatiques** déployés pour protéger les données personnelles. Cela implique de recenser et d'identifier tous les supports numériques sur lesquels les données personnelles circulent car ces actifs numériques représentent des points de vulnérabilité potentielle, chacun nécessitant des mesures spécifiques pour renforcer leur sécurité.
Cette liste n'est pas exhaustive et devra être complétée et ajustée selon les spécificités de votre projet (par exemple, vous pourriez déjà appliquer des mesures plus strictes ou différentes).
Enfin, notez que certaines mesures de sécurité peuvent être déployées de manière polyvalente : ce qui est efficace pour un actif pourrait l'être également pour d'autres types d'actifs.

Bien entendu, il est évident que si le projet de recherche implique plusieurs membres, ces mesures de sécurité doivent s'appliquer à chacun d'eux qui traite ou est amené à traiter des données personnelles.

Selon le guide de la CNIL sur la recherche scientifique (hors santé) [1], les mesures de sécurité technique à mettre en œuvre peuvent être regroupées en quatre catégories : gérer les accès aux données (1), sécuriser les équipements (2), conserver les données (3) et superviser la diffusion des données (4). La plupart des recommandations qui suivent en sont directement inspirées.

Pour plus de facilité, la grille complète des mesures de sécurité techniques à déclarer est disponible en annexe de ce document : ANNEXE 3.

[1] https://www.cnil.fr/fr/recherche-scientifique-hors-sante/mesures-de-securite-et-de-confidentialite

Veuillez lire attentivement chaque point et cocher uniquement les cases correspondant aux mesures déjà appliquées ou que vous vous engagez à mettre en œuvre. N'hésitez pas à ajouter des commentaires pour préciser vos pratiques ou proposer des mesures supplémentaires non listées.
Attention : toute mesure cochée doit pouvoir être justifiée et prouvée en cas d'audit.

1) Gérer les accès aux données

Authentifier les utilisateurs : Il est essentiel de s'assurer que **seuls les utilisateurs autorisés puissent accéder aux données personnelles dont ils ont besoin**.

✅ Bonnes pratiques en matière d'authentification

- Chaque utilisateur doit être doté d'un couple identifiant/mot de passe qui lui est propre. Il est en particulier recommandé de ne pas utiliser de comptes partagés entre plusieurs utilisateurs.
- En fonction de la sensibilité des données conservées, la CNIL estime qu'un mécanisme d'authentification multifacteur, comprenant au moins deux facteurs différents d'authentification, doit être mis en œuvre.

🔍 FOCUS : Gestion sécurisée des mots de passe

- Ne partagez jamais vos mots de passe et veillez à les garder strictement confidentiels.
- Stockez-les de manière sécurisée, en utilisant un gestionnaire de mots de passe ou un fichier chiffré, plutôt que sur un support papier ou dans un endroit facilement accessible. De même, évitez de vous les envoyer par e-mail.
- Protégez l'accès à vos mots de passe enregistrés en activant un mot de passe maître si vous les conservez dans votre navigateur.
- Personnalisez immédiatement les mots de passe par défaut dès la première utilisation.
- Créez des mots de passe uniques et robustes, sans lien direct avec vous (évitez noms, dates de naissance, etc.).
- Ne réutilisez jamais un même mot de passe sur plusieurs services, notamment en évitant d'utiliser vos identifiants institutionnels sur des sites personnels.

💡 Mieux vaut un seul mot de passe solide que des changements trop fréquents, qui peuvent être contre-productifs. Modifiez votre mot de passe uniquement en cas de suspicion de compromission.

Gérer les habilitations : Définir des profils d'habilitation permet de restreindre l'accès des utilisateurs **aux seules données strictement nécessaires en fonction des tâches et domaines de responsabilité de chacun**, afin que seuls ceux qui en ont besoin puissent y accéder.

✅ Bonnes pratiques en matière d'habilitation

- Créer et utiliser des comptes individuels pour chaque utilisateur afin de garantir un suivi sécurisé.
- Accorder à chaque utilisateur uniquement les privilèges nécessaires à l'accomplissement de ses tâches, en respectant le principe du moindre privilège.

- Supprimer les comptes des utilisateurs ayant quitté le projet ou changé de mission dès que possible pour maintenir la sécurité et éviter tout accès non autorisé.
- Utiliser un compte avec des privilèges limités pour les tâches quotidiennes et n'élever les privilèges d'administrateur que lorsque cela est strictement nécessaire pour éviter tout risque de mauvaise manipulation ou de sécurité.

Tracer les accès aux données : Selon la nature des recherches, le nombre d'accès et la sensibilité des données, il peut être utile de mettre en place un **système de traçabilité des accès** (grâce à la mise en place précédente d'un mot de passe et identifiant personnel permettant de contrôler les accès) et des **procédures pour gérer les incidents**, notamment en cas de violation de données. Cela permet de réagir rapidement et d'identifier l'origine de l'incident (accès frauduleux, abusif, etc.). Le système de journalisation peut comporter l'enregistrement des activités des utilisateurs comme : identifiant, horaires de connexion et déconnexion, actions effectuées etc. pour suivre l'accès aux données.

2) Sécuriser les équipements

Les risques d'intrusion dans les systèmes informatiques sont importants et **les postes de travail en constituent un des principaux points d'entrée**. Il est donc indispensable de prévenir les accès frauduleux, l'exécution de virus, la prise de contrôle à distance ou le vol d'un équipement.

Protéger son poste de travail : Idéalement, ces équipements sont fournis et administrés par les services informatiques des organismes employant les personnels de recherche, afin que ces derniers puissent se charger pour vous des bonnes pratiques ci-dessous. Si l'utilisation d'un équipement personnel est nécessaire, il est crucial de mettre en place les mesures de sécurité appropriées :

✅ Bonnes pratiques en matière de poste de travail

- Authentifier les utilisateurs à l'ouverture de session (cf. partie précédente).
- Mettre à jour régulièrement le système d'exploitation et les logiciels de mon matériel pour corriger les failles de sécurité et prévenir les risques de piratage. Si besoin, activer les mises à jour automatiques.
- Être équipés d'un antivirus régulièrement mis à jour.
- Disposer de pare-feu (firewall).
- Bénéficier d'un disque dur chiffré en cas de perte ou de vol de matériel.

🔍 FOCUS : séparer usage professionnel et personnel

- Je réserve le matériel institutionnel à un usage strictement professionnel et évite d'y stocker ou télécharger des fichiers personnels (photos, vidéos, etc.) pour limiter les risques d'infection.
- Je ne me connecte pas à mes comptes personnels (réseaux sociaux, messagerie privée) sur le matériel de l'institution afin d'éviter les risques de phishing et de confusion entre données personnelles et professionnelles.
- Je ne partage pas mon matériel institutionnel avec des proches pour prévenir toute consultation accidentelle de données sensibles, installation de logiciels non sécurisés ou contamination par des malwares.

Sécuriser l'informatique mobile / nomade : La mobilité est souvent une nécessité, vous conduisant à travailler depuis des lieux variés, tels que votre domicile, des espaces de coworking, des laboratoires ou même en déplacement. Les voyages, parfois fréquents, notamment à l'étranger, accentuent cette dynamique. Cependant, ce mode de travail présente des vulnérabilités accrues pour la sécurité de vos équipements : **près de 40 % des vols ou pertes de matériel professionnel surviennent lors de déplacements**, exposant ainsi les données à des risques considérables. Ainsi, si vos activités impliquent des déplacements fréquents pour vous ou vos équipes, il est essentiel d'accorder une attention particulière à la sécurité des appareils et terminaux mobiles.
Par exemple, en janvier 2025, la CNIL polonaise a infligé une amende de 5 700 € suite à la perte d'un sac contenant un ordinateur et des données personnelles dans le métro, ayant entraîné une violation de données.

✅ Bonnes pratiques en matière de sécurité de l'informatique mobile

- Authentifier les utilisateurs à l'ouverture de session (cf. partie précédente).
- Mettre en œuvre des mécanismes de sauvegardes ou de synchronisation.
- Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes etc).
- Lors de vos déplacements, privilégiez l'utilisation de connexions à des réseaux sécurisés et fiables, de préférence ceux que vous connaissez. À défaut, optez pour le partage de connexion via votre mobile. Évitez absolument les réseaux Wi-Fi publics, qui présentent des risques majeurs pour la sécurité de vos données.
- Pour préserver la confidentialité de vos travaux, évitez de travailler dans des lieux publics ou dans les transports. En cas d'impossibilité, utilisez des filtres de confidentialité sur vos écrans afin de vous protéger des regards indiscrets.

🔍 FOCUS : protéger ses données en cas de départ à l'étranger

Outre les mesures listées ci-dessus, lors de déplacements à l'étranger, il est parfois nécessaire de prendre des mesures de sécurité spécifiques pour protéger vos équipements et vos données, car les risques d'espionnage industriel ou de confiscation de matériel par les autorités locales sont bien réels :
- Voyager léger en données : Emportez uniquement les informations strictement nécessaires à votre mission. Limitez les données personnelles ou sensibles autant que possible. Rappelez-vous que dans les pays hors UE, le RGPD ne s'applique pas, et vos données seront soumises à la législation locale.
- Appareils sécurisés : Préférez un smartphone "propre", dépourvu de données sensibles, spécifiquement réservé à ce type de déplacement. Utilisez un ordinateur avec un disque dur vierge, contenant uniquement les fichiers requis pour votre mission. Si possible, empruntez un appareil dédié pour les voyages à l'étranger.
- Utilisation d'un VPN : Dans les pays à risque en matière de vie privée, téléchargez et utilisez un VPN avant de partir pour protéger vos connexions et contourner une éventuelle censure ou surveillance.
- Authentification renforcée : Activez la double authentification sur tous vos comptes avant votre départ et conservez vos codes de secours dans un endroit hors ligne.

- Mots de passe temporaires : Modifiez vos mots de passe avant votre départ et changez-les de nouveau à votre retour. Cette précaution est essentielle, car certaines autorités locales pourraient vous demander l'accès à vos appareils pour inspection.
- Désactivation de la biométrie : Désactivez les fonctionnalités de reconnaissance faciale et d'empreintes digitales sur vos appareils afin de limiter les risques de contournement ou d'abus en cas de confiscation.

3) Conserver les données

Organiser les modalités de conservation : Toute utilisation de données personnelles dans un cadre de recherche suppose d'avoir **anticipé** les modalités d'utilisation qui en seront faites.

✅ Bonnes pratiques en matière de conservation

- Définissez des durées de conservation adaptées aux objectifs poursuivis (cf. fiche 10) et mettez en place des alertes, archivages ou purges automatisées.
- Effectuez des sauvegardes régulières des données papier et électroniques, et testez leur fiabilité (cf. fiche 9) pour éviter toute perte ou altération.
- Utilisez des supports de stockage sécurisés en évitant les services de cloud grand public hébergés hors UE, ainsi que les clés USB et disques durs externes non protégés. Privilégiez le chiffrement[2] pour assurer la confidentialité des données sensibles (cf. fiche 9).

Garantir la confidentialité : Que les données utilisées pour la réalisation des travaux de recherche soient au format papier (carnets d'enquêtes, notes d'entretiens, questionnaires, etc.) ou numérique, il est nécessaire de s'assurer que seules les personnes autorisées sont en mesure d'y accéder. Si des tiers parviennent à y accéder (même uniquement en consultation), **cela constituerait une violation de données dont vous seriez responsable, ce qui pourrait entraîner des sanctions**.

✅ Bonnes pratiques en matière de confidentialité

Au niveau informatique :
- En fonction de la sensibilité des données, mise en place d'un chiffrement conformément aux recommandations de l'ANSSI [3], pour garantir la sécurité des données (méthodes de chiffrement et des clés de taille appropriée, conservation des clés de chiffrement…).
- Prévoir une procédure de verrouillage automatique de session et verrouiller son ordinateur dès que l'on quitte son poste de travail en utilisant les raccourcis clavier Windows+L ou Crtl+Commande+Q.

Au niveau physique : Il est essentiel de garantir la sécurité des accès aux locaux où sont stockées les données utilisées dans le cadre de la recherche (bureaux, salles serveurs, etc.). Cela inclut :

- La mise en place de mesures telles que l'accompagnement des visiteurs, l'utilisation de badges d'accès et/ou l'installation de portes verrouillées.
- Ranger et sécuriser les documents contenant des données personnelles utilisées pour les travaux de recherche, en évitant de les laisser sans surveillance sur un bureau ou dans un véhicule. Les données scientifiques sous format papier doivent normalement être conservées

[2] https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires
[3] https://cyber.gouv.fr/publications/mecanismes-cryptographiques

dans des espaces et équipements sécurisés, tels qu'une armoire ou un coffre-fort fermé. Seules les personnes habilitées doivent avoir l'accès à ces espaces, via une clé, un code ou un badge, afin de préserver la confidentialité et l'intégrité des informations.

4) Superviser la diffusion des données

Sécuriser les échanges : La réalisation de travaux de recherche en partenariat peut nécessiter la réalisation d'échanges de données entre différentes équipes. Comme expliqué précédemment, **une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités et à porter ainsi atteinte au droit à la vie privée des personnes**.

✅ Bonnes pratiques en matière de sécurisation des échanges

- Chiffrez les fichiers sensibles avant toute transmission numérique. Il en va de même pour les supports physiques (clés USB, disques durs portables, etc.), qui doivent être chiffrés avant d'être remis en main propre, confiés à un coursier ou par voie postale.
- Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).
- Certains organismes employant les personnels de recherche peuvent également proposer la mise à disposition de plateformes sécurisées spécialement dédiées aux échanges de données. Il est recommandé dans ce cas de recourir autant que possible à ces ressources.

📌 Exemples de sécurisation des échanges

L'Université Paris 1 vous propose, via votre espace ENT [4], le service « FILEX » pour l'envoi sécurisé de fichiers volumineux. Ce service offre la possibilité de définir un mot de passe ou d'exiger une authentification pour garantir la sécurité des transferts.
Si vous êtes à l'aise avec GitHub, vous pouvez également explorer « Eurydice », une solution open source développée par l'ANSSI, qui permet de transférer des informations de manière sécurisée entre deux réseaux de niveaux de sécurité différents [5]. Ou encore plus simplement le nouveau service étatique France transfert.

Canaux de transmission : Il est également nécessaire de veiller à la sécurité des données lors des **échanges en dehors des espaces de travail collaboratif** :

✅ Bonnes pratiques en matière de transmission des données

- Utilisez le chiffrement de vos données sensibles AVANT l'envoi ou vérifiez si l'application que vous utilisez propose cette fonctionnalité. Cela permet de garantir que les informations restent confidentielles pendant leur transmission.
- Si cela n'est pas possible, assurez-vous a minima que l'accès aux documents est protégé par un mot de passe, afin de limiter leur consultation uniquement aux personnes autorisées.
- Envisagez d'ajouter des filtres ou des filigranes sur vos documents, comme avec des outils tels que Filigrane Facile [6] afin d'éviter le vol ou la réutilisation des données.

[4] https://filex-ng.univ-paris1.fr/
[5] https://github.com/ANSSI-FR/eurydice/blob/master/README.md
[6] https://filigrane.beta.gouv.fr/

- Bannissez la transmission de fichiers contenant des données personnelles en clair via des messageries « grand public » non sécurisées.
- Rappel : privilégiez l'utilisation de connexions à des réseaux sécurisés et fiables, de préférence ceux que vous connaissez. À défaut, optez pour le partage de connexion via votre mobile. Évitez absolument les réseaux Wi-Fi publics, qui présentent des risques majeurs pour la sécurité de vos données.

Encadrer le partage et/ou la publication : La diffusion de jeu de données ayant permis la réalisation de travaux de recherche est de plus en plus demandée aux personnels de recherche (revue par les pairs, publication de résultats dans une revue scientifique…). **Ces prérogatives de science ouverte doivent cependant s'accorder avec les impératifs de protection des données**.

✅ Bonnes pratiques en matière de partage et de publication

Anonymiser les données permet de les sortir du cadre de la protection des données personnelles, car les données anonymisées ne sont plus considérées comme personnelles. Cependant, cette opération implique souvent une perte significative d'informations, ce qui peut être problématique pour certains travaux de recherche. Si l'anonymisation n'est pas envisageable, la pseudonymisation constitue une alternative intéressante et moins contraignante. Elle permet de réduire les risques liés à l'identification tout en préservant l'intégrité des données. Contrairement à l'anonymisation, la pseudonymisation peut être mise en place de manière plus simple et avec moins de pertes d'informations pour le chercheur, puisque les données restent associées à un identifiant codé qui peut être réutilisé dans le cadre des travaux scientifiques. De plus, la pseudonymisation doit être systématiquement appliquée avant toute publication (thèse, articles scientifiques, etc.) pour garantir le respect des exigences de confidentialité et de protection des données personnelles.

🔍 FOCUS : Anonymisation VS Pseudonymisation

L'anonymisation et la pseudonymisation sont deux techniques de protection des données personnelles, mais elles ne garantissent pas le même niveau de protection. L'anonymisation vise à rendre impossible toute réidentification d'une personne à partir des données traitées, même en croisant différentes sources d'information. En pratique, c'est un processus rare et complexe, car il est très difficile de garantir qu'aucune donnée résiduelle ne permettrait de remonter à une personne, notamment avec l'évolution des technologies et des capacités de corrélation des données.
À l'inverse, la pseudonymisation consiste à remplacer les éléments identifiants par un code ou un alias, tout en conservant une possibilité de réassociation avec l'identité réelle via une clé de correspondance. Une donnée est également considérée comme pseudonymisée lorsqu'il subsiste un risque de réidentification par recoupement avec d'autres informations (âge, parcours, réponses spécifiques à un questionnaire, etc.). Ainsi, si la pseudonymisation réduit les risques en limitant l'identification directe des personnes concernées, elle ne les rend pas anonymes pour autant.

Quelles sont les mesures de sécurité organisationnelles ?

Les mesures organisationnelles englobent **l'ensemble des politiques, procédures et méthodes établies** pour assurer une gestion appropriée des données personnelles. Elles ne remplacent en aucun cas les mesures techniques, mais viennent plutôt les compléter pour renforcer la protection des données.

Tout comme pour les mesures techniques, cette liste présente les principales mesures organisationnelles que vous pouvez mettre en place. Elle n'est cependant pas non plus exhaustive.

- **Analyse d'impact sur la protection des données** : Dans le cadre du traitement de données sensibles, une AIPD a-t-elle été planifiée conformément à l'article 35 du RGPD ? (cf. fiche pratique 14).

- **Formations** : Le chercheurs membres de l'équipe ont-ils été sensibilisés aux obligations et enjeux de la protection des données personnelles ? Si oui, qui a réalisé cette formation et à quelle date ? Ont-ils tous signé des engagements de confidentialité ?

- **Contrôle des sous-traitants** : Un encadrement des sous-traitants et prestataires manipulant des données personnelles a-t-il été prévu ? Cela inclut-il des contrats mentionnant la protection des données et des engagements de confidentialité ?

- **Politique de sécurité informatique** : Existe-t-il une politique de sécurité informatique au sein de votre laboratoire ou unité, et celle-ci est-elle appliquée ? Si oui, vous devez respecter et vous appuyer sur les textes et mesures internes de votre établissement.

- **Procédures de gestion des données** : Y a-t-il des procédures pour détecter, signaler et répondre aux violations de données ? Des vérifications régulières sont-elles effectuées pour garantir le respect et l'efficacité des mesures de sécurité ?

- **Comité d'éthique** : Le comité d'éthique de l'université ou d'un autre organisme a-t-il été consulté ? Quelle a été sa réponse ?

Que dois-je indiquer dans la fiche du registre ?

Tout comme cette fiche, le registre inclut une section dédiée à la « **Sécurité des données (technique)** » suivie d'une section sur la « **Sécurité des données (organisationnelle)** ».

Dans la première section, vous pourrez remplir deux champs concernant la méthode d'authentification et le chiffrement des données. Si vous avez des doutes sur l'authentification, vous pouvez laisser ce champ vide, tandis que pour le chiffrement, vous aurez l'occasion de fournir des détails plus précis par la suite.

Je vous encourage à énumérer toutes les mesures de sécurité techniques que vous avez identifiées dans le champ « **Autres précisez** », ce qui vous permettra de développer votre travail.

Vous pouvez présenter ces mesures sous forme de liste à puces organisée par actif, comme indiqué dans cette fiche, ou selon une autre structure de votre choix.

De même, vous pourrez répertorier toutes les mesures organisationnelles mises en place dans le champ libre prévu à cet effet.

✅ Bonnes pratiques et recommandations d'hygiène numérique

L'application des mesures techniques et organisationnelles mentionnées ci-dessus doit être complétée par des bonnes pratiques essentielles, qui restent fondamentales pour garantir la sécurité.
- Restez vigilant(e) lors de votre navigation sur Internet en évitant les sites non sécurisés ou douteux. Privilégiez toujours les sites en HTTPS pour vous protéger contre les infections par des logiciels malveillants.
- Téléchargez uniquement des logiciels et applications depuis les sites officiels des constructeurs. Cela vous permet d'éviter les programmes modifiés ou corrompus, assurant ainsi une meilleure sécurité pour vos données.
- Ne cliquez jamais sur des liens suspects ou malveillants envoyés par email. Une seule erreur peut entraîner une attaque par phishing ou l'installation d'un logiciel malveillant. Prenez quelques secondes pour vérifier l'origine du message, l'expéditeur, et survolez les liens sans cliquer pour lire l'adresse complète avant de valider.
- Évitez d'insérer des clés USB qui ne vous appartiennent pas, que vous les ayez trouvées, empruntées ou reçues en cadeau. Ces supports peuvent contenir des virus et des malwares susceptibles de compromettre la sécurité de votre ordinateur.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Sécurité des données (technique)** incluant les champs **Authentification**, **Données chiffrées** et **précisions**.
- **Sécurité des données (organisationnelle)**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr