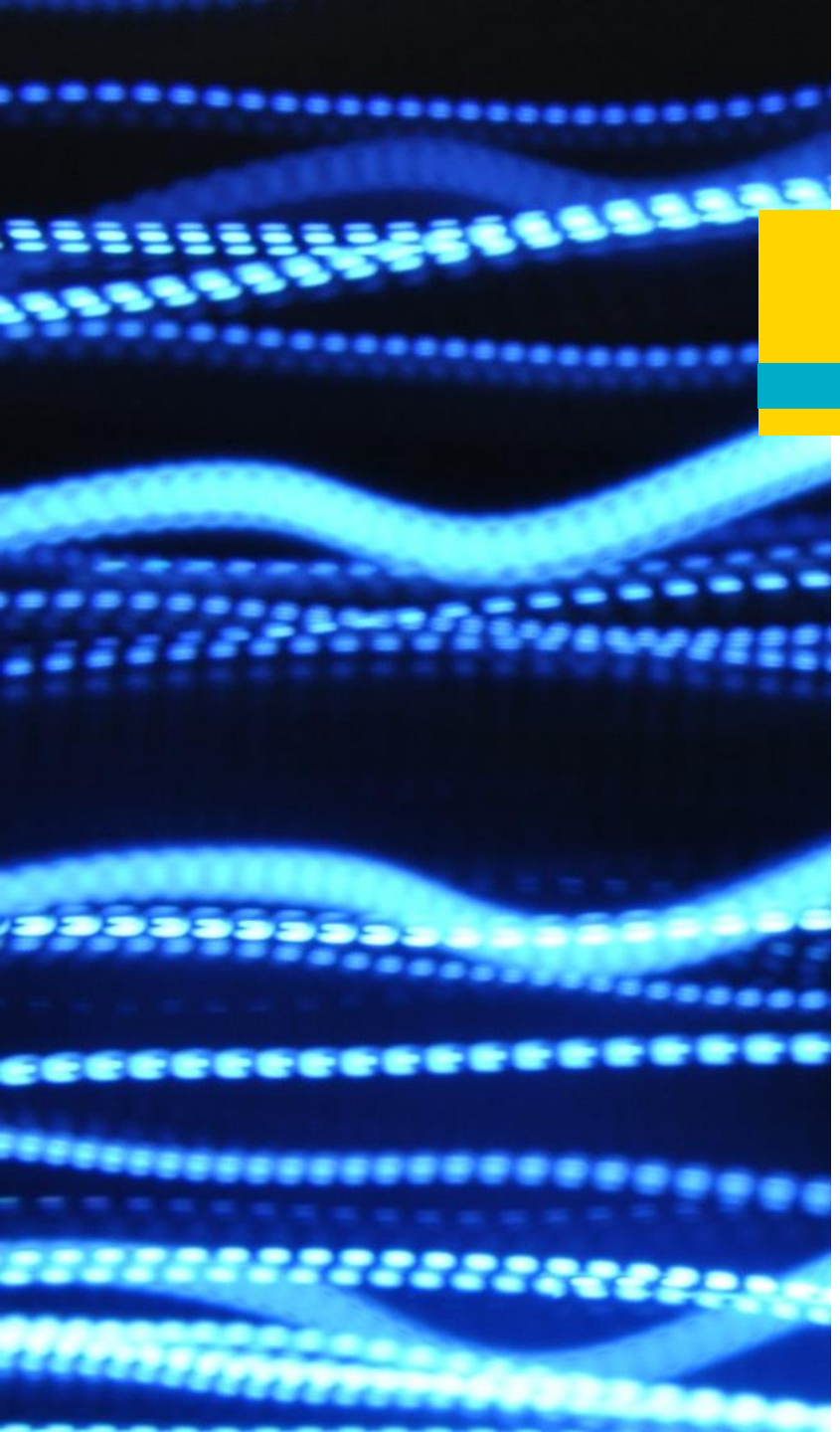


MOOC RGPD

OTOS 13 Formation

Fondamentaux

Le RGPD en bref

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. **Il est entré en application le 25 mai 2018.**

- Le RGPD établit des règles sur la collecte et l'utilisation des données sur le territoire français selon 3 objectifs :
  - renforcer les droits des personnes
  - responsabiliser les acteurs traitant des données
  - crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

- Ce règlement est destiné à tout citoyen européen qui voit ses droits renforcés
- Chaque traitement est réputé conforme par défaut, les contrôles sont effectués à posteriori
- Le Délégué à la Protection des Données – DPO – est la personne chargée de la protection des données au sein d'une organisation

Source : www.economie.gouv.fr

Histoire

Le **RGPD** s'inscrit dans la continuité de la Loi française **Informatique et Libertés** de 1978
Avant le RGPD — dont le nom plus solennel est le **règlement du Parlement européen et du Conseil** du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données — existait une directive sur la protection des données personnelles qui date de 1995. Ce texte est abrogé par le RGPD.

Enjeux du RGPD

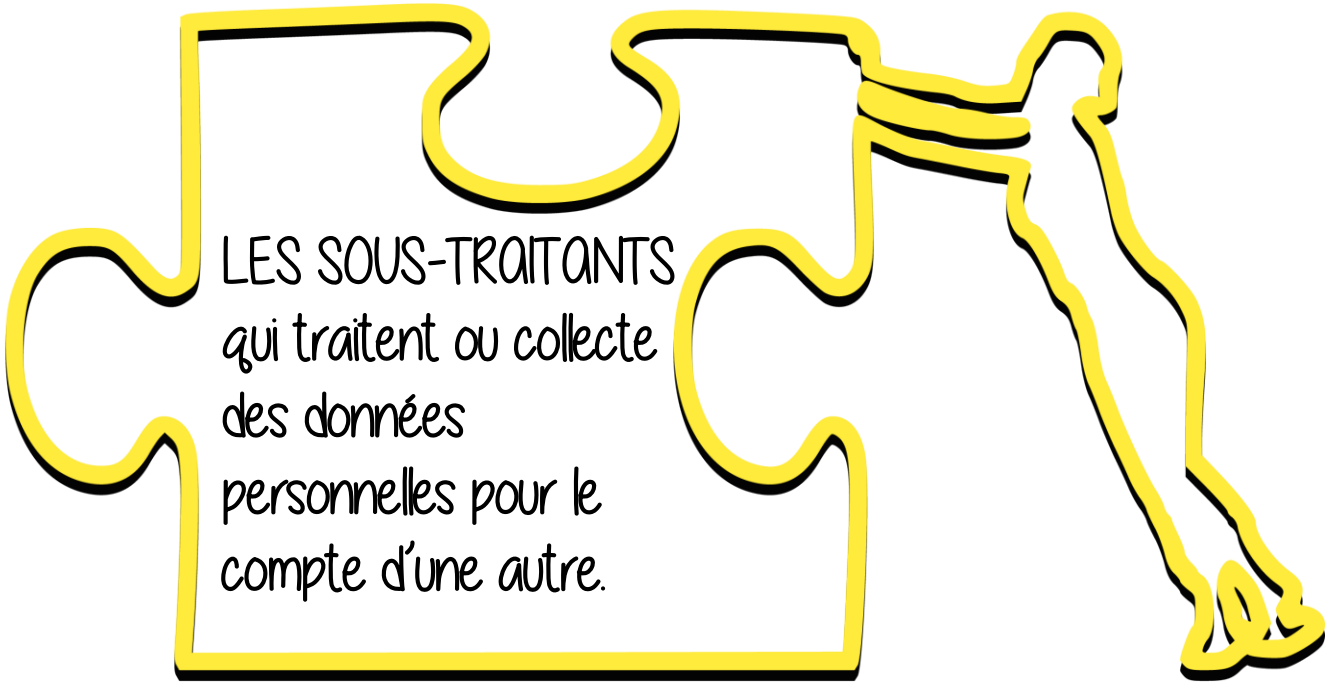
1. Créer la confiance : la confiance est le fer de lance de l'humanité. Sans confiance il n'y a pas de collaboration. C'est un point majeur.

2. Sécuriser les données. Tout responsable de traitement des données doit sécuriser ses données. Cela implique d'abaisser le seuil des déclarations à faire auprès des organismes de régulation : la CNIL en France.

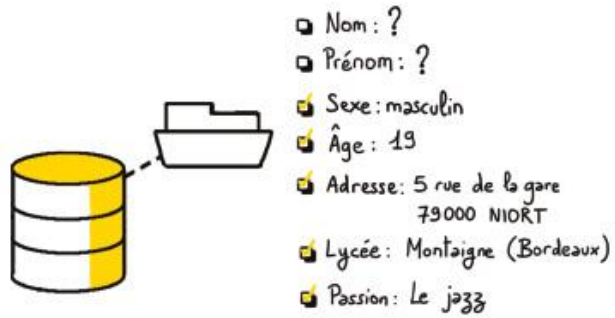
3. Responsabiliser les acteurs et les sous-traitants.

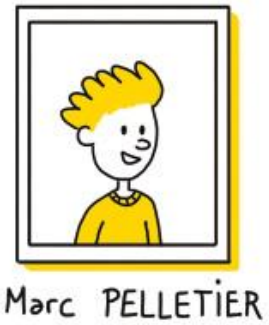
Sources www.numerama.com - www.village-justice.com

Êtes-vous concerné par le RGPD ?



Organismes de l'Union Européenne ou implanté hors de l'UE dont l'activité cible directement des résidents européens.





Données personnelles

La **donnée personnelle** décrite par la CNIL : « toute information se rapportant à une personne physique identifiée ou identifiable ».
2 types d'identifications :

- identification directe (nom, prénom...)
- identification indirecte (identifiant, numéro…)

Les données de santé = données sensibles (au sens RGPD), sont couvertes par le secret médical. Le RGPD les protège.

Une opération ou un ensemble d'opérations portant sur des données personnelles est un **traitement de données personnelles**.

Exemple de traitement des données :

- tenue d'un fichier clients
- collecte de coordonnées de prospects via un questionnaire
- mise à jour d'un fichier fournisseurs

Vos outils de gestion de la conformité

Le RGPD offre une boîte à outils pour gérer votre conformité et montrer que vous respectez la règlementation

- **Le registre des activités de traitement** recense vos traitements de données et indique leur usage.
- **Les exemples de mentions d'information** vous aident à informer les personnes en conformité au RGPD.
- **Les cadres de référence** guident les organismes dans la mise en conformité de leur traitement.
- **L'analyse d'impact relative à la protection des données (AIPD)** : Méthode et catalogues de bonnes pratiques, un logiciel open source réalise cette analyse.
- **Le transfert de données hors UE et les BCR** - Transfert de données hors de Union européenne possible mais un niveau de protection des données suffisant/approprié. Encadrés avec outils juridiques.
- **La certification et les codes de conduite**, sceaux de confiance, initiés par la CNIL ou un secteur professionnel.
- **Les normes et les dispenses** sont des cadres de référence adoptés par la CNIL.
- Les responsables de traitement s'y conformant ont une dispense de déclaration ou des formalités allégées.

Les17 fiches didactiques de la CNIL

Cet outil traite des précautions à prendre lorsque vous traitez des données personnelles et des bases de la sécurité informatique

1. Sensibiliser les utilisateurs
2. Authentifier les utilisateurs
3. Gérer les habilitations
4. Tracer les accès et gérer les incidents
5. Sécuriser les postes de travail
6. Sécuriser l'informatique mobile
7. Protéger le réseau informatique interne
8. Sécuriser les serveurs
9. Sécuriser les sites web
10. Sauvegarder et prévoir la continuité d'activité
11. Archiver de manière sécurisée
12. Encadrer maintenance et destruction des données
13. Gérer la sous-traitance
14. Sécuriser les échanges entre organismes
15. Protéger les locaux
16. Encadrer les développements informatiques
17. Chiffrer, garantir l'intégrité ou signer

CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

> Sécurité : Authentifier les utilisateurs

Sécurité : Authentifier les utilisateurs

CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

> Sécurité : Sensibiliser les utilisateurs

Sécurité : Sensibiliser les utilisateurs

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.

Les précautions élémentaires

Sensibiliser les utilisateurs travaillant avec des données à caractère personnel aux risques liés aux libertés et à la vie privée, les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement. Organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique, etc.

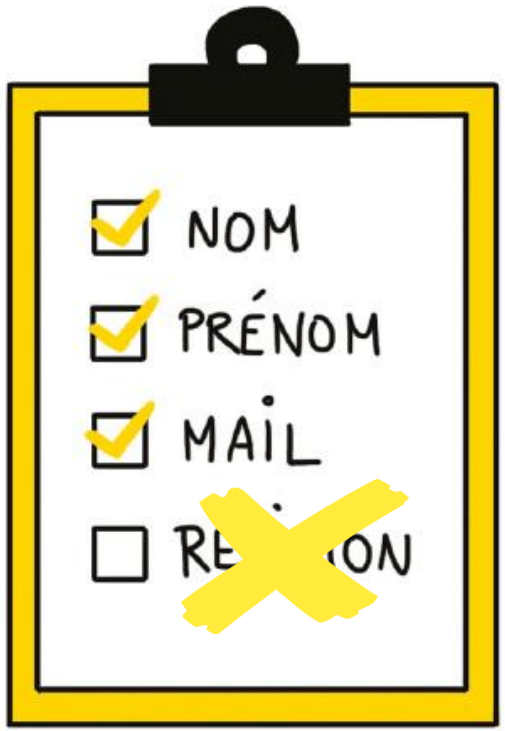
Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données à caractère personnel, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.

Rédiger une charte informatique et lui donner une force contraignante (ex. annexion au règlement intérieur).

Cette charte devrait au moins comporter les éléments suivants :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non respect de celles-ci.
2. Le champ d'application de la charte, qui inclut notamment :
   - les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
   - les moyens d'authentification utilisés par l'organisme ;
   - les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
   - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
   - ne jamais confier son identifiant/mot de passe à un tiers ;
   - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
     - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
     - ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;
     - respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supé- rieur hiérarchique et en respectant les règles de sécurité.
3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :

Principe de proportionnalité



Je m'assure que les données collectées servent bien l'objectif prévu

3ème principe posé par l'article 6 : les données sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ». Seules les données à caractères personnel qui sont indispensables à l'opération envisagée ne peuvent faire l'objet d'un traitement sinon le traitement est illicite.

A partir de quand peut-on considérer que le traitement d'une donnée à caractère personnel est indispensable ? 2 considérations :

- La finalité du traitement
- La nature des données collectées

La CNIL a refusé en 2000 un projet de contrôle d'accès biométrique à l'Académie de Lille (empreintes digitales). L'objectif était un accès rapide et sécurisé aux bâtiments par les employés. La Commission refusé du fait que la finalité, qui était d'assurer la fluidité de l'entrée du personnel, « ne paraissait pas justifier dans sa généralité, la constitution d'une base de données d'empreintes digitales de l'ensemble du personnel ».

Oubli – Personnes fichées Données interdites

Le droit à l'oubli

- Le terme strict « droit à l'oubli numérique » - ou « droit à l'oubli en ligne » - ne figure aujourd'hui dans aucun texte officiel, il est pratiqué par la Cour de Justice de l'Union Européenne (CJUE). « L'exploitant d'un moteur de recherche est considéré comme un responsable du traitement de données à caractère personnel et, en tant que tel, est tenu de supprimer les données traitées relatives à une personne physique sur simple demande de cette dernière. »

- Un européen peut exiger suppression partielle/complète de résultats de recherche nominatifs.

- Depuis mai 2014, Google met à disposition un formulaire de «droit à l'oubli» («de demande de suppression») pour effacer du contenu en ligne (Google, Bing, Yahoo!)

Les personnes fichées - Les personnes concernées gardent la maîtrise des informations les concernant. Le responsable de fichier explique la procédure et a un mois pour leur répondre.

Sont interdits - article 9 RGPD : traitement des données sur l'origine raciale/ethnique, opinions politiques, convictions religieuses/philosophiques ou appartenance syndicale, traitement des données génétiques, biométriques d'identification d'une personne, de santé, sur la vie/orientation sexuelle d'une personne physique. Exceptions (consentement de la personne, données publiées par la personne, légitimité juridique, intérêts vitaux, associations/fondations, intérêt public …) sous réserve d'appliquer la limitation nécessaire.
Sources : www.droit-oubli-numerique.org et www.cnil.fr/fr/respecter-les-droits-des-personnes

Régulation

au niveau français, européen et international

CNIL et CEPD

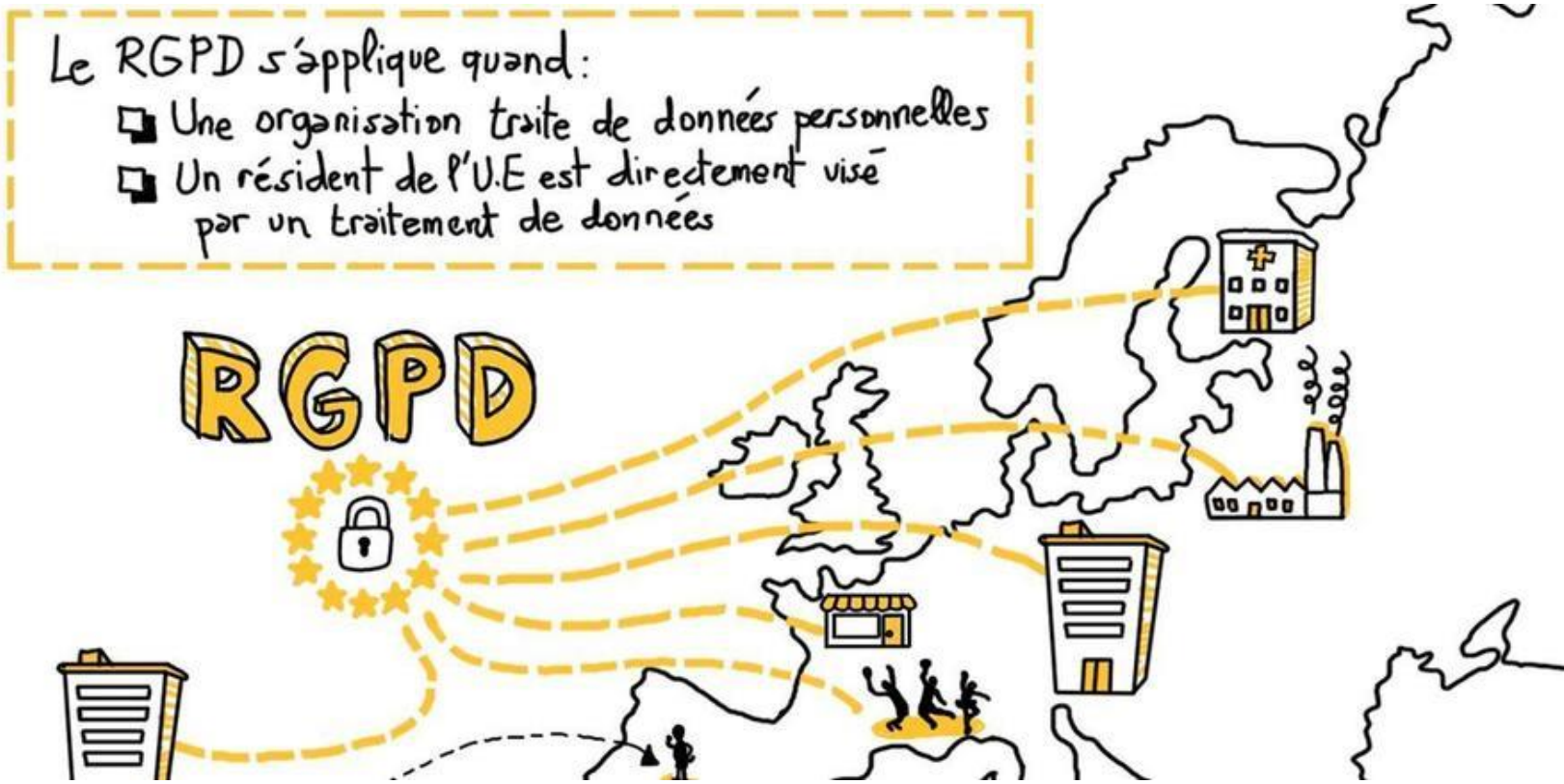
Depuis juin 2019, la loi du 6/01/1978 « **Informatique et Libertés** », est en vigueur dans une nouvelle rédaction. Le RGPD y autorise des « marges de manœuvre nationales » et elle transpose en droit français la Directive « police-justice ».

La **CNIL** contrôle les organismes qui traitent des données à caractère personnel (Entreprises privées, associations, organismes publics)

Le « **Comité Européen de la Protection des Données** » - CEPD, institué par le Règlement européen sur la protection des données, a pris suite au groupe de l'article 29 (le G29).

La CNIL, rapporteur au niveau européen, coordonne des experts au sein du CEPD. Depuis **mai 2018**, le CEPD développe **une nouvelle doctrine européenne** de la protection des données avec les autorités nationales.

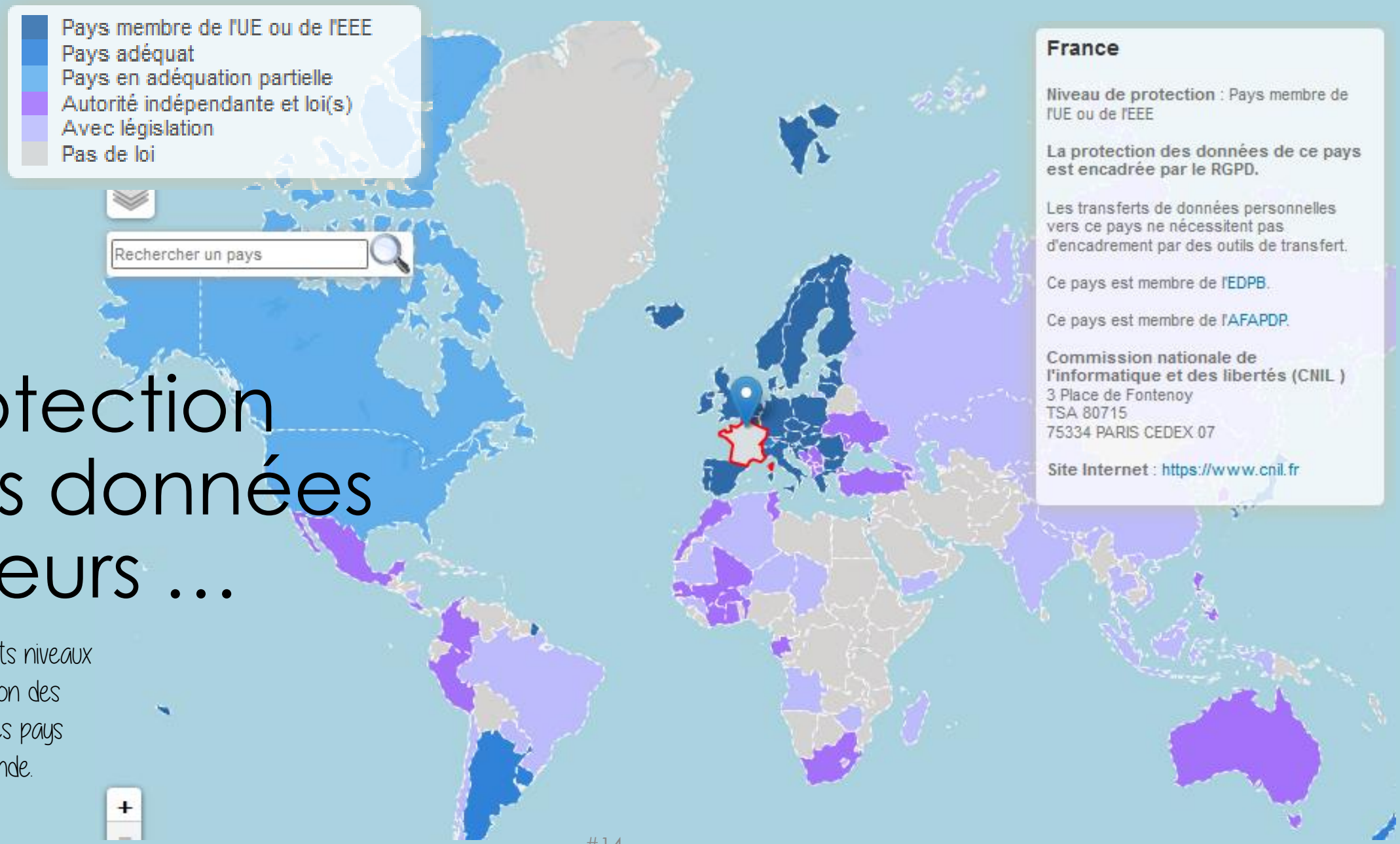
En Europe



Le **guichet unique** est une nouvelle procédure mise en place par le Règlement général sur la protection des données (RGPD). Il harmonise en Europe les décisions des autorités de protection des données sur les traitements transfrontaliers. Ces autorités doivent désormais se coordonner.

Protection des données ailleurs …

les différents niveaux de protection des données des pays dans le monde.



Sécurité et confidentialité

des données

Confidentialité, failles de sécurité et politique de sécurité

Confidentialité des données personnelles - « s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé » (ISO). Contrôles physiques et numériques. La **sécurité** est un risque minimal pour la donnée (risque et importance). RGPD les relie dans la sécurité : **la sécurité est seule garante de la confidentialité des données.**

Comment protéger pour assurer confidentialité, intégrité et sécurité : pseudonymisation des données (anonymisation) ; chiffrement (les données ne peuvent être lues) ; rétablir les données lors d'incident physique ou technique, procédure de test d'efficacité des mesures mises en place.

Les sous-traitants sous l'autorité d'un responsable de traitement ne traitent les données que sur ordre direct de celui-ci et garantit de bonnes conditions de sécurité par contrat, et ne peut faire sous-traiter sans autorisation.

Failles de sécurité - Violation de données personnelles accidentelle ou illicite : destruction, perte, altération, divulgation non autorisée ou accès non autorisé. Le **RGPD oblige à les notifier** à la CNIL sous 3 jours, sinon justifier le retard. Sans signalement : 5 ans de prison + 300 000 €. Si le risque est fort, informer l'utilisateur.

Mise en œuvre d'une politique de sécurité des systèmes d'information - PSSI

- Loi Informatique et Liberté : « mettre en place en interne des précautions » ; RGPD2 synthétise.
- RGPD mentionne le « Privacy by Design » : protéger les données dès la conception, lors du traitement.
- Politique générale sur le périmètre (acteurs, missions, risques, mise en œuvre, reporting et contrôle).
- Responsable traitements ou ingénieur en sécurité SI garantit la sécurité; DPD, non responsable, conseille.
- Procédures de sécurité physique (accès physique, dommage/intrusion dans les lieux des données), modalités de traitement : stockage, destruction, sécurités logicielles, sauvegardes et archivage.

Source : zestedesavoir.com

Privacy Impact Assessment - PIA

Le PIA est un **processus d'amélioration continue**. Il devrait être dès la conception d'un nouveau traitement de données à caractère personnel.

Comment ? Démarche de conformité mise en œuvre en menant un PIA sur 2 piliers :

- 1. Principes et droits fondamentaux, « non négociables », fixés par la loi et devant être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- 2. Gestion des risques sur la vie privée pour déterminer des mesures techniques et une organisation appropriées de protection des données.

Source : CNIL

Pour mener un PIA …

1. **Étude du contexte** : délimiter et décrire le contexte du(des) traitement(s) considéré(s) ;

2. **Étude des principes fondamentaux** (mesures garantissant le respect des principes fondamentaux) : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;

3. **Étude des risques liés à la sécurité des données** : apprécier les risques sur la vie privée et vérifier qu'ils sont convenablement traités ;

4. **Formaliser la validation du PIA** selon les éléments précédents ou bien décider de réviser les étapes précédentes.

Cloud computing, transferts de données personnelles hors UE

Ce qui change avec le RGPD - Les responsables de traitement et les sous-traitants peuvent transférer des données hors de l'UE et de l'EEE : assurer un niveau de protection des données suffisant, approprié et encadré juridiquement.

Le pays vers lequel je transfère offre-t-il un niveau de protection reconnu par l'UE ?

- **Vérifier le niveau de protection**
- **Privacy shield** – transfert vers les USA : les entreprises destinataires de données sont référencées et doivent respecter les obligations et les garanties de fond.
- **Clauses Contractuelles Types de la Commission Européenne** : modèles de contrats de transfert de la Commission européenne.
- **Binding Corporate Rules**. Code de conduite définissant la politique sur les transferts et offrant une protection adéquate.

Dérogations pour des situations particulières au principe d'encadrement général des transferts vers un État non membre de l'Union - article 49 RGPD. Situations particulières : liste des arrangements administratifs visant à encadrer le transfert de données personnelles entre 2 organismes.
Source CNIL

DPO

Le délégué à la protection des données

LE DPO

- Délégué à la Protection des Données - DPO : salarié ou externalisation
- Depuis le 27/4/2016, application 25/5/2018
- Personne physique ou morale
- Il informe, conseille, contrôle le respect du RGPD, dispense des conseils sur l'analyse d'impact de la protection des données
- Point de contact, il coopère avec l'autorité de contrôle
- Agit avec déontologie, éthique et indépendance
- Obligation dans le secteur social et médico-social

Traitement, audit, TPE et PME

Recensement des traitements par le DPO

Le registre des activités de traitement recense vos traitements de données personnelles et leur utilisation. Document de recensement et d'analyse, il reflète la réalité des traitements pour identifier :

- parties prenantes: représentant, sous-traitants, co-responsables…
- catégories de données traitées,
- utilisation des données, qui y accède, destinataires,
- temps de conservation, mode de sécurisation.

Source : CNIL

Mission d'audit « informatique et libertés »

- Un audit « Informatique et libertés » vérifie que les traitements de données à caractère personnel sont conformes à la loi n°78-17 du 6/01/1978 sur l'informatique, fichiers et libertés, modifiée par la loi n°2004-801 du 6/08/2004.
- Il concerne les traitements de données à caractère personnel mis en œuvre dans un périmètre délimité : lieux, unités organisationnelles, activités, processus ou période de temps couverte, types de traitements ou de traitements particuliers.

Source : www.legifrance.gouv.fr

Conséquences du RGPD pour les TPE-PME

- Elles sont toutes concernées par le RGPD.
- Elles collectent, stockent, utilisent des données personnelles ? Elles sont "responsables de traitements".
- Elles traitent des données personnelles pour d'autres entreprises ? Elles sont "sous-traitantes".

La CNIL a créé, avec la Banque publique d'investissement - BPIfrance, un guide spécial pour les TPE-PME

Protéger la vie privée

Prospection commerciale et projet de règlement e-privacy

Peu abordé par le RGPD, la directive ePrivacy – 2002 protège les personnes démarchées. Prospection électronique, transfert de données personnelles à des « partenaires commerciaux » prospectant également ou à des « courtiers de données », la Cnil a publié en 2018 :

- « La personne doit donner son consentement avant toute transmission à des partenaires » ;
- « La personne doit pouvoir identifier les partenaires, destinataires des données, sur le formulaire de collecte des données » ;
- « La personne doit être informée des évolutions de la liste des partenaires et notamment de l'arrivée de nouveaux partenaires» ;
- « Le consentement recueilli par la société collectant les données pour le compte de ses partenaires n'est valable que pour ces derniers » ;
- « Les partenaires sollicitant à leur tour les personnes indiquent, lors de leur première communication, la manière d'exercer leurs droits, en particulier d'opposition, et la source des données ».

Fraude et e-commerce

Les fraudes en ligne

- **Vol d'identité**
- **Fraude amicale** : rejet de commande, déclaration vol des infos bancaires. Le commerçant rembourse, le voleur garde l'achat.
- **Fraude propre** : achat avec carte de crédit volée, puis manipulations pour éviter les détections des processeurs de paiement.
- **Fraude d'affiliation** : pour augmenter ses ventes, augmenter le trafic soit de façon automatisée, soit réellement avec de fausses transactions.
- **Triangulation Fraude** : Fausse boutique en ligne à bas prix pour obtenir des infos de carte de crédit/adresse. Achat des produits en ligne avec les cartes volées, expédition au client d'origine de la fausse vitrine. Utilisation frauduleuse des cartes volées.
- **Fraude marchande** : Vol simple, achat en ligne sans expédition.

Amazon et Alibaba sont sensibles. Les ventes mobiles font + l'objet d'une fraude. Le commerce électronique n'est jamais à l'abri.

Loi anti-fraude janv. 2018 : réduire la fraude e-commerce à la TVA (mise à jour système de caisse : gestion stocks, comptabilité).

Droit de la consommation et e-commerce - Informer

Article L.221-5 du Code de la consommation : lors de contrat de vente à distance, informer sur :

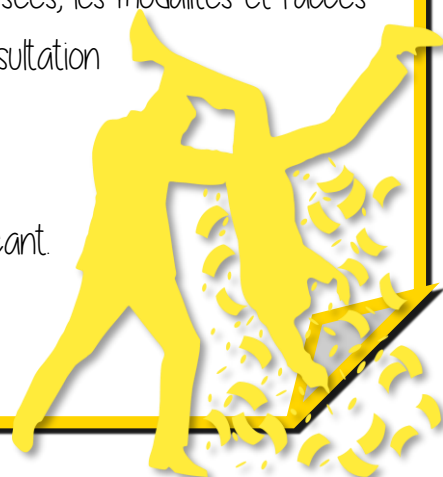
▶ conditions, délais et modalités du droit de rétractation ainsi que formulaire type de rétractation ;

▶ frais de renvoi du bien si rétractation ou si contrat de service commencé avant fin du délai de rétractation ;

▶ informer si le consommateur ne bénéficie pas d'un droit de rétractation ou si il le perd ;

▶ coordonnées du professionnel.

Article 1127-1 du Code civil : l'offre par voie électronique énonce les étapes du contrat, comment identifier/corriger les erreurs de saisie avant la conclusion du contrat, les langues proposées, les modalités et l'accès au contrat archivé, la consultation en ligne des règles professionnelles et commerciales du commerçant.



Cyber surveillance des salariés

La **vie privée** pourrait être définie, par exclusion, comme étant tout ce qui ne touche pas à la vie publique (droit à la vie sentimentale, droit à la vie familiale, secret de la résidence, droit à l'image…). Droit de nouer des relations avec ses semblables. Elle est même protégée dans la vie professionnelle.

Cybersurveillance, qu'en est-il du respect de la vie privée des salariés ?

La CNIL souhaite mettre en place des « garde-fous » car le cadre juridique actuel n'est pas suffisant.

Source : Sarah ZEROUALI - Droit-Travail-France

Une multitude de dispositifs

Filtrage informatique et historique : logiciel autorisant ou refusant l'accès aux sites internet. L'employeur a une visibilité sur les visites. Salariés et représentants sont informés.

Contrôle de la messagerie : L'utilisation personnelles de la messagerie est permise, l'employeur peut fixer des limites et ne peut pas consulter ces échanges. Le salarié indique « personnel » sur les fichiers pour interdire la consultation.

Écoute en temps réel et enregistrement des appels. Besoin reconnu, ponctuel et lié à des objectifs, non permanent - exception services d'urgence - article 9 du Code civil protégeant l'intimité de la vie privée. Salariés et représentants sont informés.

Vidéosurveillance ou vidéoprotection. Caméras installées uniquement aux « entrées et sorties des bâtiments, issues de secours, voies de circulation », zones de chargement, déchargement et stockage. Un panneau visible informe employés et visiteurs.

Géolocalisation du véhicule professionnel. Les finalités sont justifiées, déclarées à la CNIL. Le salarié en a connaissance. Il peut refuser en cas de contrôle de vitesse, de déplacements. Ses représentants sont informées.

RGPD et données de santé

Les données de santé, données sensibles (sens du RGPD), sont couvertes par le secret médical. Le RGPD les protège.

DONNÉE DE SANTÉ ? état de santé physique, mental, présent, futur (soins reçus, données génétiques, caractéristiques physiques, handicap, risque maladie...) Usage et finalité concernés.

L'INTERDICTION DE PRINCIPE DU TRAITEMENT DES DONNÉES DE SANTÉ

- Interdit sauf consentement du patient/exceptions du RGPD.
- Informer de la finalité. Règle stricte possible.
- Exceptions à l'obligation de consentement :
  - gestion des systèmes, services de santé ou de protection sociale
  - préservation de la santé publique (propagation maladies)
  - appréciation médicale, intérêts vitaux du patient en incapacité
- Utilisation restreinte, interdiction de les commercialiser.

L'ENTREPRISE RESPONSABLE DU TRAITEMENT DES DONNÉES DE SANTÉ doit nommer un DPO, tenir un registre des traitements et faire une analyse préalable d'impact des risques.

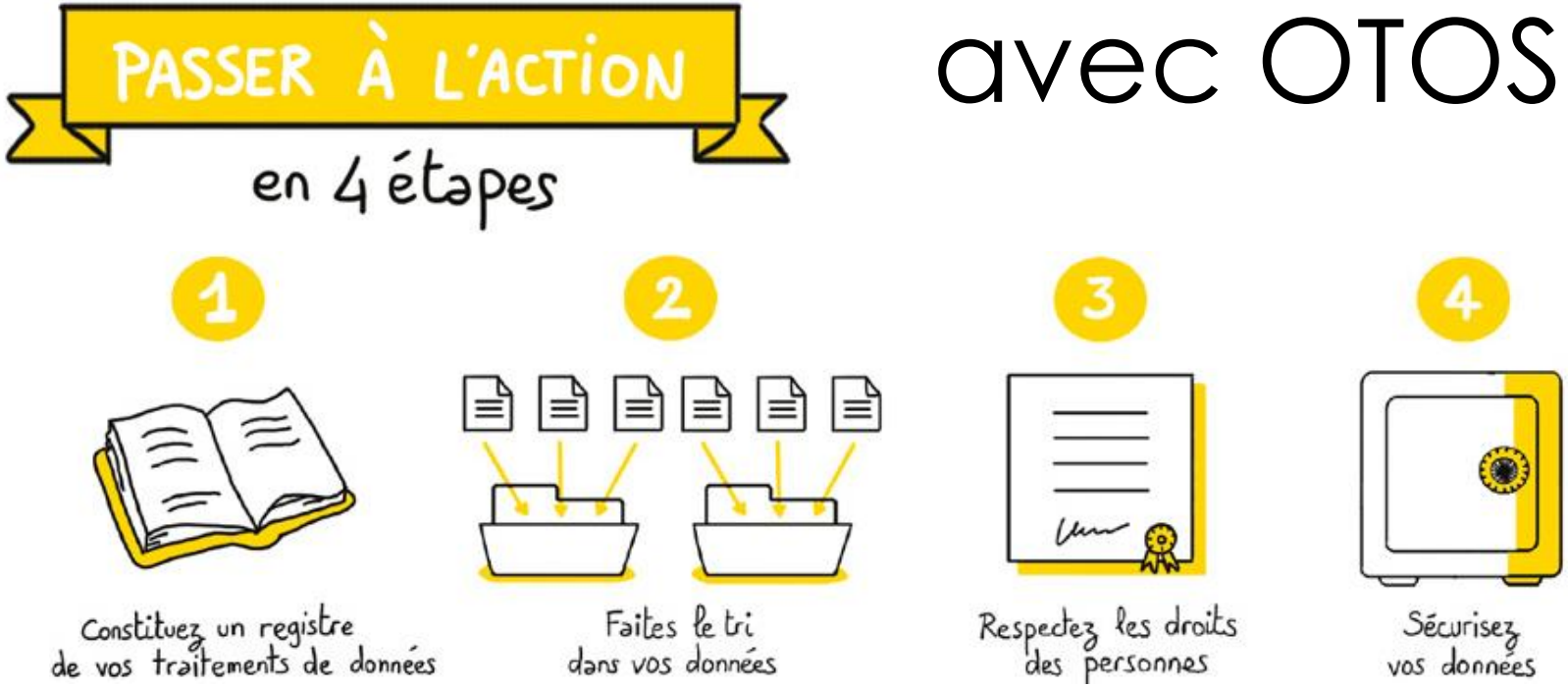
Consultation préalable de la CNIL avant tout traitement.

Source : www.legalplace.fr

.

RGPD

avec OTOS



❶ **Je rédige une procédure** où figure :

- Le registre de traitements des données personnelles et sensibles avec l'usage que je fais des données personnelles
- Comment je reconstruis/remets en route mon système d'information en cas de sinistre important ou d'incident critique
- L'archivage des données informatiques/physiques (stockage papier, 10 ans conservation des données contractuelles…)

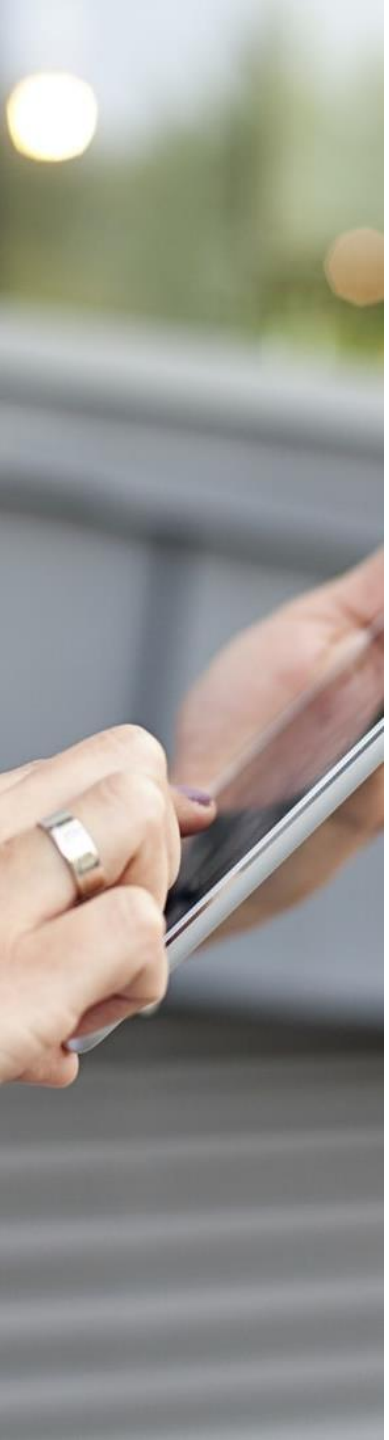
❷ **Je fais le tri dans mes données** et je ne **collecte que les données nécessaires**

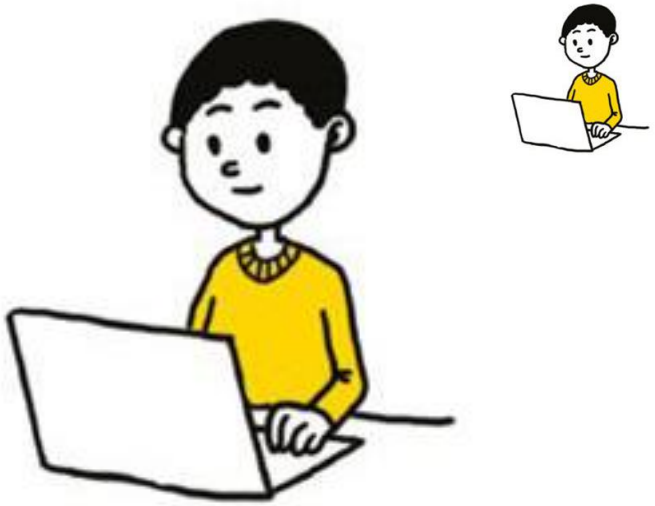
❸ **Je respecte le droit des personnes** sur la consultation, rectification ou suppression des données personnelles

❹ **Je sécurise les données personnelles** :

- Je stocke ces données sur un disque dur externe, je les transfère sur une plateforme sécurisée : LockSelf (gratuit)
- Je protège les fichiers de données personnelles avec mot de passe (Dash Lan) que je change régulièrement
- Je n'utilise pas d'adresse gmail pour le transfert des données

💻 **Je mets à jour mon site web** : mentions légales, cookies, accord formulaires de saisie, https ventes en ligne …





Je rédige ce courrier pour OTOS. Je le communique par un canal sécurisé.

« J'autorise OTOS à partager mon CV avec ses partenaires.
Je communique à OTOS mes nom, prénom, copie de ma carte d'identité, attestation RC, RIB, attestation URSSAF, SIRET, casier judiciaire - OTOS s'engage à détruire ce dernier à réception et à ne pas le conserver.
J'autorise OTOS à conserver mes données personnelles dans un fichier interne et pour une durée n'excédant pas la durée légalement en vigueur.
Je m'engage dans mes évaluations à utiliser un vocabulaire non discriminant et très respectueux. »

CONCLUSION

La règlementation RGPD a été créé dans l'intérêt d'un public vulnérable avec un risque partagé de pénalité en cas de non respect.

Acteur avec OTOS, vous vous engagez conjointement à respecter cette réglementation.

La CNIL met à votre disposition des kits pratiques pour mettre en place au mieux le RGPD.

Merci de compléter le questionnaire ci-après !

Source : CNIL