HANDELS- UND INDUSTRIEVEREIN
DES KANTONS BERN
Berner Handelskammer

Kramgasse 2, Case postale, 3001 Berne
Téléphone 031 388 87 87, Téléfax 031 388 87 88
www.bern-cci.ch

RGPD 2018

Guide de mise en œuvre pour les entreprises concernées

Avec le soutien de :

iGESCO INFORMATIQUE · GESTION · CONSEIL

CREDIT SUISSE

Kellerhals Carrard

MAZARS AUDIT • TAX • ADVISORY

GEST CONSEIL SA Prévoir | Conseiller | Assurer

swisscom

delacruz beranek RECHTSANWÄLTE • ATTORNEYS AT LAW

Table des matières

Survol

La nouvelle législation européenne RGPD – Règlement général de protection des données – contraint toutes les entreprises concernées à se doter d'outils adaptés, pour faire face aux enjeux de sécurité et de conformité actuels. Cela peut nécessiter des changements importants en termes de collecte, d'utilisation et de gouvernance des données.

Cette nouvelle approche des données personnelles favorise une gouvernance globale optimisée des données et l'amélioration du capital-confiance de l'entreprise.

Pourquoi les entreprises suisses sont-elles aussi concernées ?

Le RGPD ne s'applique pas uniquement aux entreprises ayant leur siège dans l'Union européenne (UE), il peut aussi concerner les entreprises suisses, même si elles ne disposent pas de succursales ou de filiales sur le territoire de l'UE.

Le champ d'application du RGPD couvre le traitement des données par toutes les entreprises, dès lors que celles-ci offrent des biens ou des services à des personnes dans l'UE (par exemple les exportateurs, vendeurs à distance, exploitants de plateformes de commande en ligne, etc.) ou qu'elles analysent le comportement de ces personnes (y compris sur des sites internet ou des applications smartphone). Peu importe que les données soient traitées en Europe ou en Suisse.

Un avant-goût de la future législation suisse

Certains éléments de la nouvelle législation européenne seront repris par la Suisse au titre de l'acquis Schengen.

Pour cette raison, un projet de révision de la loi fédérale sur la protection des données LPD se trouve devant les Chambres fédérales.

Cette dernière concernera évidemment toutes les entreprises suisses. Le RGPD européen donne l'occasion de se préparer à cette future évolution du droit suisse.

Le RGPD est aussi une opportunité pour se démarquer

La protection de la sphère privée devient une préoccupation majeure de la population, surtout suite aux dérapages commis par de grandes sociétés internationales.

Sa prise au sérieux par une entreprise est un gage important de son engagement par rapport à ses clients.

Les principes de base du RGPD en un clin d'œil

Pour être en conformité avec les exigences du RGPD, le traitement des données personnelles par votre entreprise devra satisfaire les principes suivants.

Licéité, loyauté, transparence	Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée.
Limitation des finalités	Le traitement des données doit servir des finalités déterminées, explicites et légitimes et les données ne peuvent être utilisées que pour ces finalités concrètes.
Minimisation des données	Seules les données nécessaires au regard des finalités (définies) peuvent être traitées.
Exactitude	Les données à caractère personnel doivent être exactes. Toutes les mesures raisonnables doivent être prises pour que les données inexactes soient effacées ou rectifiées sans tarder.
Limitation de la conservation	Les durées de conservation des données à caractère personnel ne doivent pas excéder la durée minimale nécessaire.
Intégrité et confidentialité	La protection des données à caractère personnel doit être garantie à l'aide de mesures techniques ou organisationnelles appropriées, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.
Responsabilité	Le responsable du traitement des données est responsable du respect des principes cités et doit pouvoir démontrer que ces principes sont respectés. Le responsable au sens du RGPD est une personne physique ou morale, une autorité, une institution ou un service qui décide seul ou collectivement des finalités du traitement des données à caractère personnel et des moyens utilisés pour traiter ces données.

Droits de la personne concernée

Le RGPD définit des droits pour les personnes concernées par toute forme de collecte de données. Le tableau ci-dessous en résume les principaux sans être exhaustif.

Droit à l'information (art. 13 et 14 RGPD)	Lorsque des données sont collectées, la personne concernée doit être informée. Cela vaut aussi si les données ne sont pas collectées directement auprès d'elle.
Droit d'accès (art. 15 RGPD)	La personne a le droit de savoir si les données à caractère personnel la concernant sont ou ne sont pas traitées par l'entreprise, et si oui, quelles données. Cela inclut le droit à l'information sur les finalités du traitement, les catégories de données, les (catégories de) destinataires, la durée de conservation des données, le droit de la personne concernée de demander la rectification, l'effacement, la limitation des données, le droit de s'opposer à leur traitement, le droit d'introduire une réclamation, de connaître la source des données et, le cas échéant, l'existence d'une prise de décision automatisée.
Droit à la rectification et à l'effacement des données (« droit à l'oubli », art. 16 et 17 RGPD)	La personne concernée a le droit de faire rectifier les données erronées. Les données à caractère personnel doivent, entre autres, être effacées dans les meilleurs délais lorsqu'un des motifs suivants s'applique : ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ; la personne concernée retire son consentement sur lequel est fondé le traitement des données et il n'existe pas d'autre fondement juridique au traitement (p. ex. obligation légale) ; la personne concernée s'oppose au traitement de ses données.
Le droit à la limitation du traitement (art. 18 RGPD)	La personne concernée a le droit, dans certains cas prévus par la loi, d'obtenir du responsable du traitement la limitation de ses données. Lorsqu'une telle limitation est demandée, le responsable de traitement ne pourra plus que stocker les données. Aucune autre opération ne pourra, en principe, avoir lieu sur ces données personnelles
L'obligation de notification du responsable (art. 19 RGPD)	Cet article met en place une obligation de notification à charge du responsable de traitement qui l'oblige à communiquer à chaque destinataire des données toute rectification, effacement ou limitation du traitement

Droit à la portabilité des données (art. 20)	La personne concernée peut demander que le responsable des données lui fournisse, dans un format structuré, couramment utilisé et lisible par machine, les données qu'elle lui a transmises. Le droit à la portabilité des données ne peut être exercé qu'à la condition que le traitement initial ait été fondé sur un consentement en application ou un contrat en application et réalisé au moyen d'une procédure automatisée.
Droit d'opposition (art. 21 RGPD)	La personne concernée peut s'opposer au traitement de ses données. Lorsque la personne concernée s'oppose au traitement de ses données par exemple à des fins de prospection, les données à caractère personnel ne peuvent plus être traitées à ces fins.
Le droit de ne pas être soumis à une décision individuelle automatisée (art. 22 RGPD)	La personne concernée a le droit de ne pas être soumise à une décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. Le profilage y est expressément inclus.
Le droit à la communication d'une violation de données à caractère personnel (art.34 RGPD)	Le responsable de traitement est obligé de notifier à la personne concernée les violations de données susceptibles de l'exposer à un risque élevé à ses droits et libertés.

Obligations de l'entreprise

Les entreprises soumises au RGPD sont tenues aux obligations suivantes :

Obligation d'informer	Les informations sur la collecte de données doivent être fournies à la personne concernée d'une façon concise, transparente, compréhensible et facilement accessible.
Obligation d'effectuer une analyse d'impact (données sensibles)	Une analyse d'impact relative à la protection des données est une analyse des risques réalisée préalablement au traitement des données à caractère personnel. Elle comprend entre autres une description des opérations de traitement envisagées, les risques qui en découlent pour la personne concernée et les mesures à prendre pour limiter ou réduire ces risques. L'analyse d'impact relative à la protection des données ne concerne toutefois que les traitements de données présentant un risque élevé pour les droits et libertés des personnes (p. ex. données sur la santé, qui sont traitées par les caisses-maladie, p.ex. pour des clients, utilisateurs, collaborateurs, etc.).
Protection des données dès la conception et par défaut	Des mesures doivent être prises qui respectent le principe de protection des données dès la conception (Data Protection by Design) et de protection des données par défaut (Data Protection by Default). Il convient donc de s'assurer que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement des données sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.
Obligation de documentation	Les responsables du traitement des données doivent tenir un registre (écrit ou électronique) sur leurs activités de traitement. Ce registre doit comporter, entre autres, les points suivants : noms et coordonnées du ou des responsables, du représentant du responsable du traitement des données ainsi que d'un éventuel délégué à la protection des données ; la finalité du traitement ;la description des catégories de personnes concernées et des catégories de données à caractère personnel (p.ex. clients et fournisseurs ; données de factures, coordonnées) ; les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées (p. ex. police, assurances sociales), y compris les destinataires établis dans des pays tiers ou des organisations internationales (maison mère aux États-Unis); dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données; dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles pour protéger les données.

Définition d'une « donnée personnelle »

Une donnée personnelle concerne toutes les informations qui se rapportent à une personne physique identifiée ou identifiable, par exemple nom et prénom, adresse, date de naissance, numéro de téléphone, adresse e-mail, moyens de payement, etc.

Définition d'une « donnée personnelle sensible »

Une donnée personnelle sensible fait apparaître, directement ou indirectement, des informations liées à : la santé ; la sphère intime ou l'origine raciale ou ethnique ; des mesures d'aide social ; des opinions ou activités religieuses, philosophiques, politiques ou syndicales ; des poursuites ou sanctions pénales et administratives ; des données biométriques et génétiques, etc.

Définition du DPO Data Protection Officer ou « Responsable du traitement »

Le DPO ou « Responsable du traitement » est juridiquement garant que les règles du RGPD – respectivement de la LPD suisse – sont observées par l'entreprise. Il lui revient de mettre en œuvre les solutions techniques nécessaires au respect de la législation. C'est aussi lui qui sert d'interlocuteur avec les autorités en cas de violation des normes en vigueur.

Cette fonction ne peut pas être assumée par la direction générale de l'entreprise. Elle peut être confiée soit à un collaborateur, soit à un administrateur, soit à un tiers hors de l'entreprise.

À ce jour, il n'existe pas encore de formation spécifique pour la fonction de DPO adaptée aux besoins d'une PME. Une solide connaissance de la législation lui est cependant indispensable.

1. L'esprit de la loi et l'identification des risques de non-conformité

Il revient aux entreprises d'apprécier les risques et de prendre les mesures appropriées quant à la conformité et à l'application de cette loi. Protection des données et documentation rigoureuse restent fondamentales. Le support, à l'instar de ce qui se fait dans un système de management de la qualité, doit permettre, à tout moment, de prouver la conformité au RGPD, et ce, dans une logique de responsabilisation des entreprises.

À ce titre, celles-ci doivent tenir à jour le **registre des traitements** et tout autre document prouvant leur conformité (registre des PIA/Privacy Impact Assessment, politique de sécurité documentée, processus internes, preuve du consentement, etc.)

Le RGPD définit un certain nombre de **principes** pour protéger les données personnelles. Les entreprises devront définir, selon leur situation et leur contexte, les moyens appropriés pour y répondre, et **ce tout au long du cycle de vie des données ; enregistrement, conservation, accessibilité, droits à la consultation...**

Les responsabilités sont également étendues aux sous-traitants. Les prestataires traitants des données personnelles pour le compte de l'entreprise doivent eux-mêmes être conformes au RGPD et ont des obligations en matière de confidentialité et de sécurité des données. Ils peuvent également avoir un rôle de conseil auprès de l'entreprise en cas de faille de sécurité, de destruction de données, etc.

- ✓ **Risque juridique : le défaut de conformité au RGPD peut faire l'objet de lourdes sanctions.** Celles-ci vont de l'amende forfaitaire à une amende représentant un pourcentage du CA de l'entreprise. Au-delà de l'amende, cette dernière a bien sûr obligation de prendre les mesures nécessaires, y compris la collecte de fonds, pour une mise en conformité.

- ✓ **Risque sécuritaire :** avec le RGPD, la sécurité des données n'est plus une option, elle fait partie des standards à respecter. **Investir dans une politique de sécurité des données devient indispensable** aussi bien pour limiter le risque juridique, **les primes d'assurances** (la pratique d'audits de sécurité par des cabinets d'assurance devient d'ailleurs courante avant d'établir le montant de la prime) et les coûts induits par une cyberattaque (pertes de données, perte d'activité, perte de réputation...)

- ✓ **Risque de réputation :** il est lié à la sécurité des données, car selon les cas d'attaque et de violation de données personnelles, les entreprises doivent notifier les personnes concernées ainsi que les autorités de contrôle sous 72 heures. Dès qu'une entreprise se fait pirater, la nouvelle se répand très vite et la réputation de cette dernière est forcément mise à mal. S'il est difficile de mesurer précisément les impacts financiers liés à la réputation de l'entreprise, le Breach Level Index de Gemalto fait tout de même apparaître que deux tiers des entreprises victimes de failles de sécurité ont été impactées au niveau du prix de l'action cotée en bourse.

- ✓ **Risque financier :** les sanctions pour les grandes entreprises peuvent se traduire par des amendes administratives s'élevant jusqu'à 20 millions d'euros ou **4% de leur chiffre d'affaires annuel** global.

2. Domaines et champs d'application de la loi

Une obligation de garantir la sécurité des données traitées

Il faut effectuer une caractérisation des différentes typologies de données, par exemple les données sensibles, stratégiques, obsolètes ou redondantes. Cette première phase permet de nettoyer les bases de données et diminuer le coût du stockage (quelles données sont stockées ? Comment ont-elles été obtenues ? Sont-elles à jour ? À quoi servent-elles, etc.). De nombreuses PME disposent de plusieurs bases de données, pas ou peu entretenues, souvent sous-utilisées et à ce point morcelées qu'elles ne savent plus d'où proviennent les données.

Pour remédier à cela, il faut

- Revoir la pertinence de la politique de traitement : collecte, modification, extraction, archivage, destruction, des données en entreprise.

- Soumettre les employés traitant les données de vos clients à une obligation de confidentialité.

- Signaler à votre client toute violation de ses données.

- Prendre toutes les mesures permettant de garantir un niveau de sécurité adapté aux risques. À cet effet, un recensement exhaustif pour évaluer la pertinence des données au regard des axes de développement est nécessaire.

Droit au consentement des personnes renforcées

Lors de chaque collecte de données personnelles, les utilisateurs doivent être en mesure de donner **expressément un consentement** éclairé ou de refuser. Faire accepter une politique générale de confidentialité des données ne suffit plus. L'utilisateur doit comprendre quelles données sont collectées, avec **quelle finalité**, combien **de temps elles seront conservées,** quelles sont les conséquences pour l'utilisateur de son consentement ou de son refus. Il appartient à l'entreprise de rédiger des mentions d'information claires et intelligibles lors de chaque collecte de données et de conserver la preuve du consentement des personnes.

Informer les personnes concernées qu'elles peuvent, à tout moment, accéder à leurs données personnelles, les faire supprimer ou transférer. Cela passe par la modification de vos contrats, dénis de responsabilité (disclaimers) sur site, etc.

- ✓ **Droit à l'oubli : l**'entreprise doit aussi être en mesure de déréférencer un client sur simple demande. La problématique de la **durée de conservation des** données porte également sur la conservation des données concernant le personnel ayant quitté l'entreprise. Attention toutefois d'observer les prescriptions de l'Ordonnance suisse concernant la tenue et la conservation des livres de comptes (Olico), qui définit des données et des durées de conservation qui doivent être observées malgré une demande de suppression de la part d'une personne concernée.

- ✓ **Notification en cas de violation des données :** dans les 72 heures suivant une violation de données, l'entreprise doit notifier les personnes concernées ainsi que les autorités de contrôle compétentes. Attention, cela est uniquement applicable dans le cas où une entreprise suisse est soumise au RGPD et a nommé un représentant au sein de l'UE.

- ✓ **Encadrement des transferts de données hors de la Suisse :** les transferts de données hors de la Suisse sont possibles seulement s'ils sont encadrés avec des outils assurant un niveau de protection suffisant et appropriés. Cela concerne également la mise sur «**cloud**» de données personnelles. **La loi veille à assurer l'intégrité et la protection de ces données dans tous les environnements.**

- ✓ **Sécurité et documentation :** la politique de sécurité des données est un aspect important de la conformité au RGPD. L'entreprise doit prendre les mesures **organisationnelles et techniques** afin que les données personnelles qu'elle gère bénéficient du plus haut niveau de sécurité. Ce dernier doit bien sûr être adapté **en fonction des risques et de la sensibilité des données**. Il s'agit également de garantir l'intégrité du système d'information, sa disponibilité et sa **résilience en cas d'incident**

Une information doit figurer sur le registre des traitements pour une **meilleure traçabilité,** ce qui facilitera également la rédaction des mentions d'information.

Identifier les lieux où sont hébergées les données ainsi que les éventuels risques de transferts hors de Suisse.

L'identification des personnes traitant les données et, le cas échéant, les agents externes impliqués pour chaque traitement, contribue à la traçabilité des données.

Procédures internes : fixer un cadre à même d'assurer cette sécurité par l'émission de directives et de circulaires claires à disposition des acteurs concernés.

Garantir la conformité de vos futures actions marketing : préparer toute nouvelle action marketing en intégrant le respect des droits des personnes et la sécurité des données dès le départ.

De très nombreuses pratiques marketing reposent sur la notion de profilage, c.-à-d. de collecte de données à caractère personnel dans le but de dresser le profil de vos prospects, clients ou utilisateurs afin de leur proposer des offres ou services personnalisés.

Le profilage à des fins de marketing est autorisé pour autant qu'il réponde aux conditions fixées par le RGPD (la personne doit en être informée et doit pouvoir s'y opposer).

Opt-in (option d'adhésion à) renforcé et gestion des cookies : l'obligation d'information accrue de l'internaute implique qu'il puisse donner librement son consentement pour des traitements parfaitement identifiés (nature et finalité de la collecte doivent être précisés).

Sauf exception, l'internaute doit donner son accord préalable pour le dépôt de cookies. Un bandeau d'information doit donc être présent sur tout site internet.

COLLECTE DES DONNÉES	VALORISATION DES DONNÉES
Il faudra désormais informer le client de manière précise **au sujet de l'exploitation des données** qu'il va générer.	Si vous comptez exploiter les données personnelles dans vos campagnes marketing, il sera nécessaire de **solliciter l'autorisation préalable du client et lui permettre de refuser.**
L'entreprise doit demander le consentement du client **de manière claire et informée** (mise à disposition des conditions d'utilisation de sa data).	Lors du partage de ses données, le client devra pouvoir signifier s'il souhaite ou non **être ciblé par ces campagnes marketing**.
Le consentement éclairé est une notion centrale du RGPD : le client devra désormais toujours avoir **une visibilité élargie** sur les intentions de l'entreprise.	Le client pourra également signifier **son refus d'être profilé**, c.-à-d. que ses données soient exploitées via un algorithme à des fins marketing et commerciales.

3. Préparation : méthodes et outils à disposition

Cartographier le traitement des données

La première étape consiste **à inventorier** tous les traitements de données à caractère personnel de l'entreprise

- Les différents traitements de données personnelles.
- **Les catégories de données** personnelles traitées, par degré de sensibilité.
- **Les objectifs poursuivis** par les opérations de traitement de données.
- **Les acteurs** (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants.
- **Les flux** en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels **transferts de données hors de la Suisse** et en assurer une **traçabilité** fiable

Dans le cadre du futur règlement, les organismes doivent **tenir une documentation interne complète** sur leurs traitements de données personnelles et s'assurer qu'ils respectent bien les nouvelles obligations légales.

Pour chaque traitement de données personnelles, posez-vous les questions suivantes

QUI ?	✓ Inscrivez dans le registre le nom et les coordonnées du **responsable du traitement (**services opérationnels) le cas échéant, du **délégué à la protection** des données. ✓ Établissez la liste **des sous-traitants**.
QUOI ?	✓ Identifiez les catégories de données traitées. ✓ Identifiez les données susceptibles de soulever des risques en raison de leur **sensibilité** particulière (par exemple : les données relatives à la santé ou les infractions).
POURQUOI ?	✓ Indiquez-la ou les finalités pour lesquelles vous collectez ou traitez ces données (par exemple : gestion de la relation commerciale, gestion RH...).
OÙ ?	✓ Déterminez le lieu où les données sont hébergées. ✓ Indiquez vers quels pays les données sont éventuellement transférées

JUSQU'À QUAND ?	✓ Indiquez, pour chaque catégorie de données, combien de temps vous les conservez (archivage des données et conservation injustifiée et hors des délais officiels autorisés).
COMMENT ?	Précisez les mesures de sécurité mises en œuvre pour minimiser les **risques d'accès non autorisé aux données** et donc d'impact sur la vie privée.

Gestion et transfert de données

L'entreprise ne pourra désormais plus conserver indéfiniment les données. La durée doit être liée à la finalité. D'autre part, les responsables du traitement de la data devront conserver un registre détaillé des traitements.

Le transfert des données personnelles vers des pays étrangers à l'UE sera soumis à vérification. Une anonymisation et un cryptage des données sont rendus obligatoires lors du transfert de data vers d'autres entreprises. Enfin, seules les personnes habilitées devront avoir accès à la data. Cela protège les utilisateurs, mais aussi vos bases de données !

Vous aurez franchi cette étape si

- ✓ ***Vous avez rencontré les services et les entités qui traitent des données personnelles, vous avez établi la liste des traitements par finalité principale et sensibilité.***
- ✓ ***Vous avez identifié les sous-traitants intervenant dans ce processus***
- ✓ ***Vous savez où ces données sont stockées, quels acteurs y ont accès et combien de temps.***

Prioriser les actions à mener

Sur la base du registre des traitements de données personnelles, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir.

Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

- Vérifier et réviser les clauses de contrat **avec les sous-traitants** si nécessaire
- Prévoir les procédures d'exercice des droits des personnes (droit à la portabilité, etc.)
- Vérifier le **niveau de sécurité actuel** des traitements en place

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

Points d'attention, quels que soient les traitements de données :

- **Assurez-vous** que seules les données **strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.
- **Identifiez la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- **Révisez** vos mentions d'information afin qu'elles soient **conformes** aux exigences du règlement.
- **Vérifiez** que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
- **Prévoyez** les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).
- **Vérifiez** les mesures de sécurité mises en place.

Points d'attention nécessitant une vigilance particulière

En plus des points mentionnés dans le paragraphe précédent, les cas cités dans le tableau ci-dessous demandent une attention particulière !

Vous traitez certains types de données…	• Des données qui révèlent l'origine prétendument raciale ou ethnique. • Les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale. • Des données relatives à la santé ou l'orientation sexuelle. • Des données génétiques ou biométriques. • Des données d'infraction ou de condamnation pénale. • Des données concernant des mineurs.

Votre traitement de données personnelles a pour effet…	• La surveillance systématique à grande échelle d'une zone accessible au public. • L'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.
Vous transférez des données hors de Suisse ?	• Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par les autorités de contrôle. • Dans le cas contraire, encadrez vos transferts.

Vous aurez franchi cette étape si :

✓ ***Vous avez mis en place les premières mesures pour protéger les personnes concernées par vos traitements***

4. Gestion, identification et minimisation des risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, **Privacy Impact Assessment ou PIA**).

C'est un outil incontournable qui vous permettra de minimiser les risques futurs et de prévenir les violations de données en amont.

Cette étude ou cet audit consiste à :

- Identifier la nature des risques encourus pour la vie privée dès la conception d'un nouveau produit ou service, soit une évaluation de la pertinence et de la proportionnalité du traitement au regard du risque.
- Déterminer la nature de traitement des données personnelles et sa finalité.
- Inventorier les moyens mis en place pour sécuriser le traitement et garantir la confidentialité des données.
- Valider les solutions (techniques et organisationnelles) pour minimiser les risques inhérents au traitement.

L'étude d'impact sur la protection des données permet :

- **De mettre sur pied** un traitement de données personnelles ou un produit respectueux de la vie privée.
- **D'évaluer** les impacts sur la vie privée des personnes concernées.
- **De démontrer** que les principes fondamentaux du règlement sont respectés.

Les outils pour vous aider

- **Éléments à protéger** : minimiser les données, chiffrer, anonymiser (anonymous), permettre l'exercice des droits, etc.
- **Impacts potentiels** : sauvegarder les données, tracer l'activité, gérer les violations de données, etc.
- **Sources de risques** : contrôler les accès, gérer les tiers, lutter contre les codes malveillants, etc.
- **Supports** : réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier, etc.

Vous aurez franchi cette étape si :

✓ ***vous avez mis en place des mesures permettant de répondre aux principaux risques et menaces qui pèsent sur la vie privée des personnes concernées***

Réorganiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place en interne des procédures et pratiques garantissant la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles (par exemple : failles de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire, etc.).

Implications de l'organisation des processus

- **Prendre en compte l**a protection des données personnelles **dès la conception** d'une application ou d'un traitement.
- **S'assurer** du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données, de **sensibiliser et d'organiser** la remontée d'information en construisant notamment un plan de **formation et de communication** auprès de vos collaborateurs.
- Tout collaborateur susceptible de manipuler des données sensibles doit être au fait des bonnes pratiques garantissant leur protection et leur confidentialité.

- **Traiter les réclamations** et les demandes des personnes concernées quant à l'exercice de leurs droits **(droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement)** en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen).

- **Anticiper** les violations de données en prévoyant, dans certains cas, la notification dans les 72 heures à l'autorité de protection des données, et dans les meilleurs délais aux autorités de contrôle et aux personnes concernées.

Vous aurez franchi cette étape si :

✓ ***Les réflexes relatifs à de la protection des données sont acquis et appliqués au sein des services qui mettent en œuvre des traitements de données ; votre organisme sait quoi faire et à qui s'adresser en cas d'incident.***

5. Bien documenter sa conformité

Votre entreprise a parcouru un long chemin pour **garantir sa conformité** au nouveau règlement européen. Afin de prouver sa conformité, il vous faudra **produire différents documents à maintenir à jour régulièrement.**

Cette réactualisation doit assurer une protection des données en continu.

- Registre des traitements rédigés au complet
- Analyses d'impact (PIA) menées sur tous les traitements à risque
- Mentions d'informations révisées
- Procédures de recueil de consentement et d'exercice des droits utilisateurs mis en place
- Clauses de contrat avec les sous-traitants révisées

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les mesures organisationnelles et techniques sont réexaminées et actualisées si nécessaire.

Votre dossier devra notamment comporter les éléments suivants

D'une part, la documentation sur vos traitements de données personnelles (nom et prénom, mots de passe, date de naissance, etc.)

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants).

- **Les analyses d'impact sur la protection des données** (PIA ; voir chapitre 4 « Préparation : mesures à entreprendre ») pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes, l'encadrement des transferts de données hors de la Suisse.

D'autre part, l'information communiquée aux personnes au sein et hors de l'entreprise (collaborateurs, clients, fournisseurs, etc.)

- Les mentions d'information.

- Les modèles de recueil **du consentement** des personnes concernées.

- **Les procédures mises en place** pour l'exercice des droits des personnes.

- Les procédures internes en cas de **violations** de données.

6. Questionnaire et mesures techniques concrètes

- Se préparer à la possibilité d'une fuite de données : mettre en place les procédures d'escalade qui seront activées en cas de violation de données personnelles.

- Informez-vous les internautes accédant à votre site des droits *(effacement, portabilité des données)* dont ils disposent ?

- Les champs obligatoires de vos formulaires sont-ils signalés par un astérisque ?

- Les internautes consentent-ils à la réception de cookies lorsqu'ils visitent votre site ?

- La durée de conservation des données que vous avez collectée est-elle illimitée ?

- Avez-vous répertorié les traitements des données que vous effectuez ?

- Toute autre disposition organisationnelle et technique.

Nécessité de traiter l'ensemble des données de façon similaire en matière de confidentialité et de sécurité

- Un système d'opt-in (option d'adhésion à consentement) en matière d'e-mailing (newsletter par exemple), a-t-il été mis en place ?
- Les données collectées hors de la Suisse (filiales, partenaires, serveurs...) sont-elles transférées ?
- Nécessité de documenter les données personnelles collectées, leur origine et avec qui elles seront partagées.
- Nécessité de revoir les déclarations de confidentialité existantes et y apporter les changements nécessaires.
- Nécessité de revoir les procédures afin de respecter les nouveaux droits dont bénéficient les personnes physiques.
- Nécessité de planifier la manière dont seront traitées les requêtes dans le respect des nouvelles échéances et fournir les informations requises.
- Nécessité d'identifier et de documenter les principes juridiques pour chaque type d'activité de traitement de données.
- Nécessité de s'assurer que les procédures adéquates ont été mises en place pour détecter, signaler et examiner les violations de données.

Stocker et communiquer les informations sensibles de manière sécurisée

- Segmenter le réseau et surveiller qui y entre et qui en sort, prévoir des registres de traitement (documents/formulaires de décharge).
- Sécuriser les documents papier, les supports physiques et les appareils.
- S'assurer que les départements clés sont informés du changement de réglementation et anticipent l'impact du RGPD.
- Avoir des procédures de maintien de la sécurité et de **correction des vulnérabilités.**

Sécuriser l'accès à distance

- S'assurer que les **prestataires de services externes** mettent en place des mesures de sécurité.

Gestion des accès – Une gestion saine des identités et des accès inclut l'authentification, les accès à distance sécurisés, la sécurité adaptative/basée sur le risque, la gestion des mots de passe et le contrôle des identifiants des utilisateurs. Pour accéder aux données sensibles, le législateur préconise l'authentification avec une sécurisation renforcée (par ex. avec des mots de passe sécurisés de 12 caractères alphanumériques, dont au minimum un caractère spécial, régulièrement changés).

Protection du périmètre – déployer des pare-feu (firewall) de nouvelle génération (NGFW) pour réduire l'exposition du réseau aux cyber menaces, prévenir les risques de fuites et appliquer les mesures correctrices appropriées suite à une faille.

Accès mobiles sécurisés – Les données concernées doivent pouvoir circuler en totale sécurité et les salariés doivent pouvoir accéder aux applications et aux données dont ils ont besoin, comme ils l'entendent, via les terminaux de leur choix.

Sécurité des e-mails – prévenir les menaces de phishing et autres attaques d'information protégée par e-mail, tout en préservant l'échange sûr et conforme des données sensibles et confidentielles.

Sensibiliser tous les travailleurs – attirer l'attention de ces derniers sur la fuite de données et à la nécessité de sécuriser leur traitement, prévoir des formations le cas échéant : si les problèmes de «hacking» (piratage informatique) font les gros titres de la presse, la fuite de données peut prendre des formes beaucoup plus communes et moins spectaculaires: vol d'ordinateur professionnel, envoi d'une pièce jointe contenant des données d'un autre client, etc.

Examiner la manière dont les consentements sont demandés, obtenus et conservés.

7. Conclusion

Les entreprises suisses sont nombreuses à avoir déjà mis en route les adaptations nécessaires. Voici quelques-unes des mesures prises en priorité

- **Désignation :** nommer un Data Protection Officer (DPO) qui s'assurera de la conformité du traitement des données.
- **Inventaire :** tenir un registre de traitement des données.
- **Identifier :** identifier le périmètre des données sensibles. Le RGPD impose le cryptage ou la pseudonymisation pour ces données.
- **Garantir les droits des personnes** : droit à l'oubli, droit à la portabilité des données, etc.
- **Formation :** rédiger une charte de bonnes pratiques pour les salariés, incluant les sanctions encourues en cas de non-respect de la loi.
- **Adaptation :** insérer des clauses dans les contrats de vos sous-traitants et de vos salariés garantissant qu'ils respectent les dispositions légales quant aux données qu'ils vous confient.

- **Validation :** adaptation des logiciels et des applications afin d'assurer la conformité aux nouvelles règles et aux normes mise en place par le RGPD et ISO.

- **Gérer :** se préparer à la possibilité d'une fuite de données. À cet effet, mettre en place les procédures d'escalade qui seront activées en cas de violation de données personnelles.

- **Protection :** gestion des droits d'accès aux données personnelles et des accès internet.

Plus d'informations

- Synthèse en une page www.bern-cci.ch

- Test d'autodiagnostic en ligne www.bern-cci.ch

Contacts et adresses utiles

- Union du Commerce et de l'Industrie du canton de Berne www.bern-cci.ch
- IGESCO Suisse SA, Spécialiste IT pour PME, www.igesco.ch
- Kellerhals Carrard, étude d'avocats, www.kellerhals-carrard.ch
- Swisscom Solutions PME, www.swisscom.com
- Credit Suisse, www.credit-suisse.com
- Mazars Suisse, fiduciaire et audit, www.mazars.ch
- GestConseil SA, conseiller et courtier en assurances, www.gestconseil.ch
- De la Cruz & Beranek Rechtanwälte, www.delacruzberanek.com
- Préposé cantonal valaisan à la protection des données et à la transparence, www.prepose.tv

Disclaimer

La présente fiche d'information et le test en ligne servent uniquement à des fins d'information et de sensibilisation. Ils ne peuvent pas remplacer un conseil juridique. L'Union du Commerce et de l'Industrie du canton de Berne ainsi que ses partenaires déclinent toute responsabilité en cas d'actions ou d'omissions en lien avec la consultation de la fiche d'information et l'utilisation du test en ligne.

Impressum

Union du Commerce et de l'Industrie du canton de Berne
Chambre Valaisanne de Commerce et d'Industrie

Bern, avril 2019