Réglementations relatives à la protection des données dans le monde

La société dans laquelle nous évoluons en tant qu'individu ou entrepreneur est de plus en plus numérisée. En effet, l'utilisation des outils numériques et d'Internet s'est fortement démocratisée dans de multiples domaines, ce qui a apporté de nombreux changements et induit de nouveaux modes de consommation et d'interaction.

De nombreuses données sont désormais numérisées, stockées dans des systèmes informatiques et mises en ligne. La protection des données est donc cruciale pour protéger les utilisatrices et utilisateurs. Pour rester compétitives, les entreprises ont été contraintes d'intégrer les nouvelles technologies mais également de se mettre en conformité avec les nouveaux cadres juridiques. De nos jours, la question de la protection des données est devenue à la fois cruciale et stratégique pour garantir la pérennité de l'entreprise et renforcer sa réputation. Il est ainsi indispensable pour les entreprises de bien comprendre les cadres juridiques relatifs à la protection des données à travers le monde afin d'être en conformité avec ceux-ci. Ce guide offre aux entreprises un aperçu des différentes réglementations concernant la protection des données. Il ne se veut pas exhaustif.

Qu'est-ce que la protection des données et pourquoi la réglementer ?

Les lois sur la protection des données protègent les droits fondamentaux et la personnalité des personnes physiques. Leur but premier est la protection de la personne et non la protection de la donnée elle-même.

La protection des données fait référence à la pratique de sécuriser et de préserver les informations personnelles et sensibles des individus ou des organisations contre tout accès, utilisation, divulgation ou altération non autorisés. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des données, tout en respectant les droits fondamentaux à la vie privée et à la protection des données.

Ne pas confondre données personnelles et données personnelles sensibles

Selon la loi sur la protection des données (LPD), les **données personnelles** font référence à toutes les informations concernant une personne physique identifiée ou identifiable.

Les **données personnelles sensibles** regroupent les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'origine raciale ou ethnique, les données génétiques, les données biométriques identifiant une personne physique de manière univoque, les données sur des poursuites ou sanctions pénales et administratives et les données sur des mesures d'aide sociale.

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

hegh e g
Haute école de gestion Genève

UNIVERSITÉ DE GENÈVE

En savoir +

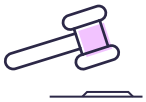
Enjeux de la protection des données

- **Droits individuels**
  Garantir aux individus le droit de maîtriser, d'accéder et de rectifier leurs données personnelles.

- **Menaces croissantes**
  Avec l'essor du numérique, les risques de violation des données ont augmenté, notamment la destruction, la perte, l'altération, la divulgation et l'accès non autorisé comme par exemple le piratage.

- **Confiance des consommateurs**
  Renforcer la confiance des clientes et des clients et des partenaires envers les entreprises, sachant que leurs données sont traitées de manière sécurisée.

- **Responsabilité des entreprises**
  Les entreprises ont l'obligation d'adopter des mesures de sécurité appropriées et d'être transparentes sur la manière dont elles utilisent les données.



- **Sanctions**
  En cas de non-conformité, les entreprises et/ou les personnes physiques peuvent être soumises à des amendes importantes, renforçant ainsi l'importance de la conformité.

- **Harmonisation internationale**
  La réglementation aide à établir des normes communes pour la protection des données à travers les frontières, facilitant ainsi les échanges internationaux d'informations.

La loi fédérale sur la protection des données (LPD)

En Suisse, la législation concernant la protection des données est la **loi fédérale sur la protection des données (LPD)**, en allemand Datenschutzgesetz (DSG). La première LPD date de 1992. Avec notamment l'apparition d'Internet, une révision complète de la LPD a été nécessaire afin d'assurer à la population une protection adéquate de ses données et adaptée aux récentes évolutions technologiques. Une révision de cette loi était également indispensable afin que le droit suisse continue à être compatible avec le droit européen et notamment le **règlement général sur la protection des données (RGPD)**. La libre circulation des données avec l'Union européenne est ainsi garantie.

La nouvelle LPD est entrée en vigueur le 1er septembre 2023, avec effet immédiat, remplaçant intégralement l'ancienne loi de 1992. Elle vise à améliorer le traitement des données personnelles et accorde de nouveaux droits aux citoyennes et citoyens suisses, mais elle s'accompagne également d'un certain nombre d'obligations pour les entreprises.

Les dispositions d'exécution de la loi, inscrites dans la nouvelle **ordonnance sur la protection des données (OPDo)** et dans **l'ordonnance sur les certifications en matière de protection des données (OCPD)** sont entrées en vigueur en même temps que la LPD, le 1er septembre 2023.

Les 7 principes guidant la protection des données

- licéité
- bonne foi
- proportionnalité
- finalité
- exactitude
- sécurité
- transparence

Un peu d'histoire

24 juin 1976
adoption de la loi sur les informations traitées automatiquement par ordinateur (LITAO).

19 juin 1992
entrée en vigueur de la loi fédérale sur la protection des données (LPD).

25 mai 2018
entrée en vigueur du règlement général sur la protection des données (RGPD).

1er mars 2019
révision partielle de la LPD.

25 août 2023
entrée en vigueur des réglementations européennes Digital Services Act (DSA) et Digital Market Act (DMA) pour les grandes plateformes.

1er septembre 2023
entrée en vigueur de la nouvelle loi fédérale sur la protection des données (LPD).

17 février 2024
entrée en vigueur des réglementations européennes Digital Services Act (DSA) et Digital Market Act (DMA) pour les plateformes de plus petite taille.

Les entreprises concernées par la loi sur la protection des données

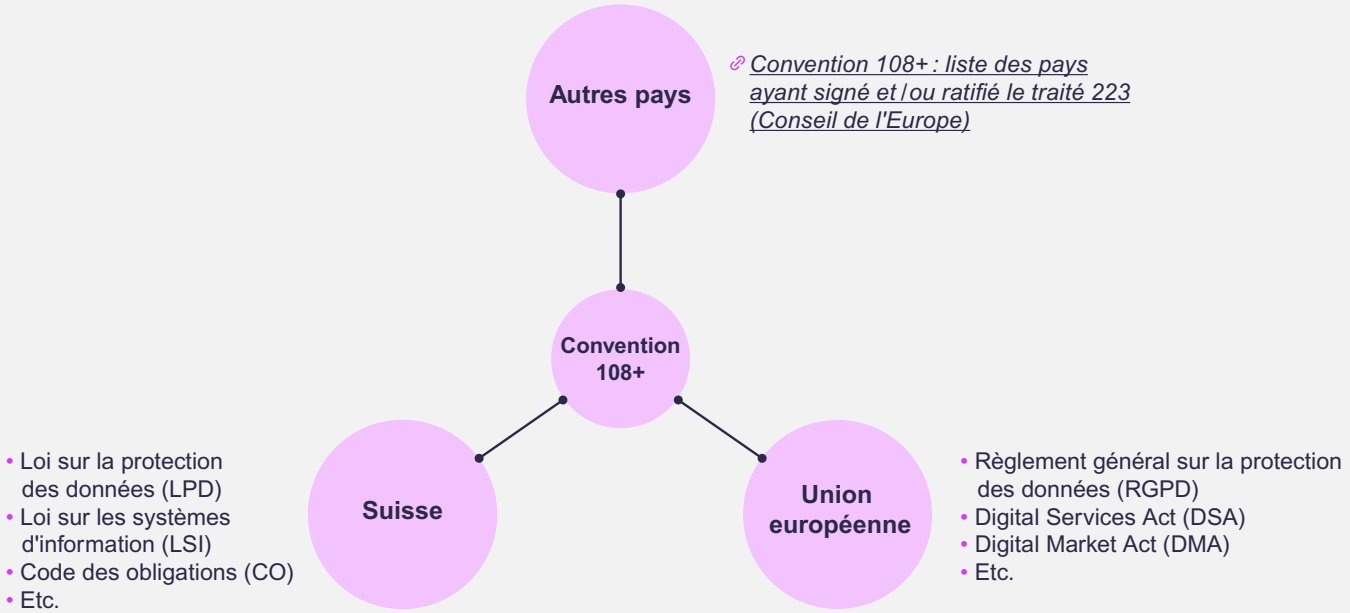
Toutes les entreprises actives en Suisse ou déployant des effets en Suisse sont concernées et ont l'obligation de se mettre en conformité sans délai avec les nouvelles dispositions de protection des données.

La Suisse et la Convention 108+

Bien que la Suisse ne soit pas membre de l'Union européenne, elle a signé la Convention 108+, s'engageant ainsi à adopter des pratiques similaires à celles des autres États ayant ratifié cette convention en matière de traitement des données personnelles.

La Convention 108+ est un traité établi par le Conseil de l'Europe et portant sur la protection des données des individus dans le cadre du traitement automatisé de leurs données personnelles. Elle a pour objectif de définir les lignes directrices de la protection des données afin d'assurer le respect des droits et libertés des personnes, notamment en ce qui concerne leur vie privée lors de l'utilisation de leurs informations.

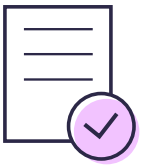
La Convention 108 a été introduite en 1981 et fut le premier instrument international juridiquement contraignant. Une mise à jour a eu lieu en 2018 sous l'appellation Convention 108+. Cette mise à jour renforce les droits des individus et modernise les principes de protection des données à l'ère numérique, notamment par une protection accrue face aux risques liés aux traitements automatisés. La Convention 108+ est ouverte aux États qui ne sont pas membres du Conseil de l'Europe. Elle déploie ainsi ses effets en dehors de l'Europe.



Convention 108+ : liste des pays ayant signé et / ou ratifié le traité 223 (Conseil de l'Europe)

La nécessité de respecter les cadres réglementaires concernant la protection des données personnelles

Dans le plupart des pays, les réglementations relatives à la protection des données ont été conçues pour sauvegarder les intérêts tant des individus que des entreprises contre les conséquences préjudiciables d'une utilisation non régulée des informations personnelles. Ces réglementations n'encadrent pas seulement l'usage des données pour garantir les droits des personnes mais établissent plus largement des principes et des bonnes pratiques en matière de collecte, de traitement et de gestion des données. Ainsi, elles assurent aux entreprises et aux personnes ayant à traiter des données, le maintien de la confidentialité et une exploitation sécurisée et éthique des informations. En Suisse, il est à noter que la LPD protège les personnes physiques mais pas les personnes morales.



La mise en conformité avec les réglementations sur la protection des données est essentielle non seulement pour éviter les risques juridiques, mais également pour assurer un développement et une exploitation pérenne de l'activité. La confiance numérique est un enjeu stratégique pour les entreprises permettant de se différencier sur leur marché, de conserver et développer la confiance de leur clientèle et d'assurer la prospérité de l'activité.

Les infractions peuvent coûter cher !
Selon le pays concerné, la gravité des faits et la réglementation, les amendes peuvent être importantes, allant de quelques milliers de francs à plusieurs millions de francs.

En Suisse, les sanctions de la LPD concernent les personnes physiques avec un plafond de CHF 250'000.-. Si aucun auteur ne peut être trouvé avec des efforts proportionnés, la LPD prévoit une obligation d'amende subsidiaire pour les entreprises à hauteur de maximum CHF 50'000.-.

Des peines beaucoup plus lourdes sont appliquées dans l'Union européenne; le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial.

« La loi sur la protection des données introduit de nouvelles obligations pour les entreprises, mais elle s'annonce également comme un vecteur d'opportunités économiques inédites, propices à l'innovation et à la croissance sectorielle. »

Dessislava Leclère, Maître d'enseignement
à la Haute École de Gestion de Genève

La nécessité de respecter les cadres règlementaires concernant la protection des données personnelles

Se mettre en conformité représente également de nombreuses opportunités pour les entreprises :

- Investir dans la protection des données, c'est investir dans la cyber-sécurité de son entreprise. En allouant les ressources adéquates à la sécurité des données et des systèmes d'informations, les entreprises renforcent leur résistance face aux menaces et risques liés au numérique.
- En garantissant la confidentialité, l'intégrité et la disponibilité des données, l'entreprise renforce et développe sa réputation et la confiance auprès de sa clientèle, de ses partenaires et de ses équipes.
- Se mettre en conformité permet à une entreprise de se protéger des conséquences pouvant entrainer une perte de confiance au sein de l'organisation, de sa clientèle ou des partenaires, telles qu'une mauvaise publicité et une couverture médiatique négative, des difficultés de recrutement et une baisse d'attractivité si l'entreprise est perçue comme négligente en matière de sécurité, d'éthique et de confidentialité.
- En se conformant aux cadres réglementaires et en anticipant les risques liés à la protection des données, l'entreprise peut ainsi maintenir l'accès au marché et en développer de nouveaux. Elle évite le risque d'être exclue des marchés publics exigeants des garanties de conformité avec les réglementations et pratiques de protection des données.
- Adopter une démarche responsable et transparente vis-à-vis de ses parties prenantes permet à l'entreprise de promouvoir ses actions et ses valeurs et ainsi se démarquer de la concurrence.
- En mettant en place des mesures adéquates de gestion des risques numériques, l'entreprise évite les risques financiers. Ces risques peuvent être les suivants : des amendes pouvant être élevées, des coûts liés à la réparation des dommages subis par les parties prenantes, des coûts liés à la mise en place de mesures correctives après un incident, une augmentation des primes d'assurance, une baisse de la valeur des actifs telles que la base de données clients si elle est dérobée, etc.
- Différents risques opérationnels et techniques peuvent survenir, entrainant une interruption de tout ou partie de l'activité, des impacts sur la bonne marche opérationnelle et des affaires de l'entreprise et une augmentation des risques de cyber-attaques si des actions préventives et normatives ne sont pas mises en place.
- L'entreprise évite une exposition à des risques judiciaires et contractuels si elle respecte les cadres réglementaires en vigueur, tels que des risques de poursuite judiciaire de la part de la clientèle, des partenaires ou même de gouvernements, ainsi que des restrictions ou des interdictions potentielles de traiter certaines données. Ainsi, elle endosse également la responsabilité du bon respect du cadre réglementaire par ses sous-traitants. Elle doit donc veiller à la bonne application des lois pour elle-même et ses sous-traitants.

Préposés à la protection des données

Le Préposé cantonal à la protection des données et à la transparence (PPDT) surveille l'application de la loi cantonale en matière de protection des données et de transparence. À Genève, il s'agit de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), qui s'applique au secteur public genevois.

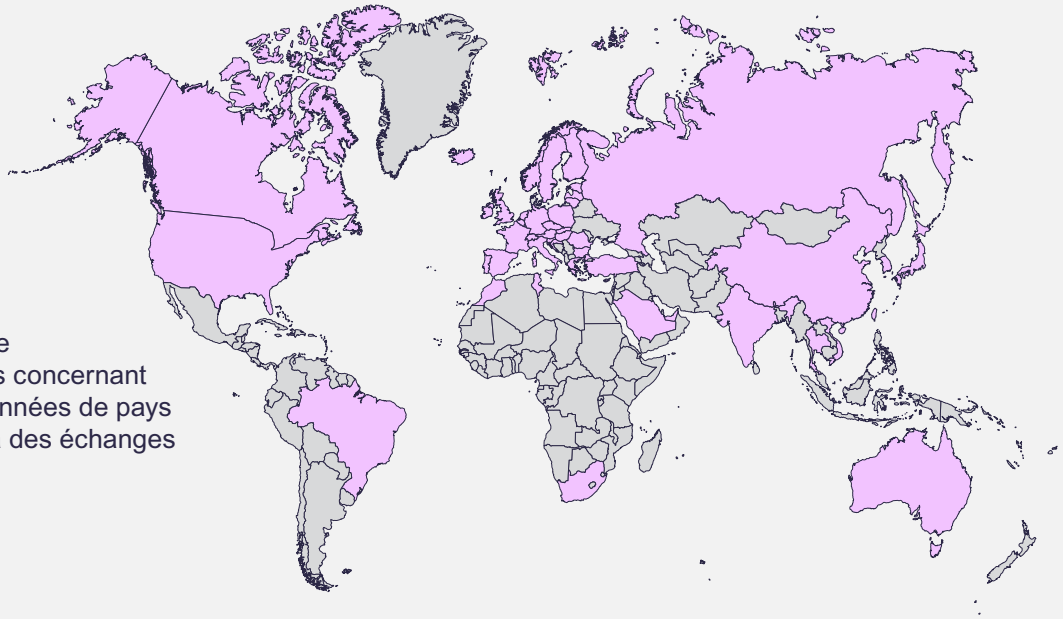
Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est chargé de surveiller la bonne application des dispositions fédérales de protection des données. Il surveille notamment le traitement des données effectué par les entreprises. Il est également l'organe de médiation pour l'accès aux documents officiels.

Les cadres réglementaires dans le monde

Alors que de nombreuses données sont quotidiennement échangées en ligne, la nécessité de préserver la vie privée et de garantir la sécurité des données apparait de plus en plus comme importante au sein de nombreux pays.

Selon la Conférence des Nations Unies sur le Commerce et le Développement (CNUCED), fin 2021, 137 pays sur 194 avaient mis en place une réglementation directe ou indirecte pour protéger les données et la vie privée.

Liste non-exhaustive des réglementations concernant la protection des données de pays avec qui la Suisse a des échanges commerciaux



Suisse	Loi sur la protection des données (LPD) / Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) / Nuova legge sulla protezione dei dati (LPD)	2023
Union européenne	Règlement général sur la protection des données (RGPD)	2018
Royaume-Uni	UK General Data Protection Regulation	2021
Norvège	Personvernforordningen GDPR	2021
Islande	Almenna persónuverndarreglugerði	2018
Turquie	Kişisel verilerin korunmasi kanunu	2016
États-Unis	Lois spécifiques par État	2020
Canada	Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)	2020
Brésil	Lei Geral de Proteção de Dados Pessoais	2020
Tunisie	Loi sur la protection des données à caractère personnel	2004
Maroc	Loi relative à la protection des données des personnes physiques à l'égard des traitements des données à caractère personnel	2009
Afrique du Sud	The Protection of Personal Information Act (POPIA)	2020
Emirats arabes unis	القانون الاتحادي بشأن حماية البيانات الشخصية	2021
Russie	О персональных данных	2006
Inde	Information Technology Act	2020
Chine	Personal information protection law (PIPL)	2021
Hong Kong	Personal Data (Privacy) Ordinance	1996
Japon	個人情報の保護に関する法律	2017
Corée du Sud	개인정보 보호법	2011
Taïwan	Personal Data Protection Act	2015
Singapour	Personal Data Protection Act	2012
Thaïlande	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	2019
Vietnam	Nghị định bảo vệ dữ liệu cá nhân (Nghị định BVDLCN)	2023
Australie	Privacy Act	1988

Obligations relatives aux différentes réglementations liées à la protection des données

États dans lesquels un niveau de protection adéquat des données est garanti	Évaluation du niveau de protection adéquat incluant les transferts des données. *Ordonnance sur la protection des données (OPDo)*
Obligation d'information	Toutes les entreprises ont l'obligation de communiquer de manière claire et transparente aux personnes et/ou entités concernées, les finalités, sources et méthodes de traitement des données personnelles.
Registre des activités	Les entreprises sont tenues de maintenir à jour un registre de leurs activités, recensant toutes les opérations de traitement des données personnelles.
Analyse d'impact	Selon la catégorie de données traitées par les entreprises, celles-ci doivent effectuer une analyse d'impact sur les risques d'un traitement de données personnelles pour garantir leur protection.
Consentement en cas de traitement de données sensibles	Selon le type de traitement et de données traitées, les entreprises doivent obtenir le consentement explicite et éclairé des personnes dont elles traitent des données.
Notification de cas de violations de données	Les entreprises sont contraintes d'informer les autorités et éventuellement les personnes concernées en cas d'une faille de sécurité entraînant l'accès, la divulgation ou la perte de données personnelles.
Privacy by design/by default	Les entreprises doivent intégrer la protection des données dès la conception d'un produit ou d'un service (privacy by design). De plus, les paramétrages par défaut des services ou des logiciels doivent garantir le plus haut niveau de confidentialité et de sécurité sans intervention de l'utilisateur (privacy by default).
Présence d'un délégué à la protection des données	Les entreprises sont tenues de nommer une personne responsable de la protection des données personnelles (délégué à la protection des données) afin de veiller au respect des réglementations en vigueur.
Sanctions	Les entreprises sont sujettes à des sanctions en cas de violation des lois sur la protection des données.
Droit à la transparence pour les personnes	Les entreprises doivent informer les individus sur la manière dont leurs données personnelles sont collectées, utilisées et partagées.
Droit d'accès	Les entreprises sont dans l'obligation de fournir aux personnes qui le leur demandent une copie de leurs données personnelles qu'elles détiennent.
Droit de rectification	Les entreprises sont tenues de corriger ou mettre à jour les informations personnelles inexactes ou incomplètes qu'elles détiennent à la demande d'un individu.
Droit d'effacement	Les entreprises ont l'obligation de supprimer les données personnelles des individus qui le leur demandent.
Droit de limitation du traitement	Dans certaines circonstances spécifiques, les entreprises doivent restreindre temporairement le traitement des données d'une personne si celle-ci le leur demande.
Droit de portabilité	Les entreprises ont l'obligation de transmettre aux individus qui le leur demandent leurs données personnelles dans un format couramment utilisé et de les transférer à une autre entreprise si demandé.
Droit d'opposition	Les entreprises doivent permettre aux individus de s'opposer au traitement de leurs données personnelles pour des motifs légitimes.
Droit de ne pas faire l'objet d'une décision entièrement automatisée	Les individus peuvent exiger des entreprises qu'un traitement automatisé de leurs données débouchant sur une décision fasse l'objet d'une révision par un individu.

Tableau comparatif

	Suisse	Union européenne	Royaume-Uni	Norvège	Islande	Türkiye	États-Unis	Canada	Brésil	Tunisie	Maroc	Afrique du Sud	Émirats arabes unis	Russie	Inde	Chine	Hong Kong	Japon	Corée du Sud	Taïwan	Singapour	Thaïlande	Vietnam	Australie
États dans lesquels un niveau de protection adéquat des données est garanti **(Lien ici)**	●	●	●	●	●			●																
Obligation d'information	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●
Registre des activités	●	●	●	●	●	●	○	●	●	●	●	●							○			○	●	
Analyse d'impact	●	●	●	●	●	○	○	●	●			●	○	○	○	●							●	
Consentement pour le traitement de données sensibles	●	●	●	●	●	●	○	●	●	●	●	●	●	●		●	○	●	●	●	●	●	●	●
Notification en cas de violations de données	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●	●	●	●
Privacy by design/by default	●	●	●	●	●	○	○	●	○														●	
Présence d'un délégué à la protection des données	○	●	●	●	●	○	○	●	●	○	○	●	○	○	○	●			●		●	○	○	
Sanctions	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Droit à la transparence pour les personnes	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
Droit d'accès	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Droit de rectification	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Droit d'effacement	●	●	●	●	●	●	○	●	●	●	○	●	●	●	○	○	○	●	●	○	○	●	●	○
Droit de limitation du traitement	●	●	●	●	●	●	○	●	●	●		●	●			●		○	●			●	●	
Droit de portabilité	●	●	●	●	●		○		●	●			●			●			●			●	●	
Droit d'opposition	●	●	●	●	●	●	○	●	●	●	●	●	●		●	●	○	○	●		●	●	●	
Droit de ne pas faire l'objet d'une décision entièrement automatisée	●	●	●	●	●	○	○	●	●	●		○	●	○		○			●					

● = *Oui*
○ = *Oui dans certains cas, états ou provinces. Toujours se référer à la réglementation en vigueur.*

Ces informations sont données à titre indicatif. Il convient de toujours s'assurer des informations en lisant la réglementation en vigueur dans le pays concerné.

Étapes pour une gestion optimale des données et de la conformité réglementaire

Identifier les marchés dans lesquels l'entreprise est active. Il convient tout d'abord de lister les pays, régions ou états dans lesquels l'entreprise est active. Il faut ensuite identifier les types d'activités commerciales ou de gestion qu'opère l'entreprise dans ces régions et voir si elles sont soumises à la réglementation en vigueur.

Lire et comprendre les réglementations en vigueur dans les pays dans lesquels l'entreprise est active. Les cadres réglementaires varient selon les régions et le type d'activités des entreprises. Il est indispensable de se renseigner sur les réglementations en vigueur dans les pays dans lesquels l'entreprise est active afin d'être en conformité avec les lois en vigueur.

Collecter uniquement les données nécessaires. Il faut s'assurer que le traitement des données est licite et minimiser au strict nécessaire la collecte de données en se limitant à la finalité du traitement convenu par l'entreprise et annoncé lors de la collecte de données. Il est également nécessaire de préciser combien de temps ces informations devront être conservées.

Inventorier et cartographier les données détenues par l'entreprise. Cet état des lieux permet d'identifier les éventuelles informations dont l'entreprise ne devrait pas disposer afin de se mettre en conformité et d'appliquer le traitement requis de ces données.

Gérer le cycle de vie des données. Il est important de déterminer combien de temps les données collectées ou produites seront nécessaires et convenir d'une date de suppression des données. Lorsque les données ne sont plus nécessaires au regard des finalités du traitement, elles doivent être détruites ou anonymisées.

Développer et appliquer une politique de transparence dans le traitement des données. Tout comme lors de la collecte des données, il est indispensable d'être transparent concernant les données détenues, l'objectif de leur traitement et leur utilisation prévue par l'entreprise ou ses partenaires.

Protéger les données. Il est important de mettre en place toutes les mesures nécessaires pour protéger les données détenues et gérées par l'entreprise. Cela concerne notamment des mesures techniques et la formation de toute personne ayant accès aux données.

Pour plus d'informations, référez-vous au guide cyberrisques.

Genève, canton pionnier en matière de droit à l'intégrité numérique
Le 18 juin 2023, les genevoises et genevois ont accepté à 94.21% la modification de la constitution de la République et canton de Genève afin d'introduire un droit fondamental visant à protéger l'intégrité numérique des citoyennes et des citoyens, principalement dans le cadre de leurs relations avec les administrations publiques.

Impressum

Les guides « Entreprises & Numérique » ont été élaborés sous l'impulsion du Département de l'économie et de l'emploi (DEE) de l'État de Genève.

Ils sont destinés aux entreprises pour les accompagner dans leur transition et transformation numériques. Les contenus ont été rédigés dans un objectif de vulgarisation et d'accessibilité au plus grand nombre. Ces guides constituent une base d'information pour les entreprises. L'évolution rapide et continue des technologies ainsi que des cadres réglementaires impliquent de se référer aux informations les plus récentes disponibles sur Internet ou dans la littérature, et également aux spécialistes du domaine concerné et d'y faire appel pour être accompagné ou conseillé.

Ces guides sont publiés sous licence Creative Commons afin que d'autres contributrices et contributeurs continuent de les faire évoluer et également encourager leur diffusion et leur utilisation. L'ensemble des contenus de ces guides est publié sous réserve d'erreurs ou de modifications.

Remerciements en particulier aux personnes suivantes pour leurs contributions à la réalisation de ces guides :

Ciarán Bryce, Haute École de Gestion de Genève

Nicolas Bongard, État de Genève

Michel Deriaz, Haute École de Gestion de Genève

Alexie Duarte Da Silva, Haute École de Gestion de Genève

Alexandre Epalle, État de Genève

Arnaud Gaudinat, Haute École de Gestion de Genève

Michael Kleiner, État de Genève

Dimitri Konstantas, Université de Genève

Dessislava Leclère, Haute École de Gestion de Genève

Julien Levallois, Université de Genève

Eric Ménétré, Université de Genève

Jean-Henry Morin, Université de Genève

Anne Nicole, État de Genève

Laurent Niggeler, État de Genève

Pascal Oehrli, État de Genève

Athanasios Priftis, Haute École de Gestion de Genève

Jean-Philippe Trabichet, Haute École de Gestion de Genève

Stéphane Werly, État de Genève

Responsables du projet et rédaction :

Samuel Mellot, État de Genève

Célia Rütsche, État de Genève

Direction artistique :

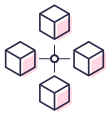
Mostra Communication visuelle

Découvrez l'ensemble des guides Entreprises & Numérique

Responsabilité numérique des entreprises (RNE)

Cyber-risques

Intelligence Artificielle (IA)



Blockchain

Open Data

Réglementations relatives à la protection des données dans le monde

Commerce et numérique *(Prochainement disponible)*

Consultez les guides sur https://entreprisesetnumerique.ge.ch