SWITZERLAND GLOBAL ENTERPRISE

Règlement européen sur la protection des données (RGPD)

Contexte

Le Règlement général de l'Union européenne sur la protection des données (RGPD, (UE) 2016/679) est entré en vigueur le 25 mai 2018. Bien qu'il s'agisse d'un règlement européen, il s'applique également aux entreprises suisses dans certaines circonstances.

La loi suisse sur la protection des données (LPD) est elle aussi en cours de révision et sera alignée sur le droit européen. La LPD suisse devrait entrer en vigueur en 2019 au plus tôt.

La présente notice fournit une vue d'ensemble des aspects du RGPD applicables aux entreprises suisses et des mesures que celles-ci doivent prendre. Elle est conçue comme un outil d'assistance et ne prétend pas être exhaustive; une analyse individuelle de chaque entreprise concernée est indispensable.

À qui s'applique le RGPD?

Le RGPD concerne **tout traitement de données à caractère personnel** (collecte, conservation, effacement, anonymisation, transmission, etc., collectivement «traitement») réalisé par une entreprise suisse si celle-ci

- **possède un établissement dans l'UE**, qu'il s'agisse d'une succursale, d'une agence, d'un bureau de représentation local ou d'une filiale, et que l'établissement n'agit pas indépendamment mais pour le compte de la société mère en Suisse, qui traite des données se rapportant à des personnes physiques dans l'UE. Par exemple: une succursale en France vend des produits ou des services pour le compte du siège en Suisse en utilisant les noms et adresses des clients finaux et ou des contacts de l'acheteur en France;
- **ne possède pas de succursale dans l'UE**, mais propose des biens ou des services dans l'UE. Par exemple: une entreprise en Suisse distribue des biens ou fournit des prestations en Allemagne via une plateforme en ligne ou propose à des clients dans l'UE des logiciels en tant que services (SaaS) ou observe le comportement de personnes établies dans l'UE (exemple: le site web d'une firme suisse utilise des cookies permettant d'observer le comportement des visiteurs du site et d'analyser les données recueillies).

Principes relatifs au traitement des données à caractère personnel du RGPD

Le traitement de données doit être effectué en conformité avec les principes suivants:

- **Licéité:**

  Les données personnelles ne peuvent être traitées que conformément à la législation et en toute bonne foi (droit, contrat, consentement, intérêt légitime, etc.).

- **Limitation des finalités:**

  Les données personnelles doivent être collectées pour des fins déterminées, explicites et légitimes et ne doivent pas être traitées ultérieurement de manière incompatible avec ces fins.

- **Transparence:**

  La collecte de données à caractère personnel et, en particulier, la finalité de leur traitement doivent être reconnaissables et compréhensibles pour la personne concernée. Le sous-traitant doit activement informer les personnes concernées du traitement de leurs données personnelles. Les personnes concernées disposent d'un droit d'information.

- **Exactitude des données:**

  Tout acteur qui traite des données à caractère personnel doit en permanence s'assurer de leur exactitude et de leur actualité.

- **Minimisation des données et limitation de la conservation:**

  Le traitement doit être approprié et limité à la mesure nécessaire aux fins du traitement.
  La durée de conservation doit être définie de façon que les données ne soient stockées que le temps nécessaire pour la finalité du traitement (mise en œuvre de procédures d'archivage et d'effacement).

- **Intégrité et confidentialité:**

  Les données à caractère personnel doivent toujours être protégées par des mesures de sécurité adéquates (notamment des mesures techniques et organisationnelles appropriées contre l'accès non autorisé ou illicite et contre la perte, la destruction ou les dommages accidentels) lors de leur traitement.

- **Responsabilité:**

  Le sous-traitant chargé du traitement des données est responsable du respect des principes susmentionnés et doit pouvoir le démontrer.

Quelles mesures organisationnelles et opérationnelles faut-il prendre?

Les entreprises suisses soumises au RGPD mais n'ayant pas de succursale dans l'UE doivent désigner un représentant local dans l'UE[1]. Dans certains cas[2], un délégué à la protection des données doit aussi être désigné.
Les entreprises soumises au RGPD doivent satisfaire à de nombreuses exigences. En premier lieu, elle doivent publier des directives, modèles et autres documents destinés à garantir que les exigences suivantes sont remplies (liste non exhaustive):

- les activités nécessaire à la mise en œuvre des exigences doivent être organisées et documentées (p.ex. organisation de la protection des données, établissement de règlements et d'instructions, formation des collaborateurs);
- les entreprises doivent tenir un registre des activités de traitement[3] des données à caractère personnel effectuées sous leur responsabilité
- les personnes concernées doivent être informées de points prédéterminés avant le début du traitement des données (en particulier via une charte de confidentialité);
- la période de conservation des données à caractère personnel doit être déterminée à l'avance et les données doivent être supprimées dès la fin de leur traitement, lorsque la période de conservation a expiré et, dans certaines circonstances et sous réserve d'obligations de conservation, à la demande des personnes concernées;
- en cas de violation des données, le responsable du traitement doit informer, sans délai et au plus tard 72 heures après en avoir pris connaissance, l'autorité de protection des données concernée si cette violation entraîne un risque pour les droits et libertés des personnes concernées. En cas de risque élevé, la personne concernée doit également en être informée;
- avant tout traitement de données risqué, il convient d'effectuer une analyse d'impact relative à la protection des données;
- les personnes concernées ont différents droits sur leurs données personnelles (p.ex. droit d'accès ou à l'effacement), auxquels il faut généralement donner suite dans un délai d'un mois, ce qui exige de prendre des mesures internes appropriées;
- il faut conclure avec les prestataires («sous-traitants») qui traitent des données personnelles des conventions contractuelles par écrit;
- avant tout transfert de données à caractère personnel vers un pays hors d'Europe/de l'EEE ou hors de Suisse, il faut veiller à ce que le pays en question bénéficie d'un niveau élevé de protection. Si ce n'est pas le cas, des mesures appropriées doivent être prises (p.ex. signature de contrats de protection des données).

1 Les exceptions à cette disposition sont énumérées à l'article 27.2 du RGPD.

2 Voir l'article 37 du RGPD.

3 L'article 30.5 du RGPD prévoit des exceptions à cette disposition pour les entreprises de moins de 250 salariés.

Conséquences en cas de non-respect du RGPD

En cas de non-respect du RGPD de l'UE, les entreprises encourent les conséquences suivantes:

- Les autorités européennes peuvent infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d’une entreprise, jusqu’à 4% du chiffre d'affaires annuel mondial.
- Les contrats exigent le respect de la législation applicable en général ou de la protection des données en particulier. En présence d’un contrat, le non-respect du RGPD peut entraîner des pénalités contractuelles, une résiliation anticipée, des actions en dommages-intérêts et la perte de certains droits.
- De nos jours, les violations peuvent être très répandues, en particulier chez les entreprises de renom, qui traitent des données sensibles, ont déjà enfreint la réglementation ou travaillent dans des domaines exposés. Ces violations peuvent entraîner aussi des atteintes à leur réputation.

RGPD : Mesures recommandées par S-GE – nouvelles dispositions

Traitement des données des cartes de visite

Traitement des données des cartes de visite lorsque celles-ci sont:

- déposées dans une boîte de collecte (lors de salons/manifestations dans l'UE)
- remises directement à une entreprise (en main propre)

Les informations figurant sur les cartes de visite sont des données à caractère personnel. Celles-ci doivent donc être traitées conformément au règlement. Le traitement est considéré comme étant juridiquement valable s'il est fondé sur la législation, le consentement ou une raison justifiée (p.ex. l'intérêt légitime du responsable du traitement).

Pour ce qui est du traitement des données personnelles figurant sur les cartes de visite, il n'y a pas encore de pratique établie et il faut considérer chaque cas individuellement.

Cependant, dans la plupart des cas, on peut supposer que l'entreprise qui reçoit des cartes de visite sur un salon peut faire valoir un intérêt légitime à traiter ces données et que les participants à la manifestation s'attendent normalement à ce que leurs cartes de visite soient utilisées à cet effet.

Une information simple (à la réception de la carte de visite, p.ex. sur une fiche signalétique ou lors du premier contact avec la personne) est donc en principe suffisante; un consentement explicite n'est généralement pas nécessaire. L'information peut s'énoncer comme suit:

> *Nous vous informons que [nom de la société / destinataire de la carte de visite] enregistrera dans son système informatique les données personnelles figurant sur votre carte de visite. Ces données se limitent à votre nom, votre fonction, votre adresse électronique et votre numéro de téléphone.*
>
> *Vos données seront conservées afin que nous puissions rester en contact avec vous et vous tenir au courant de nos activités. Veuillez nous informer si vous ne souhaitez pas recevoir d'actualités, d'invitations ou de newsletters de notre part.*
>
> *Nous ne transmettrons pas vos données à caractère personnel à des tiers.*

Pour une plus large utilisation des données (p.ex. la transmission à des tiers), un consentement devra être obtenu. Le consentement n'est valable que s'il a été donné en toute connaissance de cause. Une vérification est donc recommandée dans chaque cas.

Dans le cas d'une transmission des données à des tiers, le consentement pourrait être donné selon l'exemple ci-après. Le consentement doit, le cas échéant, être donné par le porteur de la carte de visite en cochant une case (soit sur une fiche signalétique, avec signature, ou lors du premier contact, mais dans tous les cas avant le transmission des données):

☐ *J'accepte que [nom de l'entreprise / destinataire de la carte] transmette à des tiers mes données personnelles (nom, fonction, e-mail, adresse postale, numéro téléphonique), à des fins de marketing dans les domaines suivants: [liste].*

Vous pouvez retirer votre consentement à tout moment et demander la suppression de vos données personnelles. Pour cela, veuillez nous écrire à [adresse e-mail].

Questions importante que toute PME suisse devrait se poser

- **Une PME suisse doit-elle désigner un délégué à la protection des données?**

  D'après l'article 37 du RGPD, un délégué à la protection des données doit être désigné, si

  a) Les **activités de base de l'entreprise** consiste en des opérations de traitement qui, du fait de leur nature, portée ou finalité, exigent un **suivi régulier et systématique** des personnes concernées, ou

  b) Les **activités de base de l'entreprise** consiste en un **traitement à grande échelle de catégories particulières de données** (c.-à-d. des données à caractère personnel indiquant l'origine raciale et ethnique, les opinions politiques, la religion, les convictions philosophiques ou l'appartenance syndicale ainsi que des données génétiques ou biométriques permettant l'identification précise d'une personne physique, des données relatives à la santé, la vie ou l'orientation sexuelle d'une personne physique**)** ou de données relatives à des condamnations pénales et à des infractions.

  Les critères guidant la décision de désigner un délégué à la protection des données ne sont pas clairement définis; il faut donc analyser les activités effectives de l'entreprise ainsi que les activités de traitement de données mises en place.

- **Quelles sont les conditions supplémentaires à remplir par une PME suisse pour ne pas encourir de sanctions?**

  Il n'y a pas de réponse catégorique à cette question, car l'ampleur des mesures de protection des données dépend du traitement individuel des données à caractère personnel. Chaque entreprise doit donc être considérée au cas par cas.

  Dans tous les cas, il faut tenir compte des considérations suivantes:

  - Dans le traitement de données, observez les principes suivants:
    - ✓ licéité et bonne foi
    - ✓ limitation des finalités
    - ✓ transparence
    - ✓ exactitude des données
    - ✓ minimisation des données et limitation de la conservation
    - ✓ intégrité et confidentialité
    - ✓ responsabilité

- Adoptez une bonne gouvernance d'entreprise
  - ✓ Vous devez connaître vos processus internes et procéder avec systématique pour vous acquitter de vos obligations en matière d'information et d'accès à tout moment
  - ✓ Coopérez étroitement avec votre service informatique
  - ✓ Accordez des autorisations et restrictions d'accès
  - ✓ Formez vos collaborateurs et publiez des instructions internes
  - ✓ Définissez les responsabilités en matière de protection des données et de la vie privée

- Etablissez une charte de protection des données
- Vérifiez si vous devez désigner un représentant dans l'Union européenne en vertu de l'article 27 du RGPD.
- Assurez-vous qu'en cas de violation de la protection des données, vous êtes en mesure de respecter le délai de 72 heures pour la signaler à l'autorité de surveillance
- Établissez un répertoire des activités de traitement conformément à l'article 30 du RGPD
- Prenez les mesures techniques et organisationnelles nécessaires pour respecter les principes de protection des données («Privacy by design / Privacy by default»).
- Vérifiez si vous devez désigner un délégué à la protection des données.

Pour de plus amples renseignement, rendez-vous sur www.s-ge-com/fr/exporthelp ou écrivez-nous à suisse-romande@s-ge.com ou appelez-nous au 021 545 94 94.