Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Aide-mémoire

Règlement général de l'UE sur la protection des données (RGPD) - Aide-mémoire à l'usage des petites et moyennes entreprises

1. Contexte

Le nouveau Règlement général de l'UE sur la protection des données (RGPD) entre en vigueur le 25 mai 2018, en remplacement de la Directive du 24 octobre 1995. Le RGPD a pour but d'élever et d'uniformiser le niveau de protection des données dans l'Union européenne (UE) et l'Espace économique européen (EEE), afin de mieux répondre aux exigences de la numérisation de l'économie et de la société et de renforcer ainsi la confiance dans le marché unique européen du numérique. S'agissant d'un règlement, il est directement applicable dans les Etats membres de l'UE. Néanmoins, chaque Etat membre édicte encore des lois d'exécution.

Le RGPD a également des conséquences directes sur un grand nombre d'entreprises suisses, et cela indépendamment de la façon dont sera conçue la loi révisée sur la protection des données (LPD), dont délibère actuellement le Parlement et qui entrera en vigueur en 2019 au plus tôt. La LPD veut cependant aussi, dans la mesure du possible, transposer le niveau européen de protection des données de manière telle que l'UE continue de reconnaître la Suisse comme un Etat tiers disposant d'un niveau approprié de protection des données et que les flux transfrontières de données restent ainsi (facilement) possibles. Dans ce sens, certaines entreprises suisses – même si elles ne sont pas liées à l'Europe – se verront tôt ou tard confrontées à des normes « européennes » de protection des données.

Bien que le RGPD soit fondé sur les mêmes principes que la directive qu'il remplace (licéité, loyauté, transparence, limitation des finalités, exactitude, etc.), les droits et obligations des personnes et entreprises concernées s'en trouvent considérablement étendus. Si le champ d'application matériel[1] reste inchangé, le champ d'application territorial est plus large que dans la directive et s'étend aussi, sous certaines conditions, au traitement de données à l'extérieur de l'UE (extraterritorialité).

2. Quelles sont les entreprises suisses concernées ?

En accord avec la jurisprudence de la Cour européenne de justice relative aux moteurs de recherche (Google), le RGPD étend le champ d'application territorial selon le critère du lieu où se tient le marché (marché cible), ce qui peut entraîner une application extraterritoriale.

De ce fait, le droit européen de la protection des données devient applicable aux entreprises suisses dans les situations suivantes (cf. article 3 RGPD) :

- **Critère de l'établissement :** le traitement des données est effectué par une entreprise (ou un tiers mandaté) dans le cadre de l'activité d'un établissement ayant son siège à l'intérieur de l'UE, que le traitement ait effectivement lieu ou non dans l'UE.

  Exemples :

  - Une entreprise suisse a une filiale dans l'UE. Du moment que la société mère a accès aux données personnelles, le RGPD s'applique.
  - Une entreprise suisse ayant une filiale dans l'UE traite des données personnelles dans le cadre de l'organisation informatique centrale en Suisse.

[1] Aux termes de l'article 2, le RGPD s'applique au traitement (relevé, saisie, classement, enregistrement, modification, transmission, etc.) de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel (personnes physiques identifiées ou identifiables) contenues ou appelées à figurer dans un fichier. Sont notamment exceptées les activités strictement personnelles et domestiques.

- **Critère du ciblage :** le traitement des données par une entreprise (ou un tiers mandaté) non établie dans l'UE se rapporte à des personnes qui se trouvent dans l'UE, à condition que

  a) les activités de traitement soient liées à l'offre de biens ou de services à ces personnes, dans l'UE, contre paiement ou gratuitement ;

  b) le comportement de ces personnes dans l'UE soit surveillé.

  Exemples :

  - Un magasin suisse en ligne traite des données personnelles de clients qui résident dans l'UE.
  - Un hôtel, en Suisse, offre à ses clients – de Suisse et de l'UE – un système de réservation via un site internet.

Les entreprises suisses qui ne possèdent pas de succursale dans l'UE, qui ne proposent pas de biens ou de services à des personnes ayant un établissement dans l'UE ou dont le comportement n'est pas non plus surveillé, ne tombent donc pas sous le coup du RGPD.

La simple possibilité d'accéder au site internet d'une entreprise suisse n'est pas un indice de l'intention de l'entreprise d'offrir dans l'UE des biens ou services. Si, par exemple, des offres en euros sont formulées ou que l'offre s'adresse manifestement à des personnes qui sont dans l'UE, l'entreprise est en revanche soumise au RGPD.

Pour qu'une entreprise suisse puisse déterminer si elle entre ou non dans le champ d'application du RGPD, il peut lui être utile de répondre aux questions suivantes :

- L'entreprise dispose-t-elle d'un établissement ou d'une filiale dans l'UE ?
- L'entreprise traite-t-elle des données de ressortissants de pays membres de l'UE (données clients en tous genres, données utilisées par les visiteurs du site internet ou les utilisateurs d'une application) ?
- L'entreprise offre-t-elle des biens et services à des personnes qui sont dans l'UE ?
- L'entreprise exploite-t-elle une plateforme de commandes en ligne à l'intention de personnes qui sont dans l'UE ?
- L'entreprise traite-t-elle des données pour une entreprise de l'UE ?

Si l'entreprise répond par l'affirmative à l'une ou à plusieurs de ces questions, il est très probable qu'elle entre dans le champ d'application du RGPD.

3. A quelles règles les entreprises concernées sont-elles astreintes ?

Les entreprises suisses qui tombent sous le coup du RGPD doivent notamment tenir compte des règles suivantes :

Les **principes relatifs au traitement des données** sont définis à l'article 5 :

- **Licéité :** le traitement de données à caractère personnel doit être fondé sur le consentement de la personne concernée ou reposer sur une autre base légale.
- **Loyauté :** le traitement des données doit être effectué de manière loyale et digne de confiance.
- **Transparence :** le traitement des données doit être transparent pour la personne concernée.
- **Limitation des finalités :** le traitement des données doit être effectué pour des finalités déterminées, explicites et légitimes.
- **Minimisation des données :** les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

- **Exactitude :** les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour.
- **Limitation de la conservation :** les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
- **Intégrité et confidentialité :** les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée.
- **Responsabilité :** les entreprises sont responsables de l'observation de ces principes et en mesure de démontrer qu'ils sont respectés.

Ces principes sont commentés concrètement dans de nombreux articles et dans des notes explicatives.

Il importe en premier lieu de respecter le principe de la **licéité** : selon les articles 6 ss, le traitement n'est licite que si au moins une des conditions suivantes est remplie :

a) la personne concernée a expressément consenti au traitement de ses données à caractère personnel ;

b) le traitement est nécessaire à la conclusion ou à l'exécution d'un contrat ;

c) le traitement est nécessaire au respect d'une obligation légale ;

d) le traitement est nécessaire à la sauvegarde d'intérêts légitimes et les intérêts de la personne concernée ne prévalent pas (sauvegarde des intérêts vitaux).

Un consentement exprès est clairement requis. Il est toujours lié à une finalité déterminée. Un accord tacite ne suffit pas. Un consentement exprès implique par ex. une notification ou l'action consistant à cocher une case. Pour le traitement de données sensibles (affiliation religieuse ou politique, données biométriques), un consentement exprès est toujours indispensable. La personne concernée doit pouvoir retirer son consentement à tout moment. La personne concernée doit être informée de son droit de retirer son consentement avant de le donner. La conclusion d'un contrat ne peut pas dépendre du traitement d'autres données.

Des prescriptions particulières sont applicables au consentement des enfants (article 8) et au traitement portant sur des catégories particulières de données à caractère personnel (articles 9 à 11).

Il faut en outre tenir compte des **droits et obligations** des personnes concernées suivants :

- **Devoir d'information :** lorsque des données à caractère personnel sont collectées auprès de la personne concernée, celle-ci doit en être informée de manière exhaustive (cf. articles 13 et 14).
- **Droit d'accès :** la personne concernée a le droit d'obtenir la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, d'obtenir des informations complètes notamment sur la durée de conservation des données, leur source, le droit d'introduire une réclamation, etc. (cf. article 15).
- **Droit de rectification, droit à l'effacement et à la limitation du traitement :** la personne concernée a le droit de faire rectifier les données inexactes (cf. article 16), d'obtenir dans certaines conditions leur effacement (cf. article 17) ou la limitation du traitement (cf. article 18).
- **Droit à la portabilité des données :** la personne concernée a le droit de recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et elle a le droit de transmettre ces données à un tiers (cf. article 20).
- **Droit d'opposition :** la personne concernée a le droit de s'opposer à un traitement des données à caractère personnel la concernant (cf. article 21).

Par ailleurs, les dispositions suivantes du RGPD sont particulièrement importantes pour les entreprises suisses :

- **Protection des données dès la conception et protection des données par défaut :** des mesures techniques et organisationnelles appropriées doivent être prises afin de mettre en œuvre les principes relatifs à la protection des données dès la conception et à la protection des données par défaut (cf. article 25). Dès la phase de planification du traitement des données (via le système informatique), le risque d'atteinte à la personnalité doit être réduit, par ex. au moyen d'une anonymisation standardisée. Seules doivent être traitées de manière standardisée les données personnelles requises par la finalité spécifique à laquelle le traitement est ordonné.
- **Registre des activités de traitement :** les entreprises doivent tenir un registre des activités de traitement des données (devoir de documentation, cf. article 30). Ce registre doit permettre une vue d'ensemble des procédures et processus dans lesquels sont traitées des données à caractère personnel. L'obligation ne s'applique pas aux entreprises qui occupent moins de 250 collaborateurs, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et libertés des personnes concernées.
- **Sécurité du traitement :** le traitement des données doit répondre à certaines exigences en matière de protection des données et des mesures de sécurité sont requises, telles que la pseudonymisation, le chiffrement, etc. (cf. article 32).
- **Analyse d'impact relative à la protection des données :** lorsqu'un type de traitement est susceptible d'engendrer un risque élevé, une analyse de l'impact des opérations de traitement doit être effectuée (cf. article 35 s.). Elle est notamment requise lorsque l'opération consiste en une évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.
- **Désignation du délégué à la protection des données et d'un représentant dans l'UE :** lorsque l'activité principale d'une entreprise implique la surveillance régulière et systématique de personnes ou concerne des catégories particulières de données, elle doit désigner un délégué à la protection des données chargé des tâches et attributions en la matière (cf. articles 37-39). Les entreprises sans sous-traitant soumises au RGPD sont tenues de désigner un représentant dans l'UE. Cette obligation ne s'applique pas lorsque le traitement est occasionnel, ne porte pas sur des catégories particulières de données et n'est pas susceptible d'engendrer un risque (cf. article 27).
- **Codes de conduite et certification :** les associations peuvent édicter des codes de conduite précisant la manière d'appliquer le règlement général (cf. article 40 s.). Des mécanismes de certification peuvent être mis en place (cf. article 42 s.).
- **Notification obligatoire d'une violation de données :** les violations de données à caractère personnel doivent être dénoncées dans un délai de 72 heures aux autorités nationales de surveillance compétentes, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques (cf. article 33). Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé, le responsable du traitement doit communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais (cf. article 34).

4. Quelles sont les suites en cas d'infraction ?

Le RGPD prévoit une série de pouvoirs d'enquête (exigences en matière d'information, audits concernant la protection des données, perquisitions, etc.) de même que le pouvoir d'adopter des mesures correctrices (avertissements, publication de communiqués officiels, limitation temporaire ou définitive du traitement, etc. ; cf. article 58).

Les autorités nationales de surveillance compétentes peuvent également sanctionner les infractions au RGPD sous la forme d'amendes administratives qui soient effectives, proportionnées et dissuasives (cf.

article 83). Selon le genre d'infraction et les circonstances à prendre en considération, ces amendes peuvent s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent.

Le RGPD régit également l'entraide judiciaire entre les Etats membres de l'UE (cf. article 61) et permet l'entraide judiciaire au profit d'Etats tiers (cf. article 50). L'entraide judiciaire internationale avec des Etats tiers doit également être développée dans le cadre de la révision en cours de la LPD. De manière générale, il faut s'attendre à une intensification de la coopération entre la Suisse et l'UE dans le domaine de la protection des données. On peut toutefois se demander si les amendes infligées par les autorités européennes de surveillance à des entreprises en Suisse seront exécutoires.

Il convient également de prêter attention au fait que, le cas échéant, une indemnité doit être versée pour réparer le préjudice subi, même si elle résulte d'une action judiciaire (cf. article 82). En outre, il faut s'attendre à des risques de réputation dans l'éventualité où des violations de la protection des données deviendraient publiques.

5. Qu'est-il recommandé de faire ?

Pour une entreprise suisse tombant sous le coup du RGPD européen, il est notamment recommandé de clarifier ou de régler les aspects suivants :

- Qui assume la responsabilité de la protection des données au sein de l'entreprise ?
- Les collaborateurs de l'entreprise sont-ils sensibilisés ou instruits en matière de protection des données ?
- Quelles données personnelles sont traitées et de quelle manière ? Est-il nécessaire de traiter des données sensibles ?
- Sur quelles dispositions légales (licéité) se base le traitement des données personnelles ?
- Traiter ces données est-il absolument indispensable du point de vue de l'entreprise ou ces données peuvent-elles être effacées ?
- Les dispositions que comportent les contrats de l'entreprise, les conditions générales et les chartes de confidentialité sont-elles conformes aux prescriptions légales en matière de protection des données ?
- L'entreprise est-elle suffisamment informée pour remplir ses obligations en matière de protection des données et pouvoir en fournir la preuve de manière adéquate ?

6. Remarque importante et disclaimer

Le but du présent aide-mémoire est exclusivement d'informer. Il ne constitue pas une liste de contrôle exhaustive et ne saurait tenir lieu d'avis de droit. L'Union suisse des arts et métiers usam décline toute responsabilité qui pourrait lui être imputée du fait de son utilisation ou de toute action ou omission qui s'ensuivrait. Pour tout renseignement complémentaire, elle recommande en outre de s'adresser à l'organisation professionnelle compétente de la branche concernée.

Etat au 16 mars 2018

Responsable du dossier

Dieter Kläy, responsable du dossier
Tél. : 031 380 14 45 ; mél. d.klaey@sgv-usam.ch