Nouveau règlement général européen sur la protection des données (RGPD) – applicabilité et conséquences pour les établissements d'hébergement en Suisse

(état décembre 2017)

---

1. Applicabilité du RGPD pour les entreprises suisses

Le nouveau règlement général sur la protection des données (RGPD) de l'UE entre en vigueur le 25 mai 2018. Il ne s'applique pas uniquement aux entreprises établies dans l'UE, mais, dans certaines circonstances, indirectement aussi aux entreprises suisses. C'est le cas par exemple lorsque ces entreprises ont des clients dans l'UE et qu'elles leur proposent là-bas des marchandises ou des services, ce qui les amènent à traiter des données personnelles (nom, adresse, e-mail, date de naissance, données bancaires, etc.).

Les établissements d'hébergement suisses sont donc tenus d'observer les dispositions du nouveau RGPD s'ils proposent leurs prestations de services (hébergement) à des ressortissants de l'UE au sein de l'UE. L'offre peut notamment être proposée sur le site web de l'hôtel que les ressortissants de l'UE peuvent utiliser pour effectuer leurs réservations. Les entreprises qui proposent leurs services exclusivement en Suisse ne sont pas concernées par ces dispositions.

Au vu de ce qui précède, il est à prévoir que la majorité des établissements hôteliers sera soumise au RGPD, dans la mesure où ces établissements traitent des données personnelles concernant des ressortissants de l'UE.

Le terme « traiter » englobe la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction de données personnelles.

2. Les principes de base du RGPD

- **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.

3. Les principales dispositions du RGPD (extrait)

3.1 Licéité du traitement des données

Le traitement des données (p. ex. collecte pour la première fois de données de clients) n'est licite que si au moins une des conditions suivantes est remplie :

- ⇨ Le traitement des données est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de **mesures précontractuelles** prises à la demande de celle-ci (p. ex. dans le cadre de la conclusion d'un contrat hôtelier ou d'une réservation).

- ⇨ Le traitement des données est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis (p. ex. obligation pour les hôtes de remplir le bulletin d'arrivée).

- ⇨ Le traitement **est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers** (p. ex. publicité directe à d'anciens clients)**,** à moins que ne prévalent les intérêts ou les droits fondamentaux de la personne concernée.

- ⇨ La personne concernée a donné son **consentement** express.

Le **consentement** doit être donné par un acte positif clair (p. ex. en cochant une case). Un consentement tacite ou une check box déjà pourvue d'une coche ou une check box sur laquelle il faut cliquer (option opt-out) ne répondent pas aux exigences.

Le traitement de **données sensibles**, p. ex. concernant la religion, la santé ou les données biométriques (photo, empreinte digitale) requiert toujours un consentement express de la personne concernée.

Lors de plusieurs traitements de données distincts, le consentement doit être donné pour chaque activité de traitement.

La personne concernée peut retirer son consentement à tout moment. Il convient de s'assurer que le consentement peut être retiré aussi simplement qu'il est donné (p. ex. avec un lien de désabonnement dans la newsletter).

Important : la personne concernée doit être informée du droit qu'elle a de retirer son consentement avant de le donner.

Lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment, de s'opposer à ce traitement. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information.

Exemple de formulation :

« Le partenaire contractuel accepte que ses données personnelles (p. ex. nom, adresse e-mail) puissent être stockées et utilisées par l'Hôtel XX pour … (p. ex. l'envoi d'infolettres ou de matériel publicitaire sur les prestations de services de l'Hôtel XX). Ce consentement peut être retiré à tout moment pour … (les coordonnées, l'adresse e-mail) ».

3.2 Droits de la personne concernée et obligations du responsable du traitement des données

- Obligation d'informer

Lorsque des données sont collectées, la personne concernée doit en être informée ; cela vaut aussi pour le cas où les données ne sont pas collectées directement auprès de la personne concernée. Ces informations doivent être fournies d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. La transmission des informations se fait par écrit ou par d'autres moyens, y compris, lorsque c'est approprié, par voie électronique.

Lors d'une réservation via le site web de l'hôtel par exemple, les informations devraient être directement accessibles. Elles peuvent être mises en lien, le cas échéant, sur le document/le site web en question lors de la confirmation de réservation.

Les informations doivent obligatoirement contenir les éléments suivants :

- *Identité et coordonnées du responsable du traitement des données*
- *Coordonnées du délégué à la protection des données (si disponibles)*
- *Les finalités du traitement et la base juridique du traitement*
- *Les intérêts légitimes poursuivis par le responsable du traitement (lorsqu'ils sont mentionnés comme motif du traitement)*
- *Les destinataires ou les catégories de destinataires des données à caractère personnel*
- *L'intention d'effectuer un transfert des données vers un pays tiers ou à une organisation internationale (lorsque cela est prévu)*
- *La durée de conservation des données à caractère personnel*
- *Information sur l'existence d'un droit d'accès aux données, à leur rectification, leur effacement, à une limitation de leur traitement, ou du droit de s'opposer à leur traitement et du droit à la portabilité des données.*
- *Information sur l'existence d'un droit à retirer son consentement à tout moment*
- *Information sur l'existence d'un droit d'introduire une réclamation auprès d'une autorité de contrôle*
- *Information sur la question de savoir si l'exigence de fourniture des données a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat ainsi que sur les conséquences éventuelles de la non-fourniture de ces données.*
- *Le cas échéant : l'existence d'une prise de décision automatisée, y compris un profilage (p. ex. vérification de solvabilité automatisée)*
- *Lorsque les données n'ont pas été collectées auprès de la personne concernée : information sur la provenance des données et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public*
- *Information sur une modification possible de la finalité du traitement des données*

- Droit d'accès

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

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.

o Droit à la portabilité des données

La personne concernée peut demander que le responsable des données (p. ex. établissement hôtelier) lui fournisse, dans un format structuré, couramment utilisé et lisible par machine, les données qu'elle lui a transmis. 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.

o Droit d'opposition

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.

3.3 Autres obligations des responsables du traitement des données (extrait)

o Obligation d'effectuer une analyse d'impact relative à la protection des données

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.). Le traitement usuel des données par les établissements hôteliers ne devrait en principe pas comporter un tel risque.

o Protection des données dès la conception et protection des données 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.

- Obligations 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 USA);
- 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.

4. Conséquences possibles en cas de violation des obligations : amendes élevées

L'UE menace d'infliger des amendes lourdes. Pour des infractions simples, comme la violation des obligations du responsable du traitement des données, des amendes jusqu'à 10 millions d'euros ou 2% du chiffres d'affaires mondial de l'année précédente sont infligées. En cas de violations graves, les amendes peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'année précédente.

5. Protection des données en Suisse

La loi sur la protection des données en Suisse fait actuellement l'objet d'une révision. De nombreuses dispositions du RGPD seront reprises telles quelles ou légèrement adaptées. Le nouveau projet de loi doit maintenant être débattu au Parlement. La LPD révisée entrera probablement en vigueur début 2019. Aussi il est conseillé de tenir compte dès à présent des nouvelles règles sur la protection des données.

6. Recommandations sur la manière de procéder

- ☐ Déterminez qui dans votre établissement est/sera responsable de la protection des données.
- ☐ Vérifiez à quelle catégorie de personnes exactement appartiennent les données que vous traitez (hôtes, collaborateurs, fournisseurs, utilisateurs web, etc.), en particulier lorsqu'il s'agit de ressortissants de l'UE.
- ☐ S'agit-il de données sensibles (p. ex. données sur la santé, la religion) ?
- ☐ Vérifiez la base juridique du traitement des données (p. ex. obligation légale, contrat, intérêts légitimes, consentement)

- ☐ Vérifiez si vous avez absolument besoin des données. Si tel n'est pas le cas, effacez-les.
- ☐ Vérifiez vos contrats, CG, déclarations de protection des données au regard de leur compatibilité avec le RGPD.
- ☐ Vérifiez/établissez les procédures/documents afin de pouvoir remplir vos obligations en matière d'information, d'accès, de documentation, de portabilité des données, etc.
- ☐ Vérifiez l'état de la sécurité technique des données.

Autres ressources :

- HOTREC guidelines on the General Data Protection Regulation

- Liste de contrôle utile sur le site de la Chambre autrichienne du commerce

Remarque importante :

Ce mémento renferme une compilation d'informations relatives au nouveau règlement de l'UE sur la protection des données. Il vise à donner un premier aperçu des principales dispositions et sert d'orientation, sans engagement. Les informations ont été réunies avec le plus grand soin, sans garantie toutefois quant à leur exhaustivité, leur exactitude et/ou leur actualité.

hotelleriesuisse / décembre 2017