Suisse Tourisme.

mll

Livre blanc

Protection des données et tourisme

Zurich, 1er février 2018

Suisse Tourisme

www.MySwitzerland.com
Tödistrasse 7 | CH-8027 Zurich

Meyerlustenberger Lachenal SA
Avocats - Attorneys at Law

www.mll-legal.com | www.mll-news.com
Zurich | Genève | Zoug | Lausanne | Bruxelles

Livre blanc sur la protection des données dans le secteur du tourisme

En Europe, la règlementation sur la protection des données fait face à des changements fondamentaux. A l'échelle de l'Union Européenne (UE), le Règlement Général sur la Protection des Données (RGPD) entrera en vigueur le 25 mai 2018. Une révision totale de la loi sur la protection des données (LPD) est également en cours en Suisse. A l'heure actuelle, la question de savoir quels changements concrets la révision apportera et à partir de quand ceux-ci s'appliqueront est encore incertaine.

Néanmoins, une chose est sûre: le législateur suisse s'appuiera en grande partie sur le modèle de l'UE. Les nouveautés affecteront toutes les entreprises et organisations, ainsi que la quasi-totalité des processus opérationnels, toutes branches confondues. Le secteur du tourisme doit ainsi lui aussi faire face à un défi majeur.

Dans ce contexte, le présent Livre blanc expose dans un premier temps en quoi l'entrée en vigueur du RGPD est d'ores et déjà pertinente pour les entreprises et les organisations de la branche touristique suisse. Dans un deuxième temps, il présente les thèmes centraux et les prescriptions ainsi que la nécessité pour la branche touristique d'agir.

Suisse Tourisme.

mll

Table des matières

I. La protection des données concerne la quasi-totalité des opérations commerciales!

L'expérience montre que les entreprises n'ont fréquemment pas conscience de la mesure dans laquelle les règles relatives à la protection des données affectent leurs activités quotidiennes.

> La législation relative à la protection des données s'applique à toute transaction commerciale impliquant des données personnelles.

L'énumération des «traitements» concernés donne déjà un aperçu de la portée du règlement. Selon la définition légale, les traitements concernés englobent notamment les suivants: «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».

→ **Exemple:**

La législation relative à la protection des données ne concerne donc pas seulement les cas où les coordonnées du client d'un hôtel sont communiquées à un office du tourisme; **elle s'applique également aux processus strictement internes**, p. ex. lorsque le client d'un hôtel est attribué à un certain segment de clientèle dans la base de données interne.

En outre, la condition en vertu de laquelle il doit s'agir de «données à caractère personnel» ne restreint pas autant le champ d'application que ce l'on pourrait - à tort - penser. L'information concernée doit certes pouvoir être attribuée à une personne (physique) déterminée. Cependant, ceci comprend aussi les données pseudonymisées. Ainsi par exemple, lorsque les données personnelles (nom, adresse, etc.) d'un client sont remplacées par un numéro dans une base de données, les données de commande pour ce numéro gardent leur qualité de données personnelles si une personne au sein de l'entreprise ou même un tiers peut être en mesure d'identifier le client en question sur la base du numéro. Il en résulte que l'exploitation de sites internet ne respecte souvent pas la protection des données.

→ **Exemple:**

Si un utilisateur recherche des informations sur le site internet de Suisse Tourisme pour ses prochaines vacances en Suisse, il laisse une trace avec un grand nombre d'informations techniques (notamment son adresse IP) du seul fait d'avoir consulté la page d'accueil. Ces informations sont (automatiquement) enregistrées sur le serveur du site internet et doivent être traitées comme des données à caractère personnel, comme confirmé par la jurisprudence, et ce même si l'utilisateur ne communique pas ou n'a pas encore communiqué son nom.

.

II. En quoi le RGPD concerne-t-il les entreprises suisses?

Deux des nouveautés les plus importantes par rapport à la législation en vigueur jusqu'en mai 2018 soulignent la pertinence du RGPD pour les entreprises suisses. Premièrement, une violation de la réglementation entraîne le risque de se voir imposer une amende administrative allant jusqu'à plusieurs millions. Deuxièmement, le RGPD a un champ d'application qui s'étend bien au-delà des frontières du marché intérieur de l'UE.

1. Durcissement drastique des sanctions en cas de violation des dispositions relatives à la protection des données

S'agissant des responsables du traitement, la législation actuelle a déjà fait l'objet de critiques du fait que les sanctions pour violation de la réglementation relative à la protection des données n'étaient pas suffisamment dissuasives. En conséquence, les entreprises étaient peu incitées à entreprendre les mesures nécessaires aux fins de se conformer à la réglementation en matière de protection des données.

Avec l'entrée en vigueur du RGPD, la donne va radicalement changer:

> À l'avenir, **les sanctions administratives en cas de manquement au RGPD peuvent s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.**

Le barème des amendes a été considérablement rehaussé ainsi qu'uniformisé dans toute l'UE. Le plafond «alternatif» de la sanction dépend de la valeur la plus élevée des deux valeurs (soit 20 millions d'euros ou 4% du chiffre d'affaires). À l'heure actuelle, il est difficile d'estimer dans quelle mesure les autorités de surveillance compétentes auront recours à cette «échelle de sanctions» et à quelle fréquence ces sanctions seront appliquées. Cela étant, combinés aux risques réputationnels existants, la perspective de sanctions administratives représente une incitation importante à se conformer à la réglementation en matière de protection des données.

Par ailleurs, les personnes concernées par le traitement de leurs données disposent également de différents moyens afin de faire valoir leurs droits par la voie civile. Elles peuvent ainsi notamment obtenir une interdiction judiciaire de certaines actions et, selon les circonstances, réclamer des dommages et intérêts. En Allemagne notamment, les infractions aux dispositions relatives à la protection des données peuvent entraîner un avertissement, suivi le cas échéant par une procédure judiciaire subséquente. Les décisions judiciaires rendues dans ce cadre à l'encontre d'entreprises en Suisse sont généralement exécutoires sans autre formalité. Enfin, les législations nationales des États membres prévoient des sanctions pénales pour certains manquements à la réglementation en matière de protection des données.

2. Quand le RGPD s'applique-t-il aux entreprises suisses?

Au vu du risque significatif encouru en cas de manquement au RGPD, la question se pose tout d'abord de savoir à qui ce règlement s'applique. Différents cas de figure peuvent servir à clarifier ce point. Comme le montrent les exemples suivants, le champ d'application du règlement est volontairement très large:

> Le RGPD ne concerne **pas seulement le traitement des données au sein de l'UE.** La réglementation s'applique en effet **à de nombreuses entreprises n'ayant pas de succursale dans l'UE.**

Un nombre plus important d'entreprises et d'organisations de la branche touristique suisse est concerné par le RGPD, par rapport à d'autres règles UE. Il est peu surprenant de constater qu'un grand nombre d'entreprises n'a pas encore conscience du fait que le RGPD leur est également applicable.

a. Les entreprises touristiques suisses ayant une succursale dans l'UE

Un premier cas de figure concerne les cas où l'application du RGPD ne semble à priori pas surprenante.

Les entreprises dont le siège est situé en Suisse doivent respecter le RGPD dès lors qu'elles disposent d'une succursale dans l'UE et qu'elles traitent des données à caractère personnel dans le cadre de leurs activités.

La notion de succursale inclut notamment les sociétés filles. Ainsi par exemple, si la société mère assume la fonction RH pour sa succursale située dans l'UE et que, dans ce cadre, elle traite les données des collaborateurs de cette succursale, le RGPD s'applique.

Il convient de noter que le terme «succursale» doit être compris de façon large. Sont notamment inclus les simples succursales, les départements ou les «établissements permanents».

→ **Exemple:**

Les représentations dans l'UE de Suisse Tourisme peuvent également être considérées comme des succursales. Le RGPD s'applique donc au traitement des données par ces représentations dans l'UE.

b. Les entreprises touristiques suisses n'ayant pas de succursale dans l'UE

En sus des cas précités avec une succursale dans l'UE, trois autres cas de figure existent dans lesquels **des entreprises suisses n'ayant aucun établissement dans l'UE tombent dans le champ d'application du RGPD**. Ces cas illustrent la portée des futures règles, qui s'étend bien au-delà des frontières de l'UE. Les deux premiers cas concernent principalement des états de fait avec une composante en ligne.

1. Offre de biens et de services à des clients dans l'UE

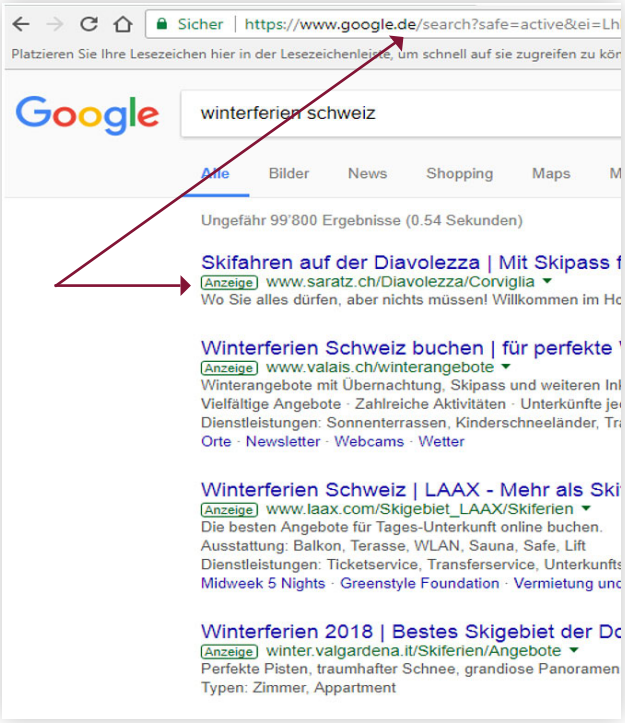
Sont également concernées par la législation UE relative à la protection des données les entreprises suisses qui proposent leurs biens ou services à des clients situés dans l'UE et qui traitent des données à caractère personnel dans ce cadre.

Le fait d'«offrir des biens ou services» doit être compris uniquement comme une «offre manifestement proposée» à des clients situés dans l'UE. Ainsi par exemple, une société de chemin de fer de montagne suisse ne devrait pas déjà être soumise au RGPD du seul fait que des personnes situées dans l'UE ont la possibilité de commander des forfaits de ski en ligne. Néanmoins, le point de savoir si une offre s'adresse (également) à des personnes situées dans l'UE sera déterminé sur la base de critères qui, dans d'autres domaines juridiques, sont interprétés de façon très large. Le critère déterminant sera celui de savoir si la société de chemin de fer de montagne déploie volontairement et de manière ciblée des efforts pour attraire des clients potentiels domiciliés dans l'UE.

Si tel est le cas, l'offre est alors réputée s'adresser aux clients de l'UE et ces derniers pourront faire valoir leurs droits en vertu du RGPD en cas de traitement de leurs données personnelles par la société de chemin de fer.

→ **Exemple:**

Une entreprise qui offre aux visiteurs de son site internet l'option de choisir «son pays» dans une menu déroulante s'adresse à tout le moins aussi aux clients des pays figurant dans une telle liste. Dans l'exemple de Suisse Tourisme, le RGPD s'applique de ce fait.



Le fait de fournir l'indication supplémentaire des prix en euros ou les frais d'expédition vers des pays membres de l'UE constituent un élément clairement en faveur d'une telle intention. Si une offre cible des clients de l'UE par le biais d'une publicité en ligne (p. ex. via des campagnes d'AdWords ciblées géographiquement), il s'agit d'une preuve évidente de ce que l'offre publiée s'adresse aux clients sur le territoire concerné. Dans un tel cas de figure, le traitement des données en lien avec l'offre doit respecter les dispositions du RGPD.

→ **Exemple:**

Celui qui réserve des annonces pour les mots-clés «Vacances d'hiver Suisse» sur google.de, destine son offre en particulier à des clients allemands.
Le RGPD devrait donc s'appliquer aux prestataires suivants, dans la mesure où d'autres aspects ne s'opposent pas manifestement à une application transfrontalière:

En raison du large champ d'application du RGPD, **les offres gratuites** tombent également sous le coup du règlement. Partant, même les opérateurs de sites web purement informatifs, tels que p. ex. les sites web de la plupart des destinations touristiques et des communes, sont soumis au RGPD lorsque le site web concerné s'adresse (également) à des personnes situées dans l'UE. Les critères principaux pour déterminer à quel public le site web s'adresse sont notamment les langues dans lesquelles le site web est disponible, le domaine de premier niveau (Top Level Domain) ou l'indication de l'indicatif international. Toute forme de marketing en ligne dans des marchés de l'UE constitue notamment une preuve claire d'orientation vers l'UE.

2. Observation du comportement des personnes dans l'UE

L'application du RGPD n'est pas limitée à l'offre de biens et de services ; elle s'étend également

au simple fait d'observer le comportement de personnes situées dans l'UE.

Sur cette base, le RGPD vise principalement les états de fait impliquant internet. Sont notamment compris les traitement de données permettant d'observer le comportement de personnes situées dans l'UE, essentiellement à des fins publicitaires.

Partant, le RGPD s'applique à toutes les méthodes de «User/Customer Tracking», en particulier celles qui utilisent des cookies.

→ **Exemple:**

Si une organisation de tourisme emploie des outils d'analyse sur son site web pour analyser les visites ainsi que le comportement de clic (tel que par ex. Google Analytics), il y a lieu de considérer qu'elle est soumise au RGPD.

3. Engager/mandater une entreprise de l'UE

Une entreprise suisse sans succursale dans l'UE peut également être soumise au RGPD si elle entretient des «liens de sous-traitance de données». Ceci est pertinent lorsqu'une entreprise suisse mandate une autre entreprise ou un tiers quelconque afin de traiter les données propres de l'entreprise suisse (p. ex. les données de ses collaborateurs ou de ses clients) à ses propres fins.

→ **Exemple:**

Si une entreprise suisse a recours aux services d'un fournisseur de services cloud ayant une succursale dans l'UE, p. ex. pour sauvegarder des données personnelles, le RGPD s'applique. Il en va de même lorsqu'une entreprise suisse traite des données personnelles pour le compte d'une entreprise de l'UE. Si p. ex. le traitement centralisé des données d'une chaîne hôtelière est effectué par une entreprise suisse mais pour le compte d'hôtels appartenant à la chaîne et situés dans l'UE, les dispositions du RGPD doivent être respectées.

Dans les cas susmentionnés de sous-traitance de traitement des données, l'applicabilité du RGPD, respectivement la portée de son application peut être difficile à déterminer dans le cas d'espèce. De tels cas requièrent un examen minutieux des traitements de données envisagés.

III. Quelles règles s'appliquent désormais au traitement des données personnelles, p. ex. au traitement des données de clients?

Le RGPD et la révision totale actuelle de la législation suisse sur la protection des données entraînent des changements significatifs en lien avec le traitement des données personnelles. Il est vraisemblable que la nouvelle loi suisse sur la protection des données (LPD) aille moins loin que le RGPD sur plusieurs points.

Néanmoins, en raison du champ d'application très large du RGPD, très peu d'entreprises de la branche touristique suisse, voire aucune, échapperont au règlement UE. Par conséquent, d'éventuelles différences entre la LPD révisée et le RGPD ne concerneront en réalité que peu d'entreprises suisses. Partant, les développements suivants se concentreront sur les règles du RGPD qui entreront en vigueur le 25 mai 2018.

1. En principe, le traitement de données personnelles est interdit, sauf si...

Un concept central du point de vue des entreprises suisses est celui de l' **«interdiction soumise à autorisation»**. Une autorisation suppose l'existence d'un fondement légitime.

Tout traitement de données personnelles est interdit.

Un traitement de données, p. ex. de données clients, est licite seulement si l'entreprise peut se fonder sur un fondement légitime.

Selon le RGPD, les fondements légitimes sont les suivants:

- **«consentement»**: le traitement est licite s'il repose sur le consentement de la personne concernée. Cela étant, les conditions pour obtenir un consentement valable sont significativement plus élevées qu'auparavant et ne correspondent pas à la pratique prévalant jusque là en Suisse en matière de consentements (cf. ci-dessous).
- **«contrat»**: le traitement de données peut être licite s'il est nécessaire à l'exécution d'un contrat conclu avec la personne concernée. Ainsi, un hôtel peut traiter les données personnelles de ses clients si ce traitement est nécessaire à l'organisation et à la facturation du séjour des clients de l'hôtel.
- **«loi»**: le traitement de données est licite s'il est nécessaire à l'exécution d'une obligation légale (p. ex. obligation de conservation des données). Il convient de noter que les lois suisses ne sont pas couvertes par cette base de traitement. Ce nonobstant, en cas d'obligation légale suisse, un intérêt prédominant devra en principe exister (cf. point ci-dessous).
- **«intérêt prépondérant»**: un traitement de données peut être licite s'il est nécessaire à la préservation d'un intérêt légitime de l'entreprise. L'intérêt de l'entreprise doit l'emporter sur celui de la personne concernée, ce qui suppose une détermination au cas par cas, en particulier en cas de simples intérêts économiques à la mise en œuvre de mesures de publicité par exemple.

2. Principes de base de tout traitement des données conforme au droit

En soi, l'existence d'un fondement légitime de traitement des données ne signifie pas encore que le traitement est conforme aux exigences du RGPD. Encore faut-il que les principes fondamentaux de traitement des données soient respectés. Ces principes existent déjà sous le droit actuel de l'UE et de la Suisse. Toutefois, sous le nouveau régime, ces principes sont renforcés et, de façon importante, leur violation est désormais assortie de sanctions.

Les principes suivants méritent d'être soulignés:

- **Principe de finalité**: les données à caractère personnel ne peuvent être collectées et traitées que pour des finalités clairement définies.
- **Principe de transparence**: le traitement des données et les finalités pour lesquelles les données sont utilisées doivent pouvoir être comprises par la personne concernée dès le moment de leur collecte.
- **Principe de minimisation des données**: seules les données nécessaires à la finalité définie peuvent être collectées. Aucune donnée ne peut être conservée ni traitée ultérieurement.
- **Limitation de sauveguarde des données**: les données à caractère personnel ne peuvent être conservées que le temps nécessaire à la réalisation du traitement défini. Lorsque la finalité est atteinte, les données personnelles doivent être supprimées.

3. Nouvelles «obligations de diligence» importantes pour le traitement de données

Le RGPD impose de nombreuses nouvelles obligations formelles aux entreprises.

Les principes suivants méritent d'être mentionnés:

- **Registre des activités de traitement**: toute entreprise traitant des données à caractère personnel est désormais tenue de tenir un registre de toutes les activités de traitement pertinentes. Ce registre doit comporter pour chaque processus de traitement tout un ensemble d'informations. Ces informations doivent être documentées et décrites en

détail (p. ex. finalité, responsabilité, type de données, risques spécifiques, etc.).

- **Obligation de preuve**: le RGPD requiert explicitement que le responsable du traitement soit en mesure de prouver à tout moment que les principes de traitement des données sont respectés.
- **Analyse d'impact relative à la protection des données**: lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les personnes concernées, une analyse d'impact de ces risques doit être réalisée et documentée. Cette analyse sera potentiellement requise notamment en cas d'utilisation de nouvelles technologies et de nouveaux processus de traitement des données. L'analyse d'impact consiste en une description du traitement envisagé, d'une analyse du traitement, de la détermination des risques et de l'élaboration d'un plan de mesures visant à réduire les risques identifiés.
- **«Data Breach Notifications»**: une violation des dispositions du RGPD, en particulier l'utilisation abusive de données ou le vol de données, doit, sous certaines conditions, être notifiée à l'autorité de contrôle compétente et aux personnes concernées. La mise en œuvre de cette obligation suppose pour de nombreuses entreprises la mise en place de processus internes documentés. Ces processus supposent notamment de déterminer les cas de figure dans lesquels les employés doivent rapporter une violation et d'identifier la personne responsable à l'interne à qui rapport doit être fait.
- **«Protection des données dès la conception / par défaut»**: le traitement des données doit être structuré de telle sorte que le respect de la protection des données et l'exercice des droits des personnes concernées (droit d'accès, droit de suppression, droit de rectification) soient garantis en tout temps (Privacy by Design). De plus, tout traitement de données doit être paramétré de façon à ce que la configuration par défaut réponde aux exigences du RGPD (Privacy by Default).
- **Désignation d'un représentant**: en principe, les entreprises n'ayant pas de succursale dans l'UE doivent désigner un représentant dans l'UE.

4. Quels sont les droits des personnes dont les données sont traitées («droits des personnes concernées»)

Un traitement des données licite exige que les personnes dont les données sont traitées puissent savoir quelles données les concernant font l'objet d'un traitement et de quelle manière ces données sont traitées. Le RGPD prévoit ainsi des droits des personnes concernées. Une grande partie de ces droits existait déjà sous le régime actuel. Cependant, ces droits ont été étendus et adaptés à plusieurs points de vue.

Les personnes concernées disposent notamment des droits suivants. Elles peuvent les faire valoir à tout moment:

- **Droit d'accès**: les personnes concernées disposent d'un droit d'accès leur permettant de demander à tout moment à l'entreprise des renseignements détaillés sur le traitement des données qui les concernent. Le droit d'accès vaut également pour les employés.
- **Droit de rectification**: en sus de l'obligation générale de l'entreprise responsable du traitement de prendre des mesures pour garantir l'exactitude des données traitées, les personnes concernées peuvent à tout moment exiger la rectification immédiate des données erronées les concernant.
- **Droit à l'effacement des données et droit d'opposition**: sous certaines conditions, les personnes concernées peuvent s'opposer à ce que leur données soient traitées et demander l'effacement de ces données.
- **Portabilité des données**: selon le RGPD, les données collectées doivent être traitées de façon à ce qu'elles puissent être fournies à la personne concernée à tout moment dans un format structuré, courant et lisible par machine.

IV. Principales directives pour la branche du tourisme

La plupart des entreprises de la branche du tourisme procèdent régulièrement à des traitements de données qui entrent dans le champ d'application du RGPD (cf. ci-dessus), nonobstant le fait que le traitement ait lieu en Suisse. Ces traitements de données doivent ainsi être examinés à la lumière du RGPD et, le cas échéant, adaptés. La date butoir est le 25 mai 2018. Dans les développements suivants, quelques questions clés en matière de protection des données dans le secteur du tourisme sont exposées. En outre, les problématiques les plus significatives sont discutées.

1. Transparence du traitement des données

a. Lorsque les données sont collectées directement auprès des clients/ partenaires commerciaux

La première étape de tout processus de traitement des données est la collecte, respectivement l'acquisition de données.

> Selon le RGPD, chaque acquisition de données personnelles est soumise à l'obligation de mettre des informations complètes relatives au traitement des données envisagé activement à la disposition de la personne concernée, soit sans que cela ne doive être sollicité

La liste des informations requises par la loi lorsque des données sont collectées a été considérablement étendue avec le RGPD. Les informations à fournir doivent l'être en «des termes clairs et simples» et «de façon concise» et comprendre les points suivants:

1. Nom et coordonnées du responsable et de son éventuel représentant
2. Coordonnées de l'éventuel délégué à la protection des données
3. Finalités et base juridique du traitement des données
4. Le cas échéant, les intérêts légitimes poursuivis
5. Le cas échéant, le destinataire ou les catégories de destinataires des données personnelles, s'ils existent
6. Le cas échéant, l'intention de transmettre les données vers un pays tiers ou à une organisation internationale
7. Toute autre information utile pour garantir un traitement juste et transparent des données
8. Durée de conservation des données ou critères de fixation de la durée
9. Existence de droits des personnes concernées, tels que le droit d'accès, de rectification, d'effacement, de blocage, d'opposition ou de portabilité des données
10. Existence du droit de retirer son consentement en cas de traitement des données basé sur le consentement
11. Existence du droit d'introduire une réclamation auprès d'une autorité de contrôle
12. Le cas échéant, des informations sur la question de savoir si l'exigence de fourniture des données a été prescrite par la loi ou par contrat ou si elle est nécessaire à la conclusion du contrat
13. Existence d'une prise de décision automatisée, y compris un profilage et des informations utiles concernant la logique sous-jacente, ainsi que l'importance et l'impact escompté d'un tel traitement pour la personne concernée

Ces informations doivent être bien visibles et accessibles à chaque point où des informations à caractère personnel sont recueillies.

C'est le cas en particulier pour tout formulaire de contact ou de commande. Partant, les entreprises doivent établir de nouvelles déclarations de confidentialité comprenant

les informations obligatoires ou réviser leurs déclarations de confidentialité existantes. Les déclarations de confidentialité doivent être facilement accessibles à tout moment, en particulier via les sites internet.

➔ **Exemples:**

Même en cas de collecte de données non électronique, p. ex. en lien avec des formulaires d'inscription, des cartes CRM ou des talons de participation à des jeux-concours, il faut s'assurer de ce que ces informations soient à la disposition des personnes concernées (p. ex. imprimées sur le verso d'une carte CRM).

b. Lorsque des données proviennent de sources tierces

> Même lorsque les données sont collectées auprès de tiers, l'obligation d'information demeure et le même type informations détaillées doit être fourni, à quelques différences près.

La collecte de données auprès de tiers comprend les cas où les données ne sont pas collectées auprès des personnes concernées, mais par exemple auprès de tiers ou dans des sources publiquement disponibles.

➔ **Exemple:**

Dans la branche du tourisme, de telles collectes indirectes ont lieu lorsqu'un hôtel demande à une société de chemin de fer de montagne les coordonnées des clients ayant commandé des forfaits de ski afin de leur proposer des offres d'hébergement.
L'hôtel doit informer le client au moment de la prise de contact de quelles données l'hôtel dispose de quelles sources et pour quelle finalité. Dans cet exemple, la société de chemin de fer de montagne et l'hôtel remplissent tous deux leur obligation d'information. Dans la mesure où la transmission antérieure des données de la société de chemin de fer de montagne à l'hôtel constitue un processus usuel, la société de chemin de fer de montagne peut et devrait déjà indiquer que des données personnelles seront transmises à l'hôtel et indiquer à quelles fins cette transmission aura lieu. Le fait que la société de chemin de fer fournisse une telle information ne libère toutefois pas nécessairement l'hôtel de sa propre obligation d'information. Ceci sera particulièrement le cas si l'hôtel souhaite traiter les données collectées auprès de la société de chemin de fer à d'autres fins.

2. Consentement

Tout traitement de données personnelles doit s'appuyer sur un fondement légitime, sans quoi le traitement est interdit en vertu du RGPD. Le consentement de la personne concernée constitue un fondement clé. Les exigences relatives à la validité d'un consentement ont été considérablement rehaussées avec le RGPD.

> Pour qu'un consentement soit valable, il doit notamment reposer sur une information préalable suffisante et être donné de façon libre et univoque.

Les exigences plus élevées s'appliquent aussi lorsque la personne concernée a donné son consentement avant l'entrée en vigueur du RGPD. Autrement dit, les **«consentements anciens»** ne sont valables que s'ils remplissent les exigences du RGPD. L'une des exigences les plus centrales est celui du caractère libre du consentement. Celui-ci n'est pas donné librement s'il existe un déséquilibre évident entre les services fournis à la personne concernée dans le cadre d'un contrat et le traitement des données auquel la personne concernée consent dans le cadre du contrat.

a. Consentement libre et interdiction de subordonner un contrat au consentement

La question se pose de savoir si, à l'avenir, **une interdiction de subordonner un contrat au consentement** s'appliquera. Une telle interdiction empêcherait de subordonner l'exécution d'un contrat au consentement à des traitements ultérieurs des données qui ne sont pas nécessaires à l'exécution du contrat. Ce ne sont pas les traitements de données nécessaires à l'exécution d'un contrat qui sont visés ici, mais avant tout de l'utilisation des données à des fins publicitaires.

→ **Examples:**

Dans l'exemple susmentionné, cela signifierait que la société de chemin de fer de montagne ne serait pas autorisée à subordonner un forfait de ski au consentement du client à la transmission de ses données personnelles à l'hôtel.

Une interdiction de subordination absolue serait particulièrement problématique pour l'organisation de **jeux-concours**. Ainsi, le fait de soumettre la participation à un jeu-concours à l'octroi du consentement à l'envoi de mails publicitaires (en particulier de newsletters) serait illicite.

Il ne fait aucun doute que de telles subordinations peuvent être problématiques. En attendant une pratique établie par les autorités de contrôle, de telles pratiques comportent des risques et devraient soit être entièrement abandonnées soit, à tout le moins, offrir aux personnes concernées le choix de donner ou non leur consentement.

b. Cases précochées par défaut

Le problème de l'interdiction de subordination est accentué par le fait que les consentements ne sont valables que s'ils sont donnés par un acte positif clair.

> Le silence ou l'inactivité de la personne concernée ne suffit pas.

→ **Exemple:**

Dans l'exemple susmentionné du jeu-concours, le consentement à des fins de marketing/prospection par e-mail ne serait pas valable **s'il est fondé sur une case précochée**. Pour que le consentement soit valable, le participant concerné doit lui-même activement cocher la case par le biais d'un clic. Pour de nombreuses entreprises suisses, cette condition suppose un changement dans la politique de collecte des consentements. La pratique suisse quant à elle autorise de telles cases précochées.

3. Transfert de données

a. Généralités

De façon générale, les organisations du tourisme ont un intérêt considérable au transfert de données entre les acteurs concernés.

> Le transfert de données à des tiers constitue toutefois une «communication par transmission» et, à ce titre, constitue un traitement de données soumis aux prescriptions du RGPD dans la mesure où des données à caractère personnel sont concernées.

Une obligation d'information existe également dans ce cadre. Le transfert lui-même doit être effectué de façon transparente et une explication sur les fins du transfert doit être donnée. De plus, la personne ou l'entité transmettant les données doit pouvoir démontrer qu'un fondement légitime (p. ex. un consentement) pour le transfert existe.

> On ignore souvent que le simple fait **d'accorder l'accès**

aux données constitue déjà un transfert.

Prenons l'exemple de l'entreprise (partenaire) à qui l'on ne transfère pas les données personnelles de façon numérique, mais à qui l'on octroie p. ex. l'accès aux données du système CRM de l'entreprise qui transmet les données (c.à.d. l'hôtel pourrait p. ex. accéder directement aux données du système CRM de la société de chemin der fer de montagne au moyen d'une interface). Outre les questions de protection des données liées au transfert de données personnelles, l'octroi d'accès à des données personnes comporte des risques considérables en matière de sécurité des données.

b. «Tiers»

Dans ce contexte, il est essentiel de savoir qui doit être considéré comme un tiers.

Les entreprises n'ont souvent pas connaissance du fait que les sociétés d'un même groupe ou les membres (juridiquement indépendants) d'une association sont eux aussi des tiers.

Les prescriptions du RGPD doivent être observées aussi en cas de **transfert de données intragroupe**, soit lorsqu'une société fille ou une société sœur se voit accorder un accès à des données personnelles.

c. Sous-traitance de données

Une forme particulière de transmission à des tiers a lieu dans le cadre de la sous-traitance de données personnelles.

Il s'agit de cas dans lesquels le responsable du traitement mandate une autre entreprise aux fins de traiter ses données ou les données qu'il a collectées (p. ex. les données de ses collaborateurs ou de ses clients) en son nom et à ses fins.

Ces cas de figure sont courants et significatifs dans le quotidien des entreprises.

→ **Exemples:**

Des cas d'application fréquents comprennent, par exemple, le recours aux services, respectivement programmes suivants:

- Mailchimp pour l'envoi de newsletters
- Google Analytics pour l'analyse web
- Fournisseurs cloud pour la sauvegarde de données
- Microsoft 365 (solution cloud)
- Chatlio (fonctions de messagerie instantanée sur des sites internet)
- Outils de surveillance des réseaux sociaux (Social Monitoring Tools)
- Salesforce / Microsoft Dynamics (systèmes CRM)
- Hébergeur web (Webhoster)

Un élément essentiel est le fait que le RGPD exige explicitement la conclusion d'un contrat de sous-traitance, lequel peut aussi être établi «sous forme électronique». Dans le contexte en ligne, le contrat peut ainsi être conclu via un site internet. Le contrat doit notamment prévoir des droits d'injonction et de contrôle du responsable du traitement/mandant. En d'autres termes, le mandataire doit s'engager à ne traiter les données que selon les instructions du mandant. Un point important du contrat est celui de savoir si

le mandataire peut lui-même avoir recours à d'autres tiers **(autres sous-traitants)**. En effet, selon le RGPD, une telle autre sous-traitance est soumise à l'autorisation écrite préalable du responsable du traitement/mandant.

→ **Exemple:**

Si une entreprise de tourisme utilise le service «Google Analytics» pour analyser l'utilisation de son site Internet, Google doit être tenu de traiter les données «conformément aux instructions». Google fournit à cet effet un contrat modèle dont la conformité avec le RGPD n'a pas encore été tranchée de manière définitive.

Le mandant ne peut «externaliser» le traitement des données qu'à des entreprises qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme au RGPD. Ceci ne décharge toutefois pas le mandant, lequel demeure dans tous les cas responsable du fait que le traitement sous-traité réponde aux exigences du RGPD. En tout état de cause, de nombreuses obligations du RGPD s'imposent autant aux responsables du traitement qu'aux sous-traitants. De plus, les sanctions prévues par le RGPD peuvent également être infligées au sous-traitant.

d. Transfert à l'étranger

Une attention particulière doit être prêtée à la question de savoir vers quels pays les données sont transférées. La prudence est de mise notamment en cas de transfert vers les États-Unis.

> Les États-Unis n'offrent pas un niveau de protection des données adéquat. Pour cette raison, les données ne peuvent y être transférées sans que des précautions particulières n'aient été prises.

Le mécanisme d'auto-certification pour les entreprises destinataires des données établies aux États-Unis dans le cadre de l'accord «Bouclier de Protection des Données» («Privacy-Shield») reflète cette prudence particulière. Il va sans dire qu'une telle certification n'affecte en rien l'obligation de se conformer aux autres obligations du RGPD (p. ex. les obligations d'information ou de justification de la transmission des données). Dans de nombreux cas de figure, le transfert de données vers les États-Unis a lieu dans le cadre d'une sous-traitance d'un traitement de données. Dans ces cas de figure, ce n'est pas seulement le transfert des données, mais aussi le traitement des données sous-traité qui doit être conforme au RGPD.

Outre la certification «Privacy-Shield», d'autres mesures particulières sont également envisageables. A ce jour, les Clauses Contractuelles Types de la Commission européenne pour le transfert de données à caractère personnel sont considérées comme des mesures suffisantes pour les transferts de données vers les États-Unis. De plus, la plupart des modèles de contrat de sous-traitance de données prévoient déjà les dispositions nécessaires aux fins d'assurer la conformité du transfert des données vers les Etats-Unis et d'autres pays sans niveau de protection des données adéquat.

→ **Exemple:**

Un hôtel qui utilise le pixel Remarketing de Facebook sur son site internet aux fins d'effectuer un marketing personnalisé sur ses réseaux sociaux transmet ce faisant généralement des données personnelles à Facebook, dont le siège est aux États-Unis. Facebook est certifiée «Privacy Shield», si bien qu'aucune garantie supplémentaire n'est requise. Il demeure toutefois incertain - et partant, problématique - de savoir comment un contrat de sous-traitance jugé suffisant peut être conclu avec Facebook.

4. Systèmes CRM

L'entrée en vigueur du RGPD représente un défi de taille aussi pour le traitement de données dans le cadre de la gestion de la clientèle (systèmes CRM). La finalité de ces systèmes consiste notamment dans le

stockage centralisé de toutes les opérations commerciales pertinentes avec les clients individuels.

> C'est précisément la combinaison ou l'association d'une multitude de données provenant de sources diverses qui pose problème du point de vue de la protection des données.

a. Transparence et légalité

En raison de l'obligation d'information et du principe de transparence, les clients doivent être informés de l'association de leurs données ainsi que du stockage centralisé de ceux-ci. Dans ce cadre, la question du motif de justification du traitement se pose également. En effet, un traitement fondé sur une nécessité contractuelle peut certes être envisageable pour ce qui concerne le stockage de données de commande. S'agissant toutefois de l'association de données diverses, elle supposera en principe le consentement du client. Un tel consentement n'est valable que s'il est donné par le client sur la base d'informations suffisantes quant au traitement des données envisagé. Une information claire et complète des clients concernés est ainsi nécessaire en lien avec ces deux aspects.

→ **Exemple:**

L'exploitant d'un site internet permettant de réserver des randonnées sur des glaciers doit informer le client du fait que ses données sont stockées dans une base de données centralisée et qu'elles sont combinées à d'autres informations, telles que par exemple des plaintes concernant un itinéraire de randonnée insatisfaisant. Cette information doit être donnée au moment où le client remplit le formulaire avec ses données client. L'exploitant du site internet doit simultanément obtenir le consentement du client.

> Il est essentiel que les consentements donnés par les clients (y compris le moment où ils sont donnés ainsi que le contenu de la déclaration et des informations données dans le cas particulier) soient documentés et puissent être rapidement consultés en cas de besoin.

b. Principe de finalité et finalités nouvelles

Dans ce contexte, il faut s'assurer que les données existantes ne soient pas traitées à de nouvelles fins, soit des fins qui ne seraient plus couvertes par la finalité initialement communiquée. Ce point peut s'avérer particulièrement problématique en cas de **«données anciennes»**.

> Lorsque des données à caractère personnel doivent être migrées d'une base de données à une autre, il y a toujours lieu de vérifier si une telle migration n'entraîne pas un changement de finalité.

Si tel est le cas, le client concerné doit en être informé. Il doit de plus donner son consentement au traitement de ses données personnelles pour la nouvelle finalité.

Le même problème se pose lorsque de nouvelles informations sont extrapolées de données existantes. Dans le cadre d'**analyses CRM ou Big data**, il peut être difficile de définir à l'avance quels constats concrets pourront en fin de compte être établis. Il convient donc d'accorder un soin particulier à la rédaction des informations, particulièrement en ce qui concerne la finalité du traitement.

➔ **Exemple:**

Si, dans l'exemple précité de la randonnée sur glacier, le fournisseur a exposé dans sa déclaration de confidentialité que les données seraient utilisées pour attribuer un certain «score» aux clients dans le but de leur adresser une publicité personnalisée, ce fournisseur ne pourra étendre l'analyse des données clients aux fins de fixer un prix individualisé. Dans certaines circonstances toutefois, l'analyse peut aussi permettre d'établir des constats en lien avec le prix, de sorte qu'un changement de finalité existerait déjà à ce stade.

La question de savoir comment de telles analyses peuvent être conciliées avec le principe de **minimisation des données** reste incertaine. C'est cependant précisément la production et l'évaluation d'un volume de données le plus important possible qui est décisif pour la pertinence des résultats de l'analyse. Le RGPD exige que, au moment où les données sont collectées, des informations soient fournies quant à la durée de conservation des données ou, «lorsque ce n'est pas possible», sur les critères utilisés pour déterminer cette durée. Il en résulte que les entreprises doivent en tous les cas établir un **concept d'effacement, respectivement de conservation** des données à caractère personnel, y compris pour les systèmes CRM.

c. Droits d'accès et transmission

La réglementation des droits d'accès revêt également une importance particulière dans le cadre de l'utilisation conforme à la protection des données des systèmes CRM.

> Il y a lieu de s'assurer que les collaborateurs ne puissent avoir accès qu'aux données qui sont nécessaires à l'exécution de leurs tâches.

Ce **principe de «Need-to-know»** doit être mis en œuvre par le biais d'un concept d'autorisation en vertu duquel des règles d'accès sont définies pour des utilisateurs ou des groupes d'utilisateurs déterminés.

En plus de cet aspect interne, le choix du système CRM lui-même doit se conformer à certaines exigences de base. En effet, une grande partie de ces systèmes se basent sur une solution cloud dont le fournisseur ou l'hébergeur est établi à l'étranger. Dans ce cas, il convient de respecter les prescriptions relatives au **transfert à l'étranger et à la sous-traitance du traitement des données**.

5. Marketing par e-mail

Pour l'envoi d'e-mails publicitaires et, en particulier, de newsletters, d'autres questions se posent du fait de l'interaction entre la réglementation sur la protection des données et le droit de la concurrence. D'une part, des données à caractère personnel sont régulièrement traitées dans ce cadre. D'autre part, les lois nationales prévoient des règles strictes de protection contre l'envoi de courriers électroniques non sollicités (spam).

> Une particularité en droit suisse est que les infractions à la norme anti-spam sont déjà **passibles de sanctions pénales** selon le droit actuel.

Dans ce contexte, les entreprises doivent accorder une attention particulière au respect des dispositions légales lorsqu'elles se livrent à ces activités de marketing par e-mail.

a. Consentement («opt-in»)

La licéité des emails publicitaires est régulièrement sujette au **consentement** du destinataire.

Comme indiqué précédemment, le consentement n'est valable que s'il repose sur des informations suffisantes concernant le traitement des données donnant lieu à des envois publicitaires. Ces informations doivent ainsi figurer dans la **déclaration de confidentialité** ainsi que de façon visible dans le processus d'enregistrement.

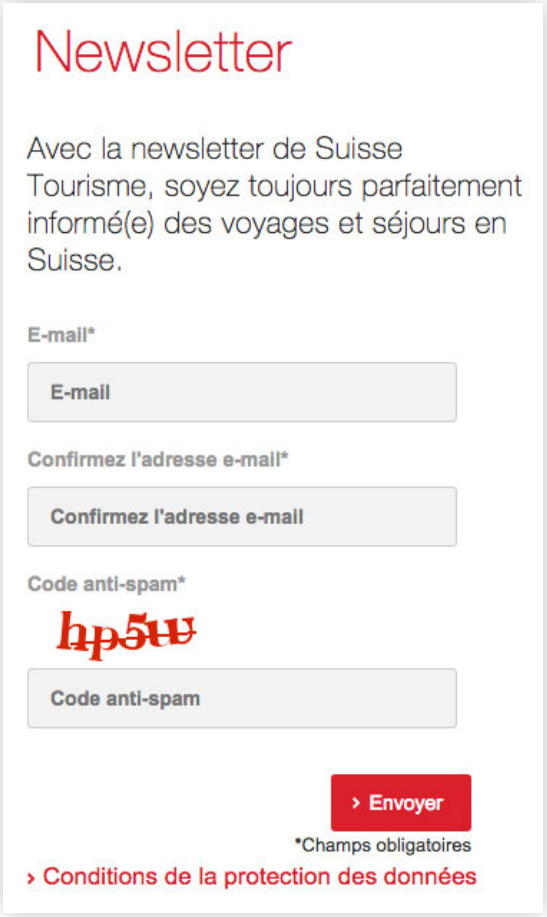
La question se pose également de savoir de quelle manière le consentement de la personne concernée peut être recueilli. Comme expliqué précédemment, les **cases précochées** ne constituent pas un consentement valable selon le RGPD. De plus, il est vivement conseillé aux entreprises de mettre en place un procédé de vérification en deux étapes (**«double opt-in»**) qui est réalisée comme suit :

1. Première étape: dans le cadre de la procédure d'inscription, un premier «opt-in» est demandé à l'utilisateur pour que l'entreprise puisse lui envoyer la newsletter.
2. Deuxième étape: immédiatement après l'inscription, un email de confirmation comportant un lien est envoyé à l'utilisateur (deuxième «opt-in»). Cette étape a lieu avant le premier envoi d'une newsletter.

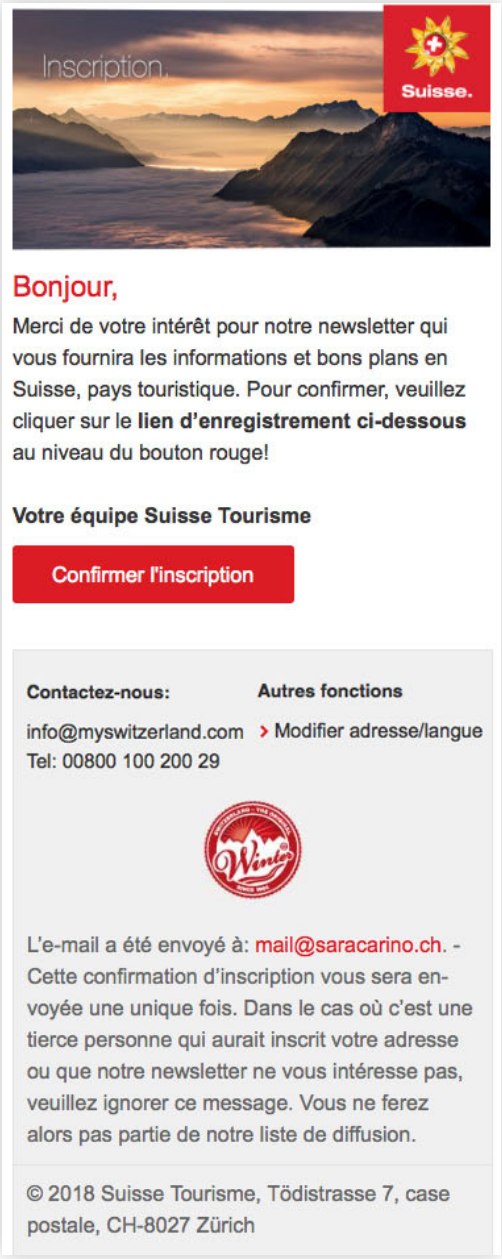
L'avantage de ce procédé est que, grâce au «deuxième opt-in», le consentement obtenu est relativement facile à démontrer.

→ **Exemple:**

Dans l'exemple de la newsletter de Suisse Tourisme, la première étape se présente comme suit:



La deuxième étape du processus de double-opt-in pourrait se dérouler comme suit:



b. Transmission à des tiers et transfert à l'étranger

Pour l'envoi de la newsletter, les entreprises ont souvent recours à des Tools de tiers. Concrètement, selon comment la newsletter est conçue, il peut y avoir un **rapport de sous-traitance de traitement des données.** Dans ce cas, les exigences susmentionnées doivent être respectées, à savoir un contrat prévoyant notamment un droit d'injonction et de contrôle du responsable doit être conclu. A cela s'ajoute que divers fournisseurs, tels que MailChimp, ont leur siège aux Etats-Unis et que les données sont stockées sur ces serveurs. Par conséquent, les exigences (en particulier l'obligation d'information et les garanties requises) relative au **transfert à l'étranger** doivent aussi être respectées.

Des exigences supplémentaires existent également lorsque l'envoi de la newsletter est transfrontalier. Si l'inscription est ouverte à des personnes intéressées de l'étranger, les **réglementations nationales des autres pays concernés** doivent, sous certaines conditions, être respectées également.

Ceci dépend en particulier de la question de savoir si le site internet et l'offre de la newsletter sont également «destinés» aux clients de ces pays, ce qui peut rapidement être le cas. En effet, les critères pertinents sont en substance les mêmes que pour la question de l'applicabilité du RGPD aux entreprises suisses n'ayant pas de succursale dans l'UE (cf. plus haut).

> Partant, les newsletters des entreprises de tourisme suisses sont régulièrement soumises aux prescriptions du droit allemand.

En droit allemand, il suffit qu' un seul email publicitaire soit envoyé sans le consentement de son destinataire pour que l'émetteur reçoive un avertissement à titre de spammer. En outre, une action en cessation peut être intentée à l'encontre de l'émetteur et le remboursement des frais d'avocat peut lui est réclamé. Par conséquent, la conception du processus relatif à une

newsletter doit tenir compte du RGPD mais aussi potentiellement de dispositions légales nationales étrangères.

6. Analyse web/Tracking

Dans le cadre d'un concept marketing, le site internet de l'entreprise joue un rôle essentiel. Pour analyser les visites du site internet, les entreprises ont recours à des services tels que Google Analytics.

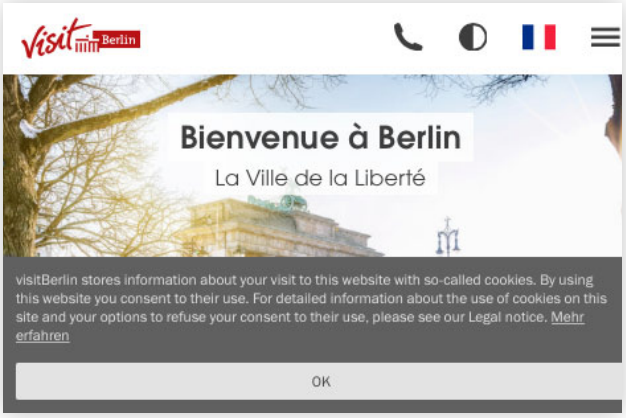
Du point de vue de la protection des données, les différentes exigences susmentionnées doivent être respectées dans ce cadre. Ainsi, comme énoncé dans l'exemple de Google Analytics, les données sont fréquemment transmises à un tiers établi aux Etats-Unis.

> Pour cette raison, les exigences en matière de sous-traitance de traitement de données et de transfert de données dans des pays tiers doivent être respectées. En outre, le recours à de tels services doit être exposé et les traitements qui y sont liés doivent être détaillés afin de satisfaire à l'obligation d'information.

Il est notoire que les Tools d'analyse se basent régulièrement sur l'**utilisation de cookies** ou de technologies similaires, par lesquels le comportement de clic de l'utilisateur peut être suivi sur plusieurs pages web. Selon le droit actuel de l'UE, l'utilisateur doit être informé de la pose de cookies et de leur finalité et son consentement doit être obtenu. En pratique, cette exigence est principalement mise en œuvre par le recours répandu à **des bandeaux cookie**, qui s'affichent lors de la consultation d'un site internet.

→ **Exemple:**

En Allemagne, l'Office du tourisme de Berlin affiche actuellement le bandeau suivant sur son site internet:



source: https://www.visitberlin.de/fr (consulté le 28.1.2018)

Il sied toutefois de noter qu'une directive stricte sur les cookies est prévue au niveau de l'UE, laquelle devra être appliquée en sus du RGPD. Le contenu exact de la directive **ePrivacy** n'est pas encore définitif. Néanmoins, il semblerait que les bandeaux cookie actuels ne suffiront plus sous le nouveau régime. Les développements dans ce cadre doivent être suivis de près.

7. Social Media Monitoring

La plupart des entreprises complètent leur concept marketing avec une présence sur les platformes des médias sociaux pertinents. Sur ces plateformes, des milliers d'utilisateurs s'expriment quotidiennement au sujet de produits et de fournisseurs. Pour de nombreuses entreprises, l'observation et l'analyse des médias sociaux en plus des médias classiques constitue une pratique courante.

Jusqu'à présent, le droit suisse et le droit allemand prévoyaient des dispositions spéciales pour le traitement de données publiquement disponibles. De telles dispositions ne sont pas prévues par le RGPD, de sorte que la situation juridique dans ce domaine se durcit de façon notable. Les pratiques de Social Media Monitoring, déjà problématiques selon le droit actuel, comportent des risques significatifs sous le RGPD.

Le respect de l'obligation d'information **soulève déjà des défis particuliers**. En effet, l'obligation d'information s'applique également lorsque les données ne sont pas collectées auprès de la personne concernée.

> Sur les réseaux sociaux, la question de savoir comment ces informations peuvent être communiquées aux personnes concernées sous une forme adéquate se pose.

A tout le moins en qui concerne les données qu'un utilisateur laisse sur le profil d'une entreprise (p. ex. lorsqu'il publie un «post»), le placement dans une rubrique séparée sur le profil est envisageable. Ce nonobstant, contrairement par exemple aux formulaires de contact sur un site internet, ces informations ne peuvent en principe pas être directement insérées à l'endroit où l'utilisateur publie son «post». Il est partant douteux que, en l'état actuel, les autorités de contrôle se satisfassent de cette pratique.

→ **Exemple:**

Il est douteux que le principe de transparence serait satisfait si Suisse Tourisme insérait, en plus des informations contenues dans les «Terms and conditions», des informations supplémentaires sur la protection des données sur son profil Facebook, sous la rubrique «Info».

Il en découle que les informations obligatoires devraient être portées à l'attention de chaque utilisateur individuel de façon subséquente. Ceci vaut particulièrement en cas de collecte de données publiées par les utilisateurs eux-mêmes dans des espaces publiquement accessibles. Dans ce cas, la question se pose toutefois de savoir si l'entreprise pourrait se prévaloir d'un fondement légitime de traitement. Cela ne sera généralement pas le cas. S'agissant de la collecte de données dans des espaces non publics, celle-ci demeure prohibée, à l'instar de ce qui vaut sous le droit actuel.

→ **Exemples:**

Si un utilisateur publie un message sur le profil Facebook publique de Suisse Tourisme avec une question sur une offre actuelle, Suisse Tourisme peut y répondre et le service requis peut en principe être fourni. En revanche, il ne serait pas possible d'intégrer ces données dans le système CRM, car une telle utilisation nécessiterait le consentement éclairé de l'utilisateur.

Si un utilisateur publie sur son profil Facebook non publique une photo et des commentaires sur son week-end de ski dans

les montagnes suisses, les entreprises ne peuvent ni y répondre, ni traiter les données d'une autre manière. Un consentement éclairé de l'utilisateur sera toujours nécessaire dans un tel cas.

Vous trouverez des informations complémentaires sur cette thématique sur notre blog **mll-news.com**.

Avez-vous des questions? Nous vous conseillons volontiers.

Lukas Bühlmann, LL.M.
lukas.buehlmann@mll-legal.com
T +41 44 396 91 91

Meyerlustenberger Lachenal SA
Avocats - Attorneys at Law
Schiffbaustrasse 2 | Case postale 1765 | CH-8031 Zurich
www.mll-legal.com | www.mll-news.com

Alexandra Weber
alexandra.weber@switzerland.com
T +41 44 288 12 32

Suisse Tourisme
Tödistrasse 7 | CH-8027 Zurich
MySwitzerland.com

© 2018 Meyerlustenberger Lachenal SA Avocats