FOIRE AUX QUESTIONS RGPD

1. Qu'est-ce que le RGPD ?

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usage accru du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels.

Le RGPD est applicable à partir du 25 mai 2018.

Attention ! La prospection commerciale par voie électronique est régie par la Directive e-Privacy transposée dans chaque état membre et bientôt remplacée par le futur Règlement e-Privacy.

Le Règlement e-Privacy est attendu pour la fin de l'année 2018 ou le début 2019, il primera sur le RGPD en ce qui concerne les règles spécifiques applicables à la prospection par voie électronique.

2. Quelle est la différence entre un règlement et une directive ?

Un règlement européen, contrairement à une directive européenne, est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Il offre donc un meilleur niveau d'harmonisation.

3. Qui est concerné par le RGPD ?

Tout organisme quel que soit sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation, **publique et privée**, **qui traite des données personnelles pour son compte** (responsable de traitement) **ou pour le compte d'un tiers** (sous-traitant)**, dès lors** :

- qu'elle **est établie sur le territoire de l'Union européenne**, ou
- que son activité cible directement des **résidents européens**.

Par exemple, une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux doit respecter le RGPD.

De même, une société établie en Chine, proposant un site de e-commerce en plusieurs langues européennes et livrant des produits en Europe doit respecter le RGPD.

Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

Champ d'application territorial (Article 3)

Le RGPD s'applique dès lors que :

- **le responsable du traitement ou le sous-traitant est établi sur le territoire de l'Union européenne** (peu importe que le traitement ait lieu ou non sur le territoire de l'UE), ou

- **le traitement a lieu sur le territoire de l'Union européenne**.

Par ailleurs, lorsque le responsable de traitement ou le sous-traitant n'est pas établi dans l'Union européenne, le RGPD s'applique quand même **lorsque les activités de traitement sont liées :**

- **à une offre de biens ou de services à des personnes situées sur le territoire de l'UE***

ou

- **au suivi du comportement de personnes situées sur le territoire de l'UE**.

* la simple accessibilité d'un site internet ne suffit pas à déterminer que des biens/services sont proposés aux personnes concernées ; des facteurs peuvent être pris en compte, tels que l'emploi d'une langue ou d'une monnaie, avec la possibilité de commander des biens/services dans cette langue.

En pratique, le RGPD s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

4. Je suis un hôtel situé en dehors de l'UE, suis-je concerné par le RGPD ?

OUI, car je propose mes services à des personnes situées dans l'UE à travers le site www.AccorHotels.com ou les sites de marques (ibis.com, mercure.com, sofitel.com…) qui sont disponibles en plusieurs langues européennes et sur lesquels il est possible de payer en euros.

5. Qu'est-ce qu'une donnée personnelle ? Quelle différence y a-t-il avec une donnée « pseudonyme » et une donnée « anonyme » ?

5.1 « Donnée personnelle » : un concept très large

La notion de « donnée personnelle » est à comprendre de façon très large.

Une « donnée personnelle » est *« toute information se rapportant à une personne physique identifiée ou identifiable »*.

Une personne peut être identifiée :

- **directement** (exemple : nom, prénom) **ou**
- **indirectement** (exemple : n° client PMID, un numéro de téléphone, un e-mail, plusieurs éléments spécifiques propres à son identité physique, etc.)

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine)

Exemple : une base marketing contenant de nombreuses informations précises sur l'âge, les goûts et les comportements d'achats du client est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

5.2 Qu'est-ce que la pseudonymisation ?

La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme, de telle façon qu'il ne soit plus possible d'attribuer des données à une personne concernée précise sans avoir recours à des informations supplémentaires. Cette technique permet donc la ré-identification ou l'étude de corrélations en cas de besoin particulier. Les données « pseudonymes » restent des données à caractère personnel soumises au RGPD (puisqu'elles peuvent être attribuées à des personnes physiques), mais améliorent la sécurité de ces données.

Exemple : en faisant référence à un client en utilisant son PMID (numéro client interne à Accor), plutôt que ses noms et prénoms, la sécurité des données est améliorée. Pour une personne externe à l'organisation, il sera plus difficile d'attribuer un PMID à une personne physique en particulier.

5.3 Qu'est-ce que l'anonymisation des données personnelles ?

L'anonymisation, à la différence de la seule pseudonymisation, est un mécanisme irréversible qui consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées de manière à ce que toute ré-identification d'une personne physique soit impossible.

6. Qu'est-ce qu'un traitement de données personnelles ?

Cette notion est également très large.

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, informatisé ou non, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Exemple : tenue d'un fichier clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Un traitement de données personnelles n'est **pas nécessairement informatisé :** les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir **un objectif**, une **finalité**, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour.

A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle.

7. Quels sont les grands principes à respecter si je suis concerné par le RGPD ?

Lorsque je suis concerné par le RGPD, je dois veiller à respecter 10 grands principes, les « 10 commandements de la protection des données » :

1. Je n'utilise des données personnelles que si:

- j'ai eu le **consentement de la personne**, OU
- cela est nécessaire pour **exécuter un contrat** auquel la personne est partie, OU
- c'est une **obligation légale**, OU
- cela est nécessaire pour **protéger la vie de la personne**, OU
- j'ai un **intérêt légitime** à cette utilisation et je ne porte pas atteinte aux droits des personnes.

2. Je sais expliquer **pourquoi** j'ai besoin de ces données.

3. J'utilise uniquement les données dont j'ai **vraiment besoin**, si je peux atteindre le même résultat avec moins de données, je dois le faire.

4. J'informe les personnes de la manière dont j'utilise leurs données.

5. Je permets aux personnes d'exercer leurs droits : accès à leurs données, rectification, effacement, opposition à l'utilisation de leurs données.

6. Je conserve les données pendant une **durée limitée**.

7. J'assure **leur sécurité**, c'est-à-dire leur **intégrité** et leur **confidentialité**.

8. Si un tiers intervient sur les données, je passe **un contrat écrit** avec lui et je m'assure qu'il est capable de protéger ces données.

9. Si les données sortent de l'Europe (même via une simple consultation depuis un pays hors Europe), j'encadre ce transfert avec des **outils juridiques particuliers**.

10. Si les données sont compromises (perdues, volées, endommagées, indisponibles…) je **notifie cette violation de données aux autorités** et aux personnes concernées si la violation de données est susceptible de générer un risque élevé pour ces personnes.

8. En application du RGPD, le consentement des personnes est-il toujours obligatoire pour traiter leurs données ?

NON.

Selon le RGPD, le consentement de la personne dont des données sont traitées n'est pas nécessaire lorsque ces données sont collectées :

- Pour l'exécution d'un contrat (Ex : contrat de vente, de location, de travail, etc.) ou de mesures précontractuelles (ex : un devis, des pourparlers, etc.) auxquels la personne concernée est partie ;
- Parce qu'un texte légal rend obligatoire l'utilisation des données ;
- Pour l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique ;
- Pour sauvegarder les intérêts vitaux d'une personne ;
- Pour poursuivre un intérêt légitime (ex : la prospection, la prévention de la fraude, les transferts au sein d'un groupe, la sécurité des réseaux, etc.), sauf si les intérêts ou les libertés fondamentales de la personne concernée prévalent.

9. Qu'est-ce qu'un Responsable de traitement ?

Il s'agit de la personne, du service ou de l'entreprise qui **détermine les finalités et les moyens du traitement** (c'est en quelque sorte le **donneur d'ordres**). C'est lui qui décide de mettre en œuvre le traitement et qui en définit les modalités. Il est juridiquement responsable de la conformité du traitement et veille au respect des obligations. Un traitement peut être conjointement mis en œuvre par plusieurs responsables de traitement.

Accor S.A est par exemple responsable du traitement des données personnelles des clients contenues dans sa base centrale de clients, les données étant soit collectées directement

auprès des clients *via* les sites internet ou les *call centers*, ou indirectement *via* les hôtels, les agences, etc. interconnectés avec le système central de réservation du Groupe.

10. Qu'est-ce qu'un Sous-traitant ? Quelles sont ses obligations ?

C'est la personne, le service, la direction ou l'entreprise qui **traite des données personnelles pour le compte du responsable du traitement.** Il peut s'agir d'un prestataire de services (par exemple éditeur de plateformes numériques, fournisseur de communications électroniques…).

Concrètement :

La société B est sous-traitante de la société A lorsqu'elle traite des données personnelles pour le compte, sur instruction et sous l'autorité de la société A.

La société A est le responsable du traitement des données.

Exemples : Sont sous-traitants de données personnelles :

- Les prestataires de services informatiques (hébergement, maintenance, etc.).
- Les intégrateurs de logiciels.
- Les sociétés de sécurité informatique.
- Les entreprises de service du numérique lorsqu'elles ont accès aux données.
- Les agences de marketing ou de communication qui traitent des données personnelles pour le compte de clients.

Attention ! Les fabricants de matériels (logiciels, badgeuses, matériel biométrique, etc.) ne sont pas des sous-traitants puisqu'ils n'ont pas accès et ne traitent pas de données personnelles.

Un sous-traitant est responsable de traitement pour ses propres fichiers, par exemple, de son fichier de gestion de son personnel.

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'*accountability*. Il a notamment une obligation de conseil auprès du responsable de traitement pour la conformité à certaines obligations du RGPD (études d'impact sur la vie privée, violations de données, sécurité, destruction des données, contribution aux audits)

11. Quel est l'impact du RGPD sur la relation avec les prestataires ?

Lorsqu'une entité, en qualité de responsable de traitement, fait appel à un prestataire agissant en tant que sous-traitant sur les données personnelles, le RGPD impose la conclusion d'un contrat écrit dont les dispositions obligatoires sont listées à l'article 28 du RGPD. Ce contrat doit ainsi préciser :

- L'objet et la durée du traitement
- La nature et la finalité du traitement
- Le type de données personnelles et les catégories de personnes concernées par le traitement
- Les obligations et les droits du responsable de traitement
- Les obligations du sous-traitant :
    - Le sous-traitant ne traite les données personnelles que sur instructions documentées du responsable de traitement
    - Le sous-traitant veille à ce que les opérationnels traitant les données personnelles soient soumis à une obligation de confidentialité
    - Le sous-traitant assure la sécurité du traitement
    - Le sous-traitant ne peut recruter de sous-traitant ultérieur qu'après avoir obtenu l'autorisation écrite préalable (spécifique ou générale) du responsable de traitement
    - Le sous-traitant répercute à tout nouveau sous-traitant ultérieur les mêmes obligations prises avec le responsable de traitement
    - Le sous-traitant aide le responsable de traitement à respecter ses obligations à l'égard des personnes dont les données sont traitées
    - Le sous-traitant aide le responsable de traitement pour la conformité à certaines obligations du RGPD (études d'impact sur la vie privée, violations de données, sécurité, destruction des données, contribution aux audits)
    - Selon le choix du responsable de traitement, le sous-traitant supprime les données personnelles ou les retourne au responsable de traitement au terme de la prestation et détruit les copies existantes
    - Le sous-traitant met à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, ou inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

12. Qu'est-ce que la protection des données dès la conception et par défaut (« *privacy by design & by default* ») ?

Le "Privacy by Design" a pour objectif de garantir que la protection des données personnelles soit prise en compte dès la conception d'un projet et tout au long de son exécution.

Pour chaque nouvelle application, produit ou service traitant des données à caractère personnel, les entreprises doivent offrir à leurs utilisateurs ou clients le plus haut niveau possible de protection des données.

Le « Privacy by Default » consiste à prendre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, la plus grande protection des données personnelles soit garantie.

Exemples de mesures à mettre en œuvre :

- Réduire au minimum la quantité de données traitées
- Garantir la transparence du traitement
- Pseudonymiser les données personnelles dès que possible
- Mettre en place des mesures de sécurité et les améliorer de manière continue

Privacy by design : le responsable de traitement doit prendre en compte la protection des données personnelles dès la conception d'un nouveau produit ou service.

Privacy by default : Les paramètres de confidentialité les plus stricts s'appliquent automatiquement et par défaut lorsqu'un client acquiert ou utilise un nouveau produit ou service.

13. Quelles mesures de sécurité des données mettre en œuvre ?

Le responsable de traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Exemple :

- Des mesures de sécurité physiques : sécurité des accès aux locaux ;
- Des mesures de sécurité informatiques : antivirus, sécurisation des mots de passe, etc.

Le responsable de traitement et le sous-traitant doivent également veiller à ce que seuls les destinataires autorisés puissent accéder aux données.

A savoir : le fait de faire appel à un sous-traitant ne décharge pas le responsable de traitement de son obligation de sécurité et de confidentialité.

Attention : la communication d'informations à des personnes non-autorisées ou même leur divulgation par imprudence peuvent être sanctionnées !

14. Qu'est-ce que l'*Accountability* ?

Le RGPD introduit une nouvelle notion : le principe de responsabilité, mieux connu sous sa dénomination anglaise, l'*accountability*.

L'objectif premier de ce changement est de rendre activement responsable le responsable de traitement de la mise en conformité des traitements de données.

L'*accountability* désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes (mesures techniques et organisationnelles) appropriées pour s'assurer que les traitements de données personnelles sont effectués en conformité avec le RGPD et être en mesure de le démontrer.

Ainsi, les entreprises doivent prendre des mesures efficaces et appropriées pour être conforme au RGPD, mais également identifier et documenter les mesures prises afin d'en rapporter la preuve à une autorité de contrôle.

15. Qu'est-ce qu'une étude d'impact sur la vie privée (EIVP ou PIA) ?

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent de l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

16. Qu'est-ce qu'une violation de données ?

Il s'agit d'une violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

17. Qu'est-ce qu'un DPO, quand est-il nécessaire d'en avoir un et que doit-il faire?

Un DPO est un Data Protection Officer ou, en Français, un Délégué à la Protection des Données. Il s'agit d'une nouvelle fonction spécifiquement créée par le RGPD.

Les responsables de traitement et les sous-traitants ne doivent obligatoirement désigner un délégué que dans certaines hypothèses, à savoir :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données reste bien sûr possible.

Lorsqu'un délégué est désigné, il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du RGPD et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

A savoir : Le groupe Accor a désigné un DPO et chaque BU possède un relais en charge de la protection des données à son niveau, un « *Regional Data Protection Coordinator* » (RDPC).

Si vous avez des questions, vous pouvez ainsi contacter votre RDPC (voir la liste des RDPCs)

Pour le siège corporate (DPO) : **Accorhotels.data.protection.officer@accor.com**

18. Quels sont les risques en cas de non-respect du RGPD ?

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du RGPD.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% jusqu'à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

Autres risques pour les responsables de traitement et les sous-traitants : un risque d'image et réputationnel pouvant conduire à une perte de clients.

19. Quelles sont les conséquences du Brexit sur l'application du RGPD au Royaume-Uni ?

La procédure de sortie du Royaume-Uni de l'Union européenne doit s'achever le 29 mars 2019. Jusqu'à cette date, le Royaume-Uni reste un État membre de l'Union européenne.

L'autorité britannique de la protection des données personnelles (Information Commissioner's Office - ICO) a donc indiqué que le règlement européen entrerait en vigueur au Royaume-Uni le 25 mai 2018, comme dans l'ensemble des États membres de l'Union européenne.

20. Le RGPD impacte-t-il les règles en matière de prospection commerciale par voie électronique ?

NON ! Aussi étonnant que cela puisse paraitre, il n'y a pas dans le RGPD de dispositions spécifiques applicables à la prospection par voie électronique. Le RGPD n'affecte ainsi pas les règles déjà applicables en matière de e-marketing, que ce soit en B2C ou B2B.

En effet, la prospection par voie électronique est actuellement régie par la Directive e-Privacy transposée dans chaque état membre et qui sera remplacée par le futur Règlement e-Privacy.

Le Règlement e-Privacy est attendu pour la fin de l'année 2018 ou le début 2019, il primera sur le RGPD en ce qui concerne les règles plus spécifiques applicables en matière de prospection par voie électronique.

21. Rappel : quelles sont les règles applicables pour envoyer de la prospection commerciale par voie électronique (Opt-in / Opt-out) ?

Conformément à la Directive e-Privacy qui sera bientôt remplacée par le Règlement e-Privacy prévu d'ici la fin de l'année 2018 ou le début 2019 et qui prévaut sur le RGPD :

i) Par principe, toute prospection par voie électronique nécessite un consentement préalable du destinataire (notion d'Opt-In).

ii) Par exception, ce consentement n'est pas nécessaire (notion d'Opt-Out) si:

- Les coordonnées du destinataire ont été collectées directement auprès de lui à l'occasion d'une vente ou d'une prestation de services
- La communication concerne des produits ou services analogues à ceux déjà fournis par l'entreprise
- Au moment de la collecte, le client a été informé de l'utilisation de ses données à des fins de prospection, et
- Le client se voit donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation de ses données :
    - au moment où elles ont été collectées, et
    - lors de chaque message.

iii) Dans tous les cas, chaque message électronique doit obligatoirement :

- préciser l'identité de l'annonceur, et
- proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations (par exemple *via* lien pour se désinscrire à la fin du message).

Attention ! si vous opérez vous-même un mailing, mettez toujours les destinataires de vos messages électroniques en copie cachée !

22. Quelles mesures prendre pour protéger les données des collaborateurs ?

De très nombreuses données personnelles relatives aux collaborateurs sont nécessaires pour la gestion de leur carrière.

Par exemple, vous avez besoin de beaucoup d'informations pour assurer :

- la rémunération et les déclarations sociales obligatoires,
- la gestion administrative du personnel,
- l'organisation du travail.

Ne demandez à vos employés que les informations utiles pour accomplir leurs missions, et évitez de traiter des données dites « sensibles » (activité syndicale, opinions politiques, religion, origine ethnique, santé). Si vous devez en traiter, des obligations particulières sont applicables. Prenez contact avec le DPO (pour le siège) ou le RDPC compétent dans votre région (pour les BUs).

Assurez-vous de garantir la confidentialité et la sécurité des données personnelles de vos employés.

Seules les personnes habilitées doivent prendre connaissance de ces données personnelles.

23. Quelles obligations de conformité pèsent sur les sièges Accor et sur les hôtels du Groupe ?

La conformité des outils « centraux » est prise en charge par les équipes des sièges (Tars, ResaWeb, le programme de fidélité, HotelLink, etc.).

La conformité de l'utilisation des données personnelles faite par les hôtels est de leur responsabilité (par exemple : les données RH ou les données du PMS).

Pour vous aider, le Groupe diffusera des directives sur les mesures à mettre en place pour traiter les données personnelles conformément à la règlementation, y compris sur ce périmètre.

24. Le RGPD impacte-t-il ma relation avec un client corporate (par exemple Microsoft, Air France, IBM, AMEX) ? Que dois-je faire si mon client corporate me transmet un contrat ou une clause portant sur la protection des données personnelles ?

Lorsqu'un collaborateur d'un client corporate effectue une réservation à un tarif préférentiel au titre du contrat conclu par ce client corporate, Accor S.A et l'hôtel agissent ici en qualité de responsable de traitement à l'égard des données personnelles des clients collaborateurs.

Le client corporate reste, quant à lui, responsable de traitement concernant le traitement des données personnelles de ses employés à des fins de gestions des voyages et des déplacements.

Par conséquent, le contrat conclu entre un bureau de vente ou un hôtel avec un client corporate doit préciser que chaque partie s'engage, en tant que responsables de traitement, à collecter, traiter et stocker les données personnelles pour leur propre besoin, en conformité avec la règlementation sur la protection des données.

Il n'est donc pas nécessaire d'adopter des mesures contractuelles spécifiques (comme indiquées dans l'article 28 du RGPD) car ni Accor S.A, ni la BU, ni l'hôtel ne traite de données personnelles pour le compte du client corporate.

Attention ! Si un client corporate vous transmet un document prévoyant une sous-traitance de données entre un responsable de traitement et un sous-traitant, ce document n'est pas applicable à votre situation.

- Adressez-vous à la direction juridique corporate si Accor S.A est partie au contrat : un modèle de clause vous sera transmis
- Adressez-vous au RDPC si un bureau de vente locale gère la relation avec le client corporate: un modèle de clause vous sera transmis

Nous travaillons actuellement sur la mise à jour des modèles de contrats !

25. Puis-je utiliser l'email professionnel d'un *Account Manager* d'une société avec laquelle je travaille pour l'inviter à des évènements ?

Conformément aux règles applicables à la communication par voie électronique (cf. question 21) : la personne doit avoir été informée de l'utilisation qui sera faite de son email au moment de la collecte et du droit de s'y opposer, sauf dispositions locales particulières.

Dans tous les cas, chaque message électronique doit obligatoirement :

- préciser l'identité de l'annonceur, et
- proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations (par exemple *via* lien pour se désinscrire à la fin du message).

Attention ! si vous opérez vous-même une campagne d'emailing, n'oubliez pas de mettre les destinataires de vos messages électroniques en copie cachée.

26. **Où puis-je trouver les politiques et procédures du Groupe en matière de protection des données personnelles ?**

Nous mettons actuellement en place un espace dédié sur l'intranet. Vous pourrez y retrouver toutes les informations nécessaires.

Vous pouvez d'ores et déjà trouver la charte données personnelles présente sur le site internet www.Accorhotels.com à travers ce lien : https://www.Accorhotels.com/security-certificate/index.fr.shtml

27. **Qui sont les personnes à contacter pour des questions relatives à la protection des données personnelles ?**

Pour le siège corporate : Accorhotels.data.protection.officer@accor.com

Pour les BUs : le RDPC (voir la liste des RDPCs)

A suivre…