Deloitte.
Private

Comment protéger votre entreprise et être prêt pour ce 25 mai 2018?

Questions et réponses webinar

1. Lors de la création d'un nouveau site internet, en B2B, que doit-on absolument mettre en place pour être en conformité avec le RGPD? Les données récoltées sont l'adresse e-mail, le nom, le prénom et le numéro de téléphone du client?
Dans le cadre du RGPD, il convient notamment d'indiquer la finalité pour laquelle vous allez utiliser ces données et la durée durant laquelle vous allez les conserver ainsi que les coordonnées de contact pour que les personnes concernées puissent exercer leurs droits. Il faut être transparent vis-à-vis de votre clientèle.

D'autres questions doivent être analysées: ne récoltez-vous que les données nécessaires à votre finalité? Procédez-vous à du tracking via les cookies? Etc.

Enfin, outre le RGPD, il convient de s'assurer que les mentions légales obligatoires soient présentes sur votre site internet.

2. Sur un site internet, doit-on en plus d'une politique de confidentialité affichée, automatiquement activer des cookies pour être conforme au RGPD?
Le RGPD n'impose pas qu'il y ait des cookies sur un site internet. Toutefois si des cookies sont utilisés et permettent d'identifier les utilisateurs, ceux-ci doivent être informés sur les cookies utilisés et leur finalité. Il convient ensuite d'obtenir leur consentement (l'utilisateur doit avoir la possibilité d'accepter ou non les cookies en fonction du type).

Comme vous l'indiquez, votre site internet doit reprendre une politique de confidentialité des données dès l'instant où il y a un traitement de données à caractère personnel.

3. Le sous-traitant du sous-traitant est-il autant responsable que le responsable du traitement?
Oui, le RGPD prévoit une responsabilité solidaire entre toutes les parties intervenant dans le cadre d'un même traitement de données.

Chacun doit pouvoir être tenu responsable, dans sa totalité, d'un dommage causé par le traitement.

Comme indiqué lors de notre exposé, cette responsabilité solidaire peut être équilibrée entre parties via la conclusion de 'Data Processing Agreements' (DPA). Le but de ces conventions est de clarifier contractuellement les obligations respectives de chacune des parties au traitement.

4. Faut-il un Délégué à la protection des données dans chaque entreprise privée?

Non. La désignation d'un délégué est obligatoire pour:

- Les autorités ou les organismes publics;
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle;
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites 'sensibles' ou relatives à des condamnations pénales et infractions.

Toutefois, même si vous ne rentrez pas dans l'une de ces hypothèses, nous vous conseillons de désigner un 'Responsable RGPD' interne à votre entreprise. Cette personne sera notamment l'interlocuteur privilégié des personnes souhaitant poser des questions relatives aux traitements des données à caractère personnel et sera chargée de la mise à jour du registre de traitement des données.

5. Qu'entend-on par traitement à 'grande échelle'?

Le RGPD ne définit pas la notion de 'grande échelle'. Chaque entreprise devra apprécier sa propre situation en tenant compte des critères suivants:

- Le nombre de personnes concernées;
- Le volume des données traitées;
- La durée du traitement;
- L'étendue géographique du traitement.

6. Le responsable IT peut-il être Délégué à la protection des données?

Un Délégué ne doit pas être en position de conflit d'intérêts. Les missions du Délégué sont, selon nous, incompatibles avec les fonctions du responsable IT.

En effet, il convient d'éviter qu'un travailleur doive, d'une part, décider des modalités du traitement de données et, d'autre part, s'interroger sur la compatibilité de ces modalités avec le RGPD.

7. En ce qui concerne les CV, que faire avec une photo laissant comprendre la couleur de peau ou indiquant spontanément une donnée pouvant être considérée comme sensible? Lors d'un entretien, que faire si la personne parle un dialecte laissant comprendre qu'elle appartient à un type ethnique?

Dans le cadre de la phase de recrutement, une entreprise ne doit collecter que les données pertinentes et strictement nécessaires à la finalité du traitement. Il s'agit du principe de minimisation des données consacré par l'article 5 du RGPD.

A cet égard, il convient de distinguer, d'une part, les CV qui vous sont spontanément transmis par les candidats et, d'autre part, l'éventuel formulaire de candidature à remplir via lequel des données qui ne sont pas nécessaires au traitement sont récoltées.

Si un CV contient plus de données que celles qui sont pertinentes, cela ne vous empêchera pas de traiter le CV. Toutefois, il vous reviendra de respecter le RGPD et notamment d'informer le candidat sur l'utilisation que vous entendez faire des données ainsi récoltées. Par ailleurs, le RGPD interdit de conserver les données des candidats de façon indéfinie. Il vous revient de fixer une durée limitée de conservation.

Lors d'un entretien, si la personne parle un dialecte laissant comprendre qu'elle appartient à un type ethnique, il n'y a sur cette base pas de traitement de données à caractère personnel. La situation peut toutefois être différente si vous indiquez cette information dans un rapport d'interview écrit.

8. Dans le cadre de la participation à des foires (B2B), nous recevons la liste des participants à cette foire. Y a-t-il un intérêt légitime?

Sous réserve d'une analyse plus approfondie, il revient à l'organisateur de la foire d'informer les participants du fait que leurs données feront l'objet d'un traitement et des finalités de ce traitement. Il doit également s'assurer que les entreprises présentes feront un traitement de ces données conformément au RGPD. Il convient ensuite d'analyser ce que vous faites des données reçues. En fonction du traitement que vous réalisez, il convient de déterminer s'il y a un intérêt légitime ou pas.

9. A partir de combien de travailleurs devons-nous nous mettre en conformité avec le RGPD? Nous sommes une société de 45-50 personnes.

Toute entreprise qui traite des données à caractère personnel (relatives au personnel, à la clientèle, aux fournisseurs, etc.) doit se mettre en conformité au RGPD. Le nombre de travailleurs mais aussi la taille de l'entreprise et son chiffre d'affaires, importent peu. Il y a un seuil de 250 travailleurs mais il ne concerne que la tenue d'un registre.

10. Je suis concessionnaire automobile. Je dois respecter les règles du RGPD pour Monsieur X qui utilise un véhicule client. Mais pour l'entreprise à laquelle je facture mes prestations (SPRL COCA COLA), dois-je appliquer les règles du RGPD?

Il est certain que le traitement des données à caractère personnel sera moindre si l'on est en B2B plutôt qu'en B2C. Cependant, on oublie souvent que derrière une entreprise se trouve toujours une/des personne(s) physique(s). Dès lors que vous possédez les données de cette personne (aussi minimes qu'elles soient, comme simplement la possession de son nom, son prénom, son numéro de téléphone (professionnel ou non) et son adresse e-mail), vous devez appliquer les règles du RGPD.

11. La durée de conservation des données clients est-elle liée aux règles de conservation de 8 ans pour nos factures?

En effet, les durées légales d'archivages sont un bon indicateur de la durée de conservation des données personnelles. Toutefois, si vous avez un intérêt légitime, vous pouvez les conserver plus longtemps mais il faudra le justifier.

12. De quelle manière gérer le 'privacy by design'?

Le 'privacy by design' est le principe qui impose de prendre en compte la problématique des données personnelles au sein de l'entreprise et au sein des processus mêmes, depuis la conception du service ou du produit jusqu'à sa mise en œuvre.

Cela signifie que tous vos processus, votre manière de fonctionner au sein de l'entreprise, que ce soit de manière virtuelle (programmes informatiques, logiciels, etc.) ou physique (classement des armoires, clés, codes, etc.) doivent être conformes au RGPD et respecter les grands principes du RGPD dont principalement le principe de limitation de traitements, de limitation d'accès, de proportionnalité et de stockage à durée limitée.

En pratique, le 'privacy by design' impliquerait que tous les process susmentionnés soient revus/réadaptés pour être 100 % conformes au RGPD.

13. De quelle manière mettre à jour les règlements de travail?

En général, nous préconisons plutôt d'ajouter une annexe au règlement de travail afin de tenir compte du traitement des données à caractère personnel des travailleurs. Cette annexe traitera de manière générale des aspects RGPD ainsi que des règles relatives à l'utilisation d'internet et des e-mails (IT Policy).

14. L'APD belge va-t-elle auditer une organisation belge, sans qu'il y ait violation ou perte de données ou plainte?

L'APD pourra en effet exercer son pouvoir d'enquête (similaire à celui des administrations sociale et fiscale lors d'un contrôle) et contrôler spontanément les entreprises afin d'évaluer leur mise en conformité au RGPD.

15. Quid d'une base de données clients? Obligation légale par rapport à la comptabilité? Puis-je conserver cette base de données ad vitam aeternam?

Tout dépend de la finalité pour laquelle vous constituez votre base de données clients. Nous pouvons donc distinguer plusieurs cas:

- Vous constituez votre base de données clients en vue de la prestation de votre service/la vente de votre produit, et uniquement dans le but d'encadrer cette prestation/cette vente.
  Exemple: un garagiste constitue une base de données clients et envoie des rappels lorsqu'il est temps de faire l'entretien voiture, de changer les pneus, etc.
- Vous constituez votre base de données clients car vous avez une obligation légale de recueillir certaines données à caractère personnel de ces derniers.
  Exemple: la loi anti blanchiment exige que l'on tienne un registre UBO en collectant certaines données à caractère personnel des personnes détenant plus de 25 % du capital de la société cliente.

- Enfin, vous pouvez constituer OU utiliser, votre base de données clients à des fins commerciales et de marketing (envoi de newsletters, de promotions, de catalogues, de publicités, etc.). Dans ce cas, que cette BDD soit constituée uniquement à des fins de marketing, ou bien que vous profitiez de la BDD constituée en vertu de l'un des deux points précédents, le RGPD vous impose de demander le consentement de chaque personne reprise dans cette BDD.

Notez qu'un des grands principes du RGPD est la notion de conservation limitée. Sous ce nouveau règlement, il ne sera plus permis de conserver des données à caractère personnel ad vitam aeternam. Dès lors, vous serez tenu de déterminer le délai de conservation adéquat en fonction du type de donnée(s) personnelle(s) dont il s'agit, soit de manière objective par vos soins, soit parce qu'une obligation légale vous l'impose, soit parce que vous avez toujours un intérêt légitime à cette conservation.

16. Existe-t-il des exemples téléchargeables de registre?

Il existe effectivement un template de registre de traitements de données à caractère personnel disponible sur le site de la Commission vie privée.

17. Le registre des données est-il existant, fourni ou doit-on le concevoir soi-même?

Il vous est loisible de concevoir le registre vous-même mais celui-ci doit nécessairement respecter toutes les exigences imposées par le RGPD.

18. Dans le cadre de l'expédition gratuite d'un magazine, je dispose de données privées telles que le numéro de gsm et l'adresse e-mail. Dois-je demander aux personnes concernées leur accord afin de posséder et gérer leurs données? Et comment?

Tout dépend de l'objectif poursuivi par l'envoi du magazine.
Dans le cadre d'une relation de clientèle existante pour promouvoir vos propres services ou produits, vous pouvez vous baser sur la notion d'intérêt légitime. Vous devez néanmoins informer votre client du traitement qui sera fait de ses données. En pratique, nous vous conseillons en outre de signaler explicitement au client son droit de s'opposer au traitement et de faciliter l'exercice de ce droit (par exemple via une possibilité 'd'opt-out' visible et claire lors de la collecte des données et lors de chaque communication).
Si le magazine est envoyé à des tiers (non clients), il convient d'obtenir leur consentement.

Posez-vous également la question de la pertinence de collecter le numéro de gsm pour un mailing.

19. Quelles sont les procédures à mettre en place, pour les sociétés sous-traitantes de bases de données ou d'adresses comme une entreprise de routage en imprimerie?

Partant du principe que ces entreprises traitent des données à caractère personnel, elles sont soumises aux mêmes obligations que les autres. Néanmoins, le volume de données traitées pourrait avoir comme conséquence que ces entreprises doivent nommer un DPO ou faire une DPIA (à apprécier au cas par cas).

20. Y a-t-il un lien direct vers la version complète du RGPD?

Oui, sur le site:
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

21. Si je suis mandaté par un client pour traiter les données de ses clients (membres), quel accord/contrat dois-je avoir entre ma société et mon client pour nous protéger tous les deux?

Nous conseillons de conclure une DPA *(cf. question 3)* qui va permettre d'aménager le principe de responsabilité solidaire.

22. Comment l'Europe va-t-elle faire respecter cette réglementation par les entreprises situées à l'étranger (USA par exemple)?

Le RGPD s'applique à un responsable de traitement ou à un sous-traitant qui n'est pas dans l'UE mais dont les activités de traitement sont liées à l'offre de biens ou de services à des personnes dans l'UE.

Dans ce cas, le responsable du traitement ou le sous-traitant établi hors UE doit désigner par écrit un représentant dans l'UE. Ce représentant est la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives aux traitements, aux fins d'assurer le respect du RGPD.

Les entreprises établies hors UE doivent garantir un niveau de protection nécessaire au respect du RGPD.

23. Dans le cas d'une relation avec un sous-traitant, tel un comptable, faut-il un 'double accord' pour le traitement des données (société vers comptable et comptable vis-à-vis de la société)?
Oui, tout à fait. Il est recommandé que chacun s'assure que l'autre traite les données qu'il collecte d'une manière conforme au RGPD. Pour ce faire, nous conseillons de conclure une DPA *(cf. question 3)*.

24. Les données à caractère personnel peuvent-elles nous servir à faire de la prospection publicitaire?
Oui, si vous avez le consentement des personnes concernées. Pour les nuances, *cf. question 18*.

25. Est-il nécessaire d'avoir un système informatique pour supporter la procédure de traitement des données?
Non, sauf si vous avez des données à caractère personnel sous format électronique.

26. Ma société offre un service de location/livraison/installation et reprise de sanitaires portables.
Je reçois des formulaires de demandes d'offres via mon site web avec des infos telles qu'adresse, nom, téléphone. Ensuite, je les utilise dans mes plannings de livraisons et reprises. Que dois-je faire par rapport à l'utilisation de ces données?
Vous devez informer ces personnes des droits qui sont les leurs dans le cadre du RGPD et de la manière dont ils peuvent les exercer, et notamment des finalités pour lesquelles vous récoltez et traitez leurs données. Vous pouvez le faire par le biais d'une charte 'vie privée' par exemple ou en mettant à jour vos conditions d'utilisation de votre site internet.

27. En lisant la régulation, je suis tombé sur une partie parlant de certificats de conformité pour les entreprises qui souhaitent démontrer qu'elles sont en conformité avec la régulation. Pouvez-vous donner des exemples de certifications reconnues?
Pour le moment, il n'y a aucune certification reconnue/officielle.

28. Dans le cadre d'une association d'entreprises, quid des photos personnelles sur le site et des photos des manifestations? Quid des données telles que e-mails et gsm des membres?
En fonction de ce que vous faites avec les données, le consentement des personnes sera requis ou non. Il sera requis pour la publication des photos sur le site. Les données e-mails et GSM pourront être traitées sans consentement (en vous basant sur la notion d'intérêt légitime) pour autant que vous restez bien dans le cadre de la relation contractuelle avec ces membres, et que vous n'utilisez pas ces données à d'autres fins.

29. Pour mon travail de prospection/vente, je ne peux plus travailler avec les pages blanches?
Les conditions d'utilisation des 'Pages Blanches' ne vous autorisent pas à utiliser les données pour ce type d'activités.

Contactez nous:

Thierry Dekoker
Director
GDPR specialist
tdekoker@deloitte.com
0475 90 18 83

Mathilde Boucquiau
Junior legal consultant
GDPR specialist
mboucquiau@deloitte.com
0498 18 27 25

Deloitte.
Private

Accountancy & Advisory

ACCOUNTING & REPORTING TAX & LEGAL M&A & FINANCE
BUSINESS CONTROL & TECHNOLOGY STRATEGY & GROWTH