contrast

VOS ACTIVITÉS • MAI 2021

Le RGPD en 10 points clés ? Oui, c’est possible !

Ce que vous devez savoir.

Le RGPD est entré en vigueur le 25 mai 2018, soit il y a exactement 3 ans. C'est à cette époque que de nombreuses entreprises ont commencé à implémenter le RGPD, mais depuis elles n’y voient plus clair. D'autres entreprises ne savent même pas par où commencer. Et les entreprises qui ont terminé cet exercice à l’époque, se découragent de devoir aujourd’hui procéder à une évaluation et une mise à jour de l’exercice en question.

Est-ce une exagération ? Certainement pas ! Le RGPD de 88 pages compte 55 000 mots, contenus dans 173 considérants et 99 articles. Identifier de cela (toutes) les obligations concrètes n'est pas une tâche évidente. Mais il existe des outils pour ce faire !

Plusieurs autorités nationales de protection des données ont déjà publié de nombreux outils utiles : des feuilles de route du RGPD (par exemple, la CNIL française) jusqu’aux modèles concrets (par exemple, l'accord de traitement du Datatilsynet danois). Il est donc certainement utile de consulter les sites web des autorités. Toutefois, il manque encore un aperçu complet, à la fois concis et réellement pratique, qui permet, de vérifier systématiquement toutes les obligations découlant du RGPD. C'est pour cette raison que **contrast** a établi une checklist de 10 points.

Ce que vous devez faire.

Si votre entreprise ne maîtrise pas (encore) le RGPD, sachez qu'elle n'est certainement pas la seule ! Il n'est pas trop tard pour commencer, continuer ou mettre à jour l'exercice du RGPD. Ce n'est toutefois pas une tâche impossible. Chez **contrast**, nous utilisons la checklist de 10 points suivante :

1. **Finalité** : commencez par identifier les différentes finalités pour lesquelles votre entreprise traite des données à caractère personnel. Soumettez cette question aux différents services de votre entreprise : RH, ventes, marketing, etc. Vous pouvez déjà leur donner quelques idées en leur indiquant des finalités de traitement courantes (avec une description précise). Sur base de ces finalités, votre entreprise déterminera quelles données à caractère personnel sont nécessaires et pendant combien de

temps votre entreprise est autorisée à les conserver.

2. **Base** : identifiez pour chacune des finalités la base légale la plus appropriée conformément aux articles 6 à 10 du RGPD. Cette tâche revient aux juristes, en concertation avec les employés responsables du traitement au sein de votre entreprise. En fonction de la base choisie (consentement, intérêt légitime, etc.), des actions supplémentaires peuvent être requises.

3. **Droits** : vérifiez si les finalités identifiées (et toutes les informations y afférentes conformément aux articles 13 et 14 du RGPD) sont incluses dans une déclaration de confidentialité destinée aux personnes concernées. Votre entreprise traite-t-elle des données à caractère personnel via son site web ? Dans ce cas, une déclaration de confidentialité sur le site web est nécessaire. Votre entreprise décide-t-elle de créer une liste des anniversaires de ses employés afin d'envoyer des vœux d'anniversaire ? Vérifiez alors si cela figure dans la déclaration de confidentialité destinée aux employés. En outre, il est important de prévoir des procédures pour répondre aux demandes des personnes concernées conformément, entre autres, à l'article 12 du RGPD: un opt-out absolu pour le marketing direct est-il prévu, qui répondra à une demande d'accès, comment une personne concernée doit-elle prouver son identité, quels modèles (de réponse) doivent être utilisés, etc. ?

4. **Tiers** : identifiez, pour chacune des finalités, les tiers qui ont accès aux données à caractère personnel ou qui les utilisent. Demandez à un juriste de vous aider à qualifier ces tiers comme étant des sous-traitants, des responsables conjoint du traitement ou responsables de traitement distincts. Ne perdez pas de vue les entreprises du groupe ! En fonction de la qualification, vous devez vérifier si les documents (contractuels) nécessaires sont disponibles.

5. **Des pays tiers** : vérifiez si ces tiers se trouvent en dehors de l'Espace Économique Européen ou si ce sont des filiales dont la société mère se trouve en dehors de l'EEE. Dans un tel cas, votre entreprise doit mettre en place les garanties appropriées pour assurer un niveau de protection équivalent dans le pays tiers concerné. Pour ce faire, les juristes peuvent également vous aider.

6. **Sécurité et violations de données** : vérifiez, en fonction des risques liés au traitement, si la sécurité actuelle / quelle sécurité est adéquate pour protéger les données à caractère personnel contre l'accès, la perte et l'altération non autorisés. Les risques (et donc les mesures à prendre) dépendront des types de données à caractère personnel traitées, des technologies et infrastructures utilisées dans le cadre du traitement, etc. Il est conseillé de faire appel à cet effet à des consultants en sécurité (informatique). Il ne sera toutefois pas possible d'éliminer tous les risques. Par conséquent, il est important que votre entreprise prenne également des mesures pour identifier les violations de données, les répertorier en interne et les signaler à l'autorité compétente et aux personnes concernées.

7. **DPD** : vérifiez si (une ou plusieurs) des finalités entraînent que votre entreprise devra désigner un *Délégué à la Protection des Données* et le notifier aux autorités compétentes en matière de protection

des données.

8. **DPIA** (analyse d'impact relative à la protection des données) : vérifiez si (une ou plusieurs) des finalités impliquent un risque élevé pour les personnes concernées. Vous pouvez effectuer cette analyse notamment sur base des listes publiées par les autorités de protection des données ou sur base des critères du Comité Européen de la Protection des Données (EDPB). En présence d'un risque élevé, vous devez réaliser une analyse d'impact relative à la protection des données (une sorte d'analyse d'impact) et éventuellement obtenir l'approbation préalable de l'autorité compétente en matière de protection des données.

9. **Politiques et procédures** : assurez-vous - même si votre entreprise n'est pas tenue de nommer un DPD - qu'*au moins une personne* est responsable pour le suivi de la conformité au RGPD au sein de votre entreprise. Pensez également à sensibiliser et à former votre personnel. Chaque entreprise doit de toute façon disposer d'une procédure pour répondre aux demandes des personnes concernées, pour répertorier et signaler les violations de données, pour effacer les données à caractère personnel et pour assurer la sécurité des données à caractère personnel (par exemple, par système de données). Le registre (voir ci-dessous) peut être un outil utile à cet égard. Il peut également être utile, par exemple, d'inclure l'utilisation de cette checklist dans les procédures standard pour le démarrage de nouveaux projets.

10. **Registre** : veillez à ce que les informations collectées dans le cadre de la présente checklist sont incluses dans un registre des activités de traitement conformément à l'article 30 du RGPD.