

01 JUIN 2018



Association Suisse de l'industrie des Graviers et du Béton

Aux membres de l'ASGB

Berne, le 31 mai 2018 MW/ps

Règlement européen sur la protection des données – RGPD

Mesdames, Messieurs,

Le **Règlement européen sur la protection des données (RGPD)** est entré en vigueur le 25 mai.

Pour les membres de l'ASGB, le RGPD est important si

- vous adressez des offres à des clients dans l'UE (y compris EEE) ou
- vous documentez par voie électronique le comportement d'utilisateurs de l'UE et collectez des données à leur sujet (si Google Analytics ou le pixel Facebook analyse p. ex. les accès au site Internet de votre entreprise).

L'ASGB vous propose en annexe **une liste de contrôle simple** contenant 10 mesures immédiates, élaborée par la société de communication furrerhugi ag, Berne. Même si cette liste ne peut prétendre à exhaustivité, nous vous recommandons de l'appliquer si votre entreprise est concernée par le RGPD.

Toute infraction au RGPD peut impliquer des amendes allant jusqu'à 20 millions d'euros. Viennent en plus s'y ajouter des actions civiles en dommages et intérêts de la part des personnes concernées. Malgré les efforts qu'il demande, le RGPD représente aussi une opportunité en matière de communication: si vous respectez la protection des données, vous créez de la confiance sur laquelle vous pouvez vous appuyer pour renforcer votre image.

Avec nos meilleures salutations,

ASGB

Martin Weder
Directeur

Liste de contrôle
Catalogue de mesures pour le Règlement européen général sur la protection des données – RGPD

1. Créer une vue d'ensemble: notre entreprise collecte-t-elle des données? Avons-nous un système CRM? Y a-t-il un formulaire de contact sur le site Internet? Envoyons-nous des e-mails de masse (newsletter, publipostages etc.)?
2. A compter du 25.05.2018, renoncer à toute collecte et surveillance des données (tracking) ou poursuivre la lecture ...
3. La première mesure consiste à nommer quelqu'un qui s'occupe en interne de la sécurité des données et peut donner des renseignements si l'entreprise est confrontée à un cas concret.
4. Assurez-vous que votre site Internet est crypté (<https://...>). Ceci sert non seulement à la sécurité de vos données, mais améliore aussi le classement de votre site Internet sur Google. Le plus simple est de contacter votre hébergeur web.
5. Si vous collectez des données (p. ex. via un formulaire), vous devez absolument intégrer un système de double opt-in: il envoie à toute personne qui s'inscrit à une prestation un message qui doit être confirmé. Chaque modèle (template) d'envoi d'e-mails en masse doit de plus contenir une fonction de désabonnement. Chacun doit avoir la possibilité de se désabonner de la lettre d'informations notamment très simplement (processus appelé «opt-out»).
6. Ajouter des mentions légales et une déclaration de confidentialité sur votre site. La déclaration de confidentialité doit notamment expliquer en quelle mesure l'entreprise collecte des données (voir point 1). Vous trouverez des modèles correspondants sous ce lien p. ex.: <https://www.datenschutz.org/datenschutzerklaerung/>
7. Intégrer un avertissement avant l'utilisation de cookies sur votre site Internet si vous utilisez p. ex. Google Analytics ou le pixel Facebook (notez toutefois que l'opinion des experts diverge sur ces bannières de cookies et que certains doutent de leur utilité juridique).
8. Rendez-vous sur votre compte Google Analytics (<https://analytics.google.com>). Dans ce compte, Google vous demande d'accepter les nouvelles directives d'utilisation en relation avec le RGPD et notamment les paramètres concernant la durée de conservation des données. Vous devez de plus accepter l'«Avenant relatif au traitement des données» sous Gérer > Paramètres du compte.
9. Prévoir éventuellement la nomination d'un délégué en protection des données pour votre entreprise dans l'UE. Nous ne savons pas encore exactement à quel point cette mesure est vraiment nécessaire pour les PME. Nous doutons quant à son caractère urgent.
10. C'est peut-être le bon moment de mener quelques réflexions générales sur la sécurité des données de l'entreprise: le système d'exploitation est-il toujours à jour? Les logiciels antivirus sont-ils régulièrement mis à jour? Où est enregistrée la sauvegarde de nos données? Comment gérons-nous les mots de passe?

Berne, le 31 mai 2018