

Réalisation d'une analyse d'impact relative à la protection des données (AIPD)

Département: Legal & Compliance
Rédaction: Hooker Christina, Legal Counsel
Création: Bern, Septembre 2022

Description courte

BMS Building Materials Suisse (**BMS**) prend au sérieux la protection des données à caractère personnel, et met un point d'honneur à respecter la législation en vigueur. Cela signifie, entre autres, que BMS est soumise au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, connu sous le nom de règlement général sur la protection des données (**RGPD**), et à la loi suisse sur la protection des données (**LPD**), du fait que le siège social de sa société-mère, BME, soit situé aux Pays-Bas, tandis que BMS est sise et opère en Suisse. Cela implique des obligations pour BMS. La réalisation d'analyses d'impact relative à la protection des données (**AIPD**) sur les nouvelles activités de traitement de données à caractère personnel présentant un risque élevé pour les droits et les libertés de personnes physiques incombe à BMS, en tant que responsable du traitement, selon l'article 35 RGPD et l'art. 20 par. f LPD. BMS confie la réalisation effective de l'analyse et toutes les compétences y afférentes aux départements Legal & Compliance et IT, mais reste consciente que sa responsabilité demeure inchangée.

Une analyse d'impact relative à la protection des données est une procédure visant à décrire le traitement considéré, à évaluer sa nécessité et sa proportionnalité, et à mieux contrôler les risques pour les droits et les libertés des personnes physiques qu'induit le traitement de données à caractère personnel via une évaluation des risques adéquate et la création de mesures correctives. Une analyse d'impact relative à la protection des données est donc une procédure visant à garantir et à démontrer le respect des obligations légales.

Cette description courte présente les étapes nécessaires à l'élaboration d'une procédure de contrôle et de vérification:

Étape 1: Registre des activités de traitement

Le registre des activités de traitement existantes ne peut être consulté et modifié que par Legal & Compliance. Il doit en conséquence être protégé par des mesures techniques et organisationnelles adéquates.

Si la création de nouveaux produits, de nouveaux projets ou l'utilisation de nouvelles technologies entraîne la mise en place d'activités de traitement encore non répertoriées chez BMS, celles-ci doivent être notifiées par e-mail à l'adresse dataprotection@bmsuisse.ch par le responsable du nouveau projet (**responsable**) ou produit ou de la nouvelle technologie.

Étape 2: Évaluer les risques des activités de traitements nouvellement notifiées

Si, après un premier examen rapide des activités de traitement nouvellement notifiées au moyen de la liste de vérification «Évaluation des risques des activités de traitement» (non publique), Legal & Compliance décide qu'une AIPD doit être conduite, le groupe de travail

Protection des données (**GTPD**) est réuni à cette fin. Le GTPD est composé de membres des départements Legal & Compliance, IT et RH, et du responsable.

Les listes de vérifications remplies prouvent que la nécessité d'une AIPD a bien été examinée. Elles doivent être précieusement conservées par Legal & Compliance, indépendamment du résultat.

Étape 3: Analyse d'impact relative à la protection des données, si nécessaire

Si Legal & Compliance juge qu'une AIPD est requise, ses membres documentent leur décision avec les listes de vérifications susmentionnées, informent le responsable que l'activité de traitement (de la nouvelle procédure/du nouveau service/de la nouvelle application/du nouveau système, etc.) est suspendue jusqu'à nouvel ordre et convoquent le GTPD pour conduire l'AIPD.

Le responsable suspend l'activité de traitement (de la nouvelle procédure/du nouveau service/de la nouvelle application/du nouveau système, etc.) jusqu'à ce que les résultats de l'AIPD soient connus.

Legal & Compliance conduit ensuite l'AIPD avec le GTPD, conformément au guide y afférent (non public).

Le GTPD dispose alors d'un délai de quatorze (14) jours ouvrés (toute prolongation de ce délai est laissée à l'appréciation de Legal & Compliance, mais doit être justifiée) pour conduire l'AIPD et déterminer les mesures correctives appropriées.

Étape 4: Examen régulier

Il incombe au GTPD d'examiner l'analyse d'impact relative à la protection des données

A) **tous les trois (3) ans**

ou

B) **à chaque fois** que les risques liés aux opérations de traitement **changent**