5 KPI de la sécurité des données que votre entreprise doit absolument mesurer

Vous et vos collaborateurs prenez sans aucun doute les mesures nécessaires pour vous conformer au RGPD. Mais s'agit-il des mesures appropriées et les plus efficaces ? À l'aide de ces 5 KPI, vérifiez où vous en êtes concernant le RGPD. Vous saurez ainsi clairement si votre entreprise est sur la bonne voie pour tout ce qui concerne la protection des données.

1. Pourcentage des demandes relatives à la protection de la vie privée traitées dans les délais prescrits par la loi

Toute personne peut, à tout moment, s'informer auprès de votre entreprise des données dont vous disposez à son sujet. Votre entreprise doit lui répondre endéans le mois en lui fournissant une copie de ses données personnelles ainsi que les informations sur la manière dont ces données sont utilisées. Si vous ne respectez pas cette procédure, vous risquez des sanctions. Pour savoir si vos collaborateurs traitent ces demandes correctement et dans les délais, utilisez cette formule :

Demandes concernant la protection de la vie privée traitées dans les délais légaux / nombre total de demandes.

Idéalement, ce pourcentage doit être égal à 100.

2. Analyse d'impact positive relative à la protection de la vie privée

Le RGPD vous impose de conserver une **documentation interne** des activités de traitement et des mesures relatives à la sécurité dans votre entreprise.

Cette analyse d'impact relative à la protection des données (AIPD) doit comprendre au moins les éléments suivants :

- Une description détaillée des traitements et des finalités de ces traitements.
- Une évaluation de la proportion des traitements par rapport aux objectifs.
- Une évaluation des risques pour les droits et libertés des personnes concernées.
- Les mesures envisagées pour la gestion des risques.

Une AIPD n'est **obligatoire** que **pour les nouveaux processus**, mais la Commission de la protection de la vie privée recommande d'effectuer également une analyse de risque pour les processus courants à haut risque. C'est votre DPO qui est responsable de l'exécution de l'AIPD. Il/elle vous donnera les conseils adéquats en fonction des résultats, qui vous aideront à élaborer vos KPI ou à modifier les KPI existants.

5 KPI de la sécurité des données que votre entreprise doit absolument mesurer

3. Délai de détection et de résolution

Si un incident donné (fuite de données, abus…) présente un risque pour les personnes concernées, celles-ci, tout comme l'Autorité de protection des données, doivent **être informées de cette violation dans les 72 heures**.

Il est donc crucial pour la réputation de votre entreprise et des personnes concernées de réagir le plus rapidement possible après un incident et de le résoudre. Il existe des moyens simples pour **mesurer et de surveiller ce délai**. Essayez un outil comme Toggl, pour que votre équipe puisse le suivre collectivement heure par heure et minute par minute.

4. Nombre d'incidents de sécurité mineurs et majeurs

Il faut mesurer et surveiller les fuites de données ou infractions importantes relatives au RGPD, c'est évident. Mais vous devez aussi avoir l'œil sur les plus petits incidents ou ceux évités de justesse, car il s'agit souvent d'un test malicieux précédant une véritable attaque. Exemple d'incident de sécurité mineur : une escroquerie par **hameçonnage de courriels** ou une **activité inhabituelle sur votre serveur**.

Il n'est absolument pas certain qu'un seul petit incident puisse avoir un impact important sur votre entreprise, mis à part la frustration et le fait qu'il s'agisse d'un sérieux signal d'alarme. Mais des centaines d'incidents mineurs ou évités de justesse exigent des **efforts permanents** et entraînent des **frais** qui augmentent et finissent par ressembler à ceux d'un piratage plus important. Gardez donc une vue d'ensemble du nombre d'incidents de sécurité mineurs et majeurs et adaptez votre politique de sécurité si nécessaire.

5. Coûts par incident

Les frais par incident de piratage ne comprennent pas seulement ceux que votre entreprise dépense pour résoudre une attaque. Il est judicieux d'examiner à la fois les coûts par incident et le nombre de dossiers individuels.
Vous devez prendre en compte les frais pour :

- la cyber-recherche ;
- le personnel et les heures supplémentaires pour contenir l'incident ;
- une campagne RP d'information du public.

Il est possible que votre communication et votre réaction RP relatives à l'incident vous coûtent plus cher que la restauration de vos données et la suppression du logiciel malveillant de votre système. Mieux vaut donc discuter avec votre équipe de sécurité afin d'examiner toutes les conséquences de l'attaque et les moyens nécessaires pour la résoudre.

Source : Commission européenne

Conserver une vue d'ensemble de votre politique RGPD ?

Découvrez les avantages du logiciel de conformité RGPD →

E.R. : Paul De Ridder • Motstraat 30 • 2800 Malines