Initiatives clés de 2023

Formation au Code de Conduite

En 2023, 90% des collaborateurs de bpostgroup ont reçu une formation (conçue par les départements HR et Compliance) sur le Code de Conduite par le biais de sessions en présentiel pour les membres du personnel ne disposant pas d'une adresse e-mail professionnelle ou par le biais d'un module e-learning dédié pour les membres du personnel disposant d'une adresse e-mail professionnelle. Constituée de différentes sections, cette formation soulignait l'importance d'un comportement responsable envers les clients et les collègues.

Programme Speak Up

Un programme Speak Up a été lancé en 2023, avec un canal de signalement sécurisé disponible 24 heures sur 24 et 7 jours sur 7 (confidentiel ou anonyme). Tous les collaborateurs de bpostgroup ont été informés par lettre et par e-mail du lancement du programme et de la manière de signaler les incidents. Ces mêmes informations ont également été communiquées par le biais d'écrans vidéo et d'affiches dans tous les locaux de l'entreprise.

4.5 Garantir la confidentialité des données et la sécurité de nos clients et de notre personnel

Nous visons à garantir la sécurité des données de nos collaborateurs et de nos parties prenantes en appliquant pleinement et, dans certains cas, en dépassant même les normes internationales en matière de confidentialité des données dans l'ensemble de nos activités mondiales.

bpostgroup reconnaît que les informations, qu'elles appartiennent à bpost ou qu'elles soient détenues en fiducie pour le compte de ses clients et partenaires commerciaux, et les infrastructures informatiques dans lesquelles elles sont stockées sont des actifs essentiels de l'entreprise. bpostgroup s'engage dès lors à préserver la confidentialité, l'intégrité et la disponibilité de toutes les formes d'informations utilisées et conservées au nom des membres de son personnel, de ses partenaires commerciaux et de ses clients.

Par conséquent, des politiques, normes, directives et procédures spécifiques sont élaborées en vue d'aider à administrer et gérer le stockage et le traitement des informations requis dans le cadre d'activités menées de façon appropriée et légale. En traitant toutes les activités de gestion de l'information qui constituent une menace ou un risque pour les activités courantes de bpost, leur objectif est de faire en sorte que le risque soit minimisé ou accepté par le niveau de management approprié.

En outre, une feuille de route pour la sécurité de l'information a été élaborée, décrivant les étapes et les jalons nécessaires pour atteindre le niveau souhaité de sécurité de l'information. En tant que cadre d'amélioration continue, cette feuille de route est revue au moins une fois par an afin de rester à la pointe des menaces émergentes et de garantir que le cadre de sécurité de bpostgroup reste solide et que le risque de failles de sécurité est réduit au minimum.

Dans le cadre de la feuille de route sur la sécurité de l'information, un programme de gouvernance de la sécurité des données a été mis en place. Celui-ci couvre plusieurs sujets, tels que la découverte et la hiérarchisation des données, la gouvernance et les politiques, les techniques et les mesures de protection, ou la gestion des droits de l'information. Parallèlement à ce programme, d'autres initiatives visant à protéger les données et les informations à caractère sensible sont en cours ou prévues.

Du point de vue de la protection de la vie privée les priorités ont été mises sur la réorganisation de la gouvernance, l'amélioration de la gestion des incidents et la poursuite de l'automatisation des demandes d'accès par les personnes concernées.

Initiatives clés de 2023

Politique de classification des données

Dans le cadre du programme de gouvernance de la sécurité des données, la politique de classification des données a été complètement revue. L'objectif de cette politique est de fournir des conseils à toutes les parties prenantes et de les aider à comprendre la classification des données chez bpost. De plus, elle aide les propriétaires de données, propriétaires d'activités, dépositaires de données ICT, sous-traitants et fournisseurs, en vue de déterminer quel niveau de sécurité est requis pour protéger les données des systèmes bpost dont ils sont responsables. Le système de classification est basé sur la triade CIA internationalement reconnue : Confidentialité – Intégrité – Disponibilité.

Programme de détection des fuites de données

Avec le soutien d'un prestataire externe, un programme de détection des fuites de données est en cours de déploiement, à la recherche d'éventuelles fuites de données et d'informations liées à bpostgroup. Le programme se compose des aspects suivants :

- Protection de domaines via le contrôle et la détection des domaines malveillants ressemblant à des domaines authentiques de bpost et éventuellement utilisés pour lancer des campagnes d'hameçonnage et des cyberattaques ;
- Surveillance du Dark Web : détection et atténuation des attaques ciblées planifiées sur les forums du Dark Web, les apps de messagerie, etc. ;
- Prévention de la prise de contrôle des comptes en contrôlant et détectant des fuites d'informations d'identification critiques avant qu'elles ne soient compromises ;
- Prévention des violations de données via le contrôle, la détection et la sécurisation des données à caractère sensible accessibles au public avant qu'une violation ne puisse se produire.

Questionnaire sur la sécurité de l'information

Un questionnaire sur la sécurité de l'information a été élaboré en vue de se conformer à la directive de l'Union européenne NIS-2 (la législation sur la cybersécurité à l'échelle de l'UE) et plus particulièrement aux exigences relatives au risque de la chaîne d'approvisionnement. Nos fournisseurs sont invités à le compléter et, le cas échéant, à mettre en œuvre des mesures de sécurité supplémentaires. Le questionnaire étant basé sur la norme de sécurité de l'information ISO27001, la sécurité des données en fait partie intégrante.

Gestion des incidents ICT

bpostgroup a réalisé des progrès considérables dans la gestion des incidents ICT, notamment en améliorant le traitement des violations de données. Par exemple, dans le Code de Conduite, l'attention des collaborateurs de bpostgroup est spécifiquement attirée sur les incidents liés aux violations de données.