

Préparation de Broadbean au RGPD

Broadbean cherche en permanence à s'améliorer pour assurer le respect des normes appropriées eu égard à la nouvelle législation RGPD, en anticipant l'entrée en vigueur de ce règlement en mai 2018. Nous apporterons également un certain nombre de modifications à nos services et produits, afin d'accompagner nos clients dans leur démarche de respect du RGPD. Broadbean se concentre sur quatre domaines principaux, qui sont décrits ci-dessous et accompagnés d'exemples de certaines des caractéristiques de haut niveau qu'ils comportent.

Contrats

Le RGPD propose une définition plus formelle des relations entre responsable du traitement et sous-traitant et des responsabilités spécifiques pour chacun de ces rôles. Broadbean a révisé son Contrat standard de traitement de données pour définir clairement les relations contractant/sous-traitant et leurs rôles dans le cadre du contrat.

Le Contrat de traitement de données comporte également désormais des annexes définissant en détail les données à caractère personnel traitées par Broadbean pour ses clients, l'objectif de ce traitement, une annexe décrivant tous les sous-traitants ultérieurs de Broadbean et un résumé des mesures techniques et organisationnelles de haut niveau prises pour la sécurité des informations et des données.

En qualité de responsable du traitement des données, Broadbean n'est pas habilité à conserver les données à caractère personnel d'un client lorsqu'un contrat expire ou est annulé pour quelque raison que ce soit. Un certain nombre de modifications techniques simplifieront nos processus dans ce domaine, pour avertir les clients à l'approche de l'expiration de leur compte et pour supprimer toutes les informations nécessaires du compte une fois expiré.

Politique et audit

Broadbean vérifie et révisé les aspects de sa Politique de sécurité de l'information et son processus de Gestion des incidents dans le cadre de son processus standard de vérification des politiques et pour s'assurer qu'elles restent conformes au RGPD et aux bonnes pratiques du secteur.

Nous formaliserons les analyses d'impact relatives à la protection des données (DPIA) dans nos processus standard de développement des produits et nous introduirons des enregistrements améliorés de tous les accès à des Informations nominatives personnelles dans les services de Broadbean, afin de pouvoir surveiller et vérifier plus efficacement l'adéquation des accès à l'intérieur du système.

Outre la sécurité standard des informations et la formation de sensibilisation à la protection des données que nous dispensons déjà à tout le personnel, l'ensemble de notre personnel actuel et futur recevra également une formation sur le RGPD et son impact sur les différents postes.

Sécurité des informations

Broadbean met à jour et améliore continuellement ses contrôles et pratiques de sécurité de l'information. Les recommandations du RGPD et du G29 prévoient certains domaines spécifiques auxquels nous allons donner la priorité dans le cadre de cette feuille de route.

Les considérants du RGPD indiquent que les organisations devraient mettre en place des mesures pour garantir une protection des données par défaut et dès la conception. Broadbean minimisera les données détenues dans ses systèmes grâce à des politiques améliorées et des outils pour gérer la conservation des données, les comptes de test et les expirations de compte. Des analyses d'impact relatives à la protection des données (DPIA) seront utilisées dans le développement de tous les nouveaux produits pour permettre l'identification précoce du risque pour les données à caractère personnel dans le processus, minimiser l'accès et le traitement et identifier toutes les mesures de sécurité de l'information complémentaires nécessaires.

Partout où cela sera possible, nous mettrons en œuvre un chiffrement des données stockées pour les systèmes stockant des Informations nominatives personnelles et nous mettrons à jour nos intégrations avec nos portails d'emploi partenaires pour mieux soutenir le chiffrement des données en transit pour les candidatures déposées par les candidats.

Les processus existants de sauvegarde et de récupération après sinistre ainsi que la gestion des infrastructures et des correctifs sont vérifiés et mis à jour pour permettre une plus grande résistance aux attaques malicieuses et pour réduire les durées de RPO (objectif de durée de reprise) et RTA (durée de reprise réelle) dans un contexte de récupération après sinistre.

Outils pour les clients

En qualité de responsable du traitement des données, Broadbean conserve des données à caractère personnel pour le compte de ses clients. Par conséquent, nous devons être en mesure de fournir à nos clients des moyens appropriés pour gérer leurs données et leurs mesures de conformité. Nous sommes conscients que chaque client a des besoins différents à cet égard et nous fournirons donc un éventail de configurations, outils et caractéristiques pour respecter ces différentes exigences.

Par exemple, nous permettrons aux clients de définir leur propre période de conservation des données et fournirons des méthodes automatisées pour la suppression des données expirées, nous proposerons d'autres méthodes pour recueillir et redemander le consentement des candidats et nous fournirons des outils de récupération, exportation et suppression des données des candidats, pour que les clients puissent gérer les demandes des personnes concernées portant sur l'accès aux données, leur portabilité et leur suppression.