Sécurité du traitement des données (art. 32 du RGPD)

Mesures techniques et organisationnelles

Version du 21/03/2023

Ce document a pour objectif de présenter les mesures techniques et organisationnelles mises en œuvre par BigCaptain, en réponse à l'article 32 du Règlement général sur la protection des données (RGPD), traitant de la sécurité du traitement des données.

La liste et le détail de ces mesures n'étant pas figés dans le temps, ce document est amené à évoluer afin de rester en adéquation avec les changements technologiques, les nouvelles menaces en matière de sécurité et les évolutions réglementaires. Nous nous engageons à réviser régulièrement ces mesures techniques et organisationnelles pour garantir leur efficacité continue dans la protection des données des organisations sportives utilisant notre logiciel SaaS.

Caractère sensible des données et niveau du risque

Afin d'aider ses clients (les organisations sportives au sens large) de gérer efficacement leurs activités au travers du logiciel, BigCaptain permet à ses clients de stocker et gérer des données des utilisateurs finaux. Sans que cette liste soit exhaustive, les principales données personnelles (des utilisateurs finaux) susceptibles d'être enregistrées dans la base de donnés de BigCaptain sont les suivantes :

- Nom et prénom
- Date de naissance
- Nationalité
- Adresse(s)
- Adresse(s) email
- Numéro(s) de téléphone
- Mot de passe d'accès

Il est important de signaler que BigCaptain **n'enregistre pas**, dans sa version par défaut (*), de données dites "sensibles" telles que :

- Données de santé
- Données sur l'orientation sexuelle
- Données sur la prétendue origine raciale ou ethnique
- Les opinions politiques
- L'appartenance syndicale
- Les convictions religieuses
- Données génétiques et biométriques
- Données bancaires telles que les dates de validité et codes CCV des cartes de début/crédit, les soldes des comptes, etc.

(*) Il est à noter que BigCaptain permet à ses clients de créer eux-mêmes des champs personnalisés dans les fiches des clients finaux. L'utilisation ou non de ces champs, ainsi que la nature des données qui y sont stockées, sont sous l'entière responsabilité et sous le contrôle des clients de BigCaptain eux-mêmes. BigCaptain ne peut en aucun cas être tenu responsable de l'utilisation qui en est faite.

Sur base des informations fournies ci-dessus, BigCaptain estime que le **risque** relatif à des incidents de sécurité susceptibles de subtiliser ou d'endommager des données personnelles est "**modéré**" (par opposition à "faible" ou "élevé").

Mesures techniques

Chiffrement des données

Chiffrement des communications par TLS 1.3

Toutes les communications entre les utilisateurs et nos serveurs sont encryptées et authentifiées par le protocole TLS 1.3 , assurant ainsi la confidentialité et l'intégrité des données en transit.

Le protocole TLS 1.3 apporte des avantages significatifs en matière de confidentialité des données dans le contexte du RGPD (Règlement général sur la protection des données). Voici pourquoi il est essentiel :

- Chiffrement plus robuste : TLS 1.3 a abandonné la prise en charge des anciens algorithmes cryptographiques vulnérables présents dans TLS 1.2. Cela signifie que les communications sécurisées via TLS 1.3 sont moins susceptibles d'être compromises par des cyberattaques.
- Handshakes plus rapides : Les handshakes TLS dans TLS 1.3 nécessitent un seul aller-retour (ou communication aller-retour) au lieu de deux, ce qui accélère le processus de connexion. De plus, si le client s'est déjà connecté au site Web précédemment, le handshake TLS ne nécessite aucun aller-retour supplémentaire. Cela réduit la latence et améliore l'expérience utilisateur globale.
- Conformité au RGPD : Le RGPD exige que les données personnelles soient protégées

de manière adéquate. En utilisant TLS 1.3, BigCaptain renforce la sécurité des données en transit, garantissant ainsi la confidentialité des informations sensibles. Les certificats SSL/TLS signés par une autorité de certification authentifient également les serveurs, renforçant ainsi la confiance dans les échanges de données.

En somme, TLS 1.3 offre une meilleure sécurité, une confidentialité accrue et des performances améliorées, ce qui en fait un choix essentiel pour protéger les données conformément au RGPD.

Plus d'informations : https://www.kiteworks.com/fr/glossaire/transport-layer-security-tls/

Hachage des mots de passe avec BCrypt

Le hachage des mots de passe est essentiel pour garantir la confidentialité et la sécurité de ces données stockées dans la base de données de BigCaptain, en particulier dans le contexte du RGPD. Voici pourquoi il est crucial :

- Protection contre les fuites de données : Lorsque les mots de passe sont stockés en clair, comme dans une base de données non sécurisée, toute violation de sécurité expose directement les informations sensibles. En utilisant une fonction de hachage, les mots de passe sont transformés en valeurs de hachage irréversibles. Même si la base de données est compromise, les mots de passe restent inaccessibles aux attaquants.
- Non-réversibilité : Contrairement au chiffrement réversible, BCrypt génère des hachages irréversibles, et est donc un processus unidirectionnel. Les mots de passe sont transformés en une chaîne de caractères unique (le hachage) qui ne peut pas être inversée pour récupérer le mot de passe d'origine. Ainsi, même les administrateurs de la base de données ne peuvent pas accéder aux mots de passe en clair.
- Résistance aux attaques par force brute : Les fonctions de hachage comme BCrypt rendent difficile la récupération des mots de passe par des attaques de force brute. Les attaquants ne peuvent pas simplement essayer toutes les combinaisons possibles pour trouver le mot de passe d'origine. De plus, l'utilisation d'un sel (une valeur aléatoire ajoutée au mot de passe avant le hachage) renforce encore la sécurité en générant des hachages uniques pour chaque utilisateur.
- Conformité au RGPD : Le RGPD exige que les données personnelles soient protégées de manière adéquate. En utilisant l'algorithme de hachage BCrypt, BigCaptain se conforme aux exigences de sécurité et garanti que les mots de passe des utilisateurs restent confidentiels.

En somme, le hachage des mots de passe par BCrypt est un pilier fondamental pour protéger les données et respecter les réglementations en matière de confidentialité, comme le RGPD13.

Plus d'informations :
https://www.vaadata.com/blog/fr/comment-stocker-mots-de-passe-de-maniere-securisee-base-de-donnees/

Gestion des accès

Authentification par mot de passe sur BigCaptain

Les utilisateurs de type administrateur (les gestionnaires des infrastructures) et de type client (les clients de ces infrastructures) s'authentifient dans BigCaptain avec un utilisateur, typiquement leur adresse e-mail, et un mot de passe choisi par eux.

Ce mot de passe est stocké dans la base de donnée de BigCaptain avec les mesures de sécurité et de confidentialité adéquates (voir § Chiffrement des données).

Authentification protégé par Google reCaptcha sur BigCaptain

Le Google reCaptcha est utilisé dans le formulaire de connexion pour vérifier que l'utilisateur est un être humain légitime et non un robot automatisé. Cela renforce la sécurité du processus de connexion en empêchant les tentatives d'accès automatisées ou malveillantes.

Plus d'informations à ce sujet sur le site de Google :
https://www.google.com/recaptcha/about/.

Authentification forte sur BigCaptain (à venir)

Implémentation prochaine de méthodes d'authentification à deux facteurs (2FA, nécessitant ainsi plus qu'un simple mot de passe) pour accéder à son compte BigCaptain. Ces méthodes d'authentification seront alors déléguées à des services tiers spécialisés, comme Google, Azure AD ou Okta (à définir en fonction des besoins).

Authentification forte sur outils tiers

Utilisation de méthodes d'authentification à deux facteurs (2FA) ou multi-facteurs (MFA) pour renforcer la sécurité des comptes d'accès aux outils tiers (dont certains permettent d'accéder à des données personnelles des clients. Ces méthodes sont appliquées sur les outils suivants :

- Emails (Google Worskpace)
- Espace d'administration des hébergements/serveurs (Infomaniak)
- Espace de travail interne (Notion)
- Outil interne de communication (Slack)
- Outils de gestion des versions du code source de BigCaptain (Suite Atlassian)
- Outil de publipostage utilisé par BigCaptain pour communiquer vers les clients des infrastructures (MailJet)

Attribution de privilèges (profils) dans BigCaptain

Attribution de privilèges/profils d'accès en fonction des rôles et responsabilités de chaque utilisateur, limitant l'accès et/ou la nature de l'accès (consultation, modification, suppression) aux données sensibles uniquement aux personnes autorisées. Les profils d'utilisateurs suivants sont notamment disponibles (liste non exhaustive et non figée) :

- Super-administrateur

- Administrateur
- Administrateur (lecture seule)
- Réceptionniste
- Gestionnaire d'inscriptions aux activités
- Moniteurs
- Gardiens

Surveillance Continue de BigCaptain

Mise en place de mécanismes de surveillance des activités d'accès pour détecter les tentatives d'accès non autorisées ou les comportements suspects, permettant une réponse rapide en cas de menace.

Sécurité physique

Hébergement dans des centres de données sécurisés (Infomaniak)

Les serveurs du logiciel BigCaptain sont hébergés chez Infomaniak, prestataire suisse réputé notamment pour sa rigueur et sa fiabilité en matière de sécurité des données. Ceux-ci utilisent spécifiquement des centres de données certifiés et sécurisés, équipés de contrôles d'accès physiques stricts tels que des lecteurs de cartes d'accès, des caméras de surveillance et des gardes de sécurité.

Vous trouverez davantage d'informations à ce sujet dans l'espace Infomaniak dédié aux questions de sécurité.

Accès aux serveurs par SSH avec clé publique / clé privée

L'accès aux serveurs de BigCaptain, y compris donc à la base de donnée, ne peut se faire que par SSH en utilisant une paire de clés (privée/publique) propre à chaque administrateur de BigCaptain.

L'utilisation du mécanisme de clé privée / clé publique pour l'accès aux serveurs cloud de l'application BigCaptain est cruciale en matière de sécurité des données et de conformité au RGPD.

- Authentification forte : Le mécanisme de clé privée / clé publique offre une authentification robuste. Lorsqu'un utilisateur se connecte via SSH, il utilise sa clé privée pour prouver son identité. La clé publique correspondante est stockée sur le serveur. Cela garantit que seules les personnes possédant la clé privée associée peuvent accéder au serveur. Ainsi, l'accès est restreint aux utilisateurs autorisés.
- Confidentialité des données : Lors d'une connexion via SSH, la communication entre le client et le serveur est chiffrée. Les clés privées et publiques sont utilisées pour établir une connexion sécurisée. Cela protège les données en transit contre les interceptions malveillantes. Dans le contexte du RGPD, cela renforce la confidentialité des informations personnelles stockées dans la base de données.
- Gestion fine des accès : Les clés privées peuvent être attribuées à des utilisateurs

spécifiques. Vous pouvez contrôler qui a accès à quel serveur et quelles ressources. Cela permet de limiter les privilèges et de réduire les risques d'accès non autorisés. Le RGPD exige une gestion précise des accès aux données personnelles, et le mécanisme de clé privée / clé publique facilite cette tâche.

- Auditabilité : Les connexions SSH sont enregistrées dans les journaux. Cela permet de suivre qui s'est connecté, quand et depuis quelle adresse IP. En cas d'incident de sécurité ou de violation, ces journaux sont essentiels pour enquêter et prendre des mesures appropriées. La conformité au RGPD nécessite une traçabilité des accès aux données personnelles, et SSH fournit cette fonctionnalité.

En somme, l'utilisation du mécanisme de clé privée / clé publique via SSH renforce la sécurité, la confidentialité et la conformité au RGPD pour l'accès aux serveurs et aux bases de données de l'application BigCaptain.

Sauvegardes Régulières

Sauvegardes complètes et différentielles

Réalisation de sauvegardes complètes de toutes les données sur une base régulière, avec des sauvegardes différentielles pour capturer uniquement les modifications depuis la dernière sauvegarde complète, réduisant ainsi les temps de sauvegarde et de restauration. Les sauvegardes des 16 derniers jours sont garanties, ainsi qu'un nombre restreint de sauvegardes plus anciennes sur base hebdomadaire et mensuelle.

Le processus de sauvegarde mis en place par BigCaptain est conforme aux exigences du RGPD (Règlement général sur la protection des données) pour plusieurs raisons essentielles :

- Sauvegardes complètes quotidiennes : La réalisation de sauvegardes complètes chaque jour garantit que l'intégralité des données est copiée et stockée en toute sécurité. En cas de perte de données ou de défaillance du système, ces sauvegardes complètes permettent de restaurer l'état le plus récent des données. Cela répond à l'exigence du RGPD de garantir la disponibilité des données personnelles.
- Sauvegardes différentielles : Les sauvegardes différentielles capturent en outre les modifications apportées depuis la dernière sauvegarde complète. Cela réduit la quantité de données transférées et stockées, tout en préservant l'historique des modifications. Ainsi, les sauvegardes différentielles permettent de minimiser l'impact sur les ressources de stockage tout en respectant les principes de minimisation des données du RGPD.
- Stockage dans Swiss Backup (Infomaniak) : Le choix d'un stockage sécurisé chez Swiss Backup (Infomaniak) renforce la confidentialité des données. Infomaniak est réputé pour sa sécurité et sa conformité aux normes de protection des données. Le RGPD exige que les données soient stockées dans des environnements sécurisés, et Swiss Backup répond à cette exigence.
- Protection contre les fuites de données : En cas de violation de sécurité ou de perte de données, les sauvegardes permettent de restaurer les informations sans

compromettre la confidentialité. Les données stockées dans Swiss Backup sont cryptées et protégées contre les accès non autorisés.

En somme, le processus de sauvegarde complet, différentiel et sécurisé mis en place par BigCaptain contribue à la conformité au RGPD en garantissant la disponibilité, la confidentialité et l'intégrité des données personnelles.

Stockage hors site

Stockage des sauvegardes dans des emplacements sécurisés hors site, chez Swiss Backup (Infomaniak), pour garantir la disponibilité des données en cas de sinistre.

L'utilisation de Swiss Backup pour stocker les données de sauvegarde présente les avantages suivants :

- Sécurité : Swiss Backup est réputé pour sa sécurité et sa conformité aux normes de protection des données. Les sauvegardes sont stockées dans un environnement fiable et protégé.
- Confidentialité : Les données stockées chez Swiss Backup sont cryptées et protégées contre les accès non autorisés. Cela garantit la confidentialité des informations.
- Disponibilité : Les sauvegardes sont accessibles à tout moment, ce qui permet de restaurer rapidement les données en cas de besoin.

Gestion des vulnérabilités

Mise en place de correctifs de sécurité

Mise en place d'une procédure de déploiement rapide "hors release" des correctifs de sécurité dès qu'ils sont disponibles pour corriger les vulnérabilités découvertes et réduire les risques de compromission des données.

Suivi des accès et des activités

Utilisation de solutions de surveillance

Enregistrement systématique, dans un journal d'activité intégré au logiciel BigCaptain, de tout accès et de toute suppression/modification de donnés. Ce mécanisme permet alors la surveillance de ce journal en vue d'analyser les accès et les actions des utilisateurs, facilitant ainsi la détection des activités suspectes ou non autorisées, ainsi que l'analyse de cas suspicieux et des incidents éventuels.

Analyse proactive du journal d'activité (à venir)

Il est prévu de mettre prochainement en place des mécanismes d'analyse régulière et proactive du journal d'activité afin de détecter les anomalies ou les violations potentielles de la sécurité, permettant ainsi une détection anticipée et une réponse rapide aux incidents de sécurité.

Pseudonymisation et chiffrement des données à caractère personnel (à venir)

En vue de renforcer la sécurité et la confidentialité des données, il est prévu de pseudonymiser et chiffrer les données à caractère personnel stockées dans la base de données de BigCaptain afin de réduire les risques liés à leur accès non autorisé ou à leur divulgation. Ces mesures contribueront à garantir que les données sensibles sont protégées contre les violations de la vie privée et les atteintes à la sécurité.

Ce chiffrement consistera à transformer les données en un format illisible sans la clé de chiffrement appropriée. Cela garantira que même si des tiers non autorisés accèdent aux données, ils ne pourront pas les comprendre ou les utiliser.

En plus du chiffrement, l'utilisation d'identifiants (nombre entiers) permettra la pseudonymisation totale des informations stockées dans BigCaptain.

Mesures organisationnelles

Formation et Sensibilisation

Formation du personnel

Formation régulière du personnel sur les bonnes pratiques de sécurité des données, les politiques de sécurité de l'entreprise et la manipulation sécurisée des informations sensibles.

Sensibilisation des utilisateurs finaux (à venir)

Il est prévu de rédiger prochainement des ressources (FAQ, guides, aide en ligne) accessibles aux utilisateurs de BigCaptain visant à sensibiliser ceux-ci aux risques liés à la sécurité des données, afin de les aider à protéger leurs données personnelles.

Politiques de confidentialité et de protection des données

Publication d'une politique de confidentialité

Publication d'une politique de confidentialité détaillée décrivant les pratiques de collecte, d'utilisation et de protection des données des utilisateurs.

Adoption de politiques internes

Adoption de politiques internes strictes pour garantir le respect de la confidentialité des données et la conformité aux réglementations en matière de protection des données.

Conformité réglementaire

Engagement à respecter les exigences légales

Engagement à respecter toutes les exigences légales et réglementaires en matière de protection des données, y compris le RGPD.

Collaboration avec des experts juridiques

Collaboration avec des experts juridiques pour s'assurer de la conformité continue aux lois et réglementations pertinentes en matière de protection des données.

Évaluation des risques et plan de gestion

Évaluation des risques

Réalisation régulière d'évaluations interne des risques pour identifier les menaces potentielles à la sécurité des données, évaluer leur impact et leur probabilité, et déterminer les mesures appropriées à prendre pour les atténuer. Les conclusions de ces évaluations sont consignées dans un rapport d'audit interne pouvant donner lieu à la mise en œuvre de nouvelles actions concrètes (reprise dans le plan de gestion des risques).

Plan de gestion des risques

Élaboration et mise en œuvre d'un plan interne de gestion des risques décrivant les actions spécifiques à prendre pour réduire les risques identifiés, y compris les mesures techniques, organisationnelles et juridiques.

Gestion des Incidents de sécurité

Plan de réponse aux incidents (en cours de mise en oeuvre)

Élaboration d'un plan de réponse aux incidents détaillant les étapes à suivre en cas de violation de la sécurité des données, y compris la notification des autorités compétentes et des personnes concernées, ainsi que les actions correctives à prendre pour atténuer les impacts.

Formation (à venir)

Mise en place prochaine de sessions de formation du personnel aux procédures de gestion des incidents de sécurité.

Audit et surveillance continus

Audit de sécurité (à venir)

Il est prévu de réaliser, dans les mois à venir, un audit de sécurité pour évaluer la conformité aux politiques de sécurité et aux normes de l'industrie, ainsi que pour identifier les opportunités d'amélioration. Il sera ensuite prévu de répéter cet exercice à intervalles de

temps réguliers raisonnables.

Surveillance continue

Surveillance continue des environnements informatiques pour détecter les activités suspectes ou les anomalies de sécurité, permettant ainsi une réponse rapide aux menaces potentielles.