Mesures techniques et organisationnelles (MTO) chez seca

Description des mesures techniques et organisationnelles prises par seca conformément à l'article 32 du RGPD.

seca exploite un système de gestion de la sécurité de l'information certifié, intégration la gestion de la protection des données, conformément aux normes internationales ISO/IEC 27001:2022 et ISO/IEC 27701:2019.

A. Pseudonymisation et cryptage (article 32 (1) (a) RGPD)

Cryptographie

- Utilisation de la cryptographie par courriel et de procédures sécurisées pour l'échange de messages (par exemple TLS 1.2 ou 1.3) et de procédures sécurisées pour le stockage de données (par exemple AES-256)
- Gestion sécurisée des clés
- Anonymisation ou pseudonymisation lors du traitement des données de recherche
- Pseudonymisation dans les fichiers journaux (fichiers log)

B. Confidentialité, intégrité, disponibilité et résilience des systèmes et services de traitement (article 32 (1) (b) RGPD)

Organisation de la sécurité de l'information

- Utilisation d'un logiciel central pour la gestion des smartphones (Mobile Device Management)
- Possibilité de suppression à distance des données sur les appareils mobiles
- Évaluation et vérification régulière des prestataires/fournisseurs en matière de sécurité de l'information et de protection des données
- Attention particulière lors du choix du personnel de nettoyage et de sécurité

Sécurité du personnel

- Engagement des employés à respecter les directives de protection des données et de sécurité de l'information, ainsi que les exigences spécifiques des personnes tenues au secret professionnel
- Politique « bureau propre » et « écran propre »
- Formation régulière sur la protection des données et la sécurité de l'information, incluant la sensibilité au phishing, la gestion des appareils non utilisés inutilisés, la désactivation des services obsolètes et la gestion des informations d'authentification, clés et badges

Gestion des actifs

- Inventaire systématique des équipements informatiques
- Documentation de la remise et du retour des équipements informatiques
- Directive sur la gestion des documents, définissant les niveaux de confidentialité et des marquages appropriés
- Recours à des destructeurs de documents certifiés pour la destruction des fichiers et supports électroniques
- Utilisation d'un logiciel certifié pour l'effacement des supports de données électroniques
- Journalisation de la destruction ou suppression des documents et des supports de données électroniques

Contrôle des accès

- Mise en place d'un système automatisé de contrôle des accès (Identity and Access Management, IAM)
- Application d'une politique d'attribution des accès selon un modèle de droits par rôle
- Attribution des droits selon le principe du « besoin de savoir » ("Need to know")
- Processus formalisé d'attribution des droits nécessitant l'approbation du supérieur hiérarchique ou du propriétaire des données
- Suppression du compte utilisateur ou retrait des droits d'accès à la sortie de l'entreprise
- Adaptation des droits d'accès en cas de changement de fonction
- Système de connexion unique (SSO) pour toutes les applications essentielles
- Concepts de permissions de lecture/écriture pour les lecteurs et les fichiers, ainsi que pour les pages et les sections individuelles du wiki interne
- Concepts de droits de lecture/écriture pour les systèmes de tickets
- Gestion centralisée des droits via le service de domaine Microsoft Active Directory
- Politique de mot de passe incluant la longueur, la complexité, l'historique et la durée de validité du mot de passe
- Obligation de modifier le mot de passe initial lors de la première connexion
- Attribution de comptes utilisateurs supplémentaires pour les administrateurs (en plus de leur compte utilisateur personnel)
- En principe, aucun droit d'administrateur de domaine ou local pour les utilisateurs (exception : droits d'administrateur local pour les ordinateurs d'un réseau développeur spécialement partitionné)
- Accès sécurisé par badge aux imprimantes et files d'attente individuelles
- Journalisation des accès aux applications, en particulier lors de la saisie, de la modification et de la suppression de données
- Journalisation des tentatives de connexion infructueuses
- Blocage du compte utilisateur en cas de dépassement du nombre maximal de tentatives échouées
- Authentification à deux facteurs pour tous les utilisateurs
- Restriction de l'utilisation des applications via la gestion des postes de travail
- Accès au code source des programmes au sein du département Recherche et Développement (R&D) réservé aux développeurs uniquement

Sécurité physique et environnementale

- Vidéosurveillance des accès au site et des zones sensibles
- Protection par détecteurs de mouvement et barrières lumineuses
- Système d'alarme pour les zones sensibles (y compris les salles de serveurs)
- Réception ouverte et occupée à l'entrée du site pendant les heures ouvrables
- Accès aux zones sensibles par badge pour les employés
- Badges d'accès au site avec photo
- Enregistrement des visites des personnes extérieures (liste des visiteurs et badges)
- Accompagnement des visiteurs par un employé sur le site
- Emplacement des salles de serveurs dans des endroits choisis pour les protéger des accès non autorisés, des dégâts dus à l'eau ou au feu, des coups de foudre, etc.
- Emplacement des salles de serveurs redondantes dans des bâtiments différents
- Connaissance de l'existence et de l'activité dans des zones particulièrement sensibles (incluant les salles de serveurs) selon le principe du « besoin de savoir » (*Need to know*)
- Les zones particulièrement sensibles ne sont pas identifiables en tant que telles et ne sont pas directement accessibles de l'extérieur
- Accès des personnes extérieures aux salles de serveurs uniquement avec escorte
- Climatisation et surveillance de la température et de l'humidité dans les salles de serveurs
- Extincteurs et système de détection d'incendie
- Système de détection d'incendie sensible dans les salles de serveurs
- Câblage physiquement protégé
- Boîtes de distribution ou armoires fermées dans des zones particulières

Sécurité des communications et des réseaux

- Segmentation des réseaux pour protéger les zones et systèmes sensibles (par ex. développement, production)
- Séparation des réseaux WLAN pour différents usages (par ex. WLAN séparé pour les invités)
- Limitation des systèmes intégrés dans le réseau
- Contrôle automatique des terminaux connectés au réseau (Network Access Control, NAC)
- Désignation de responsables du réseau et intégration d'un prestataire de services choisi pour l'administration du réseau
- Règles strictes pour l'attribution des droits d'accès aux réseaux et aux services réseau
- Utilisation systématique de pares-feux de nouvelle génération avec technologie VPN
- Utilisation systématique de logiciels antivirus
- Utilisation de systèmes de détection d'intrusion
- Journalisation et surveillance permanents des activités et événements du réseau (Security Information and Event Management, SIEM)
- Surveillance 24/7 de l'infrastructure informatique par un Security Operations Center (SOC)

Acquisition, développement et maintenance des systèmes

- Développement de logiciels pour applications internes selon les mêmes normes et processus que pour les logiciels médicaux
- Processus de contrôle des modifications établi également pour les applications internes
- Processus de vérification et de validation des applications développées en interne et en externe
- Réseau spécialement protégé pour le développement de produits et d'applications internes
- Environnement de test spécialement protégé
- Génération de données de test spécifiques à la place de données réelles contenant des informations personnelles

Relations avec les prestataires et les fournisseurs

- Sélection rigoureuse du personnel de sécurité et de nettoyage
- Conclusion de contrats de traitement des données conformément à l'article 28 RGPD en cas de traitement de données sur mandat, ou inclusion de clauses de protection des données et accords de confidentialité en cas de mandat de prestataires de services et de fournisseurs

C. Rétablissement rapide de la disponibilité et de l'accès (article 32 (1) (c) RGPD)

Sécurité opérationnelle

- Surveillance des ressources
- Suppression régulière des données obsolètes pour optimiser l'espace de stockage
- Mise hors service des applications, systèmes, bases de données ou environnements lorsque leur utilité cesse
- Optimisation des processus batch et des plannings
- Limitation de la bande passante pour les services gourmands en ressources (par exemple, streaming vidéo)
- Séparation des environnements de développement, de test et de production pour les services cloud, les applications et les systèmes internes
- Filtre Web et blocage des téléchargements
- Abonnement aux services d'alerte et d'information pertinents
- Processus de sauvegarde des données par génération et test régulier de la récupérabilité des sauvegardes
- Stockage d'une partie des sauvegardes dans un emplacement externe
- Gestion des changements et processus d'approbation pour la mise à jour des applications
- Vérification des applications avant leur installation sur un système de test
- Utilisation de stratégies rollback pour la mise à jour des applications

Aspects de la sécurité de l'information dans la gestion de la continuité des activités

- Mise en place d'un système de gestion de la continuité des activités
- Documentation et vérification des plans d'urgence
- Utilisation d'un logiciel de gestion des urgences informatiques

- Accès à Internet d'urgence via un second fournisseur
- Alimentation électrique sans interruption (UPS)
- Groupe électrogène diesel permettant une autonomie de deux jours pour les systèmes informatiques

D. Révision, vérification et évaluation régulières de l'efficacité (article 32 (1) (d) RGPD)

- Examen, vérification et évaluation régulier dans le cadre du système de gestion de la sécurité de l'information (SGSI)
- Exécution technique par le responsable de la sécurité de l'information, qui rend compte directement à la direction générale, indépendamment du service informatique et des autres services spécialisés.

Gestion des incidents de protection des données et de sécurité de l'information

- Processus de traitement des incidents de protection des données et de sécurité de l'information

Compliance

- Assistance en matière de protection des données et de sécurité de l'information par le service juridique interne

Contrôle des sous-traitants (implication de tiers / externalisation)

- Conclusion des accords nécessaires pour le traitement des commandes en vertu de l'article 28 RGPD ou des clauses contractuelles types de l'UE en cas de sous-traitance dans un pays tiers (art. 44ss RGPD)
- Règles relatives à l'utilisation de sous-traitants supplémentaires
- Vérification régulière des sous-traitants

E. Mesures liées aux services cloud

- seca exploite ses services SaaS exclusivement sur l'infrastructure du sous-traitant Amazon Web Services EMEA SARL (AWS) spécialisé dans l'hébergement de serveurs externes, situé à Francfort-sur-le-Main (pour les clients situés dans l'UE/EEE).
- seca chiffre toutes les données personnelles dans les services SaaS afin d'empêcher tout accès non autorisé à ces données.
- La gestion des clés est assurée par seca.