Contenu

Sécurité de l'information et protection des données

Champ d'application

Les chapitres qui suivent décrivent les mesures techniques et organisationnelles prises par Transfusion CRS Suisse SA (ci-après T-CH) en matière de sécurité de l'information et de protection des données afin de préserver les données personnelles. Ces mesures s'appliquent dans les cas où T-CH traite directement les données concernées en tant que responsable. Si T-CH mandate des tiers pour traiter les données, des conventions contractuelles sont conclues afin de s'assurer que les tiers observent des mesures équivalentes à celles de T-CH.

Contrôle des accès aux locaux

Sont définies ici toutes les mesures visant à empêchant des personnes non autorisées de pénétrer sur des sites, bâtiments ou locaux, où sont traitées des données ou bien qui hébergent des systèmes de traitement des données.

Mesures techniques	Mesures organisationnelles
• Sécurisation des fenêtres et des portes • Installation de systèmes de fermeture avec badges ou clés physiques • Sécurisation de l'accès aux salles de serveurs à l'aide de badges électroniques/lecteurs biométriques • Surveillance vidéo conforme à la législation sur la protection des données dans les salles de serveurs externes	• Accueil des visiteurs à l'entrée principale (sonnette) et à la réception • Accompagnement et journal des visiteurs • Sélection soigneuse du personnel d'entretien • Elaboration d'instructions sur la sécurité physique et sur celle de l'environnement de travail • Zonage des locaux

Contrôle des accès aux systèmes de traitement des données

Le but de ces mesures est d'empêcher tout usage non autorisé des archives et des systèmes de traitement des données. Les systèmes de traitement des données, telles les applications, ne peuvent être utilisés que par des personnes habilitées dans ce sens.

Mesures techniques	Mesures organisationnelles

• Connexions VPN sûres pour les administrateurs et les collaborateurs • Cryptage des porteurs de données et des appareils finaux mobiles • Pare-feu sûrs • Logiciels anti-virus / Endpoint Detection and Response (détection et réponse des terminaux) • Authentification au moyen d'identifiants et de mots de passe • Authentification à deux facteurs • Verrouillage automatique des ordinateurs	• Réglementation relative aux clés • Directives globales, dont • Règles sur les mots de passe, y c. consignes sur la complexité des mots de passe • Directive « Clean Desk » (bureau « propre », dépourvu de tout papier) / verrouillage de l'écran • Règles d'accès pour les personnes externes/internes

Personnel digne de confiance pour les secteurs de la sécurité et de l'entretien
Génération de profils d'utilisateurs
Attribution de droits d'utilisateurs

Contrôle des accès aux porteurs de données

Sont définies ici toutes les mesures permettant d'assurer le respect des autorisations d'accès.

Mesures techniques	Mesures organisationnelles
• Elaboration de protocoles/journaux des accès à des applications et à des procédures, telle la suppression de données • Destruction des porteurs de données (documents, lecteurs) conforme à la législation sur la protection des données • Cryptage des porteurs de données et des appareils finaux mobiles • Système d'identification et d'authentification • Stockage des porteurs de données et des documents dans des locaux sécurisés • Archivage des données sécurisé grâce à des droits d'accès définis • Pseudonymisation des données dans les systèmes de test	• Manuel d'habilitation • Manuel du statut d'utilisateur et de la répartition des rôles • Adaptation du nombre d'administrateurs disposant des pleins droits d'accès • Destruction des données (porteurs de données et documents papier) par des prestataires certifiés

Contrôle des transferts

Sont regroupées ici toutes les mesures garantissant la sécurité des données personnelles lors d'un transfert de données. La notion de transfert englobe les transmissions électroniques, le transport et la sauvegarde de données personnelles.

Mesures techniques	Mesures organisationnelles
• Technologie VPN sûre • Cryptage du transport (SSL, etc.) • Cryptage des messages électroniques dans les échanges avec EMDIS	• Tenue d'une liste des activités de traitement • Contrôle périodique des destinataires de données, tenue à jour des listes de destinataires dans le CRM • Recours à des services de transport externes dignes de confiance • Formation des prestataires de transport qui ont accès à des données personnelles sensibles

Contrôle de la saisie

Mesures techniques	Mesures organisationnelles

• Elaboration automatique d'un protocole / journal de saisie, de modification et de suppression des données dans la mesure où cela est requis et soutenu par le système	• Mise en place et utilisation d'identifiants individuels • Mise en place et utilisation d'identifiants individuels pour les administrateurs • Attribution de droits d'accès

Contrôle des mandats

Le contrôle des mandats s'exerce à chaque fois qu'un mandat est traité. Il vise à garantir que le traitement des mandats est exclusivement exécuté dans le respect des instructions du mandant.

Mesures techniques	Mesures organisationnelles
• Aucune	• Sélection soigneuse du mandataire • Remise d'instructions écrites au mandataire • Conclusion de contrats sur le traitement des mandats conforme à la législation sur la protection des données • Obtention de droits efficaces de contrôle de l'activité du mandataire • Evaluation régulière du mandataire (évaluation du fournisseur)

Contrôle de la disponibilité

Lors du contrôle de la disponibilité et de la récupération des données, il faut s'assurer que les données personnelles sont suffisamment protégées de toute perte ou destruction pour pouvoir être récupérées en cas de problème.

Mesures techniques	Mesures organisationnelles
• Sécurisation des données • Protection anti-virus • Pare-feu • Doubles serveurs • Climatisation des salles de serveurs • Surveillance de la température des salles de serveurs et de celle des serveurs • ASI (alimentation de courant sans interruption) • Générateur de secours • Détecteur de fumée et à incendie • Installations d'extinction • Manuel de protection des données • Gestion des urgences informatiques • Gestion de crise	• Positionnement approprié des salles de serveurs (protection contre les risques, p.ex. inondations, incendie) • Réglementation sur la sécurisation des données • Tests de récupération des données

Contrôle des séparations

Lorsque des données personnelles sont saisies à des fins distinctes, il faut s'assurer qu'elles seront bien traitées isolément (principe de la séparation).

Mesures techniques	Mesures organisationnelles
• Séparation des environnements de production et de test • Séparation claire des données saisies à des fins distinctes • Séparation des clients dans les serveurs/les systèmes	• Séparation des clients • Droits d'accès aux banques de données et manuel d'habilitation adaptés aux séries de données • Pilotage du contrôle des séparations à l'aide du manuel d'habilitation

Vérification et évaluation

Mesures techniques	Mesures organisationnelles
• Tests de pénétration et audits ISDS menés régulièrement par l'OFSP • Surveillance du système	• Gestion des modifications • Gestion des risques • Assistance informatique et support offerts par le service informatique/système d'annonce • Gestion des fournisseurs