ANNEXE III

Mesures techniques et organisationnelles, notamment celles visant à garantir la sécurité des données

Table des matières

Contexte et objectifs

La société Perseus Technologies GmbH (« Perseus ») met en œuvre des mesures techniques et organisationnelles (« MTO ») appropriées afin de garantir la confidentialité, l'intégrité et la disponibilité des données à caractère personnel, ainsi que la résilience des systèmes. Le terme « appropriées » signifie ici que les mesures sont adaptées et proportionnées aux risques à maîtriser.

Lors de la planification, de la mise en œuvre et de l'application des mesures, Perseus tient compte de l'état de la technique, des coûts de mise en œuvre, de la nature, de la portée, des circonstances et des finalités du traitement, ainsi que de la probabilité variable de survenance et de la gravité du risque pour les droits et libertés des personnes physiques. Ces mesures comprennent notamment :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- la capacité à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services liés au traitement ;

- la capacité à rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique ;
- une procédure permettant de contrôler, d'analyser et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement.

Lors de l'évaluation du niveau de protection adéquat, Perseus tient notamment compte des risques liés au traitement (par exemple, la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel, ou l'accès non autorisé à celles-ci).

Ces exigences sont reflétées et documentées dans les catégories suivantes de mesures techniques et organisationnelles (TOM) :

- Confidentialité (art. 32, al. 1, let. b du RGPD)
- Intégrité (art. 32, al. 1, let. b du RGPD)
- Disponibilité et résilience (art. 32, al. 1, let. b du RGPD)
- Procédures de contrôle, d'analyse et d'évaluation régulières (art. 32, al. 1, let. d du RGPD, art. 25, al. 1 du RGPD)

Le présent document sert notamment à satisfaire à l'obligation de preuve des parties contractantes en matière de protection des données.

Outre les mesures techniques et organisationnelles (MTO) au sens de la législation sur la protection des données, notamment conformément à l'article 32 du RGPD, Perseus a mis en place un système de gestion de la sécurité de l'information (SGSI) qui s'appuie sur les exigences de la norme internationale ISO/IEC 27001:2013.

Portée et champ d'application

Perseus met en œuvre des mesures de sécurité des données tant pour ses propres traitements de données que pour les traitements effectués dans le cadre de la prestation des différents services de cybersécurité de Perseus. Pour assurer la prestation de ses services, Perseus fait appel à des sous-traitants qui, sur la base de contrats de sous-traitance convenus (art. 28 du RGPD), effectuent un traitement des données à caractère personnel pour son compte, en se conformant à ses instructions. Ces relations de sous-traitance et les accords correspondants constituent des relations de sous-traitance au sens du présent accord. Les sous-traitants ainsi engagés respectent au minimum les normes de sécurité fixées par Perseus. Les mesures techniques et organisationnelles (TOM) propres à Perseus ainsi que celles des sous-traitants se complètent parfaitement dans le cadre de la prestation de services et garantissent ensemble un niveau adéquat de sécurité des données.

Le présent document décrit les mesures de sécurité des données pertinentes pour la fourniture des différents services de cybersécurité de Perseus.

Description des différentes mesures

Confidentialité (art. 32, al. 1, let. b du RGPD)

Contrôle d'accès – Protection contre l'accès non autorisé aux installations de traitement des données

Technique	Organisatoire
• Système électronique de contrôle d'accès pour les sites d'exploitation utilisés par Perseus (cartes à puce/transpondeurs) • Serrures de sécurité mécaniques • Détecteurs de mouvement • Vidéosurveillance des accès • mesures adéquates en cas de	• définition de zones de sécurité pour les sites d'exploitation utilisés par Perseus • Attribution et gestion des droits d'accès basées sur les rôles et documentées (« Role Based Access Control – RBAC ») avec processus intégré « Joiner-Mover-Leaver » • Règlement relatif à l'accès des visiteurs aux

Perseus sous-traitants	sites d'exploitation utilisés par Perseus, notamment l'affectation à un collaborateur de Perseus, l'enregistrement de la visite, l'obligation de porter un badge visiteur • service de sécurité • Mesures adéquates auprès des sous-traitants

Contrôle d'accès - Protection contre l'utilisation non autorisée du système

Technique	Organisatoire
• Authentification par identifiant utilisateur + mot de passe • Authentification à deux facteurs • Pare-feu • Réseau privé virtuel (VPN) • Protection antivirus • Verrouillage automatique de l'écran • des mesures adéquates concernant les sous-traitants désignés par Perseus sous-traitants	• Attribution et gestion des droits d'accès basées sur les rôles et documentées (« Role Based Access Control – RBAC ») avec processus intégré de gestion des arrivées, des transferts et des départs • Règles relatives aux mots de passe et procédures de réinitialisation • Mesures adéquates concernant les sous-traitants

Contrôle d'accès – Protection contre la lecture, la copie, la modification ou la suppression non autorisées de données au sein d'un système informatique

Sur le plan technique	Organisatoire
• Journalisation des accès aux applications, notamment lors de la saisie, de la modification et de la suppression de données • Chiffrement des disques durs des terminaux • Chiffrement des supports de données • Utilisation de destructeurs de documents	• Classification des informations (publiques/internes/confidentielles) • Attribution des autorisations selon le principe du « besoin d'en connaître » • Attribution et gestion des droits d'accès basées sur les rôles et documentées (« Role Based

• Mesures adéquates auprès des sous-traitants	« Access Control RBAC ») avec processus intégré « Joiner-Mover-Leaver » • Règles relatives aux mots de passe et procédure de réinitialisation • Recours à des prestataires de services pour la destruction des dossiers et des données conformément à la norme DIN 66399 • Mesures adéquates concernant les sous-traitants

Principe de séparation – Traitement séparé des données

Sur le plan technique	Organisatoire
• Séparation des environnements de développement, de test et de production • Mesures adéquates auprès des sous-traitants sous-traitants	• Séparation physique ou logique des mandants • Mesures adéquates concernant les sous-traitants

Pseudonymisation – art. 32, al. 1, let. a du RGPD, art. 25, al. 1 du RGPD – Sans recourir à des informations supplémentaires, les données à caractère personnel ne peuvent être associées à aucune personne concernée spécifique

Technique	Organisational
• Séparation du fichier d'affectation et de son stockage sur un système informatique distinct et sécurisé • Mesures adéquates concernant les sous-traitants	• Vérification, pour toutes les activités de traitement, de la possibilité d'un traitement pseudonymisé des données • Mesures adéquates concernant les sous-traitants