Annexe «Mesures d'ordre technico- organisationnel» selon l'art. 9 de la BDSG

§ 1 Mesures de sécurité techniques et organisationnelles

Les parties contractantes s'accordent sur les mesures de sécurité techniques et organisationnelles selon l'art. 11 al. 2 p. 2 n° 3 LFPD en association avec l'art. 9 de la même loi.

§ 2 Organisation interne de l'autorité ou de l'entreprise du mandataire

Le mandataire structurera l'organisation interne de son entreprise de manière à respecter les exigences particulières à la protection des données. Cela nécessite notamment de mettre en œuvre des mesures adaptées au type de données ou de catégories de données personnelles à protéger.

§ 3 Concrétisation des mesures individuelles

Les mesures suivantes sont individuellement établies:

N°	Mesure	Mise en œuvre de la mesure
1	Contrôle des accès L'accès aux installations dédiées au traitement ou à l'utilisation de données personnelles doit être refusé aux personnes non autorisées.	• Définition des personnes autorisées • (internes et externes à l'entreprise) • Régime de l'Access Chip • Régime pour des tiers extérieurs à l'entreprise • Protection même en dehors des heures d'ouverture grâce à un système d'alarme • Porte avec dispositif de sécurité (fermeture électrique de porte, lecteur de badge) • Elaboration de mesures garantissant • la sécurisation des bâtiments (par ex. système d'alerte en cas d'intrusion, surveillance de l'enceinte)

2	Contrôle des accès L'utilisation des systèmes de traitement de données doit être interdite aux personnes non autorisées.	• Cryptage partiel • Attribution et garantie des clefs d'identification (User ID) • Régime des autorisations des utilisateurs • Obligation de respecter la confidentialité des données selon l'art. 5 LFPD • Régime des accès différenciés (par ex. grâce au verrouillage de l'accès à certains segments) • Enregistrement et évaluation de l'utilisation des données
3	Contrôle des autorisations Il est nécessaire de s'assurer que les personnes autorisées à utiliser un système de traitement des données le fassent uniquement dans le cadre de leur autorisation d'accès et que des données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation lors du traitement, de l'utilisation et après l'enregistrement.	• Cryptage • Régime de l'autorisation d'accès • Evaluation de protocoles • Possibilités d'accès partiel à des données stockées et à des fonctions

4	Contrôle du transfert Il est nécessaire de s'assurer que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transfert électronique, pendant leur transport ou leur stockage sur des supports de données. Il faut également être en mesure de vérifier et de déterminer à quelles instances il est prévu de transmettre des données personnelles via des installations de transmission des données.	• Cryptage • Définition des personnes autorisées • Accès sécurisé au centre de données pour la livraison et l'expédition • Remise de supports de données uniquement aux personnes autorisées (par ex. reçu de commande, document annexe) • Gestion et contrôle de l'inventaire des supports de données • Cryptage spécial des supports de données confidentiels • Armoires de sécurité • Destruction contrôlée des supports de données (par ex. erreurs d'impression) • Régime de réalisation de copies • Documentation des programmes d'interrogation et de transmission • Utilisateurs autorisés • Consignes d'emballage et d'expédition (expédition dans des conteneurs fermés par ex.) • Retrait direct, service de coursier, accompagnement du transport • Suppression des données restantes avant l'échange de supports de données
5	Contrôle de la saisie Il est nécessaire de s'assurer qu'il est possible de vérifier et de déterminer ultérieurement si, et par qui, des données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement de données.	• Justificatif des responsabilités définies au niveau de l'organisation en matière de saisie • Enregistrement des saisies • Enregistrement de l'utilisation des données • Organisation des processus, des programmes et des opérations • Obligation de respecter la confidentialité des données

6	Contrôle des mandats Il est nécessaire de s'assurer que les données personnelles traitées lors d'un mandat le sont uniquement selon les instructions du donneur d'ordre.	• Respect des contrats de traitement des données • Transport sécurisé des données et supports de données (en règle générale DHL) • Traitement sécurisé des données • Suppression sécurisée des données à l'achèvement du mandat • Processus internes d'exécution du mandat et surveillance des processus • Processus Standard Change Management (selon ITIL)
7	Contrôle de disponibilité Il est nécessaire de s'assurer que les données personnelles soient protégées contre une éventuelle destruction ou perte.	• Mesures de protection des données (physiques/logiques) • Sauvegardes • Procédures de sauvegarde et archivage • Restauration de l'infrastructure (Disaster Recovery) • Protection contre les «Malicious Codes»
8	Contrôle de la séparation Il est nécessaire de s'assurer que les données collectées puissent être traitées de manière séparée en fonction des objectifs.	• Mesures de traitement séparé (enregistrement, modification, suppression et transfert) de données utilisées à des fins différentes • Séparation des mandants • Séparation des fonctions • Séparation des systèmes de test et productifs