ANNEXE 1

Description des mesures techniques et organisationnelles

de la société Julius Zorn GmbH

I. Confidentialité [art. 32 par. 1 pt b) RGPD]

1. Contrôle des accès

Mesures visant à empêcher les personnes non autorisées à accéder à des systèmes de traitement de données, avec lesquels les données personnelles sont traitées et utilisées :

Julius Zorn GmbH
Juliusplatz 1
D 86551 Aichach

Industriestraße
D 86551 Aichach

Mesures :

L'ensemble des zones d'accès aux locaux techniques se trouve sur une zone limitée. Les bureaux individuels sont fermés à clé. Le portail est occupé de 7h45 à 17h30 pour les consultations. Sécurisation par accès par puce. Il existe un service de sécurité.

Les accès aux locaux sont sécurisés à plusieurs niveaux. Les locaux seront ouverts et fermés au début et/ou à la fin du travail. Lors de la remise des clés, un accusé de réception est établi. Il existe un concept de verrouillage et un concept de gestion des clés. Seules certaines personnes possèdent une clé principale (elles sont mentionnées sur un document).

L'accès au bâtiment du site se fait par l'entrée. Il existe des zones de traitement et des zones publiques. Les visiteurs sont reçus par le collaborateur correspondant immédiatement après identification. Les visiteurs sont inscrits dans une liste de visiteurs et sont tenus de porter un badge visiteur. Les entreprises extérieures restent ainsi en permanence sous surveillance dès leur entrée sur le site, à l'exception des participants de l'académie qui séjournent dans les locaux de l'académie.

Il existe des systèmes d'alarme.

Les serveurs et certains ordinateurs se trouvent dans un local séparé. L'accès est uniquement possible avec une puce dédiée à certains groupes de personnes.

Les opérations de nettoyage sont effectuées par un prestataire externe. Celui-ci obtient une puce d'accès aux bâtiments.

La présence des collaborateurs est vérifiée par une puce. Les courtes périodes d'absence sont en outre consignées.

2. Contrôle d'accès

Mesures visant à empêcher l'utilisation de systèmes de traitement de données par des personnes non autorisées :

Le **contrôle d'accès** empêche des personnes non autorisées à pénétrer dans les systèmes de traitement des données (ci-après : TD).

Pour protéger l'installation TD contre toute intrusion, des procédures d'identification et d'authentification sont utilisées et contrôlent l'accès :

Avant d'accéder aux données ou aux programmes, la connexion exige la saisie d'un mot de passe personnel associé à un identifiant utilisateur (ID utilisateur). La première connexion est suivie d'un changement de mot de passe immédiat. Les tentatives de connexion sont consignées. Les collaborateurs sont invités à modifier leur mot de passe régulièrement.

Système de contrôle d'accès :

Pour compliquer la divulgation du mot de passe, une longueur minimale de 6 caractères ainsi qu'une expiration automatique du mot de passe au bout de 90 jours sont spécifiées. Le mot de passe doit être composé de caractères, de chiffres et de caractères spéciaux. Les majuscules et les minuscules sont activées.

Si le mot de passe est saisi de manière incorrecte 3 trois, le compte doit être déverrouillé par l'administrateur.

Les données de base d'un utilisateur sont résumées dans une fiche utilisateur. Cette dernière contient par ex. les autorisations d'un utilisateur. L'utilisateur peut se connecter au système uniquement en cas de création d'une fiche utilisateur. Durant le processus de connexion, il est ainsi possible de vérifier les autorisations de l'utilisateur. Les données d'accès sont stockées dans des systèmes sous forme cryptée. Chaque collaborateur possède son propre compte utilisateur avec un accès limité, à l'exception des accès liés à l'utilisateur comme par ex. les postes SDE, etc.

Les équipements de traitement des données sont protégés contre tout accès abusif en appliquant les mesures suivantes :

- Protection https
- Verrouillage automatique de l'écran au bout de 10 minutes

3. Contrôle d'accès

Mesures visant à garantir que les personnes autorisées à utiliser un système de traitement des données puissent avoir accès exclusivement aux données couvertes par leur autorisation d'accès et que les données personnelles ne puissent pas être consultées, copiées, modifiées ou supprimées lors du traitement, de l'utilisation et après l'enregistrement :

Un **contrôle d'accès** efficace exige un examen ordonné et une cession d'autorisations. Le contrôle d'accès doit empêcher toute activité non autorisée dans les systèmes TD en dehors des autorisations accordées. Les données personnelles ne peuvent être consultées, copiées, modifiées ou supprimées sans autorisation.

Le concept d'autorisation et les droits d'accès correspondent aux exigences liées à la tâche et relatives à la protection des données. Il existe différentes autorisations destinées à l'analyse, la prise de connaissance, la modification et la suppression. Les attributions des utilisateurs sont réglementées de manière subjective par une procédure d'identification et d'authentification.

Seul un accès limité des collaborateurs aux lecteurs externes est possible.

D'un point de vue objectif, les autorisations des utilisateurs sont limitées sur le plan fonctionnel par des profils, rôles, transactions et objets définis dans le système et dans le domaine de la gestion des données par des applications limitées à la lecture, l'écriture, la modification ou la suppression par rapport aux fichiers, groupes d'éléments et champs de données.

Le cryptage, les pare-feux et autres mesures de protection visent à protéger contre les accès internes et externes non autorisés.

Les supports de données sont inventoriés et archivés 2 fois. L'archivage a lieu à deux endroits différents, accessibles uniquement aux personnes munies d'une puce. Les supports de données sont situés dans un coffre-fort, accessible uniquement à certaines personnes.

Le même principe s'applique à l'utilisation ou à la suppression des supports de données. L'utilisation de supports de données privés à des fins commerciales et le transport de supports de données à des fins privées ainsi que l'utilisation de supports de données commerciaux dans le domaine privé sont interdits.

Pour la destruction de fichiers, de supports de données optiques et magnétiques, ou pour l'élimination d'impressions inutiles ou d'erreurs d'impression, les éléments sont remis personnellement par le collaborateur dans une déchiqueteuse ou détruits physiquement et/ou les données sont effacées.

L'accès aux programmes des systèmes, des applications et aux programmes utilitaires stockés sur des systèmes servant au traitement des données personnelles, est soumis à des contrôles d'accès natifs au moyen du système d'exploitation utilisé (ID utilisateur + mot de passe).

Les autorisations d'accès sont attribuées par un petit groupe de collaborateurs, responsable du système correspondant.

Les droits d'accès sont accordés selon le principe de connaissance sélective « Need-To-Know ». Seul le nombre de droits d'accès nécessaires à la réalisation des tâches du rôle respectif est attribué.
Les écrans sont verrouillés par l'utilisateur dès qu'il quitte son poste de travail (instruction organisationnelle). En outre, un économiseur d'écran avec protection par mot de passe s'active au bout d'une période définie.

Une importance majeure est accordée à la séparation des données. Il est interdit d'apporter des supports de données extérieurs ou privés dans l'entreprise.

4. Contrôle de la séparation

Mesures visant à garantir que les données collectées à différentes fins puissent être traitées séparément :

La séparation des données doit garantir que les données personnelles collectées à différentes fins sont traitées séparément. Le respect de l'affectation de la finalité dans le traitement des données personnelles nécessite des mesures techniques et organisationnelles assurant la séparation systématique des données.
Les unités de stockage sont configurées de manière redondante (sauvegarde sur disque, puis sauvegarde sur bande).

Les systèmes utilisés doivent garantir une séparation interne des clients. La séparation des clients est incorporée dans le système.

5. Pseudonymisation [art. 32 par. 1 pt a) RGPD ; art. 25 par. 1 RGPD]

La pseudonymisation est le traitement des données personnelles de telle manière que les données ne puissent plus être attribuées à une personne donnée sans insertion d'informations supplémentaires. La condition préalable nécessite que ces informations supplémentaires soient conservées séparément et soient également soumises aux mesures techniques et organisationnelles correspondantes.

II. Intégrité [art. 32 par. 1 pt b) RGPD]

1. Contrôle de la transmission

Mesures visant à garantir que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées lors de la transmission électronique ou pendant leur transport ou leur enregistrement sur un support de données, ainsi que les mesures visant à garantir qu'il soit possible de vérifier et de déterminer à quelles instances des données personnelles peuvent être transmises par des installations de transmission de données.

Le **contrôle de la transmission** doit empêcher que des données personnelles soient lues, copiées, modifiées ou supprimées sans autorisation lors d'une transmission électronique.
Ceci vaut également pour le traitement des transactions et le traitement des commandes.

Un transport des supports de données n'est pas effectué avec les filiales en ce qui concerne les données personnelles.

Les supports de données à détruire sont rendus illisibles par des mesures appropriées et/ou détruits mécaniquement dans une presse, pour empêcher toute reconstruction. Des procès-verbaux écrits sont établis sur la destruction.

Collaborateurs

Les collaborateurs sont informés conformément au § 5 RGPD sur le secret et la confidentialité.

En outre, il existe d'autres obligations spécifiques à l'activité, comme :

§§ 88 et suivants. Loi allemande sur les télécommunications (TKG)
§ 39 Loi allemande sur la poste (PostG)
§ 35 Code allemand de la sécurité sociale I (SGB I)

L'obligation de se conformer aux instructions, les obligations d'information et les droits de contrôle sont réglementés contractuellement. Il a été procédé à une formation à ce sujet avec signature des collaborateurs.

Les obligations découlant des lois susmentionnées, restent valables même après la cessation de l'activité chez le mandataire mentionné. Il est également garanti que les anciens collaborateurs n'ont plus d'autorisation d'accès. Toutes les connexions sont également bloquées.

2. Contrôle de la saisie

Mesures visant à vérifier et déterminer par la suite si et par qui les données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données :

Si des opérations sont effectuées à domicile (Home office), les opérations sont enregistrées sur le système de l'entreprise.

La documentation de la procédure de saisie avec définition des personnes autorisées à créer des supports de données et à traiter des données a été établie.

Il existe une réglementation écrite détaillée sur les relations de travail et la formalisation de l'ensemble du processus de commande, ainsi que sur l'intervention de sous-traitants. Il existe des règles claires de compétences et de responsabilité.

3. Contrôle des commandes

Mesures visant à garantir que les données à caractère personnel traitées dans la commande puissent l'être uniquement de manière conforme aux instructions du commanditaire :

Les accords contractuels entre le commanditaire et le mandataire sont établis par écrit, dans la mesure requise par le commanditaire. Les tâches des partenaires commerciaux sont définies, les compétences et les obligations sont clairement délimitées entre le commanditaire et le mandataire.

Un éventuel sous-traitant mandaté doit prouver au mandataire mentionné ici qu'il a pris des mesures de sauvegarde de données suffisantes et appropriées.

La sélection des mandataires éventuels est effectuée de manière rigoureuse, également selon des critères de sélection liés à la protection des données.

Un contrôle régulier des résultats du travail est effectué.

III. Disponibilité et capacité de résistance art. 32 par. 1 pt. b) RGPD

Contrôle de la disponibilité

Mesures visant à garantir que les données personnelles sont protégées contre toute destruction ou perte accidentelle :

Le contrôle de la disponibilité doit protéger les données personnelles contre toute destruction ou perte accidentelle. Les dangers potentiels sont les dégâts des eaux, la foudre, les incendies, le sabotage ou le vol. Un plan de reprise après sinistre assure la récupération des données endommagées.

En cas de dommages physiques causés par le feu ou l'eau, un détecteur de fumée est installé dans la salle informatique et dans l'ensemble des locaux. Les extincteurs d'incendie sont situés dans la salle informatique et dans des endroits facilement identifiables et accessibles dans l'ensemble du bâtiment. Il existe des portes coupe-feu au niveau du local de production et de la salle des serveurs. Une alimentation sans interruption (ASI) est mise en place. Des dispositifs efficaces de protection contre l'eau sont installés.

Les supports de données de sauvegarde sont conservés séparément. Les procédures de sauvegarde ont été effectuées dans le bâtiment.

La sauvegarde des bases de données est assurée par la mise en miroir des disques durs, les procédures de sauvegarde, la protection antivirus et les pare-feux, et par un transfert sur un support de stockage externe. La sauvegarde intégrale comprend toutes les données du disque dur, ainsi que le système d'exploitation et les programmes d'application. L'avantage de cette méthode réside dans le fait qu'il est ainsi toujours possible de restaurer le dernier état de l'ordinateur au moment de la sauvegarde. Une copie de sauvegarde créée régulièrement est conservée séparément de l'équipement de traitement des données dans un compartiment coupe-feu séparé et à l'extérieur des locaux du mandataire. Les mots de passe système requis ont été créés.

Des logiciels supplémentaires sont utilisés pour garantir la protection des accès pour la lutte antivirus.

Il est interdit aux collaborateurs d'ouvrir des pièces jointes suspectes.

Seuls des produits logiciels et matériels sous licence ou développés en interne sont utilisés.

Tous les ordinateurs sont équipés d'un antivirus mis à jour en permanence pour assurer la protection contre les virus, les chevaux de Troie, etc.

IV. Procédure d'examen, d'analyse et d'évaluation réguliers art. 32 par. 1 pt d) RGPD ; art. 25 par. 1 RGPD

1. Gestion de la protection des données

Notes / Exemples :

Il s’agit d’une planification, d'une organisation, d’un contrôle et d'un suivi systématiques des exigences légales et opérationnelles de la protection des données.

Mesures envisageables :
Mesures visant à garantir que l'organisation interne de l’entreprise respecte les exigences spécifiques en matière de protection des données. Mise en place de nomenclatures visant à améliorer les processus opérationnels dans le domaine de la protection et de la sécurité des données grâce à des systèmes de gestion de la protection des données, des systèmes de gestion de la qualité ou de systèmes de gestion de la sécurité de l'information. En outre, il est possible de créer un registre des activités de traitement dans le but de faciliter la vue d'ensemble de tous les processus métier. Par ailleurs, il est nécessaire et judicieux de prévoir une évaluation des risques relative à la protection des données conformément à l’art. 35 RGPD.

Un responsable externe de la protection des données a été désigné.

Il existe des réglementations écrites sur le fonctionnement et les procédures de traitement des données ainsi que sur les différentes mesures de sécurité des données, par ex. directives, instructions de travail et descriptions de poste. Les sauvegardes des données sont effectuées selon un schéma défini.

Pour la sécurité informatique, il est fait appel à la norme IT ISO 9001, 13485.

Une vérification a lieu automatiquement. Des procès-verbaux sont tenus et actualisés.

En cas de traitements de données importants, par ex. lors de l’analyse de la vidéosurveillance, le principe du double contrôle est utilisé.

2. Gestion de la réponse aux incidents [Plans de réponse aux incidents]

Notes / Exemples :

La gestion de la réponse aux incidents englobe l'ensemble du processus de réponse technique et organisationnel aux incidents de sécurité ou aux perturbations détectés et/ou présumés dans le but d’une restauration la plus rapide possible du service.

Mesures envisageables :
Processus de surveillance 24h/24, 7j/7, procédures subséquentes graduelles définies pour les perturbations

Mesures prises par le mandataire :
Surveillance des lignes importantes, des serveurs, des applications via WhatsUp
Disponibilité