Autodéclaration relative aux mesures techniques et organisationnelles pour le traitement des commandes | Date : 20.10.2021

Conformément aux dispositions du règlement général de l'UE sur la protection des données (art. 28 RGPD), le client doit vérifier, avant le début du traitement des données, si des mesures techniques et organisationnelles appropriées ont été mises en place et sont respectées par le sous-traitant afin de garantir la confidentialité, l'intégrité, la disponibilité, la résilience et la récupérabilité des données. Le résultat de cette vérification doit être documenté. Afin de faciliter cette vérification, l'auto-déclaration ci-dessous est fournie. Pour une lecture rapide et une présentation transparente des mesures, l'auto-déclaration est conçue comme une liste de contrôle. Certaines mesures soutiennent plusieurs objectifs de protection des données du RGPD. Afin d'éviter les répétitions, les mesures sont donc classées en fonction de leurs objectifs. Dans l'ensemble, les mesures couvrent les objectifs de protection des données du RGPD.

Les questions ne concernent que les employés et les systèmes, procédures et équipements chargés de fournir les services ou de réaliser les traitements demandés ou utilisés pour ces traitements.

Les mesures techniques et organisationnelles décrites ci-dessous ont été mises en place afin de pouvoir effectuer un traitement des commandes sûr et conforme à la protection des données.

Exigence	Répond à		Remarque / explication
	J	N	
1. informations générales			
Un délégué à la protection des données a-t-il été désigné ?	☑	☐	Thorsten Schröers SAFE-PORT Consulting GmbH datenschutz@trilux.com | privacy@safe-port.de
Le délégué à la protection des données suit-il une formation continue régulière ?	☑	☐	Chambre de commerce et d'industrie d'Arnsberg / Sauerland ITKservice GmbH IQ-Zert GmbH & Co. KG
Quel(s) poste(s) le délégué à la protection des données occupe-t-il en plus de cette fonction ?			Aucune autre activité, car délégué à la protection des données externe
Les employés sont-ils tenus de respecter la confidentialité conformément aux dispositions du RGPD ?	☑	☐	Tous les collaborateurs du groupe TRILUX sont tenus de respecter la confidentialité et la protection des données conformément au RGPD et à la BDSG.
L'engagement est-il documenté de manière vérifiable ?	☑	☐	Par écrit dans le dossier personnel
Les collaborateurs sont-ils formés en permanence aux exigences de la protection des données, le cas échéant comment ?	☑	☐	Type d'enseignement ☑ Formations en ligne ☑ Instructions écrites ☑ Réunions d'équipe régulières
Existe-t-il un concept d'effacement avec une réglementation des délais de conservation ou d'enregistrement et pour l'effacement ou la destruction des données dans les délais et en toute sécurité ?	☑	☐	
Existe-t-il une gestion systématique de la protection et de la sécurité des données avec une procédure réglementée de vérification et d'évaluation ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
Existe-t-il une certification relative à la sécurité informatique ou à la gestion de la sécurité informatique ou tout autre certificat attestant d'une mise en œuvre conforme à la loi de la protection des données dans l'entreprise ?	☑	☐	Le traitement des données a lieu dans un centre de données d'un fournisseur de cloud établi dans l'UE. Celui-ci est certifié selon la norme DIN EN/ISO IEC 2700x et est soumis à une routine de contrôle régulière.
Existe-t-il un concept de protection des données ou un manuel de protection des données pour la réglementation et la mise en œuvre de la protection des données dans l'entreprise ?	☑	☐	
Existe-t-il un manuel de sécurité informatique ou d'autres règles concernant les mesures techniques et organisationnelles relatives à la protection des données ?	☑	☐	
Des sous-traitants sont-ils utilisés ?	☒	☐	
Le cas échéant, les sous-traitants sont-ils soumis aux mêmes obligations que celles définies entre le pouvoir adjudicateur et le contractant ?	☑	☐	
Existe-t-il également avec les entreprises de maintenance et autres prestataires de services les accords ou obligations nécessaires en matière de protection des données, le cas échéant de quelle nature ?	☑	☐	Tous les prestataires de services sont tenus par écrit de respecter les lois actuelles sur la protection des données.
Le traitement des données est-il effectué sur le territoire de la République fédérale d'Allemagne ou au sein de l'Union européenne ou des États de l'Espace économique européen ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
2. mesures techniques et organisationnelles			
2.1 Confidentialité (article 32, paragraphe 1, point b) du RGPD)			
2.1.1 Accès à l'entreprise			
Le terrain et les bâtiments sont-ils protégés contre tout accès non autorisé en dehors des heures de service ?	☑	☐	☑ Personnel de garde ☑ Détecteur de mouvement/système d'alarme ☑ Système de contrôle d'accès ☑ Système de fermeture central, serrures de sécurité
Les entrées et les sorties sont-elles sécurisées ?	☑	☐	Portes d'entrée du bâtiment ☑ Oui☐ Non Portes de secours/sorties de secours ☑ Oui☐ Non☐ Sans objet Echelles et escaliers de secours ☑ Oui☐ Non☐ Sans objet Aires de réception et de livraison ☑ Oui☐ Non☐ Sans objet
Le guidage et la surveillance des visiteurs sont-ils réglementés ?	☑	☐	☑ Réception ☑ Livret de visite ☑ Carte de visiteur ☑ Guide personnel du visiteur
Le personnel extérieur, par exemple le personnel de maintenance et de service, est-il supervisé ?	☑	☐	Le personnel d'entretien et de service est toujours supervisé par une personne responsable de la zone concernée.

Exigence	Répond à		Remarque / explication
	J	N	
Des sécurités d'accès sont-elles mises en place ?	☑	☐	☑ Système de contrôle d'accès ☑ avec ☐ sans zones de sécurité ☑ Système de fermeture central avec régulation par clé Les autorisations d'accès ne sont accordées à un employé qu'à la demande de son supérieur hiérarchique et/ou du service des ressources humaines. Le principe de nécessité est pris en compte lors de l'attribution des autorisations.
Des zones de sécurité ont-elles été définies, par exemple la salle des serveurs, le système de télécommunication, les archives, les répartiteurs de réseau, et protégées séparément contre tout accès non autorisé ?	☑	☐	
Ces zones de sécurité sont-elles spécialement protégées contre l'accès non autorisé, le cas échéant comment ?	☑	☐	Type de protection ☑ Système de contrôle d'accès ☑ Système de fermeture central avec Réglementation des clés
Les autorisations d'accès à ces zones de sécurité sont-elles réglées et documentées dans un concept d'autorisation d'accès ?	☑	☐	L'attribution et la gestion des clés s'effectuent selon un processus défini qui régit l'octroi ou le retrait des autorisations d'accès aux locaux, tant au début qu'à la fin d'une relation de travail.
D'autres mesures de protection ont-elles été mises en place pour ces locaux ?	☑	☐	☑ Portier ☑ Système d'alarme ☑ Carte d'identité de l'entreprise

Exigence	Répond à		Remarque / explication
	J	N	
2.1.2 Accès aux systèmes de traitement des données			
Des mesures ont-elles été mises en place pour contrôler l'accès au bureau et aux systèmes en réseau ?	☑	☐	Identification sécurisée de l'utilisateur ☑ Mot de passe sécurisé Blocage de la répétition☑ du mot de passe après 3 tentatives infructueuses Pour avoir accès aux systèmes informatiques, les utilisateurs doivent disposer d'une autorisation d'accès correspondante. Pour ce faire, les administrateurs attribuent des droits d'accès aux utilisateurs. Toutefois, cela n'est possible que si le supérieur hiérarchique en fait la demande. La demande peut également être faite par le biais du service du personnel.
Existe-t-il des règles de mot de passe pour tous les niveaux d'accès (réseau, serveur, applications) afin de garantir un mot de passe sûr et confidentiel ?	☑	☐	L'utilisateur reçoit un nom d'utilisateur et un mot de passe initial qui doit être modifié lors de la première connexion. Les consignes relatives au mot de passe comprennent une longueur minimale de 8 caractères, le mot de passe devant satisfaire aux exigences de complexité.
Le respect de ces règles est-il contrôlé de manière automatisée à tous les niveaux lors de la saisie ?	☑	☐	Les mots de passe sont changés régulièrement. Un changement automatique de mot de passe - est indexé. Un historique des mots de passe est enregistré. Cela permet de s'assurer que les 10 mots de passe précédents ne peuvent pas être réutilisés. Les mots de passe sont en principe enregistrés sous forme cryptée.
Un circuit de pause (économiseur d'écran) protégé par un mot de passe et programmé est-il mis en place ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
Les systèmes sont-ils protégés contre les intrusions non autorisées et contre l'Internet ?	☑	☐	☑ Pare-feu ☑ Scanner antivirus ☑ Séparation du réseau Tous les systèmes serveurs et clients disposent d'un logiciel antivirus dont la mise à jour des signatures est assurée quotidiennement. Tous les serveurs sont protégés par des pare-feux, qui sont toujours entretenus et pourvus de mises à jour et de correctifs. L'accès des serveurs et des clients à Internet et l'accès à ces systèmes via Internet sont également protégés par des pare-feux. Ainsi, il est également garanti que seuls les ports nécessaires à la communication concernée sont utilisables. Tous les autres ports sont bloqués en conséquence.
Des protocoles/mesures de surveillance ont-ils été mis en place, lesquels, le cas échéant ?	☑	☐	☑ Configuration des utilisateurs et des droits ☑ Modifications du système ☑ Tentatives d'accès erronées ☑ Surveillance du système ☑ Connexion et déconnexion aux procédures de traitement des données
Les données de journalisation sont-elles - stockées de manière à pouvoir être révisées et protégées contre l'accès ?	☑	☐	
Les données des journaux sont-elles - vérifiées en temps réel et régulièrement afin de détecter les actions et les opérations ayant une incidence sur la sécurité ?	☑	☐	☑ Manuellement et en fonction de l'événement
L'accès aux systèmes de traitement des données est-il limité au cercle d'utilisateurs requis par un système de droits ?	☑	☐	☐ Profils de droits et gestion des droits ☐ Limitation fonctionnelle des terminaux Les autorisations pour les systèmes informatiques et les applications sont exclusivement mises en place par les administrateurs.
L'accès à partir d'organismes externes est-il sécurisé, le cas échéant comment ?	☑	☐	☑ Connexion VPN ☑ Cryptage ☑ Logiciel spécial en cas de télémaintenance/assistance à distance

Exigence	Répond à		Remarque / explication
	J	N	
2.1.3 Protection des données contre les accès non autorisés			
Existe-t-il un profil d'autorisation documenté qui garantit que chaque collaborateur ne dispose que des droits d'accès dont il a besoin pour accomplir ses tâches ?	☑	☐	Sous quelle forme ? Si nécessaire, différencier également selon : ☑ Autorisation de lecture ☑ Autorisation d'écriture Les autorisations sont en principe attribuées selon le principe du "besoin de savoir". Par conséquent, seules les personnes qui - entretiennent et gèrent ces données, applications ou bases de données ou qui sont actives dans le développement reçoivent des droits d'accès aux données, bases de données ou applications. Il existe un concept d'autorisation basé sur les rôles avec la possibilité d'attribuer des droits d'accès différenciés, qui garantit que les employés reçoivent des droits d'accès aux applications et aux données en fonction de leur domaine d'activité respectif et, le cas échéant, en fonction du projet.
Des mesures de limitation du stockage, notamment de pseudonymisation ou d'anonymisation, ont-elles été mises en place ?	☑	☐	
Les autorisations définies et leurs modifications sont-elles documentées de manière compréhensible ?	☑	☐	
Une gestion des droits a-t-elle été mise en place pour l'attribution documentée des droits, garantissant la suppression en temps réel des droits qui ne sont plus nécessaires, même en cas de modification du domaine d'activité ?	☑	☐	La condition préalable est une demande d'autorisation correspondante pour un collaborateur par un supérieur hiérarchique. Un processus de check-out est mis en place à cet effet.
Existe-t-il d'autres mesures de contrôle d'accès, le cas échéant lesquelles ?	☑	☐	☑ Procédure de vérification et de validation des programmes ☑ Consignation et évaluation des incidents critiques pour la sécurité

Exigence	Répond à		Remarque / explication
	J	N	
2.2 Intégrité (article 32, paragraphe 1, point b) du RGPD)			
2.2.1 Protection des données lors de leur transfert et de leur transmission			
Les données sont-elles protégées lors de leur transmission contre toute prise de connaissance non autorisée ?	☑	☐	☑ Cryptage ☑ Connexions sécurisées, VPN
La sécurité de l'effacement, de la destruction et de l'élimination des supports de données est-elle garantie ?	☑	☐	Tous les membres du personnel ont pour instruction de déposer les informations contenant des données à caractère personnel et/ou des informations sur les projets dans les conteneurs de destruction désignés à cet effet.
L'effacement/la destruction des supports de données est-il(elle) confié(e) à une entreprise de services ?	☑	☐	La destruction des supports de données et du papier est effectuée par un prestataire de services qui garantit une destruction conforme à la norme DIN 66399.
Existe-t-il un contrat/mandat à cet effet conformément aux dispositions de l'article 28 du RGPD ?	☑	☐	
La mise hors service sécurisée et confidentielle des appareils contenant des supports de données (p. ex. serveurs, appareils multifonctions, etc.) est-elle - réglée ?	☑	☐	
En cas de télémaintenance, l'accès aux données et aux systèmes des clients s'effectue-t-il uniquement via des lignes sécurisées ?	☑	☐	Sécurisation des lignes : ☑ Cryptage VPN ☑ Les accès à distance aux systèmes informatiques se font toujours via des connexions cryptées.
Une identification/authentification sûre est-elle garantie en cas de maintenance à distance ?	☑	☐	
En cas de télémaintenance, les lignes sont-elles surveillées par des dispositifs de sécurité appropriés, par exemple l'enregistrement et l'analyse des protocoles ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
2.2.2 Contrôle de la saisie des données			
Les processus de connexion aux systèmes des clients sont-ils consignés et surveillés de manière compréhensible ?	☑	☐	L'introduction, la modification et la suppression de données à caractère personnel traitées sur mandat sont en principe consignées. Les collaborateurs sont tenus de toujours travailler avec leur propre compte. Les comptes d'utilisateurs ne doivent pas être partagés ou utilisés avec d'autres personnes.
L'utilisation des systèmes de traitement des données et la saisie des données sont-elles consignées ?	☑	☐	Consignation de l'utilisation des fichiers : ☑ Oui☐ Non Consignation des entrées et des modifications : ☑ Par champ de données ☑ En fonction de l'enregistrement
Des autorisations d'utilisateur avec des profils de droits différenciés sont-elles mises en place ?	☑	☐	Droits : ☑ Lire, modifier, supprimer ☑ Accès partiel aux données et aux fonctions
Une procédure permettant d'attribuer des droits et de les modifier ou de les supprimer de manière compréhensible a-t-elle été mise en place ?	☑	☐	Les autorisations sont en principe attribuées selon le principe du "besoin de savoir". Par conséquent, seules les personnes qui - entretiennent et gèrent ces données, applications ou bases de données ou qui sont actives dans le développement reçoivent des droits d'accès aux données, bases de données ou applications. La condition préalable est une demande d'autorisation correspondante pour un collaborateur par un supérieur hiérarchique. Un processus de check-out est mis en place à cet effet.
Le principe du minimum est-il respecté lors de l'attribution des droits ?	☑	☐	
Les services d'attribution/d'autorisation des droits et de création des droits sont-ils séparés ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
2.2.3 Contrôle des opérations de sous-traitance			
L'exécution de la commande du client/de l'-action de service est-elle surveillée de manière compréhensible afin de garantir - une exécution conforme à la commande ?	☑	☐	Les dispositions correspondantes figurent dans le contrat de traitement des commandes.
Des mécanismes de journalisation et d'évaluation appropriés sont-ils mis en place pour surveiller les accès non autorisés aux systèmes et aux données des clients ?	☑	☐	Les dispositions correspondantes figurent dans le contrat de traitement des commandes.
Existe-t-il des dispositions relatives au traitement des incidents et à l'exercice des obligations de notification au donneur d'ordre ?	☑	☐	Les dispositions correspondantes figurent dans le contrat de traitement des commandes.
Les dispositions de l'article 28 du RGPD sont-elles respectées lors de l'attribution d'un contrat de service (par ex. service informatique, maintenance, etc.) ?	☑	☐	☑ Sélection du contractant ☑ Vérification des mesures techniques et organisationnelles chez le contractant ☑ Conclusion d'un contrat conformément à l'article 28 du RGPD ☑ Contrôle régulier du contractant
Les activités de maintenance des systèmes de traitement des commandes sont-elles surveillées et consignées de manière fiable ?	☑	☐	

Exigence	Répond à		Remarque / explication
	J	N	
2.3 Disponibilité et résilience des systèmes (article 32, paragraphe 1, point b) du RGPD)			
2.3.1 Garantie de la disponibilité des données			
Les données des clients sont-elles protégées contre la destruction et la perte par des procédures de sauvegarde appropriées ?	☑	☐	☑ Base de données en miroir ☑ Copies de sauvegarde régulières / solution de back-up Existe-t-il un concept de sauvegarde définissant la manière de procéder à une sauvegarde régulière et à la reconstruction des données ? ☑ Oui☐ Non
Des mesures ont-elles été mises en place pour sécuriser la salle des serveurs et l'infrastructure informatique ?	☑	☐	Les données des clients sont hébergées dans un centre de données certifié selon la norme DIN EN/ISO IEC 2700x.

Exigence	Répond à		Remarque / explication
	J	N	
2.3.2 Séparation de différents mandants			
Les données des différents clients sont-elles séparées de manière appropriée afin de garantir un traitement distinct ?	☑	☐	Type de séparation : ☑ Séparation des mandants

Exigence	Répond à		Remarque / explication
	J	N	
2.4 Procédures de suivi, d'évaluation et d'appréciation périodiques			
Un système de gestion de la sécurité informatique est-il en place ?	☑	☐	Les données des clients sont hébergées dans un centre de données certifié selon la norme DIN EN/ISO IEC 2700x.
L'efficacité des mesures techniques et organisationnelles de l'entreprise est-elle en outre régulièrement contrôlée par d'autres moyens ?	☑	☐	Une gestion de la protection des données est mise en place. Il existe une ligne directrice sur la protection et la sécurité des données et des directives garantissant la mise en œuvre des objectifs de la ligne directrice. Une équipe chargée de la protection des données et de la sécurité de l'information (DST) a été mise en place pour planifier, mettre en œuvre, évaluer et adapter les mesures dans le domaine de la protection et de la sécurité des données. Les directives sont régulièrement évaluées et adaptées en fonction de leur efficacité. Il est notamment garanti que les incidents de protection des données sont reconnus par tous les collaborateurs et immédiatement signalés au DST. Celui-ci enquêtera immédiatement sur l'incident. Si des données traitées pour le compte de clients sont concernées, il est veillé à ce que ces derniers soient immédiatement informés de la nature et de l'ampleur de l'incident. En cas de traitement de données à des fins propres, si les conditions de l'article 33 du RGPD sont remplies, une notification à l'autorité de contrôle sera effectuée dans les 72 heures suivant la prise de connaissance de l'incident.

Exigence	Répond à		Remarque / explication
	J	N	
2.5 Procédures de révision, d'évaluation et d'appréciation régulières			
Les exigences de la "protection des données par la technique" et des "-paramètres par défaut favorables à la protection des données" sont-elles - respectées ? ("Privacy by Design" et "Privacy by Default")	☑	☐	Dès le développement du logiciel, on veille à ce que le principe de nécessité soit déjà pris en compte dans le contexte des interfaces utilisateur. Ainsi, les champs de formulaire et les masques d'écran peuvent être conçus de manière flexible. Il est ainsi possible de prévoir des champs obligatoires ou de désactiver des champs. Le logiciel prend en charge à la fois le contrôle des entrées grâce à une piste d'audit flexible et personnalisable, qui permet de stocker de manière inaltérable les modifications apportées aux données et aux autorisations des utilisateurs. Les autorisations sur les données ou les applications peuvent être définies de manière flexible et granulaire.

Arnsberg | 20.10.2021
Lieu | Date

Signature