Contrat sur le traitement conformément à l'art. 28 du Règlement général sur la protection des données (RGPD)

Contrat-cadre, valable pour toutes les prestations

entre

[Nom complet de la société Client]
[Adresse]
[Ville]
(Responsable du traitement des données, ci-après le « **Client** »)

et

Allegion N.V.
Pontbeekstraat 2
B- 1702 Dilbeek
(sous-traitant , ci-après dénommé le « **Prestataire »**)

§ 1 Objet et durée du Contrat

(1) Objet :

Le Prestataire propose des systèmes de contrôle d'accès automatisé et d'enregistrement du temps ainsi que la Gestion avancée du personnel.

Le présent Contrat s'applique à tous les accords existants et à tous les accords conclus à l'avenir entre les parties concernant la fourniture de services informatiques spécifiques en rapport avec ces systèmes par le Prestataire au Client (ci-après dénommé « **Contrat de Service** » même en cas de plusieurs accords).

Les systèmes du Prestataire sont généralement exploités en tant que solutions sur site chez le Client et par le Client, cependant, il ne peut être exclu que - dans le cadre des services informatiques spécifiques susmentionnés - le Prestataire se voit accorder l'accès à des données à caractère personnel conformément à et sous réserve du présent Contrat.

(2) Durée, résiliation

Sauf accord contraire, le présent Contrat s'applique aussi longtemps que le Prestataire traite des données à caractère personnel dans le cadre de l'exécution du Contrat de Service.

Chacune des parties peut résilier le Contrat à tout moment sans préavis en cas de manquement grave par l'une des parties des dispositions relatives à la protection des données ou des dispositions du présent Contrat. En particulier, le non-respect des obligations énoncées dans le présent Contrat et découlant de l'art. 28 du RGPD constitue une infraction grave.

§ 2 Dispositions initiales relatives au contenu du présent Contrat

Nature et finalité du traitement des données à caractère personnel

La finalité du traitement des données à caractère personnel par le Prestataire pour le compte du Client, les types de données traitées et les catégories de personnes concernées sont décrits plus en détail dans le Contrat de Service et dans l'**Annexe 1 - Spécification en vertu de la loi sur la protection des données**.

Le traitement des données convenu a actuellement lieu exclusivement en République fédérale d'Allemagne, dans un autre État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen. Toute délocalisation ultérieure dans un pays tiers nécessite l'accord du Client et est soumise aux exigences particulières des articles 44 et suivants du RGPD. Le niveau de protection approprié peut être assuré par des clauses types de protection des données (art. 46 par. 2 alinéas c et alinéa d du RGPD), par des règles de conduite approuvées (Art. 46 par. 2, alinéa e, en liaison avec l'art. 40 du RGPD), par le biais d'un mécanisme de certification approuvé (art. 46 par. 2, alinéa f, en liaison avec l'art. 42 du RGPD) ou par d'autres mesures conformément à l'art. 46 par. 2 alinéa a, par. 3, sous-paragraphe a et sous-paragraphe b du RGPD.

§ 3 Pouvoir du Client de donner des instructions

(1) Le Prestataire traite les données à caractère personnel exclusivement pour la finalité de fourniture des services dans le cadre du Contrat de Service et conformément aux instructions documentées du Client. Ceci s'applique également à tout transfert de données à caractère personnel vers un pays tiers ou une organisation internationale, sauf si le droit de l'Union européenne ou d'un État membre auquel le Prestataire est soumis l'exige, le cas échéant le Prestataire notifie au Client une telle exigence avant le traitement, à moins que le droit en question n'interdise une telle notification pour des raisons d'intérêt public majeur. Les instructions sont données en vertu du Contrat de Service et de la mise en place et de la configuration du service par le Client. Les instructions ultérieures à la conclusion du contrat doivent être formulées sous forme de durable et écrite, que le Clientdoit les confirmer par écrit si le Prestataire le demande.

(2) Si le Client donne des instructions supplémentaires qui dépassent le cadre du Contrat de Service, le Prestataire doit donner son consentement.

(3) Si la Prestataire est d'avis qu'une instruction donnée par le Client est contraire aux dispositions légales, elle doit le signaler au Client. L'exécution d'une telle instruction peut être suspendue par le Prestataire.

§ 4 Mesures techniques et organisationnelles

(1) Avant de commencer le traitement, le Prestataire documente et soumet au contrôle du Client la mise en œuvre envisagée pour les mesures techniques et organisationnelles prévues avant l'attribution du Contrat, notamment en ce qui concerne l'exécution concrète de la mission. Si elles sont acceptées par le Client, ces mesures deviennent le fondement du Contrat. Lorsque l'examen ou l'audit du Client révèle un besoin d'ajustement, celui-ci doit être mis en œuvre d'un commun accord.

(2) Le Prestataire doit assurer la sécurité du traitement conformément à l'art. 28 para. 3 alinéa c et l'art. 32 du RGPD, en particulier en liaison avec l'art. 5 par. 1, alinéa. 2 du RGPD). De manière générale, les mesures à prendre concernent la sécurité des données et la garantie d'un niveau de protection adapté au risque en termes de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes. Dans ce contexte, l'état de la technique, les coûts de mise en œuvre et le type, la portée et les finalités du traitement, ainsi que la probabilité et la gravité variables du risque pour les droits et libertés des personnes physiques en vertu de l'art. 32 para. 1 du RGPD, doivent être prises en compte (détails dans l'annexe 2 du présent Contrat).

(3) Les mesures techniques et organisationnelles sont soumises au progrès et au développement techniques ultérieur. À cet égard, le Prestataire peut mettre en œuvre d'autres mesures adéquates, à condition que le niveau de sécurité des mesures initialement prévues ne soit pas réduit. Les changements importants sont documentés par écrit ou par voie électronique.

(4) Dans la mesure où le Prestataire exerce son activité sur place chez le Client, il n'est pas responsable des mesures techniques et organisationnelles se trouvant dans la sphère d'influence et de responsabilité du Client.

(5) Dans la mesure où le Prestataire effectue des services dans les locaux du Client, il n'est pas responsable du respect des mesures techniques et organisationnelles qui se trouvent dans la sphère d'influence et de responsabilité du Client.

§ 5 Assurance qualité et autres obligations du Prestataire

Outre le respect des dispositions du présent Contrat, le Prestataire a des obligations légales en vertu des articles 28 à 33 du RGPD. À cet égard, le Prestataire veille notamment au respect des exigences suivantes :

a) Nomination par écrit d'un délégué à la protection des données conformément aux articles 38 et 39 du RGPD.

   Les coordonnées actuelles du délégué à la protection des données doivent être facilement accessibles sur le site internet du Prestataire à tout moment.

b) Assurer la confidentialité conformément à l'art. 28 para. 3 , alinéa 2 sous-paragraphe b et aux Art. 29, 32 par. 4 du RGPD). Lors de l'exécution des travaux, le Prestataire n'emploie que du personnel tenu à la confidentialité et qui a été préalablement sensibilisé aux dispositions relatives à la protection des données qui le concernent.

c) Mise en œuvre et respect de toutes les mesures techniques et organisationnelles requises pour le présent Contrat, en vertu de l'art. 28 para. 3, alinéa 2 sous-paragraphe c et Art. 32 du RGPD(détails dans l'annexe 2 du présent Contrat).

d) Sur demande, le Client et le Prestataire doivent coopérer avec l'autorité de contrôle dans l'exercice de ses fonctions.

e) Notification immédiate au Client des mesures et des actions de contrôle de l'autorité de contrôle, dans la mesure où elles concernent le présent Contrat. Cela s'applique également lorsqu'une autorité compétente, dans le cadre d'une procédure administrative ou pénale relative au traitement de données à caractère personnel, enquête sur les activités de traitement chez le Prestataire.

f) Lorsque le Client fait lui-même l'objet de mesures de la part de l'autorité de contrôle, d'une procédure administrative ou pénale, d'une action en responsabilité d'une personne concernée ou d'un tiers ou de toute autre action relative au traitement des données à caractère personnel chez le Prestataire, ce dernier assiste le Client au mieux de ses possibilités.

g) Le Prestataire contrôle régulièrement les processus internes mis en œuvre et les mesures techniques et organisationnelles prises pour garantir que le traitement dans sa sphère de responsabilité est effectué conformément au droit applicable en matière de protection des données et que les droits des personnes concernées sont protégés.

h) À la demande du Client, le Prestataire fournira au Client la preuve des mesures techniques et organisationnelles prises dans le cadre des pouvoirs de contrôle du Client en vertu de l'article 7 du présent Contrat.

i) À la fin des prestations à fournir dans le cadre du Contrat de Service ou à la demande du Client, le Prestataire doit restituer au Client tous les documents en sa possession ainsi que tous les résultats de travail et les données produites dans le cadre du Contrat ou les effacer conformément à la loi sur la protection des données avec le consentement préalable du Client.

j) Le Prestataire conserve la documentation qui sert de preuve du traitement approprié des données conformément aux périodes de conservation applicables au-delà de la fin du Contrat. À la suite de la résiliation du Contrat, le Prestataire peut remettre cette documentation au Responsable du traitement des données.

§ 6 Relations de sous-traitance

(1) Aux fins de cette disposition, les relations de sous-traitance sont réputées se rapporter directement à la fourniture du service principal. Les services auxiliaires sous-traités, qui ne concernent pas principalement le traitement des données à caractère personnel, par exemple les services de poste, de télécommunication, de logistique, de nettoyage et les métiers spécialisés, ne sont pas inclus. Toutefois, même dans le cas de services auxiliaires sous-traités, le Prestataire doit assurer la protection et la sécurité des données à caractère personnel du Client au moyen d'accords et de mesures de surveillance adéquats et conformes à la loi.

(2) Le Prestataire peut désigner un sous-traitant externe (ci-après dénommé le « **Sous-traitant** »). En signant le présent Contrat, le Client donne au Prestataire l'autorisation générale d'employer un sous-traitant. Le Prestataire informe le Client de tout changement prévu concernant le recours à des Sous-traitants, y compris leur remplacement. Le Client peut formuler des objections à l'égard d'un sous-traitant et, si celles-ci ne sont pas résolues à l'amiable, il peut résilier le présent Contrat à compter de la date à laquelle le changement prend effet. Actuellement, aucun sous-traitant n'est engagé, sauf s'il figure dans l'annexe 3 - Sous-traitants.

(3) Le Prestataire doit, au minimum et conformément au droit applicable en matière de protection des données, transférer aux sous-traitants les obligations pertinentes en vertu du présent Contrat par le biais d'accords de (sous-)traitement, y compris les mesures techniques et organisationnelles appropriées à prendre.

(4) Le Prestataire doit conclure des accords de confidentialité avec tous les sous-traitants, à moins qu'une obligation légale de confidentialité adéquate s'applique.

§ 7 Pouvoirs de contrôle du Client

(1) Le Prestataire peut, à ses frais, avant le début du traitement des données et ensuite à intervalles réguliers, s'assurer des mesures techniques et organisationnelles prises par le Prestataire conformément à l'annexe 2 et en documenter les résultats. Cela peut se faire, *entre autres*, en obtenant une déclaration propre du Prestataire, que celui-ci peut également fournir sous la forme d'un certificat approprié d'un expert, ou par un audit sur place par le Client.

(2) Le Prestataire s'engage à fournir au Client, sur demande écrite et dans un délai raisonnable, toutes les informations nécessaires dans le cadre de l'audit applicable.

(3) Si le Client charge un tiers d'effectuer un audit (y compris un audit sur place), le Client oblige par écrit ce tiers à respecter le secret et la confidentialité, à moins que le tiers ne soit déjà soumis à une obligation professionnelle de secret. À la demande du Prestataire, le Client soumet sans délai au Prestataire les accords correspondants avec le tiers. Le Client ne peut pas confier l'audit à un concurrent du Prestataire.

(4) Tout audit sur place nécessite un préavis écrit de 30 jours, en règle générale, et est limitée aux heures ouvrables ordinaires. Tout audit doit être effectué de manière à minimiser l'impact sur les opérations commerciales du Prestataire. Tout audit de routine sur place est limité à un maximum d'une (1) fois par année civile. Le Client communiquera par écrit le résultat de son audit dans un délai de 30 jours (en règle générale) à compter de la fin de l'audit.

§ 8 Droits des personnes concernées

(1) Les droits des personnes concernées par le traitement des données à caractère personnel doivent être exercés à l'encontre du Client.

(2) Lorsqu'une personne concernée contacte directement le Prestataire pour obtenir des informations sur les données la concernant, ou pour les faire rectifier, effacer ou bloquer, le Prestataire transmet dans les meilleurs délais, cette demande au Client.

(3) Si une personne concernée fait valoir ses droits en matière de protection des données, le Prestataire doit, le cas échéant, dans des limites raisonnables et dans la mesure où cela est nécessaire pour le Client, assister le Client par des mesures techniques et organisationnelles appropriées, à condition que le Client ne puisse pas traiter une réclamation donnée sans la coopération du Prestataire.

(4) Le Prestataire doit permettre au Client de rectifier, effacer ou bloquer les données à caractère personnel ou, à la demande du Client, rectifier, bloquer ou effacer lui-même ces données si et dans la mesure où le Client ne peut pas le faire.

§ 9 Notification en cas d'infraction

(1) Le Prestataire aide le Client à se conformer aux obligations prévues aux articles 32 à 36 du RGPD en matière de sécurité des données à caractère personnel, de signalement en cas de violation des données, d'analyses d'impact sur la protection des données et de consultations préalables. Cela comprend *, entre autres,* les éléments suivants

a) assurer un niveau de protection adéquat par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement des données ainsi que de la probabilité et de la gravité prévisibles des infractions potentielles causées par des failles de sécurité et qui sont conçues pour permettre la détection immédiate des infractions pertinentes ;
b) l'obligation d'assister le Client dans son devoir d'information envers les personnes concernées, en mettant sans délai toutes les informations pertinentes à la disposition du Client ;
c) aider le Client à réaliser des analyses d'impact sur la protection des données, le cas échéant ;
d) assister le Client dans le cadre des consultations préalables avec l'autorité de contrôle.

(2) Le Prestataire est conscient que le Client peut être soumis à une obligation de notification en vertu de l'art. 33 du RGPD, qui exige la notification à l'autorité de contrôle dans les 72 heures dès la connaissance d'une circonstance. Le Prestataire doit aider le Client à satisfaire cette obligation de notification.

(3) Le Prestataire informe le Client dans les meilleurs délais, s'il a connaissance d'une violation de données à caractère personnel dans le cadre du traitement des données.

(4) Lorsque le Client est soumis à des obligations légales de notification concernant l'acquisition illégale de données à caractère personnel à la suite d'un incident, le Prestataire aide le Client à remplir ces obligations à la demande du Client dans le cadre du raisonnable et nécessaire. Cette assistance fait l'objet d'une rémunération, sauf si l'incident a été causé de manière fautive par le Prestataire ou s'il fait partie de la description des services du Contrat de Service.

(5) Si le Client utilise une solution sur site exploitée par le Client lui-même, l'obligation d'assistance du Prestataire conformément au présent site § 9 n'existe que dans la mesure où le Client ne peut pas obtenir lui-même les informations requises ou ne peut pas effectuer lui-même les activités requises.

§ 10 Rectification, effacement et limitation des données traitées

(1) Le Prestataire ne peut pas rectifier, effacer ou limiter les données traitées à sa discrétion, dans le cadre du présent Contrat, mais uniquement sur instruction documentée du Client. Lorsqu'une personne

concernée contacte directement le Prestataire à cet égard, ce dernier transmet sans délai cette demande au Client.

(2) Les données que le Prestataire traite uniquement pour l'exécution des services (par exemple la maintenance) sont effacées dès qu'elles ne sont plus nécessaires pour le service concerné (cf. annexe 2 - Contrôle d'accès).

§ 11 Responsabilité civile

Art. 82 Le RGPD s'applique. Lorsque le Contrat de Service contient des dispositions sur la responsabilité, celles-ci s'appliquent également aux relations entre les parties dans le cadre du présent Contrat.

§ 12 Obligation de payer une rémunération

(1) Lorsque le Prestataire est tenu, en vertu du présent Contrat, de fournir des services dépassant le cadre du Contrat de Service (« **Services Supplémentaires** »), ces services sont rémunérés séparément en fonction du temps et du matériel dépensés. C'est notamment le cas pour les activités énoncées dans § 1(2)§ 3(2)§ 1(2), § 5 lettre. d) et lettre. f) § 7 (à l'exception des services nécessaires en raison d'un manquement relevant de la responsabilité du Prestataire), § 8 et § 10. Pour éviter toute ambiguïté, dans la mesure où le Prestataire a causé de manière fautive des Services Supplémentaires, le Client ne doit pas de rémunération en vertu du présent § 12.

(2) Sous réserve du Contrat de Service ou de tout autre accord entre les parties, la rémunération des Services Supplémentaires des employés du Prestataire est basée sur un forfait horaire de 180 euros plus la taxe sur la valeur ajoutée légale. Pour les frais de matériel et de déplacement, le Prestataire facture au Client le montant effectivement encouru, majoré de la taxe sur la valeur ajoutée. Si le Prestataire est en mesure de prouver l'existence de coûts supplémentaires, il peut facturer le montant total.

§ 13 Divers

(1) Les modifications et les avenants du présent Contrat sont effectués par écrit. Cela s'applique également à toute dérogation à cette exigence de forme écrite.

(2) Si une disposition du présent Contrat s'avérait juridiquement invalide, la validité des autres dispositions resterait inchangée. La disposition invalide est remplacée rétroactivement par une disposition qui se rapproche le plus possible de la disposition originale en termes de contenu et d'effet commercial.

(3) L'exercice du droit de conservation est exclu en ce qui concerne les données traitées pour le Client et les supports de données associés.

(4) Si les données du Client sont mises en péril par le Prestataire en raison d'une saisie, d'une procédure d'insolvabilité ou d'autres événements ou mesures prises par des tiers, le Prestataire en informe immédiatement le Client. Le Prestataire informe immédiatement toutes les personnes responsables dans ce contexte que la souveraineté et la propriété des données reviennent exclusivement au Client en tant que responsable du traitement en vertu du RGPD.

[page de signature à suivre]

Allegion N.V.	**Nom du Client**
Signature	Signature
Nom, fonction	Nom, fonction
Date, timbre	Date, timbre

Annexe 1 - Spécification en vertu de la loi sur la protection des données

La présente annexe 1 (Spécification en vertu de la loi sur la protection des données) complète le Contrat de Service conclu applicable. Il va de soi que seules les données à caractère personnel qui font partie de l'objet des services convenus seront traitées.

Catégories de personnes concernées :

1. Les employés qui utilisent le système IF
2. Visiteurs/travailleurs externes, si nécessaire avec un badge visiteur/intervenant pour le système IF, si le module correspondant fait partie de l'objet du Contrat de Service.

Types de données par composants de service :

Les types de données suivants (définis en détail ci-dessous), s'ils font partie de la mission de traitement, peuvent être traités par le Prestataire :

	Services du Prestataire associés au traitement (art. 28 du RGPD).				
	Mise en service et réparation des terminaux de réservation	**Mise en service du logiciel**	**Mises à niveau et mises à jour du logiciel pour le(s) système(s) IF d'Interflex**	**Maintenance du logiciel sous forme de dépannage**	**Traitement des données via un accès à distance sécurisé (par exemple, une connexion VPN)**
Produits/Systèmes					
IF 6020 *Le système Interflex IF-6020 est une application logicielle modulaire. Dans la majorité des applications, des terminaux pour l'enregistrement du temps et/ou le contrôle d'accès sont connectés.*	- Données de réservation, accès - Données de réservation, enregistrement du temps	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges

		- Données sur les visiteurs/tiers	- Données sur les visiteurs/tiers	- Données sur les visiteurs/tiers - Données sur la planification et la gestion du personnel	- Données sur les visiteurs/tiers - Données sur la planification et la gestion du personnel
Produits/Systèmes					
IF 6040 *Le système Interflex IF-6040 est une application logicielle modulaire. Dans la majorité des applications, des terminaux pour l'enregistrement du temps et/ou le contrôle d'accès sont connectés.*	- Données de réservation, accès - Données de réservation, enregistrement du temps	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges - Données sur les visiteurs/tiers	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges - Données sur les visiteurs/tiers	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges - Données sur les visiteurs/tiers - Données sur la planification et la gestion du personnel	- Données de base personnelles - Données de réservation, accès - Données de réservation, enregistrement du temps, y compris le Client internet - Données de flux de travail, contrôle d'accès - Données sur le flux de travail, enregistrement du temps - Données frontales - Comptes de paie - Données de création de badges - Données sur les visiteurs/tiers - Données sur la planification et la gestion du personnel
SP-EXPERT *Le système Interflex SP-EXPERT est une application logicielle modulaire.*	- Données de réservation, accès	- Données de base personnelles - Données variables	Pas de système IF	- Données de base personnelles - Données variables	- Données de base personnelles - Données variables

Dans la plupart des applications, des données de planification et de gestion du personnel sont générées ou utilisées.	- Détails de la réservation Enregistrement du temps	- Données sur la gestion du temps - Données de réservation, enregistrement du temps - Données frontales - Comptes de paie		- Données sur la gestion du temps - Données de réservation, enregistrement du temps - Données frontales - Comptes de paie - Données sur la planification et la gestion du personnel - Fichiers journaux - Transfert de répertoires contenant des données importées ou exportées vers d'autres systèmes	- Données sur la gestion du temps - Données de réservation, enregistrement du temps - Données frontales - Comptes de paie - Données sur la planification et la gestion du personnel - Fichiers journaux - Transfert de répertoires contenant des données importées ou exportées vers d'autres systèmes
Personnalisation des badges	Données de création de badges	Données de création de badges	Données de création de badges	Données de création de badges	Données de création de badges
Personnalisation des visiteurs/tiers	Données sur les visiteurs/tiers	Données sur les visiteurs/tiers	Données sur les visiteurs/tiers	Données sur les visiteurs/tiers	Données sur les visiteurs/tiers

Définition des types de données :

Données de réservation, accès	Accéder aux réservations avec le terminal de réservation, l'horodateur et le résultat du contrôle d'autorisation.
Données de base personnelles	Numéro de fiche, numéro de badge, nom, prénom, numéro de personnel, département et champs facultatifs, s'ils sont utilisés par le Client dans le système.
Données de réservation, enregistrement du temps, y compris le Client internet	Type d'enregistrement de temps avec terminal d'enregistrement, horodateur et soldes des comptes de temps ; motifs d'absence (travail hors site, voyage d'affaires, congé de maladie, formation, vacances, etc.) ; absences (de/ à) ; totaux d'absentéisme (heures par jour) - les options/permissibilité des entrées et notifications de « motifs d'absence » sont déterminées par le Client.
Données de flux de travail, contrôle d'accès	Demandes d'autorisations d'accès ; approbateur et accusé de réception approuvés oui/non ; adresse e-mail utilisée pour la communication du flux de travail
Données sur le flux de travail, enregistrement du temps	Demandes de corrections, motifs d'absence, absences ; approbateur et accusé de réception approuvé oui/non ; adresse électronique pour la communication du flux de travail.

Comptes de paie	Totaux horaires pour le système de paie
Données frontales	Transfert/échange de données avec le système des salaires et traitements. Les enregistrements de données consistant en : Le numéro de fiche, le numéro de badge, le nom, le prénom, le numéro de personnel, le service, les données d'enregistrement des heures et les champs facultatifs, s'ils sont utilisés par le Client dans le système. La communication des données dépend de la configuration (personnalisation) de l'interface.
Données de création de badges	Données de personnalisation de l'empreinte visible sur le support du badge (nom, prénom, signature, et éventuellement photo numérique). Ces données et éventuellement la date de signature peuvent être conservées dans le module pour la création du badge.
Données sur les visiteurs/tiers	Données d'enregistrement, si nécessaire pour l'empreinte visible sur le support de badge/passe (nom, prénom, éventuellement signature et, si nécessaire, photo numérique). Durée du séjour, données de préenregistrement, personne visitée, motif de la visite, visiteurs individuels, visiteurs permanents.
Données sur la planification et la gestion du personnel	Fonctions, qualifications, disponibilité, horaires de travail/planification des centres de travail, données statistiques de l'ACD (système téléphonique) pour la préparation des besoins en personnel, évaluations des comptes horaires.

Annexe 2 - Mesures techniques et organisationnelles

1. Confidentialité (Article 32 para. 1 sous-paragraphe b du RGPD)

- Contrôle d'accès (physique)
  Aucun accès non autorisé aux installations de traitement des données, le concept devant être compris dans l'espace.

  Mesures techniques/organisationnelles pour le contrôle d'accès, en particulier pour la légitimation des personnes autorisées :

  ⇨ Système de contrôle d'accès avec lecteurs de badges pour cartes à puce

  ⇨ Clés/attribution de clés

  ⇨ Protection des portes (ouvreurs de portes électriques, etc.)

  ⇨ Accueil des visiteurs

  L'accès aux bâtiments/parties de bâtiments d'Interflex se fait par un contrôle d'accès électronique IF. Les visiteurs/entreprises externes ne peuvent entrer dans les parties du bâtiment Interflex qu'après enregistrement et approbation. Ils sont accompagnés par la personne visitée.

- Contrôle d'accès (logique)

  Il faut empêcher l'intrusion de personnes non autorisées dans les systèmes de traitement des données.

  Mesures techniques (protection par mot de passe) et organisationnelles (fiche d'utilisateur) concernant l'identification et l'authentification des utilisateurs :

  ⇨ Procédure de mot de passe contrôlée (syntaxe d'au moins 1 caractère spécial ou 1 lettre majuscule, 1 chiffre, minuscule, longueur minimale = 10, changement régulier du mot de passe tous les 90 jours, cycle de répétition = 24)

  ⇨ Blocage automatique (par exemple, mot de passe ou circuit de pause)

  ⇨ Mise en place d'une fiche utilisateur par utilisateur et par fonction

  ⇨ Cryptage des supports de données avec le programme Zip AES 256 bits ou VeraCrypt ou des programmes similaires.

  ⇨ Cryptage/Connexion par tunnel (VPN = Virtual Private Network)

  Pour se connecter aux systèmes informatiques du Prestataire, chaque employé utilise un nom d'utilisateur et un mot de passe individuels (respectivement des informations d'identification pour les administrateurs). Si nécessaire, ils sont connectés manuellement à l'intranet en utilisant Active Directory. L'accès externe à l'intranet n'est possible que par VPN. L'accès n'est accordé que si les données d'identification de l'ordinateur, le nom d'utilisateur et le mot de passe y sont connus et correspondent. La syntaxe des mots de passe, qui doivent être modifiés à intervalles réguliers, est d'au moins 10 caractères, des caractères spéciaux ou des lettres majuscules, des minuscules et au moins un chiffre. Le cycle de répétition est de 24. Ces conditions sont automatiquement vérifiées lors de la modification du mot de passe, et si elles ne sont pas remplies, le nouveau mot de passe est rejeté. Si un mot de passe n'est pas modifié à temps, il expire et l'accès est refusé.

- Contrôle du droit d'accès

  Il faut empêcher les activités non autorisées dans les systèmes de traitement des données qui dépassent le cadre des autorisations accordées.

  Conception, en fonction des besoins, du concept d'autorisation et des droits d'accès, ainsi que de leur contrôle et de leur consignation :

⇨ Autorisations différenciées et attribution de mots de passe temporaires (selon le concept d'autorisation du système Interflex) par le Client.

⇨ Conservation des données fournies sur un ordinateur local dans des conteneurs cryptés (par exemple, en utilisant VeraCrypt ou des programmes similaires). L'ordinateur local lui-même doit être complètement crypté à l'aide d'une solution d'entreprise.

⇨ Accès limité à la personne qui effectue le traitement des données en question.

Les données fournies au Prestataire sont conservées pendant la durée du traitement dans des conteneurs locaux cryptés (par exemple VeraCrypt ou des programmes similaires) et sont supprimées après la fin des travaux à l'aide d'un système d'effacement spécial. Les supports de données locaux sur les ordinateurs sont en outre entièrement cryptés à l'aide d'une solution d'entreprise. La conservation temporaire des données est limitée aux systèmes locaux des personnes chargées de l'exécution de la mission. Seuls les utilisateurs autorisés d'Interflex ont accès au PC.

Le contrôle de l'accès aux données du système Interflex Client est réglé par le Client lui-même en attribuant/spécifiant/supprimant un mot de passe temporaire.

- Séparation des données

  Les données collectées à des fins différentes doivent être traitées séparément.

  Mesures pour le traitement séparé (conservation, modification, effacement, transmission) des données avec des finalités différentes :

  ⇨ « Capacité multi-clients interne »/earmarking

  ⇨ Séparation des fonctions/production/test

  Les données du Client sont conservées et traitées temporairement dans des conteneurs cryptés et protégés par un mot de passe, tout en étant strictement séparées des autres données du Client. En cas de traitement par télécommande en ligne, les modifications sont effectuées directement dans le système du Client. Il existe un serveur séparé pour les données de test.

- Pseudonymisation (Art. 32 para. 1 sub-para. a du RGPD ; Art. 25 para. 1 du RGPD).
  Le traitement de données à caractère personnel de telle sorte que les données ne puissent être reliées à une personne concernée spécifique sans la fourniture d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles appropriées.

  Aux fins du service, les données fournies par le Client sont généralement traitées sous une forme pseudonymisée. Si nécessaire, les données peuvent être rendues anonymes. La procédure exacte dépend du cas particulier du service.

2. Intégrité (article 32, paragraphe 1, alinéa b, du RGPD)

- Contrôle du transfert

  Traitement des aspects du transfert des données à caractère personnel: Transmission électronique, transport de données, contrôle de la transmission. Aucune lecture, copie, modification ou suppression non autorisée.

  Mesures pendant le transport, le transfert et la transmission ou la conservation sur des supports de données (manuels ou électroniques) et vérification ultérieure :

  ⇨ Cryptage/connexion par tunnel (VPN = Virtual Private Network)

⇨ Sauvegarde des données à l'aide d'un programme Zip (par exemple WinZip) et cryptage AES 256 bits avec mot de passe sur CD/DVD

⇨ Sauvegarde

En règle générale, les données ne sont pas transmises, sauf si la résolution d'un problème nécessite la coopération du service de développement du Prestataire. Si cela s'avérait nécessaire, la sauvegarde des données est soit transférée sur un CD/DVD envoyé par courrier, à l'aide d'un programme Zip, d'un cryptage AES 256 bits et d'un mot de passe, soit, pour de petites quantités de données, directement via l'Intranet à l'aide d'un programme Zip et d'un cryptage AES 256 bits. Tout transfert de ce type est documenté de manière appropriée.

- Contrôle des entrées

  Les mesures de gestion et de maintenance des données doivent être documentées pour assurer la traçabilité.

  Mesures permettant de vérifier ultérieurement si et par qui les données ont été introduites, modifiées ou supprimées (effacées) :

  ⇨ Consignation via un fichier journal dans le(s) système(s) Interflex.

  Les systèmes IF disposent d'un fichier journal dans lequel les modifications sont saisies avec l'ID utilisateur correspondant ainsi que la date et l'heure.

3. Disponibilité et résilience (art. 32 para. 1 sous-paragraphe b du RGPD)

- Contrôle des disponibilités

  Les données doivent être protégées contre la destruction ou la perte accidentelle.

  Mesures pour la sauvegarde des données (physique/logique) :

  ⇨ Absence de procédure de sauvegarde des données du Client en raison d'une suppression conforme à la protection des données après que la finalité a cessé d'être appliquée.

  ⇨ Protection contre les virus / Pare-feu

  ⇨ UPS pour serveurs

  Les sauvegardes de données des systèmes du Client ne sont pas sauvegardées sur des serveurs ayant une fonction de sauvegarde, de sorte que l'effacement de ces données conformément aux règlements sur la protection des données puisse être assuré après que la finalité a cessé d'exister.
  Tous les systèmes informatiques sont équipés de programmes anti-virus. après chaque démarrage à l'aide de Microsoft System Center Endpoint Protection. Les signatures antivirus sont mises à jour rapidement après leur publication via la solution Endpoint Protection contrôlée de manière centralisée. Un contrôle complet automatique est effectué chaque semaine. Tous les serveurs sont protégés contre les fluctuations ou les pannes de courant au moyen d'un UPS.

- Rétablissement rapide (art. 32 para. 1 sous-paragraphe c du RGPD) ;

  a) Il y a plusieurs serveurs pour les systèmes propres du Prestataire. Protection des données par des sauvegardes quotidiennes. Virtualisation des systèmes avec sauvegarde centralisée en préparation
  b) Systèmes Clients :
  Lorsque des données sont transmises à Interflex, il ne s'agit pas de données originales mais de simples copies de données et/ou de bases de données. Aucune sauvegarde n'est effectuée afin de garantir l'effacement après que la finalité du traitement a cessé d'exister, c'est-à-dire après la fin de la mission. Les données originales resteront dans le système du

Client. La responsabilité des données contenues dans le système du Client incombe à celui-ci.

4. Procédures de révision, d'appréciation et d'évaluation régulières (Art. 32 para. 1 sub-para. d du RGPD; Art. 25 para. 1 du RGPD).

- Gestion de la protection des données ;
- gestion de la réponse aux incidents : Est inclus dans le SMSI (système de gestion de la sécurité de l'information)
- Protection des données par défaut (art. 25 para. 2 du RGPD).
- Contrôle continu
- Restauration des sauvegardes à des fins de test
- Tests réguliers de l'ASI
- Contrôle des missions

  Aucun traitement de données en vertu de l'art. 28 du RGPD sans instructions correspondantes du Client

  Mesures (techniques/organisationnelles) pour délimiter les responsabilités entre le Client et le Prestataire :

  ⇨ Rédaction sans ambiguïté des contrats conformément à l'art. 28 du RGPD).

  ⇨ Passation formalisée des commandes (contrat de maintenance ou missions individuelles écrites)

  Le Prestataire exécute l'objet des services commandés par ses propres moyens, sans sous-traitants, conformément aux instructions du Client.
  Par principe, les changements commandés ne concernent que les programmes et la logique d'évaluation.

Annexe 3 - Sous-traitants

1. ☒ Actuellement, aucun sous-traitant n'est employé.

2. ☐ Actuellement, les sous-traitants suivants sont engagés :

Nom de la société sous-traitante	Adresse/Pays	Service