

Verwerkingsovereenkomst overeenkomstig art. 28 van de Algemene verordening gegevensbescherming (AVG)

Kaderovereenkomst, geldig voor alle opdrachten

tussen

[Volledige bedrijfsnaam van de Klant]

[Adres]

[Plaats]

(Gegevensverwerkingsverantwoordelijke, hierna "**Klant**" genoemd)

en

Allegion N.V.

Pontbeekstraat 2

B- 1702 Dilbeek

(verwerker, hierna de "**Contractant**" genoemd)

§ 1 Voorwerp en duur van de overeenkomst

(1) Voorwerp

De Contractant biedt systemen aan voor geautomatiseerde controle op de toegang en tijdsregistratie, alsook Advance Workforce Management.

Deze Overeenkomst is van toepassing op alle bestaande en toekomstige overeenkomsten tussen de partijen betreffende specifieke IT-dienstverlening met betrekking tot deze systemen door de Contractant aan de Klant (hierna "**Dienstverleningsovereenkomst**" genoemd, zelfs in het geval van meerdere overeenkomsten).

De systemen van de Contractant worden gewoonlijk als lokale oplossingen bij en door de Klant gebruikt, maar het is niet uitgesloten dat - in het kader van de bovengenoemde specifieke IT-dienstverlening - de Contractant toegang wordt verleend tot persoonsgegevens in overeenstemming met deze Overeenkomst voor de gegevens die eronder vallen.

(2) Duur, beëindiging

Tenzij anders overeengekomen, is deze Overeenkomst van toepassing zolang de Contractant persoonsgegevens verwerkt in het kader van de uitvoering van de Dienstverleningsovereenkomst.

Elke partij kan de Overeenkomst te allen tijde zonder opzegtermijn beëindigen indien er sprake is van een ernstige inbreuk door een van de partijen op de bepalingen inzake gegevensbescherming of op de bepalingen van deze Overeenkomst. Het verzuim om de in deze Overeenkomst opgenomen verplichtingen en die welke voortvloeien uit artikel 28 van de AVG na te leven, is met name een ernstige inbreuk.

§ 2 Initiële bepalingen met betrekking tot de inhoud van deze Overeenkomst

Aard en doel van de verwerking van persoonsgegevens

Het doel van de verwerking van persoonsgegevens door de Contractant namens de Klant, de types verwerkte gegevens en de categorieën van betrokkenen worden nader omschreven in de Dienstverleningsovereenkomst en in **Bijlage 1 - Specificatie in het kader van de wetgeving inzake gegevensbescherming**.

De overeengekomen gegevensverwerking vindt momenteel uitsluitend plaats in de Bondsrepubliek Duitsland, in een andere lidstaat van de Europese Unie of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte. Elke overdracht naar een derde land op een later tijdstip vereist de toestemming van de Klant en valt onder de bijzondere vereisten van de artikelen 44 en volgende van de AVG. Het passende beschermingsniveau kan worden gewaarborgd door standaardbepalingen inzake gegevensbescherming (artikel 46, lid 2, eerste alinea, onder c) en d) van de AVG), door goedgekeurde gedragsregels (art. 46, lid 2, eerste alinea, onder e), in samenhang met art. 40 van de AVG), door een goedgekeurd certificeringsmechanisme (art. 46, lid 2, eerste alinea, onder f), in samenhang met art. 42 van de AVG) of door andere maatregelen overeenkomstig art. 46, lid 2, eerste alinea, onder a), lid 3, eerste alinea, onder a) en b) van de AVG.

§ 3 Bevoegdheid van de Klant om instructies te geven

(1) De Contractant verwerkt de persoonsgegevens uitsluitend met het oog op het verlenen van diensten in het kader van de Dienstverleningsovereenkomst en in overeenstemming met de schriftelijke instructies van de Klant. Dit geldt ook voor elke doorgifte van persoonsgegevens aan een derde land of een internationale organisatie, tenzij de wetgeving van de Europese Unie of een lidstaat waaronder de Contractant valt, anders voorschrijft. In dat geval stelt de Contractant de Klant vóór de verwerking in kennis van een dergelijk voorschrift, tenzij de wetgeving in kwestie een dergelijke kennisgeving verbiedt op grond van een zwaarwegend algemeen belang. De instructies worden gegeven op grond van de Dienstverleningsovereenkomst; het instellen en configureren van de dienst gebeurt op instructie van de Klant. Verdere instructies na het sluiten van de Overeenkomst dienen in tekstvorm gegeven te worden en moeten door de Klant schriftelijk worden bevestigd indien de Contractant daarom verzoekt.

(2) Indien de Klant instructies geeft die buiten de werkingssfeer van de Dienstverleningsovereenkomst vallen, is daarvoor de toestemming van de Contractant vereist.

(3) Indien de Contractant van mening is dat een door de Klant gegeven instructie in strijd is met wettelijke bepalingen, zal de Contractant de Klant hierop wijzen. De Contractant kan de uitvoering van een dergelijke instructie opschorten.

§ 4 Technische en organisatorische maatregelen

(1) Vóór de aanvang van de verwerkingsactiviteiten legt de Contractant de beoogde uitvoering van de technische en organisatorische maatregelen die vóór de gunning van het contract waren vastgesteld schriftelijk vast en legt hij die ter controle voor aan de Klant, in het bijzonder met betrekking tot de concrete uitvoering van de opdracht. Indien deze maatregelen door de Klant worden aanvaard, worden zij de grondslag van de Overeenkomst. Wanneer uit het onderzoek of een audit van de Klant blijkt dat een aanpassing noodzakelijk is, moet daaraan in onderling overleg uitvoering worden gegeven.

(2) De Contractant waarborgt de beveiliging van de verwerking overeenkomstig artikel 28, lid 3, eerste alinea, onder c), en art. 32 van de AVG, in het bijzonder in samenhang met art. 5, lid 1, lid 2 van de AVG. In het algemeen hebben de te nemen maatregelen betrekking op de beveiliging van gegevens en op het waarborgen van een beschermingsniveau dat in verhouding staat tot het risico, wat betreft de vertrouwelijkheid, de integriteit, de beschikbaarheid en de veerkracht van de systemen. In dit verband moet rekening worden gehouden met de stand van de techniek, de uitvoeringskosten, de aard, de omvang en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen in de zin van artikel 32, lid 1 van de AVG, (nadere bijzonderheden in Bijlage 2 bij deze Overeenkomst).

(3) De genomen technische en organisatorische maatregelen kunnen technisch worden aangescherpt en verder worden ontwikkeld. In dit verband kan de Contractant alternatieve passende maatregelen toepassen, mits het veiligheidsniveau van de oorspronkelijk vastgestelde maatregelen niet wordt ondermijnd. Belangrijke wijzigingen moeten schriftelijk of elektronisch worden vastgelegd.

(4) Voor zover de Contractant zijn activiteit ter plaatse bij de Klant uitoefent, is de Contractant niet verantwoordelijk voor de technische en organisatorische maatregelen die binnen de invloedssfeer van de Klant liggen en onder zijn verantwoordelijkheid vallen.

(5) Voor zover de Contractant diensten verricht in de gebouwen van de Klant, is de Contractant niet verantwoordelijk voor de naleving van de technische en organisatorische maatregelen die binnen de invloedssfeer van de Klant liggen en onder zijn verantwoordelijkheid vallen.

§ 5 Kwaliteitszorg en andere verplichtingen van de Contractant

De Contractant moet niet alleen de bepalingen van deze Overeenkomst naleven, maar heeft ook wettelijke verplichtingen op grond van de artikelen 28 tot en met 33 van de AVG. In dit verband garandeert de Contractant dat hij in het bijzonder aan de volgende eisen zal voldoen:

- a) Het benoemen van een functionaris voor gegevensbescherming, schriftelijk vastgelegd, overeenkomstig de artikelen 38 en 39 van de AVG.

De actuele contactgegevens van de functionaris voor gegevensbescherming moeten te allen tijde gemakkelijk terug te vinden zijn op de website van de Contractant.

- b) Het waarborgen van de vertrouwelijkheid overeenkomstig artikel 28, lid 3, eerste alinea, onder b), art. 29 en art. 32, lid 4 van de AVG. Bij de uitvoering van de werkzaamheden stelt de Contractant uitsluitend personeelsleden tewerk die tot geheimhouding verplicht zijn en vooraf op de hoogte zijn gebracht van de bepalingen inzake gegevensbescherming die op hen van toepassing zijn.
- c) Het uitvoeren en naleven van alle technische en organisatorische maatregelen die voor deze Overeenkomst vereist zijn overeenkomstig artikel 28, lid 3, eerste alinea, onder c) en art. 32 van de AVG (nadere gegevens in Bijlage 2 bij deze Overeenkomst).
- d) De Klant en de Contractant verlenen op verzoek hun medewerking aan de toezichthoudende autoriteit bij de uitoefening van haar taken.
- e) De onmiddellijke kennisgeving aan de Klant van maatregelen en controleacties van de toezichthoudende autoriteit, voor zover zij betrekking hebben op deze Overeenkomst. Dit geldt ook wanneer een bevoegde autoriteit in het kader van een administratieve of strafrechtelijke procedure in verband met de verwerking van persoonsgegevens een onderzoek instelt naar verwerkingsactiviteiten bij de Contractant.
- f) Wanneer de toezichthoudende overheid maatregelen heeft genomen tegen de Klant zelf, of tegen de Klant een administratieve of strafrechtelijke procedure loopt, een aansprakelijkheidsclaim van een betrokkene of een derde, of enige andere eis in verband met de verwerking van persoonsgegevens door de Contractant, staat de Contractant de Klant naar beste vermogen bij.
- g) De Contractant controleert regelmatig de interne processen die worden uitgevoerd en de technische en organisatorische maatregelen die worden genomen om ervoor te zorgen dat de verwerking waarvoor hij verantwoordelijk is in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming plaatsvindt en dat de rechten van de betrokkenen worden beschermd.

- h) Op verzoek van de Klant verstrekt de Contractant de Klant het bewijs van de technische en organisatorische maatregelen die in het kader van de controlebevoegdheden van de Klant uit hoofde van artikel 7 van deze Overeenkomst zijn genomen.
- i) Bij beëindiging van de krachtens de Dienstverleningsovereenkomst te verlenen diensten of op verzoek van de Klant, bezorgt de Contractant alle in zijn bezit zijnde documenten en alle in het kader van de Overeenkomst geproduceerde werkresultaten en gegevens aan de Klant terug of wist hij deze in overeenstemming met de wetgeving inzake gegevensbescherming, na voorafgaande toestemming van de Klant.
- j) De Contractant bewaart de documentatie die als bewijs dient voor de correcte verwerking van gegevens in overeenstemming met de toepasselijke bewaartermijnen tot na het einde van de Overeenkomst. De Contractant kan deze documentatie bij beëindiging van de Overeenkomst aan de Verwerkingsverantwoordelijke overhandigen.

§ 6 Relaties met onderaannemers

(1) Voor de toepassing van deze bepaling worden relaties met onderaannemers geacht rechtstreeks verband te houden met het verlenen van de hoofddienst. Uitbestede bijkomende diensten, die niet hoofdzakelijk betrekking hebben op de verwerking van persoonsgegevens, bv. diensten in verband met post, telecommunicatie, logistiek, schoonmaak en ambachtelijke diensten, zijn niet inbegrepen. Ook in het geval van uitbestede bijkomende diensten waarborgt de Contractant echter de bescherming en beveiliging van de persoonsgegevens van de Klant door middel van adequate en wettelijk conforme overeenkomsten en toezichtsmaatregelen.

(2) De Contractant kan een externe verwerker (hierna "onderaannemer" genoemd) aanwijzen. Door ondertekening van deze Overeenkomst geeft de Klant de Contractant de algemene toestemming om een onderaannemer in dienst te nemen. De Contractant die een beroep doet op onderaannemers, stelt de Klant in kennis van elke voorgenomen wijziging in dat verband, met inbegrip van hun vervanging. De Klant kan bezwaren uiten met betrekking tot een onderaannemer en kan, indien deze niet in der minne worden opgelost, deze Overeenkomst beëindigen met ingang van de datum waarop de wijziging van kracht wordt. Momenteel zijn geen onderaannemers in dienst genomen, tenzij deze zijn vermeld in Bijlage 3 - Onderaannemers.

(3) De Contractant draagt, ten minste en in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming, de relevante verplichtingen uit hoofde van deze Overeenkomst over aan onderaannemers door middel van (sub)verwerkingsovereenkomsten, met inbegrip van te nemen passende technische en organisatorische maatregelen.

(4) De Contractant sluit vertrouwelijkheidsovereenkomsten met alle onderaannemers, tenzij een passende wettelijke vertrouwelijkheidsverplichting van toepassing is.

§ 7 Controlebevoegdheden van de Klant

(1) De Klant kan zich op eigen kosten, vóór het begin van de gegevensverwerking en vervolgens met regelmatige tussenpozen, vergewissen van de technische en organisatorische maatregelen die de Contractant overeenkomstig bijlage 2 heeft genomen, en de resultaten ervan vastleggen. Hij kan dit *onder meer* doen door van de Contractant een eigen verklaring te vragen, die de Contractant ook in de vorm van een passend certificaat van een deskundige kan overleggen, of door zelf ter plaatse een inspectie uit te voeren.

(2) De Contractant verbindt zich ertoe de Klant op schriftelijk verzoek en binnen een redelijke termijn alle informatie te verstrekken die nodig is in het kader van een passende controle.

(3) Indien de Klant een derde de opdracht geeft tot het uitvoeren van een inspectie (inclusief een inspectie ter plaatse), zal de Klant deze derde schriftelijk tot geheimhouding en vertrouwelijkheid doen verbinden, tenzij de derde beroepsmatig is gehouden tot geheimhouding. Op verzoek van de Contractant legt de Klant de desbetreffende overeenkomsten met de derde onverwijld voor aan de Contractant. Het is de Klant niet toegestaan een concurrent van de Contractant met een inspectie te belasten.

(4) Elke inspectie ter plaatse moet in de regel 30 dagen van tevoren schriftelijk worden aangekondigd, is beperkt tot de normale kantooruren en moet zo worden uitgevoerd dat de bedrijfsactiviteiten van de Contractant zo min mogelijk worden gehinderd. Eventuele routine-inspecties ter plaatse zijn beperkt tot maximaal 1 keer per kalenderjaar. De Klant deelt het resultaat van zijn inspectie schriftelijk mee binnen 30 dagen (als algemene regel) na de voltooiing van de inspectie.

§ 8 Rechten van de betrokkenen

(1) De rechten van personen die door de verwerking van persoonsgegevens worden geschaad, worden ten aanzien van de Klant uitgeoefend.

(2) Wanneer een betrokkene de Contractant rechtstreeks om informatie verzoekt over de hem betreffende gegevens, of om rectificatie, wissing of afscherming van die gegevens verzoekt, zal de Contractant dit verzoek zonder onnodige vertraging aan de Klant doorsturen.

(3) Indien een betrokkene zijn rechten inzake gegevensbescherming doet gelden, zal de Contractant, binnen redelijke grenzen en voor zover dit voor de Klant noodzakelijk is, de Klant met passende technische en organisatorische maatregelen bijstaan, op voorwaarde dat de Klant een bepaalde eis niet zonder medewerking van de Contractant kan afhandelen.

(4) De Contractant zal de Klant in staat stellen persoonsgegevens te rectificeren, te wissen of af te schermen of, op verzoek van de Klant, deze gegevens zelf rectificeren, afschermen of wissen indien en voor zover dit niet door de Klant kan worden gedaan.

§ 9 Kennisgeving in geval van inbreuken

(1) De Contractant helpt de Klant te voldoen aan de verplichtingen van de artikelen 32 tot en met 36 van de AVG inzake de beveiliging van persoonsgegevens, de melding in geval van gegevensinbreuken, gegevensbeschermingseffectbeoordelingen en voorafgaande raadplegingen van toezichthoudende autoriteiten. Dit houdt *onder meer* het volgende in:

- a) een passend beschermingsniveau waarborgen door middel van technische en organisatorische maatregelen, waarbij rekening wordt gehouden met de omstandigheden en de doeleinden van de gegevensverwerking, alsook met de voorspelde waarschijnlijkheid en ernst van mogelijke inbreuken als gevolg van beveiligingsinbreuken, en die zodanig zijn ingesteld dat relevante inbreuken onmiddellijk kunnen worden opgespoord;
- b) de verplichting om de Klant bij te staan in zijn verplichting om informatie te verstrekken aan de betrokkenen, door de Klant onverwijld alle relevante informatie ter beschikking te stellen;
- c) de Klant bijstaan met gegevensbeschermingseffectbeoordelingen, indien nodig;
- d) de Klant helpen in het kader van voorafgaande raadpleging van de toezichthoudende autoriteit.

(2) De Contractant is ervan op de hoogte dat voor de Klant een kennisgevingsplicht kan gelden krachtens art. 33 van de AVG, op grond waarvan de toezichthoudende autoriteit binnen 72 uur na het bekend worden van een omstandigheid in kennis moet worden gesteld. De Contractant zal de Klant bijstaan wat deze kennisgevingsplicht betreft.

(3) De Contractant stelt de Klant onverwijld in kennis van een inbreuk in verband met persoonsgegevens waarvan hij kennis neemt in het kader van de gegevensverwerking.

(4) Indien de Klant als gevolg van een incident wettelijke meldingsplichten opgelegd krijgt met betrekking tot onrechtmatige verkrijging van persoonsgegevens, zal de Contractant de Klant op diens verzoek binnen de grenzen van het redelijke en noodzakelijke bijstaan om aan deze verplichtingen te voldoen. Voor deze bijstand is een vergoeding verschuldigd, tenzij het incident door toedoen van de Contractant is ontstaan of deel uitmaakt van de dienstomschrijving van de Dienstverleningsovereenkomst.

(5) Indien de Klant gebruik maakt van een oplossing ter plaatse die door Klant zelf wordt aangebracht, bestaat de bijstandsplicht van de Contractant conform deze § 9 slechts voor zover het voor de Klant niet mogelijk is om zelf de benodigde informatie te verkrijgen of zelf de benodigde werkzaamheden uit te voeren.

§ 10 Rectificatie, wissing en beperking van verwerkte gegevens

(1) De Contractant mag de uit hoofde van deze Overeenkomst verwerkte gegevens niet op eigen gezag corrigeren, wissen of beperken, maar alleen na schriftelijke instructies van de Klant. Indien een betrokkene zich in dit verband rechtstreeks tot de Contractant wendt, stuurt de Contractant dit verzoek onverwijld door aan de Klant.

(2) Gegevens die de Contractant louter voor de uitvoering van de diensten (bv. onderhoud) verwerkt, worden gewist zodra zij niet langer nodig zijn voor de betrokken dienst (zie bijlage 2 - Controle op de toegang).

§ 11 Aansprakelijkheid

Art. 82 van de AVG is van toepassing. Indien de Dienstverleningsovereenkomst bepalingen inzake aansprakelijkheid bevat, zijn deze eveneens van toepassing op de relatie tussen de partijen binnen het toepassingsgebied van deze Overeenkomst.

§ 12 Verplichting tot betaling van een vergoeding

(1) Indien de Contractant krachtens deze Overeenkomst verplicht is diensten te verlenen die verder gaan dan de reikwijdte van de Dienstverleningsovereenkomst ("**Bijkomende diensten**"), worden deze diensten afzonderlijk vergoed naar gelang van de bestede tijd en het gebruikte materiaal. Dit is met name het geval voor de activiteiten die worden beschreven §1, lid 2, §3, lid 2, §1, lid 2, §5, letter d) en letter f), §7 (met uitzondering van diensten die nodig zijn ten gevolge van een inbreuk die onder de verantwoordelijkheid van de Contractant valt), § 8 en § 10. Voor alle duidelijkheid: voor zover de Contractant op eigen initiatief Bijkomende diensten heeft verricht, is de Klant geen vergoeding verschuldigd op grond van deze § 12.

(2) Onder voorbehoud van de Dienstverleningsovereenkomst of andere overeenkomsten tussen de partijen, is de vergoeding voor Bijkomende diensten van de werknemers van de Contractant gebaseerd op een vast bedrag van 180 euro per uur, vermeerderd met de wettelijke belasting over de toegevoegde waarde. Voor materiaal- en reiskosten factureert de Contractant de Klant het werkelijk gedragen bedrag, vermeerderd met de belasting over de toegevoegde waarde. Indien de Contractant extra kosten kan bewijzen, kan hij het volledige bedrag in rekening brengen.

§ 13 Diverse bepalingen

(1) Aanvullingen op deze Overeenkomst en wijzigingen daarvan dienen schriftelijk te worden vastgesteld. Dit geldt ook wanneer afstand werd gedaan van de vereiste tot schriftelijke vaststelling.

(2) Mocht een bepaling van deze Overeenkomst juridisch ongeldig blijken, dan blijft de geldigheid van de overige bepalingen onaangetast. De ongeldige bepaling wordt met terugwerkende kracht vervangen door een bepaling die qua inhoud en zakelijke gevolgen zo dicht mogelijk bij de oorspronkelijke bepaling ligt.

(3) Het is uitgesloten om een beroep te doen op het recht op retentie met betrekking tot de voor de Klant verwerkte gegevens en de bijbehorende gegevensdragers.

(4) Indien de gegevens van de Klant door de Contractant in gevaar worden gebracht door beslaglegging, door een insolventieprocedure of door andere gebeurtenissen of maatregelen van derden, moet de Contractant de Klant daarvan onmiddellijk in kennis stellen. De Contractant stelt alle in dit verband verantwoordelijke personen er onmiddellijk van in kennis dat de zeggenschap en de eigendom van de gegevens uitsluitend berusten bij de Klant als Verwerkingsverantwoordelijke in de zin van de AVG.

Allegion N.V.

Naam van de Klant

Handtekening

Handtekening

Naam, functie

Naam, functie

Datum, stempel

Datum, stempel

Bijlage 1 - Specificatie in het kader van de wetgeving inzake gegevensbescherming

Deze bijlage 1 (Specificatie in het kader van de wetgeving inzake gegevensbescherming) vormt een aanvulling op de desbetreffende gesloten Dienstverleningsovereenkomst. Het spreekt vanzelf dat alleen die persoonsgegevens worden verwerkt die deel uitmaken van de overeengekomen reikwijdte van de dienstverlening.

Categorieën van betrokkenen:

1. Werknemers, die het IF-systeem gebruiken
2. Bezoekers/externe werknemers, indien nodig met bezoekers-/gastenbadge voor het IF-systeem, indien de overeenkomstige module onder de Dienstverleningsovereenkomst valt.

Types gegevens per dienstcomponent:

De volgende types gegevens (hieronder nader omschreven) kunnen, indien zij deel uitmaken van de verwerkingsopdracht, door de Contractant worden verwerkt:

	Diensten van de Contractant in verband met de verwerking (art. 28 van de AVG)				
	Inbedrijfstelling en reparatie van de inboekterminals	Inbedrijfstelling van de software	Software-upgrades en -updates voor Interflex IF-syste(e)m(en)	Onderhoud van software in de vorm van het oplossen van problemen	Gegevensverwerking via beveiligde toegang op afstand (bv. VPN-verbinding)
Producten/Systemen					
IF 6020 <i>Het Interflexsysteem IF-6020 is een modulaire softwaretoepassing. In de meeste toepassingen is er verbinding met terminals voor tijdsregistratie en/of controle op de toegang.</i>	- Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden

				- Planning van het personeelsbestand en beheersgegevens	- Planning van het personeelsbestand en beheersgegevens
Producten/Systemen					
IF 6040 <i>Het Interflexsysteem IF-6040 is een modulaire softwaretoepassing. In de meeste toepassingen is er verbinding met terminals voor tijdsregistratie en/of controle op de toegang.</i>	- Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden - Planning van het personeelsbestand en beheersgegevens	- Masterpersoonsgegevens - Inboekgegevens, toegang - Inboekgegevens, tijdsregistratie inclusief webclient - Workflowgegevens, controle op de toegang - Workflowgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen - Gegevens voor het aanmaken van badges - Gegevens van bezoekers/derden - Planning van het personeelsbestand en beheersgegevens
SP-EXPERT <i>Het Interflexsysteem SP-EXPERT is een modulaire softwaretoepassing. In de meeste toepassingen worden gegevens over personeelsplanning en -beheer gegenereerd of gebruikt.</i>	- Inboekgegevens, toegang - Nadere inboekgegevens - Tijdsregistratie	- Masterpersoonsgegevens - Variabele gegevens - Gegevens over tijdbeheer - Inboekgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen	Geen IF-systeem	- Masterpersoonsgegevens - Variabele gegevens - Gegevens over tijdbeheer - Inboekgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen	- Masterpersoonsgegevens - Variabele gegevens - Gegevens over tijdbeheer - Inboekgegevens, tijdsregistratie - Front-endgegevens - Payrollrekeningen

				- Planning van het personeelsbestand en beheersgegevens - Logbestanden - Overdracht van registers met gegevens geïmporteerd uit of geëxporteerd naar andere systemen	- Planning van het personeelsbestand en beheersgegevens - Logbestanden - Overdracht van registers met gegevens geïmporteerd uit of geëxporteerd naar andere systemen
Personalisatie van badges	Gegevens voor het aanmaken van badges	Gegevens voor het aanmaken van badges	Gegevens voor het aanmaken van badges	Gegevens voor het aanmaken van badges	Gegevens voor het aanmaken van badges
Personalisatie voor bezoekers/derden	Gegevens van bezoekers/derden	Gegevens van bezoekers/derden	Gegevens van bezoekers/derden	Gegevens van bezoekers/derden	Gegevens van bezoekers/derden

Definitie van de gegevenstypes:

Inboekgegevens, toegang	Toegang tot inboekingen met inboekterminal, tijdstempel en resultaat van de autorisatiecontrole.
Masterpersoonsgegevens	Masterrecordnummer, badgenummer, naam, voornaam, personeelsnummer, afdeling en facultatieve velden, indien gebruikt door de Klant binnen het systeem
Inboekgegevens, tijdsregistratie inclusief webclient	Tijdsregistratie inboektype met inboekterminal, tijdstempel en saldi van de tijdrekeningen; redenen voor afwezigheid (werk buiten de kantoren, zakenreis, ziekteverlof, opleiding, vakantie, enz.); afwezigheden (van tot); verzuimtotalen (uren per dag) - opties/toelaatbaarheid van "reden voor afwezigheid"-invoeren en -meldingen worden bepaald door de Klant.
Workflowgegevens, controle op de toegang	Verzoeken om toegangsautorisaties; goedkeurder en bevestiging goedgekeurd ja/nee; e-mailadres gebruikt voor workflowcommunicatie
Workflowgegevens, tijdsregistratie	Verzoeken om correcties, redenen voor afwezigheid, afwezigheden; goedkeurder en bevestiging goedgekeurd ja/nee; e-mailadres voor workflowcommunicatie

Payrollrekeningen	Uurtotalen voor het payrollstelsel
Front-endgegevens	Gegevensoverdracht/gegevensuitwisseling met het loon- en salarissstelsel. Gegevensbestanden bestaande uit: masterrecordnummer, badgenummer, naam, voornaam, personeelsnummer, afdeling, tijdsregistratie-inboekgegevens en facultatieve velden, indien gebruikt door de Klant binnen het systeem. De gegevenscommunicatie is afhankelijk van de configuratie (aanpassing) van de interface.
Gegevens voor het aanmaken van badges	Gepersonaliseerde gegevens voor de zichtbare afdruk op de badgedrager (naam, voornaam, handtekening, en eventueel digitale foto). Deze gegevens en eventueel de datum van ondertekening kunnen in de module worden opgeslagen voor het aanmaken van de badge.
Gegevens van bezoekers/derden	Registratiegegevens, indien nodig voor de zichtbare afdruk op de badgedrager/pas (naam, voornaam, eventueel handtekening en, indien nodig, digitale foto). Duur van de afspraak, gegevens uit de registratie vooraf, persoon met wie de afspraak plaatsvond, reden voor de afspraak, individuele bezoekers, vaste bezoekers.
Planning van het personeelsbestand en beheersgegevens	Functies, kwalificaties, beschikbaarheid, dienstroosters/werkcentrumplanning, statistische gegevens van het ACD (telefoonstelsel) voor het opstellen van personeelsbehoeften, evaluaties van overzichten van gewerkte tijd.

Bijlage 2 - Technische en organisatorische maatregelen

1. Vertrouwelijkheid (artikel 32, lid 1, eerste alinea, onder b) van de AVG)

- Controle op de toegang (fysiek)

Geen ongeoorloofde toegang tot gegevensverwerkingsfaciliteiten, waarbij het begrip ruimtelijk moet worden opgevat.

Technische/organisatorische maatregelen voor controle op de toegang, met name voor de legitimatie van gemachtigde personen:

- ⇒ Systeem voor controle op de toegang met badgelezers voor chipkaarten
- ⇒ Sleutels/sleuteltoewijzing
- ⇒ Deurbeveiliging (elektrische deuropeners, enz.)
- ⇒ Onthaal voor bezoekers

De toegang tot de gebouwen/gedeelten van gebouwen bij Interflex verloopt via elektronische IF-toegangscontrole. Bezoekers/externe bedrijven kunnen de Interflex-gebouwdelen alleen betreden na registratie en goedkeuring. Zij worden vergezeld door de persoon waarmee zij een afspraak hebben.

- Controle op de toegang (logisch)

Er moet worden voorkomen dat niet-gemachtigde personen in de gegevensverwerkingssystemen binnendringen.

Technische (wachtwoordbeveiliging) en organisatorische (gebruikersmasterrecord) maatregelen met betrekking tot de identificatie en authenticatie van gebruikers:

- ⇒ Gecontroleerde wachtwoordprocedure (syntax ten minste 1 speciaal teken of 1 hoofdletter, 1 cijfer, kleine letters, minimumlengte = 10, regelmatig wachtwoord wijzigen om de 90 dagen, herhalingscyclus = 24)
- ⇒ Automatische blokkering (bv. wachtwoord of onderbreken van het circuit)
- ⇒ Opzetten van een gebruikersmasterrecord per gebruiker en functie
- ⇒ Versleuteling van gegevensdragers met AES 256-bits zipprogramma of VeraCrypt of soortgelijke programma's.
- ⇒ Versleuteling/tunnelverbinding (VPN = Virtual Private Network)

Om in te loggen op de computersystemen van de Contractant gebruikt elk personeelslid een individuele gebruikersnaam en een individueel wachtwoord (respectievelijk admin-inloggegevens voor beheerders). Indien nodig worden zij manueel op het intranet aangesloten met behulp van Active Directory. Externe toegang tot het intranet is alleen mogelijk via VPN. Toegang wordt alleen verleend indien de identificatiegegevens van de computer, de gebruikersnaam en het wachtwoord daar bekend zijn en overeenstemmen. De syntaxis van de wachtwoorden, die regelmatig moeten worden gewijzigd, bestaat uit ten minste 10 tekens, speciale tekens of hoofdletters, kleine letters en ten minste één cijfer. De herhalingscyclus is 24. Deze voorwaarden worden automatisch gecontroleerd wanneer het wachtwoord wordt gewijzigd, en indien niet aan deze voorwaarden wordt voldaan, wordt het nieuwe wachtwoord geweigerd. Als een wachtwoord niet op tijd wordt gewijzigd, vervalt het en wordt de toegang geweigerd.

- Controle op de toegangsrechten

Ongeoorloofde activiteiten in gegevensverwerkingssystemen die buiten de reikwijdte van de verleende autorisaties vallen, moeten worden voorkomen.

Op vraag gebaseerd ontwerp van het autorisatieconcept en de toegangsrechten, alsmede het opvolgen en loggen daarvan:

- ⇒ Gedifferentieerde autorisaties en tijdelijke toewijzing van wachtwoorden (volgens het autorisatieconcept van het Interflex-systeem) door de Klant
- ⇒ Opslag van gegevens op een lokale computer in versleutelde opslagruimten (bv. met behulp van VeraCrypt of soortgelijke programma's). De lokale computer zelf moet volledig worden versleuteld met behulp van een oplossing op bedrijfsniveau.
- ⇒ Toegang beperkt tot de persoon die de respectieve gegevensverwerking uitvoert

De aan de Contractant verstrekte gegevens worden voor de duur van de verwerking opgeslagen in lokale, versleutelde gegevensopslagplaatsen (bv. VeraCrypt of soortgelijke programma's) en worden na voltooiing van de werkzaamheden verwijderd met behulp van een speciale wisser. De lokale gegevensdragers op computers worden bovendien volledig versleuteld met behulp van een oplossing op bedrijfsniveau. De tijdelijke opslag van gegevens is beperkt tot de lokale systemen van degenen die met de uitvoering van de opdracht zijn belast. Alleen gemachtigde Interflex-gebruikers hebben toegang tot de PC.

De controle op de toegang tot de gegevens van het Interflex-Klantensysteem wordt door de Klant zelf geregeld door het toekennen/bepalen/verwijderen van een tijdelijk wachtwoord.

- Scheiding van gegevens

Gegevens die voor verschillende doeleinden worden verzameld, moeten afzonderlijk worden verwerkt.

Maatregelen voor afzonderlijke verwerking (opslaan, wijzigen, wissen, doorgeven) van gegevens met verschillende doeleinden:

- ⇒ "Internal multi-client capability" (mogelijkheid tot gelijktijdig gebruik door verschillende bedrijfseenheden)/earmarking
- ⇒ Scheiding van functies/productie/test

Klantgegevens worden tijdelijk opgeslagen en verwerkt in versleutelde, met een wachtwoord beveiligde opslagruimten, en worden strikt gescheiden gehouden van andere Klantgegevens. Bij verwerking via besturing op afstand worden de wijzigingen rechtstreeks in het systeem van de Klant aangebracht. Er is een aparte server voor testgegevens.

- Pseudonimisering (artikel 32, lid 1, eerste alinea, onder a) van de AVG; art. 25, lid 1 van de AVG)
de verwerking van persoonsgegevens op zodanige wijze dat de gegevens niet zonder de verstrekking van aanvullende informatie met een bepaalde betrokkene in verband kunnen worden gebracht, op voorwaarde dat deze aanvullende informatie afzonderlijk wordt bewaard en met passende technische en organisatorische maatregelen gepaard gaat.

Ten behoeve van de dienstverlening worden de door de Klant verstrekte gegevens doorgaans in gepseudonimiseerde vorm verwerkt. Indien nodig kunnen de gegevens worden geanonimiseerd. De precieze procedure hangt af van het specifieke type dienst.

2. Integriteit (artikel 32, lid 1, eerste alinea, onder b) van de AVG)

- Controle op doorgifte

Omgang met de aspecten van de doorgifte van persoonsgegevens: elektronische overdracht, gegevens-transport, controle op de overdracht. Niet lezen, kopiëren, wijzigen of verwijderen zonder autorisatie.

Maatregelen tijdens vervoer, doorgifte en overdracht of opslag op gegevensdragers (manueel of elektronisch) en verificatie achteraf:

- ⇒ Versleuteling/tunnelverbinding (VPN = Virtual Private Network)
- ⇒ Gegevensback-ups met een zipprogramma (bv. WinZip) en 256-bits AES-encryptie met een wachtwoord op CD/DVD
- ⇒ Loggen

In de regel worden de gegevens niet doorgegeven, behalve wanneer voor de oplossing van een probleem de medewerking van de ontwikkelingsafdeling van de Contractant vereist is. Mocht dit nodig zijn, dan wordt de back-up van de gegevens ofwel doorgegeven op een CD/DVD die per post wordt verstuurd, met gebruikmaking van een zipprogramma, 256-bits AES-encryptie en een wachtwoord, of, voor kleine hoeveelheden gegevens, rechtstreeks via het intranet met gebruikmaking van een zipprogramma en 256-bits AES-encryptie. Elke dergelijke overdracht wordt naar behoren schriftelijk vastgelegd.

- Controle op de invoer

Met het oog op de traceerbaarheid moeten de maatregelen voor gegevensbeheer en -onderhoud schriftelijk worden vastgelegd.

Maatregelen om achteraf na te gaan of en door wie gegevens zijn ingevoerd, gewijzigd of verwijderd (gewist):

- ⇒ Het loggen via logbestand in Interflex syste(e)m(en).

De IF-systemen hebben een logbestand waarin de wijzigingen worden ingevoerd met de respectieve gebruikers-ID, alsmede datum en tijd.

3. Beschikbaarheid en veerkracht (art. 32, lid 1, eerste alinea, onder b) van de AVG)

- Controle op de beschikbaarheid

De gegevens moeten worden beschermd tegen onopzettelijke vernietiging of verlies.

Maatregelen voor gegevensback-up (fysiek/logisch):

- ⇒ Geen back-upprocedure voor gegevensback-ups van de Klant omdat de gegevens conform de gegevensbeschermingswetgeving worden verwijderd nadat het doel is komen te vervallen
- ⇒ Virusbescherming / Firewall
- ⇒ UPS voor Servers

De gegevens van de systemen van de Klant worden niet geback-upt op servers met een back-upfunctie, zodat het zeker is dat deze gegevens in overeenstemming met de gegevensbeschermingsvoorschriften zijn gewist nadat het doel ervan heeft opgehouden te bestaan.

Alle computersystemen zijn uitgerust met antivirusprogramma's. Na elke opstart wordt gebruik gemaakt van Microsoft System Center Endpoint Protection. De antivirussignaturen worden onmiddellijk nadat ze zijn vrijgegeven bijgewerkt via de centraal beheerde Endpoint Protection-oplossing. Wekelijks wordt een automatische volledige controle uitgevoerd. Alle servers zijn beschermd tegen stroomschommelingen of stroomuitval door middel van een UPS.

- Snel herstel van de beschikbaarheid en de toegang (art. 32, lid 1, eerste alinea, onder c) van de AVG);

- a) Er zijn verschillende servers voor de eigen systemen van de Contractant. Gegevensbescherming door dagelijkse back-ups. Virtualisatie van de systemen met gecentraliseerde back-up in voorbereiding
- b) Systemen van de Klant:
Wanneer gegevens aan Interflex worden toegezonden, gaat het niet om originele gegevens, maar slechts om kopieën van gegevens en/of databanken. Er wordt geen back-up gemaakt om er zeker van te zijn dat de gegevens gewist zijn nadat het doel van de verwerking heeft opgehouden te bestaan, d.w.z. nadat de opdracht is voltooid. De oorspronkelijke gegevens blijven in het systeem van de Klant. De verantwoordelijkheid voor de gegevens in het systeem van de Klant ligt bij de Klant.

4. Procedures voor testen, beoordelen en evalueren op gezette tijdstippen (artikel. 32, lid 1, eerste alinea, onder d) van de AVG; art. 25, lid 1 van de AVG)

- Beheer van gegevensbescherming;
- incident response management: is opgenomen in het ISMS (beheersysteem voor informatiebeveiliging)
- Gegevensbescherming door standaardinstellingen (art. 25, lid 2 van de AVG)
- Voortdurend toezicht
- Herstellen van back-ups voor testdoeleinden
- Regelmatige tests van de UPS
- Controle op de toewijzing

Geen gegevensverwerking in de zin van art. 28 van de AVG zonder overeenkomstige instructies van de Klant

Maatregelen (technisch/organisatorisch) voor de afbakening van de verantwoordelijkheden tussen de Klant en de Contractant:

⇒ Ondubbelzinnige inhoud van overeenkomsten overeenkomstig artikel 28 van de AVG

⇒ Formele plaatsing van orders (onderhoudscontract of schriftelijke individuele opdrachten)

De Contractant voert de opgedragen dienstverlening uit met eigen middelen, zonder onderaannemers, overeenkomstig de instructies van de Klant.

In principe worden alleen in de programma's en de evaluatieloga wijzigingen in opdracht aangebracht.

Bijlage 3 - Onderaannemers

1. ☒ Momenteel zijn er geen onderaannemers in dienst.
2. ☐ Momenteel zijn de volgende onderaannemers in dienst:

Bedrijfsnaam van de onderaannemer	Adres/Land	Service