

SECTIE 1 VAN DE VERWERKINGSINFORMATIE BESCHRIJVING VAN DE VERWERKING PERSOONSGEGEVENS

1. PERSOONSGEGEVENS DIE ZULLEN WORDEN VERWERKT:

Product	Persoonsgegevens die verwerkt kunnen worden omvatten:	Aan wie deze kunnen toebehoren
Unit4 ERP x	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), andere contact gegevens, geboortedatum, geboorte plaats, nationaliteit, domicilie, taal, paspoort nummer, ID nummer, BSN nummer, fiscaal nummer, burgerlijke staat, details over salaris of secundaire arbeidsvoorwaarden, geslacht, informatie uit een arbeidsovereenkomst (waaronder salaris, functie, salaris schaal, competenties en persoonlijke aantekeningen), fiscale informatie, lidmaatschap van een vakvereniging, gegevens van gezins- of familieleden (waaronder naam, adres, geboortedatum, telefoonnummer, informatie voor noodgevallen), start en einddatum van de arbeidsovereenkomst, bank en/of creditcard gegevens; persoonlijke bedrijfsgegevens (naam; registratienummer en geregistreerd kantoor); directorships; BTW nummers, of documenten (schriftelijke of elektronische) die de bovenstaande gegevens bevatte.	Huidige of voormalige werknemers; Contractors of sub-contractors (van welke soort ook), agenten of directors; en Sollicitanten of mogelijke werknemers
Unit4 ERP 7	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), andere contact gegevens, geboortedatum, geboorte plaats, nationaliteit, domicilie, taal, paspoort nummer, ID nummer, BSN nummer, fiscaal nummer, burgerlijke staat, details over salaris of secundaire arbeidsvoorwaarden, geslacht, informatie uit een arbeidsovereenkomst (waaronder salaris, functie, salaris schaal, competenties en persoonlijke aantekeningen), fiscale informatie, lidmaatschap van een vakvereniging, gegevens van gezins- of familieleden (waaronder naam, adres, geboortedatum, telefoonnummer, informatie voor noodgevallen), start en einddatum van de arbeidsovereenkomst, bank en/of creditcard gegevens; persoonlijke bedrijfsgegevens (naam; registratienummer en geregistreerd kantoor); directorships; BTW nummers, of documenten (schriftelijke of elektronische) die de bovenstaande gegevens bevatte.	Huidige of voormalige werknemers; Contractors of sub-contractors (van welke soort ook), agenten of directors; en Sollicitanten of mogelijke werknemers
Unit4 Financials	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), andere contact gegevens, geboortedatum, geboorte plaats, nationaliteit, domicilie, taal, paspoort nummer, ID nummer, BSN nummer, fiscaal nummer, burgerlijke staat, details over salaris of secundaire arbeidsvoorwaarden, geslacht, informatie uit een arbeidsovereenkomst (waaronder salaris, functie, salaris schaal, competenties en persoonlijke aantekeningen), fiscale informatie, lidmaatschap van een vakvereniging, gegevens van gezins- of familieleden (waaronder naam, adres, geboortedatum, telefoonnummer, informatie voor noodgevallen), start en einddatum van de arbeidsovereenkomst, bank en/of creditcard gegevens; persoonlijke bedrijfsgegevens (naam; registratienummer en geregistreerd kantoor); directorships; BTW nummers, of documenten (schriftelijke of elektronische) die de bovenstaande gegevens bevatten	Huidige of voormalige werknemers; Contractors of sub-contractors (van welke soort ook), agenten of directors; en Sollicitanten of mogelijke werknemers
Unit4 Student Management	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), andere contact gegevens, geboortedatum, geboorte plaats, nationaliteit, domicilie, taal, paspoort nummer, ID nummer, BSN nummer, fiscaal nummer, burgerlijke staat, details over salaris of secundaire arbeidsvoorwaarden, geslacht, informatie uit een arbeidsovereenkomst (waaronder salaris, functie, salaris schaal, competenties en persoonlijke aantekeningen), fiscale informatie, lidmaatschap van een vakvereniging, gegevens van gezins- of familieleden (waaronder naam, adres, geboortedatum, telefoonnummer, informatie voor noodgevallen), start en einddatum van de arbeidsovereenkomst, bank en/of creditcard gegevens; persoonlijke bedrijfsgegevens (naam; registratienummer en geregistreerd kantoor); directorships; BTW nummers, of documenten (schriftelijke of elektronische) die de bovenstaande gegevens bevatten Aanvullend de Persoonsgegevens voor huidige en voormalige werknemers, zoals onder meer medewerker type (bijv. faculteit, adviseur, huisvestingsdirector), academische afdeling, status van de sollicitatie, medewerker status, facultyrank, publicaties, work status tracking, opleidingsniveau en kwalificaties. Aanvullend de Persoonsgegevens van huidige en voormalige sollicitanten, zoals onder meer vorige onderwijsinstelling, testresultaten en cijferlijst, gezondheidsgegevens, voormalige werkgevers. Aanvullend de Persoonsgegevens van studenten, zoals onder meer academische gegevens (inclusief cijfers en doelen, gegevens van de opleiding, voortgang en prestaties), academische resultaten, curriculum, facturatie en betalingsgeschiedenis, huisvestingsgegevens, financiële beurzen, gezondheidsgegevens (daaronder begrepen vaccinaties, allergieën, medische aandoeningen), verzekeringsgegevens, en gezondheidsgegevens.	Huidige of voormalige werknemers (inclusief faculteit of personeel); Contractors of sub-contractors (van welke soort ook), agenten of directors; en Sollicitanten of mogelijke werknemers, en Huidige, voormalige en toekomstige studenten.
Unit4 FP&A	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen). Andere Persoonsgegevens hoeven niet te worden opgeslagen of verwerkt, teneinde de doelen van het Product te behalen (zoals hieronder uiteengezet), maar andere Persoonsgegevens kunnen wel worden opgeslagen en verwerkt door het Product indien het zodanig is geconfigureerd (bijv. salarisgegevens) of indien die door de Klant in het Product zijn gezet.	Huidige of voormalige werknemers (inclusief faculteitspersoneel); Sub-contractors (van welke soort ook), agenten of directors
Unit4 Assistance PSA Suite	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen). Andere Persoonsgegevens hoeven niet te worden opgeslagen of verwerkt, teneinde de doelen van het Product te behalen (zoals hieronder uiteengezet), maar andere Persoonsgegevens kunnen wel worden opgeslagen en verwerkt door het Product indien het zodanig is geconfigureerd of indien die door de Klant in het Product zijn gezet.	Huidige of voormalige werknemers (inclusief faculteitspersoneel); Sub-contractors (van welke soort ook), agenten of directors

		<p>Ieder lid van van een projectteam (inclusief niet-werknemers)</p> <p>Sollicitanten of toekomstige werknemers</p> <p>De contactgegevens van de klanten van Klanten en leveranciersgegevens.</p>
Unit4 Talent Management	<p>Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen); andere contactinformatie (adres en land); geboortedatum; leeftijd; geboorteplaats; functieaanduiding, afdeling. Door gebruik te maken van de Leermodule: session enrolments; quiz resultaten en beoordelingen; video engagement gegevens; tekst engagement gegevens; badges; certificaties. Door gebruik te maken van de perform module: check in gegevens; OKR gegevens; feedback en beoordeling. Door gebruik te maken van de Engage module: antwoorden en feedback op engagement vragen.</p>	<p>Huidige en voormalige werknemers</p> <p>Huidige en voormalige sollicitanten;</p> <p>Contractors of sub-contractors (van welke soort dan ook), agenten of directors, en</p> <p>Sollicitanten of toekomstige werknemers.</p>
People Platform Services ("PPS"), Localisation Services en/of Unit4 Apps	<p>Omdat de PPS of Localisatie Diensten en/of Unit4 Apps services zijn die werken met, en een interface hebben met, de andere Unit4 Producten, kunnen deze allerlei soorten Persoonsgegevens verwerken zoals opgenomen in deze tabel met betrekking tot de genoemde Producten en Services.</p> <p>Verder kan Wanda verwerken: Unit4Id (die de gebruiker van IDS identificeert); ieder Persoonsgegeven dat door een gebruiker in de applicatie wordt ingevoerd, waarmee Wanda een connectie heeft (Zulke informatie wordt verwerkt of opgeslagen, tenzij de gebruiker ervoor kiest het te verwijderen); iedere andere conversatie en dialoog gegevens; metadata voorzover toe te schrijven aan een individu; en Application Insights Logs (een service van Microsoft gebruikt voor performing diagnoses).</p>	<p>Alle categorieën zoals opgenomen in deze tabel</p> <p>Afhankelijk van de applicatie of services waarmee Wanda een connectie heeft kan PPS mogelijk ieder Persoonsgeven verwerken, dat een Gebruiker invoert.</p>
Unit4 Property Management	<p>Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), home-page adres, BSN nummer, fiscaal nummer, ID card nummer, geboortedatum, identiteit klant, taal, marking of protected identity, marking for estate, BTW nummers, contact person informatie (inclusief titel/positie, belangen); bank account details, werknemersinformatie (inclusief werkgever, adres, informatie); sollicitanten details (inclusief: beroep, jaarlijks inkomen, jaar van werknemerschap, aantal personen in het huishouden, vorige verhuurder, assessment van het krediet rapport, datum van het krediet rapport; aanvrager en andere informatie, (bepaald door de Verwerkingsverantwoordelijke); rangorde; lidmaatschap (inclusief lidmaatschapsnummer, status, start en einddatum lidmaatschap, reden voor toetreding en verwijdering, eerste toetredingsdatum, hoofd lidmaatschap, aanverwante lidmaatschappen, huurpunten, home savings punten); rollen/categorieën Gebruikers (gebruikers id, type gebruiker, handtekening); huurovereenkomsten en huurders details (zoals identiteit van de ontvanger voor e-invoice, mandaat informatie deposit, garantie); zaaksbehandelingsinformatie, contractant (toewijzingen voor mailing); aantekeningen (geregistreerd door de Verwerkingsverantwoordelijke), documenten (geschreven/schriftelijk of elektronisch) dat al het voorgaande kan bevatten</p>	<p>Huidige of voormalige werknemers; Contractors of Sub-Contractors (van welke soort dan ook); agenten of directeuren, Aanvragers of mogelijke werknemers; en consumenten (property aanvragers en huurders) of management diensten.</p>

2. AARD EN DOELEINDEN VERWERKING:

In het algemeen zal de aard van de Verwerking door de Verwerker alleen zijn voor zover dat noodzakelijk is om de Verwerker in staat te stellen om aan zijn verplichtingen te voldoen en zijn rechten uit hoofde van de Overeenkomst uit te oefenen, inclusief (met betrekking tot de Persoonsgegevens) het verzamelen, opnemen, organiseren, structureren, opslaan, aanpassen of wijzigen, opvragen, raadplegen, gebruiken, openbaar maken door verzending, verspreiden of anderszins beschikbaar stellen, aanpassen of combineren, beperken, wissen of vernietigen.

Het doel van de Verwerking is het uitvoeren van de verplichtingen van de Verwerker en het uitoefenen van zijn rechten onder de Overeenkomst inclusief de uitvoering van taken of handelingen die door de Verwerkingsverantwoordelijke worden vereist of gevraagd voor de naleving door de Verwerkingsverantwoordelijke van zijn wettelijke en/of contractuele verplichtingen. Verwerker zal ook uw Persoonsgegevens verwerken om haar Producten en Diensten te verbeteren (zoals productverbetering door artificial intelligence, machine learning etc.) of voor data analyse. Met betrekking tot en afhankelijk van het Product of Dienst, omvat de Verwerking het volgende:

Product	Aard en Doeleinden van de Verwerking
Unit4 ERP x	<p>Persoonsgegevens worden ingevoerd in Unit4 ERP x om de Klant in staat te stellen processen te organiseren en te beheren die verband houden met de operationele werking en het beheer en/of de administratieve processen van zijn interne bedrijfsactiviteiten. De processen kunnen zijn:</p> <ul style="list-style-type: none"> • Verwerken van reisverzoeken; • Verwerken van onkosten nota's; • Verwerken van tijdregistratie formulieren; • Verzuimregistratie; • Processen gerelateerd aan HR en salarisverwerking, zoals

	<ul style="list-style-type: none"> ○ Salaris verwerking; ○ Verwerken van tijdregistratie formulieren ○ Verzuim management; ○ Trainingen; ○ Competentiemanagement; ○ Salaris herzieningen; ○ Verwerken van sollicitanten. <ul style="list-style-type: none"> ● Verwerken van betalingen; ● Facturatie; ● Inkoop aanvragen ● Planning van medewerkers en projecten. <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen Unit4 ERP x worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door door integratie met Unit4 ERP 7.</p> <p>Diensten</p> <ul style="list-style-type: none"> ● Verzenden en opslaan van Persoonsgegevens om aanvullend Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, (welke van toepassing is) ● Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 ERP 7 product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden.. ● Toegang tot Persoonsgegevens om configuratie en/of customisation en/of data migratie (bijv. van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
Unit4 ERP 7	<p>Persoonsgegevens worden ingevoerd in ERP 7 om de Klant in staat te stellen processen te organiseren en te beheren die verband houden met de operationele werking en het beheer en/of de administratieve processen van zijn interne bedrijfsactiviteiten. De processen kunnen zijn:</p> <ul style="list-style-type: none"> ● Verwerken van reisverzoeken; ● Verwerking van kostenvergoedingsclaims; ● Het verwerken van tijdschema's; ● Verzuim management ● HR en loonverwerkingsprocessen; ● Loonverwerking; ● Trainingen; ● Competentiemanagement; ● Salaris herzieningen; ● Beoordelingen ● Registratie van sollicitanten; ● Loonverwerking; ● Facturatie ● Verzoeken tot aankopen; ● Planning van medewerkers en projecten <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>De uitvoering door Unit4 ERP 7 van software code om de activiteiten als hierboven uiteengezet te laten plaatsvinden. Dit kan de verplaatsing van data naar of van een oplossing van een Derde Partij omvatten, die niet onder toezicht staat van de Verwerker door integratie met die oplossing.</p> <p>Diensten</p> <ul style="list-style-type: none"> ● Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of de People Platform Dienstenomschrijving

	<ul style="list-style-type: none"> • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Producten te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie en/of customisation en/of data migratie (bijv van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
Unit4 Financials	<p>Persoonsgegevens worden ingevoerd in Unit4 Financials om de Klant in staat te stellen processen te organiseren en te beheren die verband houden met de operationele werking en het beheer en/of de administratieve processen van zijn interne bedrijfsactiviteiten. De processen kunnen zijn:</p> <ul style="list-style-type: none"> • Klant/leverancier/werknemer registratie; • Verwerken van betalingen; • Facturatie; • Verwerken van onkosten nota's; • Verwerken van reisverzoeken; • Aankoop verzoeken en Orders • Planning van medewerkers en projecten; • Processen gerelateerd aan HR en salarisverwerking • Salaris verwerking; • Verwerken van tijd registratie formulieren; • Verzuim management; • Trainingen; • Competentiemanagement; • Beoordelingen; • Salaris herzieningen; • Verwerken van sollicitanten. <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>De uitvoering door Unit4 Financials van software code om de activiteiten als hierboven uiteengezet te laten plaatsvinden. Dit kan de verplaatsing van data naar of van een oplossing van een Derde Partij omvatten, die niet onder toezicht staat van de Verwerker door integratie met die oplossing.</p> <p>Diensten</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie en/of customisation en/of data migratie (bijv van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
Unit4 Student Management	<p>Persoonsgegevens worden in Unit4 Student Management ingevoerd om de Klant in de gelegenheid te stellen processen te organiseren en te managen die gerelateerd zijn aan het operationeel functioneren en managen dan wel de administratieve processen van de interne processen van de Klant. Deze processen kunnen omvatten:</p> <ul style="list-style-type: none"> • Aantrekken van toekomstige studenten; • Beantwoorden van informatie aanvragen; • Verwerken van aanmeldingen; • Het managen van de "academische loopbaan" van een student, inclusief aanname, curriculum planning. Academische voortgang, advisering, huisvesting en diploma-uitreiking; • Plannen en roosteren van faculteitsmedewerkers. <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen Unit4 Student Management worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door integratie met Unit4 Student Management.</p> <p>Diensten</p>

		<ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie en/of customisation en/of data migratie (bijv. van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
Unit4 FP&A		<p>Persoonsgegevens worden in Unit4 FP&A ingevoerd om de Klant in de gelegenheid te stellen processen te organiseren en te managen die gerelateerd zijn aan het operationeel functioneren en managen dan wel de administratieve processen van de interne processen van de Klant. Deze processen kunnen omvatten:</p> <ul style="list-style-type: none"> • Budgeteren; • Financiële and andere rapportages; • Distributie van rapporten; • Goedkeuringsprocessen; • Personeels/projectplanning. <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen Unit4 FP&A worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker maar door middel van integratie met Unit4 prevero.</p> <p>Diensten</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op de Unit4 Producten te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie en/of maatwerk en/of data migratie en/of andere consultancy diensten zoals afgenomen door de Klant te leveren.
Unit4 Management	Talent	<p>Persoonsgegevens worden in Unit4 Talent Management ingevoerd om de Klant in de gelegenheid te stellen processen te organiseren en te managen die gerelateerd zijn aan het operationeel functioneren en managen dan wel de administratieve processen van de interne processen van de Klant. Deze processen kunnen omvatten:</p> <ul style="list-style-type: none"> • Human capital management • Werknemers beoordelingsprocessen • Talent enablement • Kandidaten assessment • Leren • Feedback en beloning, en • Personeelsanalyses en engagement <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen Unit4 Talent Management worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door integraties</p> <p>Diensten</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op de Unit4 Producten te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie en/of customisations en/of data migratie (bijv. van zijn ouder systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
Unit4 Assistance Suite	PSA	<p>Persoonsgegevens worden in Unit4 Assistance PSA Suite ingevoerd om de Klant in de gelegenheid te stellen processen te organiseren en te managen die gerelateerd zijn aan het operationeel functioneren en managen dan wel de administratieve processen van de interne processen van de Klant. Deze processen kunnen omvatten:</p> <ul style="list-style-type: none"> • Automatiseren van een professionele services organisatie, inclusief financieel management en human resources management (HRM) • Tijd en project management

	<ul style="list-style-type: none"> • Geboekte uren en kosten met nota's • Het omzetten van opportuniteiten naar projecten, budgets en forecasting uren en het plannen van projecten en resources • Het bijhouden van tijd en uitgaven en factureren; • Integratie van projecten in andere applicaties; • Boekhouding om financiële data in andere oplossingen te integreren <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen Unit4 Assistance PSA Suite worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door integratie.</p> <p>Diensten</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie of customisations en/of data migratie (bijv. van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
<p>PeoplePlatform Services ("PPS"), Localisatie Diensten en Apps</p>	<p>Gegevens worden door PPS, Localisatie Diensten en/of Apps verwerkt om de doelen van de services te behalen, zoals omschreven in de toepasselijke PPS Service Description op www.unit4.com/terms.</p> <p>Daarnaast worden Persoonsgegevens in Wanda ingevoerd met behulp van de gekozen derde partijen software (bijv. Slack Integration, Facebook Messenger or other Microsoft Applications (inclusief Microsoft Teams)). Afhankelijk van het Unit4 Product of Service dat wordt gebruikt door de Klant, kan Wanda helpen om administratieve taken van de werknemers van de Klant uit te voeren.</p> <p>Taken kunnen omvatten:</p> <ul style="list-style-type: none"> • Tijdformulieren invoeren • Uitgaven invoeren • Reisverzoeken • Salarisstrook verzoeken • Verzuim invoeren • Balance invoeren • Aankoop verzoeken <p>De Verwerking omvat:</p> <p>Product (software)</p> <p>Binnen PPS worden door middel van de softwarecode de hierboven omschreven activiteiten uitgevoerd. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker maar door middel van integratie met Unit4 PPS.</p> <p>Diensten</p> <ul style="list-style-type: none"> • Wanda executing programmable software code om ervoor te zorgen dat de bovenstaande activiteiten kunnen worden. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door integratie. <p>Uitgevoerd</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op de Unit4 PPS, Localisatie Diensten en/of Apps te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie of customisations en/of data migratie (bijv. van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren. • Toegang tot Persoonsgegevens voor productverbetering via AI machine learning of data analyses.
<p>Unit4 Property Management</p>	<p>Persoonsgegevens zullen in Unit4 Property management worden ingevoerd om Klanten processen te laten organiseren en managen met betrekking tot uitvoerende functies, management en/of administratieve processen van de interne bedrijfsvoering. Processen kunnen zijn:</p> <ul style="list-style-type: none"> • Registratie van aanvragers • Verhuurmanagement • Verwerking van huurovereenkomsten • Verwerking van huurdersgegevens • Verwerking van elektronische handtekeningen

	<ul style="list-style-type: none"> • Rekeningen opmaken en printen • Verwerking van betalingen • Aanmanings processen • Wijzigingen van huur <p>De Verwerking omvat:</p> <p>Product Software (solution)</p> <p>Unit4 Property Management executing programmable software code om ervoor te zorgen dat de bovenstaande activiteiten kunnen worden. Dit kan de verplaatsing van data naar of van een oplossing van een derde partij omvatten, die niet onder toezicht staat van de Verwerker door integratie.</p> <p>Diensten</p> <ul style="list-style-type: none"> • Verzenden en opslaan van Persoonsgegevens om aanvullende Diensten te bieden zoals in detail uiteengezet in de Dienstenomschrijving of People Platform Dienstenomschrijving, welke van toepassing is. • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Support Voorwaarden. • Toegang tot Persoonsgegevens om configuratie of customisations en/of data migratie (bijv. van zijn oude systemen) en/of andere Professionele Diensten zoals afgenomen door de Klant te leveren.
--	---

3. BESCHRIJVING VERWERKING(EN) EN MIDDELEN

Verwerker zal de hiervoor genoemde Persoonsgegevens Verwerken in verband met de volgende werkzaamheden:

Wijze van Verwerken	Omschrijving	Middelen
Unit4 SaaS (Generiek)	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de Unit4 Dienstenomschrijving	<p><u>Personeel</u></p> <p>Het Unit4 Cloudoperations team heeft medewerkers in landen in de EU, (inclusief, maar niet beperkt tot Polen, Zweden, Noorwegen, Nederland, Spanje en Portugal) UK, US, Canada, Maleisie en Singapore. Deze medewerkers leveren de Unit4 SaaS.</p> <p><u>Middelen en Infrastructuur</u></p> <p>Unit4 gebruikt derde party hosting infrastructuur diensten om de Unit4 SaaS te leveren en gebruikt andere software systemen voor de werking en het management ervan. Zie voorts Sectie 3 van de Verwerkingsinformatie.</p>
U4 Talent Management SaaS	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de toepasselijke Dienstenomschrijvingen	<p><u>Personeel</u></p> <p>Het Unit4 Talent Management SaaS operations team heeft medewerkers voornamelijk in België en enkele andere EEA landen. Deze medewerkers leveren de Unit4 Talent Management SaaS Service.</p> <p><u>Middelen en Infrastructuur</u></p> <p>Unit4 gebruikt derde party hosting infrastructuur diensten om de Unit4 Talent Management SaaS Service te leveren en gebruikt andere software systemen voor de werking en het management ervan. Zie voorts Sectie 3 van de Verwerkingsinformatie.</p>
Klantenservice	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de Unit4 Support Voorwaarden.	<p><u>Personeel</u></p> <p>De Unit4 Klantenservice heeft medewerkers in landen in de EU (waaronder, maar niet beperkt tot UK, Polen, Zweden, Noorwegen, Duitsland, Ierland, Nederland, Spanje, Portugal) , UK, US, Canada (en op andere locaties waar dat voor Unit4 nodig zou mogen zijn). Deze medewerkers leveren de Unit4 Klantenservice zoals vermeld in de Unit4 Support Voorwaarden in Sectie B van de SLA</p> <p><u>Middelen en Infrastructuur</u></p> <p>Unit4 gebruikt andere software systemen voor de werking en het management van deze diensten.</p>
Professionele Diensten en consultancy	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de meer gedetailleerde Project documentatie, of statement of work, zoals overeengekomen nadat de het Project is aangevangen.	<p><u>Personeel</u></p> <p>Het Unit4 Professionele Diensten team heeft medewerkers in vrijwel alle locaties waar Unit4 actief is, waaronder UK, Ierland, Polen, Portugal, Noorwegen, Spanje, Frankrijk, Duitsland, Zweden, US, Canada, Singapore/Maleisie (en op andere locaties waar dat voor Unit4 nodig zou mogen zijn). Deze medewerkers leveren de Unit4 Professionele Diensten.</p> <p><u>Middelen en Infrastructuur</u></p> <p>Unit4 gebruikt andere software systemen voor de werking en het management van deze diensten.</p>

<p>Unit4 Professionele Diensten (indien aan een partner uitbesteed)</p>	<p>De Verwerker en Sub-verwerker zullen de voornoemde Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en (indien van toepassing) de documentatie met betrekking tot de software of diensten van de Derde Partij die als deel van de Overeenkomst zijn geleverd. Voor meer informatie, zie Sectie 3.</p> <p>De Verwerker sluit een Sub-verwerkingsovereenkomst met de Sub-verwerker, overeenkomstig de relevante bepalingen in de Overeenkomst</p> <p>De Verwerkingsverantwoordelijke heeft door het ondertekenen van deze Overeenkomst aan de Verwerker toestemming gegeven om de betrokken Sub-verwerker zoals vermeld in Sectie 3 bij de uitvoering van de Overeenkomst te betrekken</p>	<p>Zie Sectie 3 van het toepasselijke Bestelformulier.</p>
<p>Derde Partij Producten en Diensten</p>	<p>De Verwerker en diens sub-verwerkers zullen de voornoemde Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en Derde contractuele en service voorwaarden met betrekking tot de software of diensten van de Derde Partij die als deel van de Overeenkomst zijn geleverd</p>	<p>Zie Sectie 3 van het toepasselijke Bestelformulier en elke aanvullende regeling in andere schedules of Bijlagen bij de Verwerkingsinformatie indien vereist door de Derde Partij of Toepasselijk Recht</p>
<p>People Platform Services ("PPS"), Localisatie Diensten en/of Apps</p>	<p>In aanvulling op Unit4 SaaS, zal PPS, Localisatie Diensten en/of Apps (waar van toepassing) Persoonsgegevens verwerken in connectie met een privacy verklaring zoals aan de eindgebruiker verstrekt, waarbij om toestemming wordt gevraagd, indien zulke Persoonsgegevens worden verwerkt.</p>	<p><u>Personeel</u></p> <p>Het Unit4 Cloud operations team dat de PPS, Localisatie Diensten en/of Apps uitvoert heeft medewerkers in landen in de EU (waaronder, maar niet beperkt tot Polen, Zweden, Noorwegen, Nederland, Spanje en Portugal) UK, US, Canada, Maleisie en Singapore. Deze medewerkers leveren de Unit4 SaaS.</p> <p><u>Middelen en Infrastructuur</u></p> <p>Unit4 gebruikt haar eigen infrastructuur en de (shared) infrastructuur van derde partijen om de Unit4 People Platform Services, Localisatie Diensten en/of Apps te leveren. Dit omvat 3rd partij systemen (i.e. collaboration apps), waar Unit4 geen controle over heeft. PPS inclusief Wanda, Localisatie Diensten en/of Apps maakt gebruik van een aantal Microsoft producten en services, als volgt:</p> <ul style="list-style-type: none"> • Cognitive services: <ul style="list-style-type: none"> ○ LUIS Cognitive Service - <i>language understanding</i>. ○ Text Translator API – <i>translating text</i> ○ QnA Maker Cognitive service – <i>provides a questions and answers service</i> • Bot framework connectors – <i>provides for the connection of Wanda to the supported social channels.</i> • Traffic manager – <i>used for disaster recovery and failover if the primary region is unhealthy</i> • Web apps / web jobs – <i>hosts web APIs and long running web-based processes</i> • Service bus – <i>provides internal communication in the Wanda ecosystem</i> • Storage accounts – <i>used to store conversation state and user settings</i> • Cosmos DB – <i>provides storage</i> • Functions – <i>provides logical algorithms for extensions</i> • Event grid – <i>provides communication</i> • API management – <i>to manage APIs</i> • Service Plans – <i>Linux and dynamic service plans to run the Service in</i> • Storage accounts – <i>used for storage</i> • Key vault – <i>stores confidential data that is used to communicate with Microsoft services and for internal services</i>

	<ul style="list-style-type: none"> • Redis cache – <i>provides caching capabilities</i> • Application Insights – <i>Monitoring of system, includes telemetry and logging</i> • SQL server – <i>provides storage</i> • Kubernetes – <i>open source container</i> <p>Verdere informatie en details met betrekking tot die Microsoft producten en services kunnen worden gevonden op: https://azure.microsoft.com/en-us/services/.</p> <p>Daarnaast maken de PPS, Unit4 Localisatie Diensten en/of Unit4 Apps gebruik van:</p> <p>Twilio- Sendgrid- verzenden mail messages</p>
--	--

4. BEWAARTERMIJN

Verwerker zal de Persoonsgegevens bewaren **voor de duur van de Overeenkomst**.

Na de overeengekomen bewaartermijn zal Verwerker de Persoonsgegevens aan Verwerkingsverantwoordelijke retourneren in een veelgebruikte, machine leesbaar format of op eerste verzoek van Verwerkingsverantwoordelijke vernietigen of anonimiseren zonder deze nog verder te gebruiken en zonder een kopie te behouden.

5. INFORMATIE MET BETREKKING TOT HET LAND (OF PLAATS) VAN DE VERWERKING VAN PERSOONSGEGEVENS

Product – lokale installatie bij de Klant	Gegevens zijn opgeslagen op de server(s) van de Verwerkingsverantwoordelijke op zijn vestigingsplaats zoals van tijd tot tijd aan Unit4 kan worden doorgegeven.		
Product - Unit4 SaaS	Unit4 Cloud werkt in diverse data centers, inclusief een wereldwijde dekking met Microsoft Azure. Unit4 zal de Klant in de meest logische locatie onderbrengen, op grond van de plaats van vestiging van de Klant (zoals op het Bestelformulier vermeld). Alle Klantgegevens worden alleen opgeslagen in de gekozen geo-politieke zone en worden zonder toestemming van de Klant niet buiten deze locatie gebracht.		
	Cloud Model	Geo-politieke Zone	Locatie Data Center
	SaaS Cloud	EU	Dublin / Amsterdam
	SaaS Cloud	USA	Multiple locations
	SaaS Cloud	Canada	Toronto / Quebec City
	SaaS Cloud	United Kingdom	London / Cardiff
	SaaS Cloud	Asia	Singapore / Hong Kong
	SaaS Cloud	Australia	Victoria / New South Wales
Product – Talent Management SaaS	SaaS Cloud	Norway	Oslo/Stavanger
	SaaS Cloud	Sweden	Sätra en Sollentuna
Unit4 Support – Standaard Support andere standaard ondersteunings diensten	Talent Management SaaS werkt in Microsoft Azure, zowel in de EU en UK Geo-Politieke zones (zie hierboven), waarbij de zone wordt gealloceerd op basis van de locatie van de Klant. het Amazon Web Services (AWS) datacenter in Frankfurt. Alle Klantgegevens, behalve indien er wordt gedeeld met geselecteerde sub-processors uit Sectie 3 zullen alleen in de geo-politieke zone worden opgeslagen, en niet daarbuiten worden verplaatst zonder de expliciete toestemming van de klant.		
Unit4 Support gebruikt derde partijen software (zoals SalesForce/ServiceNow) om Zaken te registreren en verwerken. Deze Zaken zijn toegankelijk voor iedere Unit4 medewerker die toegang tot derde partij software heeft, zoals support engineers, cloud engineers, Professional Service Consultants en service management. Toegang wordt gecontroleerd door intern management en organisatorische processen, om te verzekeren dat Persoonsgegevens niet toegankelijk zijn voor consultants of engineers die tot dergelijke Klant gegevens geen toegang nodig hebben.	Klant Locatie	Primaire Support wordt verzorgd vanuit: (maar kan ook uit andere EU landen zijn)	
	United Kingdom and Ireland	United Kingdom, Ireland, Portugal and Poland.	
	Sweden, Norway, Denmark, Finland and Iceland	Poland, Portugal, Norway and Sweden.	

	US & Canada	Poland, Portugal, US and Canada.		
	Europe rest	Poland, Portugal and Germany.		
	APAC	Poland, Portugal and Singapore/ Malaysia.		
Unit4 Support – 24/7 Support	Door de 'follow the sun' methodologie te volgen, kan 24/7 support van Klant Cases plaatsvinden in elk van de ondersteuningslocaties zoals hierboven vermeld, alsmede Nederland, Spanje en elke andere locatie die benodigd is om Unit4's bedrijfsvoering te ondersteunen.			
Unit4 Support – EU Only Support	Indien EU Only support is gekozen, worden Cases alleen in behandeling genomen door de EU locaties voor standaard support als hierboven vermeld (gedurende Kantoortijden).			
People platform services ("PPS") (in het algemeen) inclusief IDS en Wanda (samen met iedere andere supporting services, Localisatie Diensten en/of Apps)	PPS zijn SaaS die een gedeelde infrastructuur gebruiken en Derde Partij services die mogelijk niet een geo-politieke zone isolatie leveren. Hieronder staat een overzicht van de PPS en het land (of de plaats) van de Verwerking van Persoonsgegevens indien gebruik wordt gemaakt van deze service.			
	Dienst	Geo-politieke Zone	Waar de Dienst Persoonsgegevens Verwerkt of opslaat	Primarily Support wordt geleverd uit:
	Wanda	Alle	Voornamelijk in de EU, maar kan ook elders in de wereld zijn	EU landen waaronder Ierland, Polen en Spanje, United States, en andere Global support locaties indien vereist, waar zich een Azure data centre bevindt (bijv. de US)
	PPS, Localisatie Diensten en/of Apps	Afhankelijk van Cloud deployment	Diensten worden verwerkt en data worden bewaard in de geselecteerde geo-politieke zones	Zoals hiervoor genoemd voor Unit4 SaaS
Unit4 Professionele Diensten en Unit4 customer success functie	Onderwerp	Professionele Diensten en customer success worden geleverd door:		
	Implementatie en andere project diensten	In het Land of de Klant locatie of de overeengekomen locatie en/of in Portugal, afhankelijk wat tussen Partijen is overeengekomen in de project documentatie of het Bestelformulier		
	Data Migratie	In het Land of de Klant locatie of de overeengekomen locatie en/of in Portugal, afhankelijk wat tussen Partijen is overeengekomen in de project documentatie of het Bestelformulier		
	Trouble shooting	In de van toepassing zijnde "Unit4 Support Service" locatie en Portugal.		
	Customer Success	In de van toepassing zijnde "Unit4 Support Service" locatie en Portugal.		

6. CONTACTGEGEVENS

Voor vragen of opmerkingen over de Verwerkingsinformatie is de contactpersoon:

Voor Verwerkingsverantwoordelijke: Het adres van Verwerkingsverantwoordelijke zoals aangegeven in de Overeenkomst

Voor Verwerker: Door een brief (geadresseerd aan Global Data Protection Officer met kopie aan het Global Legal Department), Postbus 5005, 3528 BJ Utrecht, Nederland of email privacy@unit4.com of aan het Unit4 adres zoals aangegeven in de Overeenkomst.

SECTIE 2 – BEVEILIGINGSMAATREGELEN

Zoals opgenomen in art. 6 van deze Verwerkingsvoorwaarden, worden hieronder de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen. De getroffen maatregelen zijn opgenomen in deze Sectie en worden aangevuld of gewijzigd indien dat nodig is. Verwerkingsverantwoordelijke acht genoemde maatregelen passend voor de Verwerking van de Persoonsgegevens.

Unit4 Bedrijfsbeveiligingsmaatregelen (samenvatting van de interne bedrijfsactiviteiten)

Beschrijving van de technische en organisatorische beveiligingsmaatregelen zoals geïmplementeerd door de Verwerker in zijn organisatie (in het algemeen):

Fysieke beveiliging:

- Fysieke toegangscontrole wordt beheerd door Unit4-faciliteiten.
- Alle kantoren beschikken over beveiligingssysteem met betrekking tot het controleren van toegang via barrières, b.v. toegangspoorten, bemande balies, branddeuren met alarm, inbraakdetectiesystemen en afsluitbare kantoren.
- Unit4 hanteert logische toegangscontroles met behulp van wat mensen weten, zoals een wachtwoord of persoonlijke toegangscode; of met behulp van wat mensen dragen, zoals een beveiligingspas;
- Serverruimten op locatie (indien van toepassing) hebben aanvullende fysieke beveiliging.
- Toegang tot beveiligde gebieden of gevoelige informatie is beperkt om ongeoorloofde toegang te voorkomen door bezoekers / onbevoegd personeel (door afsluitbare kantoren of afsluitbare kasten) en door "clean desk"-beleid.
- Bezoekers van Unit4 worden gecontroleerd bij de receptie (door een toegewijde receptionist of ander personeelslid).
- Er worden shredders of andere geschikte veilige verwijderingsmethoden voor gevoelige documenten gebruikt.

Virtuele en computerbeveiliging:

- De verantwoordelijke lijnmanager zorgt ervoor dat werknemers en contractors alle Unit4-apparatuur die zij in hun bezit hebben teruggeven na beëindiging van hun arbeidsovereenkomst of contractorovereenkomst. Hier wordt aantekening van gehouden.
- Unit4 tracht informatie te classificeren als publiek, vertrouwelijk, eigen of gevoelig. Informatie wordt dan beschermd volgens zijn classificatie.
- Media (inclusief harde schijven) worden veilig vernietigd als ze niet langer nodig zijn. Al het gevoelige materiaal (harde schijven, floppies, enz.) wordt verwijderd door verwijderingssoftware (niet door opnieuw te formatteren of verwijderen) voor fysieke vernietiging.
- Anti-malware - we gebruiken de nieuwste versie van industriestandaard-oplossingen om bescherming tegen virussen en anti-malware te bieden.
- Verder gebruikt Unit4:
 - o controle op toegewezen rechten;
 - o logging en controle van de toegang tot het systeem;
 - o herstelmaatregelen;
 - o de mogelijkheid om voortdurend de vertrouwelijkheid, integriteit, beschikbaarheid en robuustheid van Verwerkingsystemen en -diensten te waarborgen; en
 - o systemen en processen om het mogelijk te maken de beschikbaarheid en toegang tot Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident.
- Business Continuity en Disaster Recovery-plannen zijn opgesteld die informatiebeveiligingsoverwegingen bevatten.

Beveiligingspolitie en Documentatie:

- Het Global Leadership Team van Unit4 en/of zijn respectievelijke lokale managementteams hebben overzicht op zowel de wereldwijde als de lokale informatiebeheer- en beveiligingsplannen, inclusief informatiebeveiligingsbeleid dat betrekking heeft op geïdentificeerde informatiebeveiligingsrisico's en ondersteunt de bedrijfsdoelstellingen.
- Informatiebeveiliging en -beheer worden globaal toegewezen aan de Chief Information Security Officer en de Global Data Protection Officer, die middelen beheren voor het leveren van strategische en algehele naleving van het informatiebeveiligingsbeleid en -proces.
- Unit4 heeft beveiligingsbeleid geïmplementeerd dat regelmatig geüpdatet en gewijzigd wordt om te voldoen aan "good industry practices".
- Unit4 heeft een privacybeleid en een white paper over GDPR gepubliceerd op www.unit4.com/terms.
- Unit4 sluit non disclosure en geheimhoudingsovereenkomsten met Derden wanneer het vertrouwelijke informatie met betrekking tot haar bedrijfsactiviteiten deelt.
- Unit4 zorgt ervoor dat alle werknemers en contractors standaard geheimhoudingsbepalingen hebben in hun contracten.
- Unit4 biedt alle medewerkers training met betrekking tot privacy en gegevensbescherming, beveiliging en de core business principles zoals hierboven vermeld.

Extra elementen voor Unit4 SaaS op Microsoft Azure (samenvatting)

Beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn geïmplementeerd door de Verwerker met betrekking tot het aanbieden van de Unit4 SaaS :

Gegevensbescherming

Unit4 Cloud maakt gebruik van verschillende mechanismen om Persoonsgegevens in de cloud te beschermen. Hieronder vindt u een uitgebreid overzicht van toegepaste onderdelen.

Beveiligingsfuncties, proces en protocollen op netwerkniveau

- Veilige gegevensoverdracht via openbare netwerken – al het verkeer wordt beveiligd met behulp van standaardprotocollen zoals SSL / TLS en HTTPS.
- Systeembeveiliging: logische authenticatie en autorisatiemechanisme aanwezig
- Firewalls – firewalltechnologie van de volgende generatie om ervoor te zorgen dat inkomend en uitgaand verkeer wordt gecontroleerd.

Beveiligingsfuncties, proces en protocollen op databaseniveau

- Gegevensbeveiliging – Logisch authenticatie- en autorisatiemechanisme aanwezig.

- Databasebeveiliging – Elke klant heeft zijn eigen beveiligde database, wat betekent dat partitionering van databases niet nodig is en dat klantgegevens niet samengaan. Het resultaat is dat de gegevens van een klant nooit per ongeluk met anderen worden gedeeld.
- Data base back-ups worden gecodeerd met behulp van volledige database-coderingstechnologie, zoals transparante database-encryptie.

Non-transitional data en bestanden zullen worden beveiligd door standaard symmetric encryption (AES)

- Unit4 gebruikt Azure Key Vault om de controle te houden over sleutels die worden gebruikt door cloudtoepassingen en services om gegevens te coderen.

Voortdurende geteste en voortschrijdende beveiliging

Om onvoorziene kwetsbaarheden te ontdekken en onze detectie- en responsmogelijkheden te verfijnen, onderzoeken we voortdurend hoe we de beveiligingspositie kunnen verbeteren om ons te beschermen tegen mogelijke inbreuken. Het Unit4 Cloud operations team dat de Cloud-activiteiten (cloud-infrastructuur, cloud-services, producten, apparaten en interne resources) van Unit4 nauwlettend bewaakt en simuleert, bootst real-world inbreuken na – om penetratie te testen en ons vermogen te verbeteren om tegen cyberaanvallen te beschermen, deze op te sporen en daarvan te herstellen.

Bedreigdetectie, mitigatie en reactie

Naarmate het aantal, de variëteit en de ernst van cyberdreigingen toeneemt, neemt ook onze zorgvuldigheid toe bij het opsporen en beantwoorden van bedreigingen. Gecentraliseerde controlesystemen zorgen voor continue zichtbaarheid en tijdige waarschuwingen. Frequente toepassing van beveiligingspatches en updates helpt systemen te beschermen tegen bekende kwetsbaarheden. Detectie- en malwaredetectiesystemen zijn ontworpen om risico's van aanvallen van buitenaf te detecteren en te beperken. In geval van kwaadwillige activiteit volgt ons 24x7-incidentresponsteam beproefde procedures voor incidentbeheer, communicatie en herstel. Het team gebruikt best practices uit de branche om zowel interne teams als klanten te waarschuwen. Tot slot controleren beveiligingsrapporten toegangspatronen om potentiële bedreigingen proactief te identificeren en te beperken.

Gegevenssegregatie

Gegevens zijn de valuta van de digitale economie en we nemen de verantwoordelijkheid om klantgegevens te beschermen zeer serieus. Zowel technologische beveiligingen, als gecodeerde communicatie en operationele processen, helpen de klantgegevens te beveiligen. In de cloud kunnen gegevens van meerdere klanten worden opgeslagen op dezelfde IT-bronnen. Unit4 gebruikt logische isolatie om de gegevens van elke klant te scheiden van die van anderen. Unit4 SaaS is ontworpen om risico's die inherent zijn aan een multitenant-omgeving tegen te gaan. Gegevensopslag en -verwerking wordt logisch gescheiden door consumenten met behulp van bijvoorbeeld Dedicated Accounts en met afzonderlijke database-instances voor al onze klanten.

Data encryptie

Unit4 biedt standaard toegang tot alle diensten door alle gegevens in transit die op openbare netwerken worden verstuurd te versleutelen. Dit gebeurt door alleen beveiligde protocollen te gebruiken, zoals HTTPS over TLS, met behulp van de nieuwste beveiligingscodes. Het gebruikte mechanisme is een transparante, volledige database-encryptie – TDE. Microsoft Azure-klanten in het openbare SaaS-aanbod krijgen de TDE-gegevens in rust-codering als standaard.

Toegangscontrole

Klanten die Unit4-producten in de cloud gebruiken, zijn volledig bevoegd om front-end toegangscontrole naar hun toepassing uit te voeren. Dit betekent dat de verantwoordelijkheid voor het maken van nieuwe accounts, accountbeëindiging en beoordeling voor Unit4-applicaties bij de klant ligt.

Unit4 behoudt beperkte back-endoegang tot klantgegevens (via directe databaseverbinding). Toegang door Unit4 tot Persoonsgegevens is strikt beperkt tot activiteiten die nodig zijn voor het installeren, implementeren, onderhouden, repareren, oplossen van problemen of het upgraden van de oplossing. Alle toegang wordt vastgelegd en is beperkt tot een kleine groep Cloud Engineers en Support Consultants. Toegangslogboeken worden 365 dagen opgeslagen in de gecentraliseerde monitoringoplossing. In het geval van datalekken kan Unit4 het toegangsllog op aanvraag verstrekken.

Data lek notificatie

Unit4 zal de klant onverwijld informeren na kennis te hebben genomen van een datalek. De Klant moet ervoor zorgen dat de contactpersonen in de ondersteuningsportal van Unit4 altijd up-to-date zijn, omdat deze worden gebruikt voor alle communicatie.

Data privacy en security by design

Unit4 Cloud-platform is vanaf de grond af ontworpen met het oog op data beveiliging en data privacy. Unit4 verbetert continu de beveiliging van de oplossing door lessen te trekken uit jaarlijkse penetratietests en audits.

Unit4 en de exploitanten van datacenters hebben verschillende beveiligingscertificaten, voor meer informatie verwijzen wij u naar de toepasselijke Dienstenomschrijving.

Extra elementen voor Unit4 People Platform Services (samenvatting)

Beschrijving van de technische en organisatorische beveiligingsmaatregelen door Verwerker geïmplementeerd in relatie tot de levering van Unit4 People Platform Services (alleen Cloud)

Beveiliging Persoonsgegevens

Unit4 People Platform gebruikt verschillende mechanismes om Persoonsgegevens in de cloud te beschermen. Hieronder staat een uitgebreid overzicht van de toegepaste controlemechanismen..

Network level security features, process and protocols

- Beveiligde data transmission over publieke netwerken – alle verkeer is beveiligd door gebruikmaking industry standard protocols zoals SSL/TLS en HTTPS.

Authenticatie

- Alle services volgen het principe van least privilege en authenticatie voor services en hun APIs zijn beveiligd door gebruikmaking van industry standard mechanismen. OpenID Connect en het bijbehorende OAuth 2.0 protocol wordt gebruikt om authenticatie van gebruikers en/of klantservices veilig uit te voeren met vertrouwde partijen en identiteit en toegang te valideren door gebruikmaking van claims based tokens.
- HMAC (Hash-based Message Authentication) wordt gebruikt als alternatieve methode om communicatie tussen services te beveiligen.

Database level security features, processen and protocollen.

- Data, die zijn opgeslagen in storage accounts worden versleuteld, als deze in rust zijn.
- Alle storage accounts vereisen veilige transfer – alle verkeer is beveiligd door gebruikmaking van traffic industry standard protocollen zoals SSL/TLS and HTTPS.
- Alle data opgeslagen in Azure Cosmos DB wordt versleuteld in rust en in transport.
- Alle Azure SQL Servers zijn uitgerust met Transparent Data Encryption (TDE).

- Alle Azure SQL Servers werken met Threat detection en zijn auditing enabled.
- Azure KeyVault wordt gebruikt om specifieke gevoelige informatie, zoals service principal credentials, te beveiligen.

Messaging level security features, processen and protocollen.

- Alle data opgeslagen door Azure Service Bus instanties worden in rust versleuteld.
- Alle verkeer (in transit) op Azure Service Bus is beveiligd door gebruikmaking van industry standard protocollen zoals SSL

Meer gedetailleerde informatie over de Security Policy en het Security Program is te vinden op www.unit4.com/terms.

Data versleuteling

Unit4 People Platform services levert, standaard, beveiligde toegang tot al haar services door alle data in transit op publieke netwerken te versleutelen . Dit, door gebruikmaking van alleen veilige protocollen, zoals HTTPS over TLS (1.2), met de meest recente security ciphers. Alle opgeslagen data zijn versleuteld.

Datalek notificatie

Unit4 zal de Klant zonder onnodige vertraging informeren nadat Unit4 kennis heeft genomen van een datalek. De Klant moet zich ervan vergewissen dat de contactdetails opgenomen in de Unit4 Support Portal altijd up-to-date zijn, omdat deze worden gebruikt voor iedere communicatie.

Data privacy and security by design

Unit4 People Platform services werden van de grond af ontworpen met data security and privacy in gedachten. Unit4 is steeds bezig met het verbeteren van de beveiliging, door het toepassen van lessons learned van jaarlijkse penetratie testen en audits.

SECTIE 3– UNIT4 SUB-VERWERKERS

Service	Sub-verwerker	Verwerkingslocatie	Dienstverlening door Sub-verwerker
Unit4 Professionle Diensten (indien gecontracteerd met een partner)	Zoals vermeld in de Overeenkomst	Zoals vermeld in de Overeenkomst	Zoals gespecificeerd in het order formulier of schriftelijke overeengekomen met de Klant
Derde Producten en Diensten alleen van toepassing indien gekocht door de Klant	Zoals vermeld in de Overeenkomst	Zoals bepaald in de Overeenkomst of bijlagen of appendices bij de Overeenkomst met betrekking tot Derde Leverancier verwerking	Software en/of Support Services en/of SaaS Services
Unit4 SaaS	Microsoft Azure	Zoals vermeld in Sectie 1, paragraaf 5.	Verlenen van Cloud Infrastructure and Services
	Microsoft Dynamics	Zoals vermeld in Sectie 1, paragraaf 5.	Verlenen van Software Services, in het bijzonder Microsoft Dynamics (en cloud infrastructuur).
	Microsoft	Zoals vermeld in Sectie 1, paragraaf 5.	Verlenen van software tooling en Office
	Conapto	Zoals vermeld in Sectie 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	Twilio- Sendgrid	United States of America (Privacy Policy)	Verzenden van mail (EU SCCs-Zie Sectie 4)

Unit4 SaaS- Talent Management	Microsoft Azure	Dublin, Ierland	Providing solution - Suite
	LogDNA	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs- Zie Sectie 4)
	Mandrill	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs- Zie Sectie 4)
	Mixpanel	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs- Zie Sectie 4)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Providing solution - Learn (SCORM only) (EU SCCs- Zie Sectie 4)
	Sentry	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs- Zie Sectie 4)
	Slack	United States of America (Privacy Policy)	Providing solution – Perform (EU SCCs- Zie Sectie 4)
	Wistia	United States of America (Privacy Policy)	Providing solution – Learn (privacy shield link: Link) (EU SCCs- Zie Sectie 4)
People Platform Services (“PPS”) (generally) including IDS and Wanda (together with any supporting services)	Microsoft Azure	Zoals vermeld hierboven in Sectie 1, paragraaf 5 and en zoals geleverd door Microsoft: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located .	Providing Cloud Infrastructure and platform Services (as set out above) in Section 1.
	Twilio-Sendgrid	United States of America (Privacy Policy)	Versturen van mail (EU SCCs- Zie Sectie 4)

SECTIE 4 – EU SCCs

STANDARD CONTRACT BEPALINGEN (“SCB”)

Verwerkingsverantwoordelijke naar Verwerker

Unit4 is Verwerker/gegevensimporteur

Klant is Verwerkingsverantwoordelijke/gegevensexporteur

In de relatie tussen Partijen is Module Twee (Doorgifte Verwerkingsverantwoordelijke naar Verwerker) van de SCB van toepassing.

Deze standaardcontractbepalingen zijn alleen van toepassing bij doorgifte van persoonsgegevens door de Verwerkingsverantwoordelijke van binnen de EEA naar een Verwerker buiten de EEA, ook bekend als een derde land waarvoor geen adequaatheidsbesluit bestaat.

UITVOERINGSBESLUIT (EU) 2021/914 VAN DE COMMISSIE

van 4 juni 2021

betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad

BIJLAGE

STANDAARDCONTRACTBEPALINGEN

AFDELING I

Bepaling 1

Doel en toepassingsgebied

- a) Deze standaardcontractbepalingen hebben tot doel de naleving van de in Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG, algemene verordening gegevensbescherming) [\(U\)](#) bepaalde vereisten te garanderen voor de doorgifte van persoonsgegevens naar een derde land.
- b) De partijen:
- i) de natuurlijke of rechtspersonen en de overheidsinstellingen, -organen en -instanties (hierna “entiteiten” genoemd) die de in bijlage I.A bedoelde persoonsgegevens doorgeven (“gegevensexporteur”), en
 - ii) de entiteiten in een derde land die de persoonsgegevens van de gegevensexporteur ontvangen, direct of indirect via een andere entiteit die ook partij is bij deze bepalingen, zoals opgenomen in bijlage I.A (hierna “gegevensimporteur” genoemd)
- zijn deze standaardcontractbepalingen (hierna: “bepalingen” genoemd) overeengekomen.
- c) Deze bepalingen zijn van toepassing op de doorgifte van persoonsgegevens zoals opgenomen in bijlage Annex I.B.
- d) Het aanhangsel bij deze bepalingen dat de daarin genoemde bijlagen bevat, maakt integraal deel uit van deze bepalingen.

Bepaling 2

Effect en onveranderlijkheid van de bepalingen

- a) In deze bepalingen worden passende waarborgen vastgesteld, met inbegrip van afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen, overeenkomstig artikel 46, lid 1, en artikel 46, lid 2, punt c), van Verordening (EU) 2016/679 alsook, met betrekking tot gegevensdoorgiften van verwerkingsverantwoordelijken aan verwerkers en/of van verwerkers aan verwerkers, standaardcontractbepalingen overeenkomstig artikel 28, lid 7, van Verordening (EU) 2016/679, mits deze niet worden gewijzigd, behalve om de geschikte module(s) te selecteren of om informatie in het aanhangsel toe te voegen of te wijzigen. Dit houdt niet in dat de partijen de in deze bepalingen neergelegde standaardcontractbepalingen niet in een bredere overeenkomst mogen opnemen en/of andere bepalingen of extra waarborgen mogen toevoegen, mits deze niet direct of indirect in tegenspraak zijn met deze bepalingen en geen afbreuk doen aan de grondrechten of de fundamentele vrijheden van de betrokkenen.
- b) Deze bepalingen doen geen afbreuk aan de krachtens Verordening (EU) 2016/679 op de gegevensexporteur rustende verplichtingen.

Bepaling 3

Derde-begunstigden

- a) Betrokkenen mogen zich als derde-begunstigden op deze bepalingen beroepen en deze doen gelden tegen de gegevensexporteur en/of de gegevensimporteur, met de volgende uitzonderingen:
- i) Bepaling 1, bepaling 2, bepaling 3, bepaling 6, bepaling 7;
 - ii) Bepaling 8 — module een: Bepaling 8.5, punt e) en bepaling 8.9, punt b); Module twee: Bepaling 8.1, punt b), bepaling 8.9, punten a), c), d) en e); Module drie: Bepaling 8.1, punten a), c) en d) en bepaling 8.9, punten a), c), d), e), f) en g); Module vier: Bepaling 8.1, punt b) en bepaling 8.3, punt b);
 - iii) Bepaling 9 — module twee: Bepaling 9, punten a), c), d) en e); Module drie: Bepaling 9, punten a), c), d) en e);
 - iv) Bepaling 12 — module een: Bepaling 12, punten a) en d); Modulen twee en drie: Bepaling 12, punten a), d) en f);
 - v) Bepaling 13;
 - vi) Bepaling 15.1, punten c), d) en e);
 - vii) Bepaling 16, punt e);
 - viii) Bepaling 18 — modulen een, twee en drie: Bepaling 18, punten a) en b); Module vier: Bepaling 18.
- b) Punt a) doet geen afbreuk aan de rechten van betrokkenen krachtens Verordening (EU) 2016/679.

Bepaling 4

Interpretatie

- a) Wanneer in deze bepalingen in Verordening (EU) 2016/679 gedefinieerde termen worden gebruikt, hebben die termen dezelfde betekenis als in die verordening.
- b) Deze bepalingen worden gelezen en geïnterpreteerd in het licht van de bepalingen van Verordening (EU) 2016/679.
- c) Deze bepalingen worden niet geïnterpreteerd op een wijze die in tegenspraak is met de in Verordening (EU) 2016/679 vastgestelde rechten en verplichtingen.

Bepaling 5

Hiërarchie

In geval van tegenspraak tussen deze bepalingen en de bepalingen van aanverwante overeenkomsten tussen de partijen die bestonden ten tijde van het overeenkomen van deze bepalingen of die daarna werden gesloten, hebben deze bepalingen voorrang.

Bepaling 6

Beschrijving van de doorgifte(n)

De details van de doorgifte(n), en in het bijzonder de categorieën van persoonsgegevens die worden doorgegeven en het doel waarvoor zij worden doorgegeven, worden in bijlage I.B nader gespecificeerd.

Bepaling 7 — Facultatief

Docking-bepaling

- a) Een entiteit die geen partij is bij deze bepalingen mag, met het akkoord van de partijen, te allen tijde tot deze bepalingen toetreden, hetzij als gegevensexporteur, hetzij als gegevensimporteur, door het aanhangsel in te vullen en bijlage I.A te ondertekenen.
- b) Als de toetredende entiteit het aanhangsel heeft ingevuld en bijlage I.A heeft ondertekend, wordt zij een partij bij deze bepalingen en krijgt zij de rechten en verplichtingen van een gegevensexporteur of een gegevensimporteur in overeenstemming met haar benoeming in bijlage I.A.
- c) De toetredende entiteit heeft geen rechten of verplichtingen uit hoofde van deze bepalingen uit de periode voordat zij partij werd.

AFDELING II — VERPLICHTINGEN VAN DE PARTIJEN

Bepaling 8

Waarborgen inzake gegevensbescherming

De gegevensexporteur garandeert dat hij redelijke inspanningen heeft geleverd om te bepalen of de gegevensimporteur, door de uitvoering van passende technische en organisatorische maatregelen, in staat is zijn verplichtingen uit hoofde van deze bepalingen na te komen.

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

8.1. Instructies

- a) De gegevensimporteur verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de gegevensexporteur. De gegevensexporteur mag dergelijke instructies geven gedurende de duur van de overeenkomst.
- b) De gegevensimporteur stelt de gegevensexporteur onmiddellijk in kennis indien hij niet in staat is deze instructies op te volgen.

8.2. Doelbinding

De gegevensimporteur verwerkt de persoonsgegevens alleen voor het specifieke doel van de doorgifte, zoals opgenomen bijlage I.B, tenzij op basis van verdere instructies van de gegevensexporteur.

8.3. Transparantie

De gegevensexporteur maakt op verzoek een kopie van deze bepalingen, met inbegrip van het door de partijen ingevulde aanhangsel, dat gratis beschikbaar is voor de betrokkene. Voor zover dit noodzakelijk is om bedrijfsgeheimen of andere vertrouwelijke informatie, waaronder de in bijlage II beschreven maatregelen en persoonsgegevens, te beschermen, mag de gegevensexporteur een gedeelte van de tekst van het aanhangsel bij deze bepalingen redigeren voordat hij een kopie deelt, maar hij moet daarbij een relevante samenvatting verstrekken indien de betrokkene anders de inhoud ervan niet zou kunnen begrijpen of zijn/haar rechten niet zou kunnen uitoefenen. Op verzoek delen de partijen de betrokkene de redenen voor het redigeren mee, voor zover mogelijk zonder de geredigeerde informatie te onthullen. Deze bepaling doet geen afbreuk aan de verplichtingen van de gegevensexporteur op grond van de artikelen 13 en 14 van Verordening (EU) 2016/679.

8.4. Nauwkeurigheid

Indien de gegevensimporteur te weten komt dat de persoonsgegevens die hij heeft ontvangen onjuist of verouderd zijn, stelt hij de gegevensexporteur daarvan onverwijld in kennis. In dit geval werkt de gegevensimporteur samen met de gegevensexporteur om de gegevens te wissen of te rectificeren.

8.5. Duur van verwerking en wissing of terugbezorging van gegevens

Verwerking door de gegevensimporteur vindt alleen plaats voor de in bijlage I.B opgegeven duur. Na afloop van de verrichting van de verwerkingsdiensten wist de gegevensimporteur, naargelang de wens van de gegevensexporteur, alle namens de gegevensexporteur verwerkte persoonsgegevens en verzekert hij de gegevensexporteur dat hij dat heeft gedaan, of geeft hij de gegevensexporteur alle namens hem verwerkte persoonsgegevens terug en verwijdert bestaande kopieën. Totdat de gegevens zijn gewist of teruggezonden, blijft de gegevensimporteur ervoor zorgen dat aan deze bepalingen wordt voldaan. In geval van lokaal recht dat op de gegevensimporteur van toepassing is en op basis waarvan teruggave of wissing van de doorgegeven persoonsgegevens verboden is, garandeert de gegevensimporteur dat hij deze bepalingen zal blijven naleven en de persoonsgegevens alleen zal verwerken voor zover en zolang dat naar dat lokaal recht is vereist. Dit doet geen afbreuk aan bepaling 14, met name het vereiste voor de gegevensimporteur krachtens bepaling 14, punt e), om de gegevensexporteur gedurende de hele looptijd van de overeenkomst in kennis te stellen als hij redenen heeft om aan te nemen dat hij onder wetten of praktijken valt of is komen te vallen die niet overeenstemmen met de vereisten uit hoofde van bepaling 14, punt a).

8.6. Beveiliging van de verwerking

- a) De gegevensimporteur en, tijdens de toezending, ook de gegevensexporteur, neemt passende technische en organisatorische maatregelen om de beveiliging van de gegevens te waarborgen, met inbegrip van bescherming tegen een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot die gegevens (hierna "inbreuk in verband met persoonsgegevens" genoemd). Bij het beoordelen van het passende beveiligingsniveau houden de partijen naar behoren rekening met de stand van de techniek, de uitvoeringskosten, de aard, reikwijdte, context en doeleinden van de verwerking, en met de risico's die de verwerking met zich meebrengt voor de betrokkenen. De partijen overwegen met name gebruik te maken van encryptie of pseudonimisering, ook tijdens toezending, waarbij het doel van de verwerking op die manier kan worden verwezenlijkt. Bij pseudonimisering blijven de aanvullende gegevens voor het koppelen van de persoonsgegevens aan een bepaalde betrokkene waar mogelijk onder de exclusieve controle van de gegevensexporteur. Bij de naleving van zijn verplichting uit hoofde van dit punt voert de gegevensimporteur ten minste de in bijlage II vastgestelde technische en organisatorische maatregelen uit. De gegevensimporteur voert regelmatig controles uit om ervoor te zorgen dat deze maatregelen een passend beveiligingsniveau blijven bieden.

- b) De gegevensimporteur verleent zijn personeel alleen toegang tot de persoonsgegevens voor zover dit strikt noodzakelijk is voor de uitvoering, het beheer en de follow-up van de overeenkomst. Hij waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
- c) Bij een inbreuk in verband met persoonsgegevens met betrekking tot persoonsgegevens die op grond van deze bepalingen door de gegevensimporteur worden verwerkt, neemt de gegevensimporteur passende maatregelen om de inbreuk aan te pakken, waaronder maatregelen om de negatieve gevolgen ervan te beperken. Nadat de gegevensimporteur kennis heeft genomen van de inbreuk, stelt hij ook de gegevensexporteur daarvan onverwijld in kennis. Een dergelijke kennisgeving bevat de gegevens van een contactpunt bij wie meer informatie kan worden verkregen, een beschrijving van de aard van de inbreuk waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie, de waarschijnlijke gevolgen ervan en de maatregelen die zijn voorgesteld of genomen om de inbreuk aan te pakken waaronder, in voorkomend geval, maatregelen om mogelijke negatieve gevolgen te beperken. Wanneer en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, bevat de initiële kennisgeving de op dat moment beschikbare informatie en zal verdere informatie, zodra die beschikbaar is, vervolgens onverwijld worden verstrekt.
- d) Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, werkt de gegevensimporteur samen met en verleent hij bijstand aan de gegevensexporteur om deze in staat te stellen zijn verplichtingen krachtens Verordening (EU) 2016/679 na te komen, met name om de bevoegde toezichthoudende autoriteit en de getroffen betrokkenen in kennis te stellen.

8.7. Gevoelige gegevens

Indien de doorgifte persoonsgegevens betreft waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (hierna "gevoelige gegevens" genoemd) blijken, past de gegevensimporteur de in bijlage I.B omschreven specifieke beperkingen en/of extra waarborgen toe.

8.8. Verdere doorgiften

De gegevensimporteur verstrekt de persoonsgegevens uitsluitend aan een derde partij na schriftelijke instructies van de gegevensexporteur. Bovendien worden de gegevens alleen aan een derde partij verstrekt die is gevestigd buiten de Europese Unie (🇺🇪) (in hetzelfde land als de gegevensimporteur of in een ander derde land; hierna "verdere doorgifte" genoemd), indien de derde partij aan deze bepalingen is gebonden of ermee instemt daaraan gebonden te zijn, op grond van de juiste module, of indien:

- i) de verdere doorgifte naar een land is dat profiteert van een adequaatheidsbesluit overeenkomstig artikel 45 van Verordening (EU) 2016/679 waar de verdere doorgifte onder valt;
- ii) de derde partij anderszins voor passende waarborgen overeenkomstig artikel 46 of 47 van Verordening (EU) 2016/679 zorgt met betrekking tot de verwerking in kwestie;
- iii) de verdere doorgifte noodzakelijk is voor de vaststelling, de uitoefening of de onderbouwing van een rechtsvordering in de context van bepaalde administratieve, regelgevings- of gerechtelijke procedures, of
- iv) de verdere doorgifte noodzakelijk is om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.

Verdere doorgiften mogen alleen plaatsvinden indien de gegevensimporteur zich aan alle overige waarborgen krachtens deze bepalingen houdt, met name doelbinding.

8.9. Documentatie en naleving

- a) De gegevensimporteur handelt vragen van de gegevensexporteur in verband met de verwerking op grond van deze bepalingen onverwijld en op passende wijze af.
- b) De partijen moeten de naleving van deze bepalingen kunnen aantonen. De gegevensimporteur houdt met name passende documentatie bij over de verwerkingsactiviteiten die onder zijn verantwoordelijkheid namens de gegevensexporteur hebben plaatsgevonden.
- c) Op verzoek van de gegevensexporteur stelt de gegevensimporteur de gegevensexporteur alle informatie ter beschikking die nodig is om naleving van de in deze bepalingen vastgestelde verplichtingen aan te tonen, audits van de onder deze bepalingen vallende verwerkingsactiviteiten mogelijk te maken en eraan bij te dragen, en dit met redelijke tussenpozen of wanneer er aanwijzingen van niet-naleving zijn. Bij het nemen van een besluit over een toetsing of audit kan de gegevensexporteur rekening houden met relevante certificeringen waarover de gegevensimporteur beschikt.
- d) De gegevensexporteur kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke controleur daartoe te machtigen. Audits kunnen inspecties in de bedrijfsruimten of de fysieke voorzieningen van de gegevensimporteur omvatten en worden, in voorkomend geval, uitgevoerd met een redelijke aankondiging vooraf.
- e) De partijen stellen de in de punten b) en c) bedoelde informatie, met inbegrip van de resultaten van eventuele audits, op verzoek ter beschikking van de bevoegde toezichthoudende autoriteit.

Bepaling 9

Gebruik van subverwerkers

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

- a) **ALGEMENE SCHRIFTELIJKE TOESTEMMING** De gegevensimporteur heeft algemene toestemming van de gegevensexporteur om subverwerkers van een overeengekomen lijst in dienst te nemen. De gegevensimporteur stelt de gegevensexporteur ten minste 30 dagen van tevoren specifiek schriftelijk in kennis van beoogde veranderingen van die lijst door middel van de toevoeging of vervanging van subverwerkers zodat de gegevensexporteur voldoende tijd krijgt om bezwaar tegen die veranderingen te maken voordat de subverwerker(s) in dienst wordt/worden genomen. De gegevensimporteur verstrekt de gegevensexporteur de informatie die deze nodig heeft om zijn recht om bezwaar te maken uit te oefenen.
- b) Wanneer de gegevensimporteur een subverwerker in dienst neemt voor het uitvoeren van specifieke verwerkingsactiviteiten (namens de gegevensexporteur), dan doet hij dit door middel van een schriftelijke overeenkomst die, wat de inhoud betreft, voorziet in dezelfde verplichtingen inzake gegevensbescherming als die waaraan de gegevensimporteur krachtens deze bepalingen is gebonden, onder meer wat betreft de rechten ten behoeve van derden voor betrokkenen (🇺🇪). De partijen komen overeen dat de gegevensimporteur zijn verplichtingen uit hoofde van bepaling 8.8 nakomt door deze bepaling na te leven. De gegevensimporteur zorgt ervoor dat de subverwerker zich houdt aan de verplichtingen waaraan de gegevensimporteur overeenkomstig deze bepalingen is gebonden.
- c) De gegevensimporteur verstrekt op verzoek van de gegevensexporteur een kopie van die overeenkomst met de subverwerker en van eventuele daaropvolgende wijzigingen aan de gegevensexporteur. Voor zover dit noodzakelijk is om bedrijfsgeheimen of andere vertrouwelijke informatie, waaronder persoonsgegevens, te beschermen, mag de gegevensimporteur de tekst van de overeenkomst redigeren voordat hij een kopie deelt.

d)De gegevensimporteur blijft ten aanzien van de gegevensexporteur volledig verantwoordelijk voor het nakomen van zijn verplichtingen door de subverwerker uit hoofde van zijn overeenkomst met de gegevensimporteur. De gegevensimporteur stelt de gegevensexporteur in kennis van elke niet-nakoming door de subverwerker van zijn verplichtingen uit hoofde van die overeenkomst.

e)De gegevensimporteur komt een derdenbeding overeen met de subverwerker waarbij de gegevensexporteur, in geval de gegevensimporteur feitelijk is verdwenen, rehtens is opgehouden te bestaan of failliet is gegaan, het recht heeft de overeenkomst met de subverwerker te beëindigen en de subverwerker op te dragen de persoonsgegevens te wissen of terug te geven.

Bepaling 10

De rechten van betrokkenen

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

a)De gegevensimporteur stelt de gegevensexporteur onverwijld in kennis van alle verzoeken die hij van een betrokkene heeft ontvangen. Hij reageert zelf niet op dat verzoek, tenzij dit door de gegevensexporteur is toegestaan.

b)De gegevensimporteur verleent de gegevensexporteur bijstand bij het nakomen van zijn verplichtingen om te reageren op de verzoeken van betrokkenen voor de uitoefening van hun rechten uit hoofde van Verordening (EU) 2016/679. In dit verband stellen de partijen in bijlage II de passende technische en organisatorische maatregelen vast, rekening houdend met de aard van de verwerking op basis waarvan de bijstand wordt verleend, alsook de reikwijdte en de omvang van de vereiste bijstand.

c)Bij het nakomen van zijn verplichtingen uit hoofde van de punten a) en b), houdt de gegevensimporteur zich aan de instructies van de gegevensexporteur.

Bepaling 11

Verhaal

a)De gegevensimporteur brengt betrokkenen via een individuele mededeling of op zijn website, in een transparant en gemakkelijk toegankelijk formaat, op de hoogte van een contactpunt dat gemachtigd is om klachten af te handelen. Hij handelt klachten die hij van een betrokkene ontvangt onverwijld af.

[OPTIE: De gegevensimporteur stemt ermee in dat betrokkenen klachten ook bij een onafhankelijk orgaan voor geschillenbeslechting mogen indienen ⁽¹¹⁾, zonder kosten voor de betrokkene. Hij brengt de betrokkenen, op de in punt a) genoemde wijze, op de hoogte van een dergelijk verhaalmechanisme en laat hen weten dat zij niet verplicht zijn daarvan gebruik te maken, of om een bepaalde volgorde aan te houden om verhaal te halen.]

b)Bij een geschil tussen een betrokkene en een van de partijen met betrekking tot de naleving van deze bepalingen, doet die partij al het mogelijke om de kwestie tijdig in der minne te schikken. De partijen houden elkaar op de hoogte van dergelijke geschillen en werken, in voorkomend geval, samen om ze te beslechten.

c)Wanneer de betrokkene zich overeenkomstig bepaling 3 op een recht ten behoeve van derden beroept, aanvaardt de gegevensimporteur het besluit van de betrokkene om:

i)een klacht in te dienen bij de toezichthoudende autoriteit in de lidstaat waar hij/zij gewoonlijk verblijft of werkt, of de bevoegde toezichthoudende autoriteit krachtens bepaling 13;

ii) het geschil voor te leggen aan de bevoegde gerechten in de zin van bepaling 18.

d)De partijen aanvaarden dat de betrokkene vertegenwoordigd kan worden door een orgaan, organisatie of vereniging zonder winstoogmerk onder de in artikel 80, lid 1, van Verordening (EU) 2016/679 vermelde voorwaarden.

e)De gegevensimporteur schikt zich naar een besluit dat uit hoofde van het toepasselijke recht van de Europese Unie/de lidstaat bindend is.

f)De gegevensimporteur stemt ermee in dat de keuze van de betrokkene geen afbreuk doet aan zijn/haar materiële en formele rechten om overeenkomstig de geldende wetgeving verhaal te zoeken.

Bepaling 12

Aansprakelijkheid

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

a)Elke partij is ten aanzien van de andere partij(en) aansprakelijk voor schade die hij de andere partij(en) berokkent door inbreuken op deze bepalingen.

b)De gegevensimporteur is ten aanzien van de betrokkene aansprakelijk en de betrokkene heeft het recht een vergoeding te verkrijgen voor materiële of immateriële schade die de gegevensimporteur of zijn subverwerker aan de betrokkene berokkent door de rechten ten behoeve van derden uit hoofde van deze bepalingen te schenden.

c)Niettegenstaande punt b) is de gegevensexporteur ten aanzien van de betrokkene aansprakelijk en heeft de betrokkene het recht een vergoeding te verkrijgen voor materiële of immateriële schade die de gegevensexporteur of de gegevensimporteur (of zijn subverwerker) aan de betrokkene berokkent door de rechten ten behoeve van derden uit hoofde van deze bepalingen te schenden. Dit doet geen afbreuk aan de aansprakelijkheid van de gegevensexporteur en, wanneer de gegevensexporteur een verwerker is die namens een verwerkingsverantwoordelijke optreedt, aan de aansprakelijkheid van de verwerkingsverantwoordelijke uit hoofde van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725, indien van toepassing.

d)De partijen komen overeen dat als de gegevensexporteur op grond van punt c) aansprakelijk wordt gesteld voor door de gegevensimporteur (of zijn subverwerker) berokkende schade, hij het recht heeft om op de gegevensimporteur het deel van de schadevergoeding te verhalen dat overeenkomt met de aansprakelijkheid van de gegevensimporteur voor de schade.

e)Wanneer meerdere partijen verantwoordelijk zijn voor schade die als gevolg van schendingen van deze bepalingen aan de betrokkene is berokkend, zijn alle verantwoordelijke partijen hoofdelijk aansprakelijk en heeft de betrokkene het recht om voor de rechter een procedure tegen deze partijen in te stellen.

f)De partijen komen overeen dat als een van de partijen op grond van punt e) aansprakelijk wordt gesteld, deze partij het recht heeft om op de andere partij(en) het deel van de schadevergoeding te verhalen dat overeenkomt met zijn/hun deel van de aansprakelijkheid voor de schade.

g)De gegevensimporteur mag zich niet op het gedrag van een subverwerker beroepen om zich aan zijn eigen aansprakelijkheid te onttrekken.

Bepaling 13

Toezicht

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

a)[Wanneer de gegevensexporteur in een EU-lidstaat is gevestigd:] De toezichthoudende autoriteit die erop toeziet dat de gegevensexporteur Verordening (EU) 2016/679 naleeft met betrekking tot de gegevensdoorgifte, zoals aangegeven in bijlage I.C, treedt op als de bevoegde toezichthoudende autoriteit.

[Wanneer de gegevensexporteur niet in een EU-lidstaat is gevestigd, maar overeenkomstig artikel 3, lid 2, van Verordening (EU) 2016/679 onder het territoriale toepassingsgebied van die verordening valt en een vertegenwoordiger heeft aangewezen overeenkomstig artikel 27, lid 1, van Verordening (EU) 2016/679:] De toezichthoudende autoriteit van de lidstaat waar de vertegenwoordiger in de zin van artikel 27, lid 1, van Verordening (EU) 2016/679 is gevestigd, zoals aangegeven in bijlage I.C, treedt op als de bevoegde toezichthoudende autoriteit.

[Wanneer de gegevensexporteur niet in een EU-lidstaat is gevestigd, maar overeenkomstig artikel 3, lid 2, van Verordening (EU) 2016/679 onder het territoriale toepassingsgebied van die verordening valt, zonder echter een vertegenwoordiger te hebben aangewezen overeenkomstig artikel 27, lid 2, van Verordening (EU) 2016/679:] De toezichthoudende autoriteit van een van de lidstaten waar de betrokkenen wier persoonsgegevens krachtens deze bepalingen worden verwerkt in verband met het aanbieden van goederen of diensten aan hen, of wier gedrag wordt gecontroleerd, zijn gevestigd, zoals aangegeven in bijlage I.C, treedt op als de bevoegde toezichthoudende autoriteit.

b)De gegevensimporteur stemt ermee in zich te onderwerpen aan de jurisdictie van en samen te werken met de bevoegde toezichthoudende autoriteit in procedures gericht op het waarborgen van de naleving van deze bepalingen. De gegevensimporteur stemt er in het bijzonder mee in vragen te beantwoorden, zich aan audits te onderwerpen en zich aan de door de toezichthoudende autoriteit vastgestelde maatregelen te houden, waaronder corrigerende en compenserende maatregelen. Hij geeft de toezichthoudende autoriteit schriftelijke bevestiging dat de noodzakelijke maatregelen zijn genomen.

AFDELING III — LOKALE WETTEN EN VERPLICHTINGEN IN GEVAL VAN TOEGANG DOOR OVERHEIDSINSTANTIES

Bepaling 14

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

a)De partijen garanderen dat zij geen reden hebben om aan te nemen dat de wetten en praktijken in het derde land van bestemming die van toepassing zijn op de verwerking van de persoonsgegevens door de gegevensimporteur, met inbegrip van vereisten om persoonsgegevens te verstrekken of maatregelen die toegang door overheidsinstanties toestaan, de gegevensimporteur verhinderen zijn verplichtingen uit hoofde van deze bepalingen na te komen. Hierbij wordt ervan uitgegaan dat wetten en praktijken waarmee de wezenlijke inhoud van de grondrechten en fundamentele vrijheden wordt geëerbiedigd en die niet verder gaan dan hetgeen in een democratische samenleving noodzakelijk en evenredig is om een van de in artikel 23, lid 1, van Verordening (EU) 2016/679 genoemde doelstellingen te waarborgen, niet in tegenspraak zijn met deze bepalingen.

b)De partijen verklaren dat zij bij het bieden van de in punt a) bedoelde garantie met name de volgende elementen naar behoren in aanmerking hebben genomen:

i)de specifieke omstandigheden van de doorgifte, waaronder de lengte van de verwerkingsketen, het aantal betrokken actoren en de kanalen die voor de toezending zijn gebruikt; voorgenomen verdere doorgiften; het soort ontvanger; het doel van de verwerking; de categorieën en het formaat van de doorgegeven persoonsgegevens; de economische sector waarin de doorgifte plaatsvindt; de opslagplaats van de doorgegeven gegevens;

ii)de wetten en praktijken van het derde land van bestemming — waaronder de wetten en praktijken die vereisen om gegevens aan overheidsinstanties te verstrekken of toegang door dergelijke instanties toestaan — die van belang zijn in het licht van de specifieke omstandigheden van de doorgifte, en de toepasselijke beperkingen en waarborgen ⁽¹²⁾;

iii)alle relevante contractuele, technische of organisatorische waarborgen die zijn ingesteld in aanvulling op de waarborgen uit hoofde van deze bepalingen, waaronder maatregelen die worden toegepast tijdens de toezending en op de verwerking van de persoonsgegevens in het land van bestemming.

c)De gegevensimporteur garandeert dat hij bij het uitvoeren van de beoordeling op grond van punt b) al het mogelijke heeft gedaan om de gegevensexporteur van relevante informatie te voorzien en stemt ermee in dat hij met de gegevensexporteur zal blijven samenwerken om naleving van deze bepalingen te waarborgen.

d)De partijen komen overeen om de beoordeling uit hoofde van punt b) te documenteren en op verzoek ter beschikking te stellen van de bevoegde toezichthoudende autoriteit.

e)De gegevensimporteur stemt ermee in de gegevensexporteur onverwijld in kennis te stellen indien hij, na deze bepalingen te zijn overeengekomen en voor de duur van de overeenkomst, redenen heeft om aan te nemen dat hij onder wetten of praktijken valt of is komen te vallen die niet overeenstemmen met de vereisten uit hoofde van punt a), onder meer ingevolge een wijziging van de wetten in het derde land of een maatregel (zoals een verzoek om verstrekking) die duidt op een toepassing van die wetten in de praktijk die niet overeenstemt met de vereisten in punt a). [Voor module drie: De gegevensexporteur zendt de kennisgeving door aan de verwerkingsverantwoordelijke.]

f)Ingevolge een kennisgeving overeenkomstig punt e), of als de gegevensexporteur anderszins redenen heeft om aan te nemen dat de gegevensimporteur zijn verplichtingen uit hoofde van deze bepalingen niet langer kan nakomen, stelt de gegevensexporteur onverwijld passende maatregelen (bv. technische of organisatorische maatregelen om betrouwbaarheid en vertrouwelijkheid te waarborgen) vast die de gegevensexporteur en/of de gegevensimporteur moeten uitvoeren om de situatie aan te pakken, [voor module drie: in voorkomend geval in overleg met de verwerkingsverantwoordelijke]. De gegevensexporteur schort de gegevensdoorgifte op als hij van mening is dat er geen passende waarborgen voor die doorgifte kunnen worden gegarandeerd, of op basis van instructies van [voor module drie: de verwerkingsverantwoordelijke of] de bevoegde toezichthoudende autoriteit hiertoe. In dit geval heeft de gegevensexporteur het recht om de overeenkomst te beëindigen, voor zover die betrekking heeft op de verwerking van persoonsgegevens uit hoofde van deze bepalingen. Indien er meer dan twee partijen bij de overeenkomst zijn betrokken, mag de gegevensexporteur zijn recht om de overeenkomst te beëindigen alleen uitoefenen met betrekking tot de betrokken partij, tenzij anderszins door de partijen is overeengekomen. Indien de overeenkomst overeenkomstig deze bepaling wordt beëindigd, is bepaling 16, punten d) en e), van toepassing.

Bepaling 15

Verplichtingen van de gegevensimporteur in geval van toegang door overheidsinstanties

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

15.1. Kennisgeving

a)De gegevensimporteur stemt er mee in de gegevensexporteur en, voor zover mogelijk, de betrokkene onverwijld in kennis te stellen (indien nodig met behulp van de gegevensexporteur) indien hij:

i)van een overheidsinstantie, met inbegrip van rechterlijke instanties, een juridisch bindend verzoek om verstrekking van overeenkomstig deze bepalingen doorgegeven persoonsgegevens ontvangt krachtens het recht van het land van bestemming; een dergelijke kennisgeving omvat informatie over de gevraagde persoonsgegevens, de verzoekende autoriteit, de rechtsgrondslag voor het verzoek en het gegeven antwoord, of

ii)kennis heeft genomen van rechtstreekse toegang door overheidsinstanties tot de krachtens deze bepalingen doorgegeven persoonsgegevens in overeenstemming met de wetgeving van het land van bestemming; een dergelijke kennisgeving omvat alle informatie waarover de gegevensimporteur beschikt.

[Voor module drie: De gegevensexporteur zendt de kennisgeving door aan de verwerkingsverantwoordelijke.]

b)Indien het de gegevensimporteur uit hoofde van de wetgeving van het land van bestemming verboden is om de gegevensexporteur en/of de betrokkene in kennis te stellen, stemt de gegevensimporteur ermee in al het mogelijke te doen om van het verbod te worden ontheven, teneinde zo spoedig mogelijk zo veel

mogelijk informatie mee te delen. De gegevensimporteur stemt ermee in deze inspanningen te documenteren om ze op verzoek van de gegevensexporteur te kunnen aantonen.

- c) Indien toegestaan uit hoofde van de wetgeving van het land van bestemming, stemt de gegevensimporteur ermee in de gegevensexporteur, met regelmatige tussenpozen gedurende de duur van de overeenkomst, met zo veel mogelijk relevante informatie over de ontvangen verzoeken (met name het aantal verzoeken, het soort gevraagde gegevens, de verzoekende autoriteit(en), of er verzoeken zijn betwist en wat de uitkomst daarvan was enz.) te doen toekomen. [Voor module drie: De gegevensexporteur zendt de informatie door aan de verwerkingsverantwoordelijke.]
- d) De gegevensimporteur stemt ermee in de informatie overeenkomstig de punten a) tot en met c) te bewaren voor de duur van de overeenkomst en die op verzoek ter beschikking van de bevoegde toezichthoudende autoriteit te stellen.
- e) De punten a) tot en met c) doen geen afbreuk aan de verplichting van de gegevensimporteur overeenkomstig bepaling 14, punt e), en bepaling 16 om de gegevensexporteur onverwijld in kennis te stellen wanneer hij niet in staat is deze bepalingen na te leven.

15.2. Wettigheidstoetsing en gegevensminimalisering

- a) De gegevensimporteur stemt ermee in de wettigheid van het verzoek om verstrekking te toetsen, met name of die binnen de aan de verzoekende overheidsinstantie toegekende bevoegdheden blijft, en het verzoek te betwisten indien hij na een zorgvuldige beoordeling tot de conclusie komt dat er redelijke gronden zijn om aan te nemen dat het verzoek onwettig is krachtens de wetgeving van het land van bestemming, toepasselijke verplichtingen uit hoofde van het internationaal recht en beginselen van internationale courtoisie. Onder deze omstandigheden benut de gegevensimporteur de beroepsmogelijkheden. Bij het betwisten van een verzoek neemt de gegevensimporteur voorlopige maatregelen om de effecten van het verzoek op te schorten totdat de bevoegde rechterlijke instantie over de gegrondheid ervan heeft beslist. Hij verstrekt de gevraagde persoonsgegevens pas wanneer hij dat volgens de toepasselijke procedurevoorschriften moet doen. Deze vereisten doen geen afbreuk aan de verplichtingen van de gegevensimporteur krachtens bepaling 14, punt e).
- b) De gegevensimporteur stemt ermee in zijn juridische beoordeling en eventuele betwistingen van het verzoek om verstrekking te documenteren en, voor zover dit is toegestaan krachtens de wetgeving van het land van bestemming, de documentatie ter beschikking te stellen van de gegevensexporteur. Hij stelt deze documenten op verzoek ook ter beschikking van de bevoegde toezichthoudende autoriteit. [Voor module drie: De gegevensexporteur stelt de beoordeling ter beschikking van de verwerkingsverantwoordelijke.]
- c) De gegevensimporteur stemt ermee in de toegestane minimale hoeveelheid informatie te verstrekken bij het beantwoorden van een verzoek om verstrekking, op basis van een redelijke interpretatie van het verzoek.

AFDELING IV — SLOTBEPALINGEN

Bepaling 16

Niet-naleving van de bepalingen en beëindiging

- a) De gegevensimporteur stelt de gegevensexporteur onverwijld in kennis indien hij om wat voor reden dan ook niet in staat is deze bepalingen na te leven.
- b) Indien de gegevensimporteur inbreuk maakt op deze bepalingen of niet in staat is deze bepalingen na te leven, schort de gegevensexporteur de doorgifte van persoonsgegevens aan de gegevensimporteur op totdat de naleving weer wordt gewaarborgd of totdat de overeenkomst wordt beëindigd. Dit doet geen afbreuk aan bepaling 14, punt f).
- c) De gegevensexporteur heeft het recht de overeenkomst te beëindigen, voor zover die betrekking heeft op de verwerking van persoonsgegevens uit hoofde van deze bepalingen, wanneer:
- de gegevensexporteur de doorgifte van persoonsgegevens naar de gegevensimporteur overeenkomstig punt b) heeft opgeschort en de bepalingen niet binnen een redelijke termijn en in elk geval binnen één maand na de opschorting weer worden nageleefd;
 - de gegevensimporteur in belangrijke en voortdurende mate inbreuk maakt op deze bepalingen, of
 - de gegevensimporteur zich niet aan een bindend besluit van een bevoegd gerecht of een bevoegde autoriteit met betrekking tot zijn verplichtingen uit hoofde van deze bepalingen houdt.

In deze gevallen stelt hij de bevoegde toezichthoudende autoriteit [voor module drie: en de verwerkingsverantwoordelijke] in kennis van die niet-naleving. Wanneer meer dan twee partijen bij de overeenkomst zijn betrokken, mag de gegevensexporteur zijn recht om de overeenkomst te beëindigen alleen uitoefenen met betrekking tot de betrokken partij, tenzij anderszins door de partijen is overeengekomen.

- d) [Voor de modules een, twee en drie: Persoonsgegevens die voorafgaand aan de beëindiging van de overeenkomst zijn doorgegeven overeenkomstig punt c) worden, naargelang de wens van de gegevensexporteur, onmiddellijk volledig aan de gegevensexporteur terugbezorgd of gewist. Hetzelfde geldt voor eventuele kopieën van de gegevens.] [Voor module vier: Door de gegevensexporteur in de Europese Unie verzamelde persoonsgegevens die voordat de overeenkomst werd beëindigd waren doorgegeven overeenkomstig punt c) worden onmiddellijk volledig gewist, met inbegrip van eventuele kopieën daarvan.] De gegevensimporteur verzekert de gegevensexporteur ervan dat de gegevens zijn gewist. Totdat de gegevens zijn gewist of teruggezonden, blijft de gegevensimporteur ervoor zorgen dat aan deze bepalingen wordt voldaan. In geval van lokaal recht dat op de gegevensimporteur van toepassing is en op basis waarvan teruggave of wissing van de doorgegeven persoonsgegevens verboden is, garandeert de gegevensimporteur dat hij deze bepalingen zal blijven naleven en de gegevens alleen zal verwerken voor zover en zolang dat naar dat lokaal recht is vereist.
- e) Elk van de partijen kan haar toestemming om aan deze bepalingen gebonden te zijn, intrekken wanneer i) de Europese Commissie een besluit overeenkomstig artikel 45, lid 3, van Verordening (EU) 2016/679 neemt dat betrekking heeft op de doorgifte van persoonsgegevens waarop deze bepalingen van toepassing zijn; of ii) Verordening (EU) 2016/679 onderdeel wordt van het rechtskader van het land waarnaar de persoonsgegevens worden doorgegeven. Dit doet geen afbreuk aan andere verplichtingen die van toepassing zijn op de desbetreffende verwerking op grond van Verordening (EU) 2016/679.

Bepaling 17

Toepasselijk recht

Deze bepalingen worden geregeld door het recht van een van de EU-lidstaten, mits dat recht voorziet in rechten ten behoeve van derden. De partijen komen overeen dat dit het recht is zoals gespecificeerd in de Overeenkomst.

Bepaling 18

Forum- en jurisdictiekeuze

- a) Uit deze bepalingen voortvloeiende geschillen worden beslecht door de gerechten van een EU-lidstaat.
- b) De partijen komen overeen dat dit de gerechten zijn zoals gespecificeerd in de Overeenkomst.
- c) Een betrokkene kan ook gerechtelijke procedures aanhangig maken tegen de gegevensexporteur en/of de gegevensimporteur bij de gerechten van de lidstaat waar hij/zij gewoonlijk verblijft.
- d) De partijen komen overeen zich aan de jurisdictie van die gerechten te onderwerpen.

(1) Wanneer de gegevensexporteur een onder Verordening (EU) 2016/679 vallende verwerker is die namens een instelling of orgaan van de Unie optreedt als verwerkingsverantwoordelijke, garandeert de toepassing van deze bepalingen bij het in dienst nemen van een andere verwerker (subverwerker) die niet onder Verordening (EU) 2016/679 valt ook de naleving van artikel 29, lid 4, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39), voor zover deze bepalingen en de verplichtingen inzake gegevensbescherming zoals opgenomen in de overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker overeenkomstig artikel 29, lid 3, van Verordening (EU) 2018/1725 op één lijn zijn gebracht. Dat is met name het geval wanneer de verwerkingsverantwoordelijke en de verwerker zich baseren op de in Besluit 2021/915 opgenomen standaardcontractbepalingen.

(2) Dit vereist dat de gegevens op dusdanige wijze anoniem moeten worden gemaakt dat de persoon door niemand meer geïdentificeerd kan worden, overeenkomstig overweging 26 van Verordening (EU) 2016/679, en dat dit proces onomkeerbaar is.

(3) De Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) voorziet in de uitbreiding van de interne markt van de Europese Unie met de drie EER-staten IJsland, Liechtenstein en Noorwegen. De Uniewetgeving inzake gegevensbescherming, waaronder Verordening (EU) 2016/679, valt onder de EER-overeenkomst en is in bijlage XI daarbij opgenomen. Derhalve wordt een verstrekking door de gegevensimporteur aan een in de EER gevestigde derde partij voor de toepassing van deze bepalingen niet als een verdere doorgifte aangemerkt.

(4) De Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) voorziet in de uitbreiding van de interne markt van de Europese Unie met de drie EER-staten IJsland, Liechtenstein en Noorwegen. De Uniewetgeving inzake gegevensbescherming, waaronder Verordening (EU) 2016/679, valt onder de EER-overeenkomst en is in bijlage XI daarbij opgenomen. Derhalve wordt een verstrekking door de gegevensimporteur aan een in de EER gevestigde derde partij voor de toepassing van deze bepalingen niet als een verdere doorgifte aangemerkt.

(5) Zie artikel 28, lid 4, van Verordening (EU) 2016/679 en, wanneer de verwerkingsverantwoordelijke een instelling of orgaan van de Europese Unie is, artikel 29, lid 4, van Verordening (EU) 2018/1725.

(6) De Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) voorziet in de uitbreiding van de interne markt van de Europese Unie met de drie EER-staten IJsland, Liechtenstein en Noorwegen. De Uniewetgeving inzake gegevensbescherming, waaronder Verordening (EU) 2016/679, valt onder de EER-overeenkomst en is in bijlage XI daarbij opgenomen. Derhalve wordt een verstrekking door de gegevensimporteur aan een in de EER gevestigde derde partij voor de toepassing van deze bepalingen niet als een verdere doorgifte aangemerkt.

(7) Hieronder valt ook de vraag of de doorgifte en verdere verwerking persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten omvatten.

(8) Aan dit vereiste kan worden voldaan door toetreding van de subverwerker tot deze bepalingen overeenkomstig de gepaste module, in overeenstemming met bepaling 7.

(9) Aan dit vereiste kan worden voldaan door toetreding van de subverwerker tot deze bepalingen overeenkomstig de gepaste module, in overeenstemming met bepaling 7.

(10) Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met maximaal twee maanden worden verlengd. De gegevensimporteur stelt de betrokkene naar behoren en onverwijld in kennis van een dergelijke verlenging.

(11) De gegevensimporteur mag alleen onafhankelijke geschillenbeslechting via een arbitragecommissie aanbieden als hij gevestigd is in een land dat het Verdrag van New York over de erkenning en tenuitvoerlegging van buitenlandse scheidsrechterlijke uitspraken heeft geratificeerd.

(12) Met betrekking tot het effect van dergelijke wetten en praktijken op de naleving van de bepalingen, kunnen verschillende elementen worden beschouwd als onderdeel van een algemene beoordeling. Het kan hierbij gaan om relevante en gedocumenteerde praktijkervaring met eerdere gevallen van verzoeken om verstrekking van overheidsinstanties, of het ontbreken van dergelijke verzoeken, gedurende een voldoende representatief tijdsbestek. Dit heeft met name betrekking op interne registers of andere documenten die doorlopend en met de nodige zorgvuldigheid zijn opgesteld en op seniormanagementniveau zijn gecertificeerd, mits deze informatie rechtmatig met derde partijen kan worden gedeeld. Indien van deze praktijkervaring wordt uitgegaan om te concluderen dat de gegevensimporteur niet gehinderd zal worden om deze bepalingen na te leven, moet die ervaring worden ondersteund door andere relevante objectieve elementen en dienen de partijen zorgvuldig na te gaan of deze elementen wat de betrouwbaarheid en representativiteit ervan betreft samen voldoende gewicht in de schaal leggen om deze conclusie te ondersteunen. De partijen moeten er met name rekening mee houden of hun praktijkervaring wordt bevestigd en niet wordt tegengesproken door openbaar beschikbare of anderszins toegankelijke betrouwbare informatie over het bestaan of het ontbreken van verzoeken binnen dezelfde sector en/of de toepassing van het recht in de praktijk, zoals jurisprudentie en verslagen van onafhankelijke toezichthoudende organen.

AAANHANGSEL

TOELICHTING:

Het moet mogelijk zijn om de informatie die van toepassing is op elke doorgifte of categorie van doorgiften duidelijk te onderscheiden en, in dit verband, om de respectieve rol(len) van de partijen als gegevensexporteur(s) en/of gegevensimporteurs(s) te bepalen. Hiertoe is het niet noodzakelijkerwijs nodig om voor elke doorgifte/categorie van doorgiften en/of contractuele relatie afzonderlijke aanhangsels in te vullen en te ondertekenen wanneer deze transparantie ook met één aanhangsel kan worden gewaarborgd. Indien noodzakelijk om voldoende helderheid te verschaffen, dienen er echter wel afzonderlijke aanhangsels te worden gebruikt.

BIJLAGE I

A. LIJST VAN PARTIJEN

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

Gegevensexporteur(s): *[Identiteit en contactgegevens van de gegevensexporteur(s) en, in voorkomend geval, van zijn/hun functionaris voor gegevensbescherming en/of de vertegenwoordiger in de Europese Unie]*

Zoals beschreven in de Overeenkomst

Activiteiten in verband met de overeenkomstig deze bepalingen doorgegeven gegevens

Zoals beschreven in de Overeenkomst

Rol (verwerkingsverantwoordelijke/verwerker):

Zoals beschreven in de Overeenkomst

Gegevensimporteur(s): [Identiteit en contactgegevens van de gegevensimporteur(s), met inbegrip van eventuele contactpersonen die verantwoordelijk zijn voor gegevensbescherming]

Zoals beschreven in de Overeenkomst

Activiteiten in verband met de overeenkomstig deze bepalingen doorgegeven gegevens

Zoals beschreven in de Overeenkomst

Rol (verwerkingsverantwoordelijke/verwerker):

Zoals beschreven in de Overeenkomst

B. BESCHRIJVING VAN DOORGIFTE

Categorieën van betrokkenen wier persoonsgegevens worden doorgegeven

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

Categorieën van doorgegeven persoonsgegevens

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

Gevoelige gegevens die worden doorgegeven (indien van toepassing) en toegepaste beperkingen of waarborgen waarmee ten volle rekening wordt gehouden met de aard van de gegevens en de bijbehorende risico's, zoals strikte beperking van het doel, toegangsbeperkingen (waaronder uitsluitend toegang voor personeelsleden die een gespecialiseerde opleiding hebben gevolgd), het in een register bijhouden van toegang tot de gegevens, beperkingen voor verdere doorgiften, of bijkomende beveiligingsmaatregelen.

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

De frequentie van de doorgifte (bv. of de gegevens eenmalig of continu worden doorgegeven).

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

Aard van de verwerking

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

Doeleind(en) van de gegevensdoorgifte en verdere verwerking

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

De periode gedurende welke de persoonsgegevens zullen worden bewaard, of indien dat niet mogelijk is, de criteria om die termijn te bepalen

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

Voor doorgiften aan (sub-)verwerkers ook het onderwerp, de aard en de duur van de verwerking opgeven

Zoals beschreven in Sectie 1 en 3 in Unit4 Verwerkingsinformatie

C. BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

De bevoegde toezichthoudende autoriteiten identificeren in overeenstemming met bepaling 13

De bevoegde toezichthoudende autoriteit zal zijn de Autoriteit Persoonsgegevens in Nederland, tenzij Bepaling 13 anders vereist.

BIJLAGE II

TECHNISCHE EN ORGANISATORISCHE MAATREGELN WAARONDER TECHNISCHE EN ORGANISATORISCHE MAATREGELN OM DE BEVEILIGING VAN DE GEGEVENS TE WAARBORGEN

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

TOELICHTING:

De technische en organisatorische maatregelen moeten concreet (en niet op generieke wijze) worden beschreven. Zie ook de algemene opmerking op de eerste pagina van het aanhangsel, met name met betrekking tot de noodzaak om duidelijk aan te geven welke maatregelen op elke doorgifte/reeks doorgiften van toepassing zijn.

Beschrijving van de technische en organisatorische maatregelen die de gegevensimporteur(s) heeft/hebben genomen (met inbegrip van eventuele relevante certificeringen) om een passend beveiligingsniveau te waarborgen, rekening houdend met de aard, reikwijdte, context en doeleinden van de verwerking en met de risico's voor de rechten en vrijheden van natuurlijke personen.

Zoals beschreven in Sectie 2 in Unit4 Verwerkingsinformatie

BIJLAGE III

LIJST VAN SUBVERWERKERS

Doorgifte tussen verwerkingsverantwoordelijke en verwerker

TOELICHTING:

Deze bijlage moet bij specifieke toestemming van subverwerkers (bepaling 9, punt a), optie 1) worden ingevuld voor de modulen twee en drie.

De verwerkingsverantwoordelijke heeft het gebruik van de volgende subverwerkers toegestaan:

Niet van toepassing