Annex A(i) bij Appendix A
Unit4 Verwerkingsvoorwaarden

(**EER**)

Versie 1.1

1. ONDERWERP VAN DEZE VOORWAARDEN VERWERKING PERSOONSGEVENS

1.1 De Klant, hierna te noemen: **("Verwerkingsverantwoordelijke**"), is de verwerkingsverantwoordelijke, die bepaalt voor welke doeleinden en de middelen waarop Persoonsgegevens met betrekking tot een Betrokkene worden of moeten worden Verwerkt.

1.2 Unit4, hierna te noemen: ("**Verwerker"**) is de verwerker, die die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.3 Verwerker zal de Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke Verwerken . in overeenstemming met deze Verwerkingsvoorwaarden en de Data Protectie Wetgeving, inclusief eventuele bijlagen.

1.4 Bijlage 1 beschrijft onder meer het doel en de middelen van de Verwerking, het type te Verwerken Persoonsgegevens, de bewaartermijn en de land(en) en plaatsen(en) waar de Persoonsgegevens worden Verwerkt.

1.5 Bijlage 2 beschrijft de toepasselijke beveiligingsmaatregelen die worden gebruikt door de Verwerker, en waarvan de Verwerkingsverantwoordelijke bevestigt dat deze toereikend zijn.

1.6 Bijlage 3 beschrijft de details van eventuele Sub-Verwerkers

1.7 Bijlage 4 bevat de EU Standard Contractual Clauses, die van toepassing zijn indien de Verwerking van Persoonsgegevens buiten de Europese Economische Ruimte ("EER") plaatsvindt.

1.8 De Partijen zullen de Bijlagen van deze Verwerkingsvoorwaarden van tijd tot tijd aanpassen, indien nodig.

2. VERWERKING

2.1 Verwerker en Verwerkingsverantwoordelijke verstrekken elkaar over en weer tijdig alle benodigde informatie om een goede naleving van de geldende Data Protectie Wetgeving mogelijk te maken.

2.3 Verwerking van Persoonsgegevens vindt plaats in de plaats/het land zoals is aangegeven in Bijlage 1. Bij ondertekening van een Overeenkomst heeft Verwerkingsverantwoordelijke toestemming gegeven voor Verwerking van de Persoonsgegevens in de landen die zijn opgenomen in Bijlage 1.

2.3 Indien de Verwerking van Persoonsgegevens buiten de Europese Economische Ruimte ("EER") plaatsvindt, in een land waarvoor de Europese Commissie geen adequaatheidsbesluit heeft gegeven, zal Verwerking alleen plaatsvinden op voorwaarde dat er sprake is van passende waarborgen die voldoende niveau van gegevensbescherming bieden zoals de EU-Standard Contractual Clauses ("EU-SCC"), zoals opgenomen in Bijlage 4 van deze Verwerkingsvoorwaarden (of iedere andere passende waarborgen waarvan de Data Protectie Autoriteit of een bevoegde autoriteit heeft besloten dat deze een voldoende niveau van beveiliging bieden), en de Verwerkingsverantwoordelijke geeft hierbij toestemming en geeft instructies om deze Verwerking uit te voeren.

3. VERANTWOORDELIJKHEDEN VERWERKER

3.1 Verwerker zal de Persoonsgegevens op behoorlijke en zorgvuldige wijze verwerken conform deze Verwerkingsvoorwaarden en de verplichtingen van de Data Protectie Wetgeving.

3.2 Verwerker Verwerkt Persoonsgegevens uitsluitend in het kader van de uitvoering van de Overeenkomst en de schriftelijke instructies die door de Verwerkingsverantwoordelijke zijn gegeven, behoudens de Verwerker wettelijk verplicht is om de Persoonsgegevens op een manier te Verwerken die hiermee in strijd is . In dit laatste geval brengt hij de Verwerkingsverantwoordelijke op de hoogte van de wettelijke bepalingen en zijn verplichting.

3.3 Verwerker Verwerkt alleen Persoonsgegevens van de Verwerkingsverantwoordelijke voor de doeleinden waarvoor deze zijn ontvangen en om aan de uit hoofde van deze Verwerkingsvoorwaarden gedelegeerde verplichtingen te voldoen. Verwerker zal de Persoonsgegevens niet voor andere doeleinden gebruiken.

3.4 Verwerker zal de Persoonsgegevens niet aan een derde verstrekken, tenzij deze uitwisseling plaatsvindt in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting of rechterlijk bevel.

3.5 Verwerker zal de Persoonsgegevens niet wijzigen. bewerken, of op andere wijze veranderen zonder opdracht daartoe van de Verwerkingsverantwoordelijke.

3.6 Verwerker zal haar redelijke medewerking verlenen aan de verplichtingen van de Verwerkingsverantwoordelijke om aan de verzoeken van een Betrokkene te voldoen met betrekking tot zijn / haar rechten zoals vermeld in de Data Protectie Wetgeving, zoals, maar niet beperkt tot, (i) Betrokkenen inzage te geven in hun Persoonsgegevens, (ii) Persoonsgegevens op verzoek van Betrokkenen te verwijderen of corrigeren, en/of (iii) aan te tonen dat Persoonsgegevens na een verzoek daartoe van een Betrokkene verwijderd of gecorrigeerd zijn, en/of (iv) op verzoek van een Betrokkene de Persoonsgegevens verstrekken die hij/zij aan de Verwerkingsverantwoordelijke heeft verstrekt en deze laatste aan Verwerker heeft verstrekt (v) en op verzoek van de Betrokkene deze gegevens doorzenden naar een andere Verwerkingsverantwoordelijke ("data-portabiliteit"). Als wordt verzocht om Persoonsgegevens terug te geven of een kopie van de Persoonsgegevens te verstrekken, zal Verwerker de Persoonsgegevens verstrekken in een gestructureerde, gebruikelijke en machine-leesbaar format.

3.7 Indien Verwerker een verzoek of bezwaar van een Betrokkene ontvangt, (zoals een verzoek om informatie, inzage, rectificatie, wissen van gegevens, verwerkingsbeperking, of overdracht van de Persoonsgegevens), stuurt Verwerker dat verzoek onmiddellijk door naar Verwerkingsverantwoordelijke.

3.8 Verwerker houdt een register bij van alle categorieën Verwerking(sactiviteiten) die namens Verwerkingsverantwoordelijke worden verricht in overeenstemming met de in de Data Protectie Wetgeving genoemde vereisten. Verwerker zal aan Verwerkingsverantwoordelijke alle relevante informatie terzake verstrekken.

3.9 De Verwerker zal de Verwerkingsverantwoordelijke ondersteunen bij het nakomen van de wettelijke informatieverplichtingen van een toezichthoudende autoriteit of Betrokkenen en zo nodig, indien het de technologie van Verwerker betreft, assistentie verlenen bij een Privacy Impact Assessment ("PIA"). Verwerkingsverantwoordelijke zal aan Verwerker de redelijke kosten vergoeden als gevolg van de assistentie.

3.10 Indiende Verwerkingsverantwoordelijke een specifiek verzoek krijgt van een Betrokkene of een Derde Partij (anders dan de Betrokkene, of andere personen die zijn goedgekeurd door de Verwerkingsverantwoordelijke of de Verwerker om Persoonsgegevens te verwerken), die bevoegd is om zo'n verzoek te doen, zal Verwerker Verwerkersverantwoordelijke ondersteunen. Verwerker zal niets doen met betrekking tot ieder verzoek van een betrokkenen of een derde partij (anders dan de Betrokkene, of andere personen die zijn goedgekeurd door de Verwerkingsverantwoordelijke of de Verwerker om Persoonsgegevens te verwerken), behalve indien dat in overeenstemming is met vooraf gegeven instructies van Verwerkingsverantwoordelijke. Indien een Betrokkene contact opneemt met Verwerker omtrent zijn aanspraken met betrekkingtot de Data Protectie Wetgevingzal Verwerker dit verzoek doorsturen aan Verwerkingsverantwoordelijke.

4. VERANTWOORDELIJKHEDEN VERWERKINGSVERANTWOORDELIJKE

4.1 Verwerkingsverantwoordelijke is verantwoordelijk voor de rechtmatigheid van de Verwerking, de naleving van de wettelijke voorschriften inzake de bescherming van Persoonsgegevens, inclusief, maar niet beperkt tot, de bescherming van de rechten van de Betrokkenen.

4.2 Alleen Verwerkingsverantwoordelijke is verantwoordelijk voor het vaststellen van het doel en de middelen van de Verwerking van de Persoonsgegevens.

4.3 Verwerkingsverantwoordelijke is verantwoordelijk voor het informeren van de Betrokkenen en het waarborgen van de rechten die Betrokkenen op basis van de Data Protectie Wetgeving en andere toepasselijke privacywet- en regelgeving kunnen uitoefenen, en voor de communicatie met Betrokkenen.

4.4 Verwerkingsverantwoordelijke garandeert dat de Persoonsgegevens correct, ter zake dienend en niet bovenmatig zijn in het licht van de doeleinden waarvoor de Persoonsgegevens (verder) worden Verwerkt.

4.5 Verwerkingsverantwoordelijk zal onmiddellijk Verwerker informeren over fouten of onregelmatigheden met betrekking tot de Verwerking.

4.6 De Verwerkingsverantwoordelijke is verplicht om alle informatie die de Verwerker nodig heeft voor de Verwerking, tijdig beschikbaar te stellen, in het format zoals opgenomen in Bijlage 1.

4.7 Verwerkingsverantwoordelijke is verantwoordelijk en aansprakelijk voor (zowel tussen Partijen, als jegens Betrokkenen en de Data Protectie Autoriteit) voor: (i) ervoor zorg te dragen dat Betrokkenen toestemming hebben gegeven voor het verwerken van Persoonsgegevens door de Verwerker (of Sub-Verwerker); en (ii) iedere claim of klacht voortkomend uit de handelingen van Verwerker voor zover die handelingen het gevolg zijn van de instructies van de Verwerkingsverantwoordelijke.

5. SUB-VERWERKERS

5.1 Verwerker zal geen Sub-Verwerkers inschakelen zonder voorafgaande toestemming van Verwerkingsverantwoordelijke. Bij ondertekening van de Overeenkomst heeft Verwerkingsverantwoordelijke toestemming gegeven voor het inschakelen van de Sub-Verwerker(s) zoals aangegeven in Bijlage 3.

5.2 Verwerker zal Verwerkingsverantwoordelijke schriftelijk informeren over voorgenomen wijzigingen, bijvoorbeeld over het vervangen van een Sub-Verwerker. De Verwerkingsverantwoordelijke heeft de mogelijkheid om schriftelijk bezwaar te maken, binnen 7 dagen na schriftelijke kennisgeving hiervan, tegen dergelijke wijzigingen.

5.3 De inschakeling van een Sub-Verwerker beïnvloedt op geen enkele wijze de verplichtingen van Verwerker ten opzichte van de Verwerkingsverantwoordelijke. Toegang tot de relevante Persoonsgegevens mag alleen worden toegekend wanneer de Sub-Verwerker voldoet aan de van toepassing zijnde verplichtingen van deze Verwerkingsvoorwaarden. Verwerker zal met de door haar ingeschakelde Sub-Verwerkers een overeenkomst sluiten die in overeenstemming is met de relevante wet- en regelgeving en deze Verwerkingsvoorwaarden.

5.4 In Bijlage 3 staat een geactualiseerde lijst met de relevante gegevens over de Sub-Verwerkers, de verwerkingsplaats en de beschrijving van de werkzaamheden. Partijen zullen deze Bijlage, indien nodig, gedurende de looptijd van de Overeenkomst steeds aanpassen.

5.5 Indien sprake is van een door Verwerkingsverantwoordelijke goedgekeurde Sub-Verwerker, en de Sub-Verwerker zijn verplichtingen niet nakomt, blijft de Verwerker verantwoordelijk voor de uitvoering van de verplichtingen van die Sub-Verwerker.

5.6 Indien sprake is van een door Verwerkingsverantwoordelijke goedgekeurde Sub-Verwerker, mag de Verwerkingsverantwoordelijke (in sommige gevallen) instructies geven aan de Sub-Verwerker met betrekking tot de Verwerking van diens Persoonsgegevens door de Sub-Verwerker. In dat geval zal Verwerker niet verantwoordelijk zijn voor een schending van deze Verwerkingsvoorwaarden indien die schending voortkomt uit handelingen van de Sub-Verwerker die handelt op grond van instructies van de Verwerkingsverantwoordelijke, al dan niet met wetenschap daarvan van de Verwerker.

6. BEVEILIGING EN DATALEKKEN

6.1 Verwerker zal de technische en organisatorische beveiligingsmaatregelen - die voldoen aan de Data Protectie Wetgeving en de stand der techniek, - treffen die nodig zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van Persoonsgegevens te waarborgen en te beveiligen tegen verlies of onrechtmatige Verwerking. Om hieraan te kunnen voldoen zal Verwerkingsverantwoordelijke Verwerker informeren over de betrouwbaarheidseisen die op de Verwerking van toepassing zijn en tijdig de benodigde informatie verstrekken in geval van wijzigingen in de Verwerking van Persoonsgegevens.

6.2 De technische en organisatorische beveiligingsmaatregelen zullen steeds zijn beschreven in Bijlage 2 en zullen voldoen aan de daarvoor geldende algemeen geaccepteerde beveiligingsstandaarden. Verwerkingsverantwoordelijke erkent dat zij de in Bijlage 2 opgenomen afspraken voldoende acht voor een passende beveiliging van de Persoonsgegevens in overeenstemming met de Data Protectie Wetgeving.

6.3 De Verwerker zal de Verwerkingsverantwoordelijke onverwijld, zonder onnodige vertraging, in kennis stellen nadat zij zich bewust is van een Datalek.

6.4 De kennisgeving als genoemd in artikel 6.3 hiervoor zal ten minste omvatten:

1) de aard van het Datalek, waar mogelijk, de categorieën en bij benadering het benaderde aantal Betrokkenen en de categorieën en het bijbehorende aantal betrokken Persoonsgegevens;

2). de naam en contactgegevens van de Data Protection Officer of ander contactpunt waar meer informatie kan worden verkregen;

3) een beschrijving van de waarschijnlijke gevolgen van het Datalek;

4) de door de Verwerker genomen maatregelen of voorstellen om het Datalek aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige effecten ervan te beperken.

6.5 De Verwerker zal de Verwerkingsverantwoordelijke ondersteunen bij het nakomen van de wettelijke informatieverplichtingen van een toezichthoudende autoriteit of Betrokkenen, bij Datalekken.

6.6 Verwerker zal Verwerkingsverantwoordelijke onmiddellijk informeren indien de Verwerker van mening is dat een instructie tot Verwerking, gegeven door Verwerkingsverantwoordelijke in strijd is met de Data Protectie Wetgeving.

7. AANVULLENDE BEPLALINGEN GEHEIMHOUDING

7.1 Verwerker houdt de Persoonsgegevens die zij Verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal alle nodige maatregelen treffen om geheimhouding van de Persoonsgegevens te verzekeren. Verwerker zal de verplichting tot geheimhouding tevens opleggen aan haar personeel en alle door haar ingeschakelde personen die toegang hebben tot Persoonsgegevens.

7.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien Verwerkingsverantwoordelijke uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een derde partij te verstrekken, of een wettelijke verplichting of rechterlijk bevel bestaat om de Persoonsgegevens aan een derde partij te verstrekken.

8. AUDITS

8.1 Verwerker stelt Verwerkingsverantwoordelijke in staat om de naleving door Verwerker van de in deze Verwerkingsvoorwaarden genoemde verplichtingen te controleren of te laten controleren door onafhankelijke auditors, op kosten van Verwerkingsverantwoordelijke, zonder vertrouwelijke gegevens van Verwerker te gebruiken en in te zien en zonder de werkprocessen van Verwerker te verstoren. Als uit de controle blijkt dat Verwerker niet volledig voldoet aan haar verplichtingen, zal Verwerker de door de controle aangetoonde tekortkomingen zo spoedig als redelijkerwijs mogelijk beëindigen en/of herstellen. In zo een geval zal Verwerker ook de redelijke daadwerkelijk aantoonbaar gemaakte kosten van de audit dragen (waarbij betaling alleen zal worden gedaan in het geval van een echte nota van de auditor met betrekking tot die kosten).

8.2 De controle zal ten hoogste eenmaal per jaar plaatsvinden, tenzij Verwerkingsverantwoordelijke redelijkerwijs aanwijzingen heeft dat Verwerker haar verplichtingen op grond van deze Verwerkingsvoorwaarden niet nakomt. Verwerker zal Verwerkingsverantwoordelijke alle gegevens en informatie verstrekken die deze redelijkerwijs nodig heeft voor de controle.

8.3 In geval van een onderzoek door de Data Protectie Autoriteit of een andere bevoegde autoriteit zal Verwerker alle redelijke medewerking verlenen en Verwerkingsverantwoordelijke zo snel mogelijk informeren.

8.4 De Verwerker zal een persoon aanwijzen die fungeert als contactpersoon, die de Verwerkingsverantwoordelijke bijstaat bij het vervullen van verplichtingen tot openbaarmaking voortkomend uit de Verwerking en de Verwerker zal de Verwerkingsverantwoordelijke informeren over de contactgegevens van de contactpersoon.

9. WIJZIGINGEN

9.1 Verwerker zal ingeval van wijzigingen in verplichtingen onder de Overeenkomst die mogelijk gevolgen hebben voor de Verwerkingen, een bericht aan Verwerkingsverantwoordelijke sturen met de voorgestelde wijzigingen van deze Verwerkingsvoorwaarden. De Verwerkingsverantwoordelijke zal eventuele bezwaren daartegen binnen 10 Werkdagen na de ontvangst van het bericht doorgeven, en indien de Verwerkingsverantwoordelijke geen bezwaar kenbaar maakt, zal de Verwerkingsverantwoordelijke geacht worden de wijzigingen te hebben aanvaard.

9.2 Verwerker mag wijzigingen in de bijlagen maken, waarover de Verwerkingsverantwoordelijke zal worden geïnformeerd (hetgeen ook mag per elektronische mail), onder vermelding van het versienummer en de datum van ingang van de nieuwe versie. Materiele wijzigingen op de bijlagen zullen niet worden gedaan zonder de Verwerkingsverantwoordelijke de gelegenheid te geven daartegen bezwaar te maken.

10. AANSPRAKELIJKHEID

10.1 Verwerker vrijwaart Verwerkingsverantwoordelijke voor boetes en/of dwangsommen van of namens de AP die aan Verwerkingsverantwoordelijke worden opgelegd en voor aanspraken voor schade van een Betrokkene(n), indien vast is komen te staan dat deze boetes en/of dwangsommen dan wel aanspraken het gevolg zijn van het door de Verwerker bij de Verwerking niet voldoen aan de specifiek tot de Verwerker

gerichte verplichtingen van de Data Protectie Wetgeving of andere van toepassing zijnde privacywetgeving.

Om een beroep te kunnen doen op deze vrijwaring is Verwerkingsverantwoordelijke gehouden om:

i. Verwerker onverwijld schriftelijk te informeren over het bestaan en de inhoud van een aanspraak van een Betrokkene of van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van de Data Protectie Autoriteit tot het opleggen van een boete of last onder dwangsom;
ii. in samenspraak met Verwerker te handelen en te communiceren richting de Data Protectie Autoriteit dan wel betreffende Betrokkene;
iii. tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is; en
iv. de afhandeling van de zaak, waaronder het treffen van eventuele schikkingen, geheel overlaat aan Verwerker. Verwerkingsverantwoordelijke zal daartoe de nodige volmachten, informatie en medewerking aan Verwerker verlenen om zich, indien nodig in naam van Verwerkingsverantwoordelijke, tegen deze rechtsvorderingen te verweren.

10.2 Verwerkingsverantwoordelijke vrijwaart Verwerker voor boetes en/of dwangsommen van of namens de Data Protectie Autoriteit die aan Verwerker worden opgelegd en voor aanspraken voor schade van een Betrokkenen(n), indien vast is komen te staan dat deze boetes en/of dwangsommen dan wel aanspraken het gevolg zijn van het door de Verwerkingsverantwoordelijk bij de Verwerking niet voldoen aan de specifiek tot de Verwerkingsverantwoordelijke gerichte verplichtingen van de Data Protectie Wetgeving of andere van toepassing zijnde privacywetgeving.

Om een beroep te kunnen doen op deze vrijwaring is Verwerker gehouden om:

i. Verwerkingsverantwoordelijke onverwijld schriftelijk te informeren over het bestaan en de inhoud van een aanspraak van een Betrokkene of van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van de Data Protectie Autoriteit tot het opleggen van een boete of last onder dwangsom;
ii. in samenspraak met Verwerkingsverantwoordelijke te handelen en te communiceren richting de toezichthouder dan wel betreffende Betrokkene;
iii. tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is;
iv. de afhandeling van de zaak, waaronder het treffen van eventuele schikkingen, geheel overlaat aan Verwerkingsverantwoordelijke. Verwerker zal daartoe de nodige volmachten, informatie en medewerking aan Verwerkingsverantwoordelijke verlenen om zich, indien nodig in naam van Verwerker, tegen deze rechtsvorderingen te verweren.

10.3 Voor zover Partijen hoofdelijk aansprakelijk zijn jegens derde partijen, waaronder begrepen Betrokkene(n), of gezamenlijk een boete opgelegd krijgen door de Data Protectie Autoriteit, blijven de Partijen verantwoordelijk om elkaar te vrijwaren op grond van de artikelen 10.1 en 10.2, en is ieder voor het gedeelte van de schuld dat haar in onderlinge verhouding aangaat, verplicht in de schuld en kosten bij te dragen, waarbij rekening wordt gehouden met enige uitspraak van een rechtbank of bevoegd tribunaal, de Data Protectie Autoriteit en de bijdrage van iedere Partij in de niet-nakoming van de verplichtingen onder deze Verwerkingsvoorwaarden.

11. LOOPTIJD EN BEËINDIGING

11.1 Deze Verwerkingsvoorwaarden zijn van toepassing met ingang van de datum van de Overeenkomst.

11.2 Indien en zodra de Overeenkomst eindigt, zal Verwerker de documenten, computerschijven en andere gegevensdragers met daarop de Persoonsgegevens aan Verwerkingsverantwoordelijke retourneren of op verzoek van Verwerkingsverantwoordelijke vernietigen of bewaren zoals aangegeven in Bijlage 1. Voor zover de Persoonsgegevens zijn opgenomen in een computersysteem of in een andere vorm waardoor deze redelijkerwijs niet kunnen worden teruggegeven, zal Verwerker de Persoonsgegevens zoals opgenomen in haar systemen, vernietigen of anonimiseren tenzij Partijen schriftelijk anders overeenkomen.

BIJLAGEN

Bijlage 1	Beschrijving Verwerking Persoonsgegevens
Bijlage 2	Beveiligingsmaatregelen
Bijlage 3	Sub-Verwerkers
Bijlage 4	EU-Standard Contractual Clauses (“EU-SCC”)

BIJLAGE 1 BESCHRIJVING VAN DE VERWERKING PERSOONSGEGEVENS

Persoonsgegevens die zullen worden verwerkt:

Product	Persoonsgegevens die verwerkt kunnen worden omvatten:	Aan wie deze kunnen toebehoren
Unit4 Business World	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 Financials	Naam, adres, contact gegevens, telefoonnummer (inclusief mobiel nummer), email adres(sen), andere contact gegevens, geboortedatum, geboorte plaats, nationaliteit, domilicie, 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	• 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

	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, allergieen, medische aandoeningen), verzekeringsgegevens, en gezondheidsgegevens..	• Huidige, voormalige en toekomstige studenten.
Unit4 prevero	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 • Ieder lid van van een projectteam (inclusief niet-werknemers) • Sollicitanten of toekomstige werknemers • De contactgegevens van de klanten van Klanten en leveranciersgegevens.
Unit4 Intuo	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	• Huidige en voormalige werknemers • Huidige en voormalige sollicitanten; • Contractors of sub-contractors (van welke soort dan ook), agenten of directors, en

	perform module: check in gegevens; OKR gegevens; feedback en beoordeling. Door gebruik te maken van de Engage module: antwoorden en feedback op engagement vragen.	• Sollicitanten of toekomstige werknemers.
People Platform Services ("**PPS**") (iin het algemeen inclusief) IDS en Wanda (samen met iedere support service)	Omdat de PPS services zijn die werken met, en een interface hebben met, de andere Unit4 Producten, kunnen deze allerlei soorten Persoonsgevens verwerken zoals opgenomen in deze tabel met betrekking tot de genoemde Producten en Services. Verder kan Wanda verwerken: Unit4Id (die de gebruiker van IDS indentificeert); ieder Persoonsgegeven dat door een gebruiker in de applicatie wordt ingevoerd, waarmee Wanda een connectie heeft (Zulke informatie wort 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).	Alle categorieen zoals opgenomen in deze tabel Afhankelijk van de applicatie of services waarmee Wanda een connectie heeft kan PPS mogelijk ieder Persoonsgeven verwerken, dat een Gebruiker invoert.

1. 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 deze Verwerkingsvoorwaarden, 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. Met betrekking tot en afhankelijk van het Product of Dienst, omvat de Verwerking het volgende:

Product	Aard en Doeleinden van de Verwerking

Unit4 Business World	Persoonsgegevens worden ingevoerd in Unit4 Business World 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:
	
	• Verwerken van reisverzoeken;
	• Verwerken van onkosten nota's;
	• Verwerken van tijdregistratie formulieren;
	• Verzuimregistratie;
	• Processen gerelateerd aan HR en salarisverwerking, zoals
	  ○ Salaris verwerking;
	  ○ Verwerken van tijdregistratie formulieren
	  ○ Verzuim management;
	  ○ Trainingen;
	  ○ Competentiemanagement;
	  ○ Salaris herzieningen;
	  ○ Verwerken van sollicitanten.
	• Verwerken van betalingen;
	• Facturatie;
	• Inkoop aanvragen
	• Planning van medewerkers en projecten.
	De Verwerking omvat:
	Product (software)
	Binnen Unit4 Business World 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 Business World. **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Global Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description of People Platform Services (zoals uiteengezet in de People Platform Service Description). • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Business World product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Service 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	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: • 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, zoals o Salaris verwerking; o Verwerken van tijd registratie formulieren o Verzuim management; o Trainingen; o Competentiemanagement; o Salaris herzieningen; o Beoordelingen o Verwerken van sollicitanten. De Verwerking omvat: **Product (software)** 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. **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description. • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Financials Producten te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Service 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	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: • 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. De Verwerking omvat: **Product (software)** 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. **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Global Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description of People Platform Services (zoals uiteengezet in de toepasselijke People Platform Service Description). • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Student Management Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Service 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 prevero	Persoonsgegevens worden in Unit4 prevero 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: • Budgeteren; • Financiele and andere rapportages; • Distributie van rapporten; • Goedkeuringsprocessen; • Personeels/projectplanning. De Verwerking omvat: **Product (software)** Binnen Unit4 prevero 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. **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description. • 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 Terms. • 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 Intuo	Persoonsgegevens worden in Unit4 Intuo 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:

	• Human capital management • Werknemers beoordelingsprocessen • Talent enablement • Kandidaten assessment • Leren • Feedback en beloning, en • Personeelsanalyses en engagement De Verwerking omvat: **Product (software)** Binnen Unit4 Intuo 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 **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Intuo Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Intuo Cloud Service Description. • 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 Service Voorwaardenpport. • 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 PSA Suite	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: • Automatiseren van een professionele services organisatie, inclusief financieel management en human resources management (HRM) • Tijd en project management • Geboekte uren en kosten met nota's • Het omzetten van opportunities 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 financiele data in andere oplossingen te integreren De Verwerking omvat: **Product (software)** 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. **Diensten** • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Global Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description of People Platform Services (zoals omschreven in de toepasselijke People Platfrom Description). • Toegang tot Persoonsgegevens om onderhoud en support op het Unit4 Assistance PSA Suite Product te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Service 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.

People Platform Services ("**PPS**") (in het algemeen) inclusief IDS en Wanda (samen met iedere support services)	Gegevens worden door PPS verwerkt om de doelen van de services te behalen, zoals omschreven in de toepasselijke Appendix G - Service Description op www.unit4.com/terms. 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. Taken kunnen omvatten: • Tijdformulieren invoeren • Uitgaven invoeren • Reisverzoeken • Salarisstrook verzoeken • Verzuim invoeren • Balance invoeren • Aankoop verzoeken De Verwerking omvat: **Product (software)** 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. **Diensten** • 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. uitgevoerd. • Verzenden en opslaan van Persoonsgegevens om aanvullend Unit4 Global Cloud Services te bieden zoals in detail uiteengezet in de Unit4 Global Cloud Service Description of People Platform Servies (zoals omschreven in de People Platform Services Description). • Toegang tot Persoonsgegevens om onderhoud en support op de Unit4 PPS te leveren en de Klant te ondersteunen in het werken met de oplossing zoals in detail uiteengezet in de Unit4 Service 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.

3. BESCHRIJVING VERWERKING(EN) EN MIDDELEN

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

Wijze van Verwerken	Omschrijving	Middelen
Global Cloud Services (Unit4 SaaS of Unit4 Managed Cloud)	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de Unit4 Global Cloud Servcie Description en de Solution Specific Service omschrijving.	Personeel Het Unit4 Global Cloud Services operations team heeft medewerkers in Polen, Zweden, Noorwegen, UK, US, Canada, Maleisie en Singapore. Deze medewerkers leveren de Unit4 Global Cloud Services. Middelen en Infrastructuur Unit4 gebruikt derde party hosting infrastructuur diensten om de Unit4 Global Cloud Services te leveren en gebruikt andere software systemen voor de werking en het management ervan. Zie voorts Bijlage 3.
Global Cloud Services – Intuo SaaS	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de Unit4 Intuo	Personeel Het Unit4 Intuo Cloud Services operations team heeft medewerkers voornamelijk in Belgie en enkele

	Cloud Service Description en de Solution Specific Service omschrijving	andere EEA landen. Deze medewerkers leveren de Unit4 Intuo SaaS Services. Middelen en Infrastructuur Unit4 gebruikt derde party hosting infrastructuur diensten om de Unit4 Intuo SaaS Services te leveren en gebruikt andere software systemen voor de werking en het management ervan. Zie voorts Bijlage 3.
Klantenservice	De Verwerker zal Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en in de Unit4 Service Voorwaarden.	Personeel De Unit4 Klantenservice heeft medewerkers in UK, Polen, Portugal, Norwegen, Duitsland, Zweden, US, Canada (en op andere locaties waar dat voor Unit4 nodig zou mogen zijn). Deze medewerkers leveren de Unit4 Klantenservice zoals vermeld in de SLA Middelen en Infrastructuur Unit4 gebruikt andere software systemen voor de werking en het management van deze diensten.
Professional Services 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.	Personeel Het Unit4 Professional Services team heeft medewerkers in vrijwel alle locaties waar Unit4 actief is, waaronder UK, Ierland, Polen, Portugal, Norwegen, 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. Middelen en Infrastructuur Unit4 gebruikt andere software systemen voor de werking en het management van deze diensten. .
Unit4 Professionele Diensten (indien aan een partner uitbesteed)	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. De Verwerker sluit een Sub-verwerkingsovereenkomst met de Sub-verwerker, overeenkomstig de relevante bepalingen in deze Verwerkingsvoorwaarden. De Verwerkingsverantwoordelijke heeft door het ondertekenen van deze Overeenkomst aan de Verwerker toestemming gegeven om de betrokken Sub-verwerker zoals vermeld in Bijlage 3 bij de uitvoering van de Overeenkomst te betrekken	Zie Bijlage 3.
Derde Partij Producten en Diensten	De Verwerker en diens sub-verwerkers zullen de voornoemde Persoonsgegevens Verwerken ten behoeve van de activiteiten als beschreven in de Overeenkomst en	Zie Bijlage 3 en elke aanvullende regeling in andere schedules of Bjjlagen bij deze Verwerkingsvoorwaarden indien

	Derde contractuele en service voorwaarden met betrekking tot de software of diensten van de Derde Partij die als deel van de Overeenkomst zijn geleverd	vereist door de Derde Partij of toepasselijke wetgeving
People Platform Services ("**PPS**") (in het algemeen) inclusief IDS en Wanda (samen met elke supporting service)	In aanvulling op de "Global Cloud Services", zal PPS (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.	<u>Personeel</u> Het Unit4 Global Cloud Services operations team dat de PPS uitvoert heeft medewerkers in Polen, Zweden, Noorwegen, UK, US, Canada, Maleisie en Singapore. Deze medewerkers leveren de Unit4 Global Cloud Services. <u>Middelen en Infrastructuur</u> Unit4 gebruikt haar eigen infrastructuur en de (shared) infrastructuur van derde partijen om de Unit4 People Platform Services te leveren. Dit omvat 3rd partij systemen (i.e. collaboration apps), waar Unit4 geen controle over heeft. PPS inclusief Wanda maakt gebruik van een aantal Microsoft producten en services, als volgt: • Cognitive services: o LUIS Cognitive Service - *language understanding.* o Text Translator API – *translating text* o QnA Maker Cognitive service – *provides a questions and answers service* • Bot framework connectors – *provides for the connection of Wanda to the supported social channels*. • Traffic manager – *used for disaster recovery and failover if the primary region is unhealthy* • Web apps / web jobs – *hosts web APIs and long running web-based processes* • Service bus – *provides internal communication in the Wanda ecosystem* • Storage accounts – *used to store conversation state and user settings* • Cosmos DB –*provides storage* • Key vault – *stores confidential data that is used to communicate with Microsoft services and for internal services* • Redis cache – *provides caching capabilities* • Application Insights – *Monitoring of system, includes telemetry and logging* • *SQL server – provides storage* • Kubernetes – *open source container* Verdere informatie en details met betrekking tot die Microsoft producten en services kunnen worden gevonden

		op: https://azure.microsoft.com/en-us/services/.

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 Global Cloud Services	Unit4 Global 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**	**Naam**
	Managed Cloud	Benelux	Amsterdam / Ede	Digital Reality / Bit
	Managed Cloud	Sweden	Stockholm	Sungard
	Managed Cloud	UK (Wales)	Newport	NGD
	Managed Cloud	UK (England)	London	Digital Reality
	Managed Cloud	US	Multiple locations	Amazon Web Services (AWS)
	Managed Cloud	Canada	Toronto	IBM Softlayer
	SaaS/Managed Cloud	EU	Dublin / Amsterdam	Microsoft Azure
	SaaS/Managed Cloud	USA	Multiple locations	Microsoft Azure
	SaaS/Managed Cloud	Canada	Toronto / Quebec City	Microsoft Azure
	SaaS/Managed Cloud	United Kingdom	London / Cardiff	Microsoft Azure
	SaaS/Managed Cloud	Asia	Singapore / Hong Kong	Microsoft Azure
	SaaS/Managed Cloud	Australia	Victoria / New South Wales	Microsoft Azure

<table>
<tr><td>Product – Global Cloud Services – Intuo SaaS</td><td colspan="4">Intuo SaaS werkt in het Amazon Web Services (AWS) datacenter in Frankfurt. Alle Klantgegevens, behalve indien er wordt gedeeld met geselecteerde sub-processors uit Bijlage 3, zullen alleen in de geo-politieke zone worden opgeslagen, en niet daarbuiten worden verplaatst zonder de expliciete toestemming van de klant.</td></tr>
<tr><td>Unit4 Service – Standard Support andere standaard ondersteunings diensten</td><td colspan="4">Unit4 Service gebruikt SalesForce om Cases te registreren en verwerken. Deze Cases zijn toegankelijk voor iedere Unit4 medewerker die toegang tot SalesForce 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.

<table><tr><td>Klant Locatie</td><td>Primaire Support wordt verzorgd vanuit:</td></tr><tr><td>United Kingdom and Ireland</td><td>United Kingdom, Ireland, Portugal and Poland.</td></tr><tr><td>Sweden, Norway, Denmark, Finland and Iceland</td><td>Poland, Portugal, Norway and Sweden.</td></tr><tr><td>US & Canada</td><td>Poland, Portugal, US and Canada.</td></tr><tr><td>Europe rest</td><td>Poland, Portugal and Germany.</td></tr><tr><td>APAC</td><td>Poland, Portugal and Singapore/ Malaysia.</td></tr></table></td></tr>
<tr><td>Unit4 Support – 24/7 Support

(Enhanced en Premium Support)</td><td colspan="4">Door de ‘follow the sun’ methodologie te volgen, kan 24/7 support van Klant Cases plaatsvinden in elk van de ondersteuningslocaties zoals hierboven vermeld.</td></tr>
<tr><td>Unit4 Support – EU Only Support</td><td colspan="4">Indien EU Only support is gekozen, worden Cases alleen in behandeling genomen door de EU locaties voor standaard support als hierboven vermeld (gedurende Kantoortijden).</td></tr>
<tr><td>People platform services (“PPS”) (in het algemeen) inclusief IDS en Wanda (samen met iedere andere supporting services)</td><td colspan="4">PPS zijn cloud services 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.

<table><tr><td>Dienst</td><td>Geo-politieke Zone</td><td>Waar de Dienst Persoonsgevens Verwerkt of opslaat</td><td>Primarily Support wordt geleverd uit:</td></tr><tr><td>Wanda</td><td>Alle</td><td>Voornamelijk in de EU, maar kan elders zijn</td><td>Ierland, United States, en andere Global support indien vereist</td></tr><tr><td>IDS</td><td>Afhankelijk van Cloud deployment</td><td>Zoals hiervoor genoemd voor Global Cloud Service</td><td>Zoals hiervoor genoemd voor Global Cloud Service</td></tr></table></td></tr>
<tr><td>Unit4 Professionele Diensten en Unit4 customer success functie</td><td colspan="4"><table><tr><td>Onderwerp</td><td>Professionele Diensten en customer success worden geleverd door:</td></tr><tr><td>Implementatie en andere project diensten</td><td>In het Land of de Klant locatie of de overeengekomen locatie en/of in Portugal,</td></tr></table></td></tr>
</table>

		afhankelijk wat tussen Partijen is overeen gekomen 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 overeen gekomen 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 Verwerkingsvoorwaarden is de contactpersoon:

Voor Verwerkingsverantwoordelijke: Door een brief (geadresseerd aan Global Data Privacy Officer; Postbus 5005, 3528 BJ Utrecht, Nederland of email privacy@unit4.com of aan het Unit4 adres zoals aangegeven in de Overeenkomst.

Voor Verwerker: Het adres van Verwerkingsverantwoordelijke zoals aangeven in de Overeenkomst

Bijlage 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 Bijlage 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 beveiligingssystemen 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 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 Verwerkingssystemen 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.

Beveiligingspolicies 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 Global Information Security Manager en de Global Data Privacy Officer, die middelen beheren voor het leveren van strategische en algehele naleving van het informatiebeveiligingsbeleid en -proces.

• Unit4 heeft beveiligingsbeleid geimplementeerd 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/about.

• 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 Global Cloud Services 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 Global Cloud Services:

Gegevensbescherming

Unit4 Global 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.

• Back-ups worden gecodeerd met behulp van volledige database-coderingstechnologie, zoals transparante database-encryptie. Azure Storage Service Encryption om alle gegevens te versleutelen die in de opslagaccount van een klant zijn geplaatst.

• 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 Global Cloud-operatieteam dat de Global 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.

Netwerkisolatie op verschillende punten:

• Elke specifieke implementatie is geïsoleerd van andere implementaties en communiceert via privé IP-adressen.

• Klant-VM's kunnen alleen communiceren met andere VM's die eigendom zijn van of worden beheerd door dezelfde klant en met infrastructuurservicepuntpunten die bedoeld zijn voor openbare communicatie.

• Verkeer tussen VM's loopt altijd door vertrouwde pakketfilters.

Meer informatie over het beveiligingsbeleid en het beveiligingsprogramma is te vinden op www.unit4.com/about.

Data encryptie

Unit4 biedt standaard toegang tot alle diensten door alle gegevens in transit die op openbare netwerken worden vestruurd te versleutelen. Dit gebeurt door alleen beveiligde protocollen te gebruiken, zoals HTTPS over TLS, met behulp van de nieuwste beveiligingscodes. Versleuteling van gegevens in rust kan optioneel door de klanten worden besteld. 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-endtoegang tot klantgegevens (via directe databaseverbinding). Toegang door Unit4 tot persoonlijke informatie 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 toegangslog 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.

Als bewijs van veilig ontwerp en operationele activiteiten, heeft SaaS Ops van Unit4 Global Cloud Services de ISO 27001: 2013-certificering en ISAE3402 (SOC1) -rapport. Unit4 en de exploitanten van datacenters hebben verschillende beveiligingscertificaten, voor meer informatie verwijzen wij u naar de Global Cloud Service Description.

Extra elementen voor Unit4 People Platform Services (samenvatting)

Beschrijving van de technische en organisatorische beveiligingsmaatregelen door Verwerker geimplementeerd 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 networken – alle verkeer is beveiligd door gebruikmaking industry standard protocols zoals SSL/TLS (1.2) 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 date 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.

Extra elementen voor Unit4 Global Cloud Service – Intuo SaaS (samenvatting)

Intuo Saas is ISO27001 gecertificeerd en heeft een ISO27001 (fase 1&2) ondergaan en een GDPR audit. De meest relevante informatie is in de tabel beschreven en extra documentatie of informatie is op verzoek beschikbaar.

Domain	Practices
Information Security Management and Governance	De Intuo SaaS Service heeft een Information Security Management System (ISMS) onder ISO27001 geimplementeerd. Dit bevat, maar niet gelimiteerd tot, een information security policy voor alle werknemers. De policy kan op verzoek worden verstrekt. Ook zijn, voor informatiebeveiliging, management maatregelen geimplementeerd, die de risico's verminderen. Deze risico's en de waarschijnlijkheid dat deze zich verwezenlijken, zijn begrepen in ISO27001 ISMS.
Human Resources Security	De levering van Intuo SaaS Service zorgt ervoor dat alle vertrouwelijke informatie worden gehouden in een HRIS en aan ISO27001 voldoen, waarvoor de information security afdeling verantwoordelijk is.
Asset Management	Assets (zowel digitaal en niet-digitaal) worden gehouden onder een data classificatie policy
Information Access Control	Er zijn verschillende policies die werken met het principe van least privilege, zowel voor geleverde applicaties, algemene informatie en eigen data. Toegang tot eigen systemen, gehost door Amazon (AWS), is beperkt tot specifiek geindentificeerde personen en het gebruik van passwoorden is uitdrukkelijk verboden. Alleen publieke/prive sleutelparen worden gebruikt om te authenticeren met servers. De toegangsrechten per gebruiker worden bepaald in overeenstemming de vastgestelde toegangspolicy. Specifieke vragen over toegang tot informatie en de policies kunnen worden gesteld aan information security.
Operations Security	Dit valt onder de scope van onze ISMS (ISO27001).
Communications Security	Alle communicatie valt onder een data classificatie policy. Al het netwerk verkeer loopt over SSL/HTTPS, het meest gebruikelijke en vertrouwde communicatie protocol op het Internet. Interne infrastructuur wordt geisoleerd door gebruikmaking van strikte firewalls en netwerk toegangslijsten. Elk system is ontworpen voor een firewall security groep door diens functie. Standaard wordt alle toegang geweigerd en alleen uitdrukkelijk toegestane ports worden opengesteld. Persistence en storage lagen zijn versleuteld (ook in rust) en beveiligd achter VPN & VPC firewalls. Kantoren gebruiken een netwerk dat is beschermd door een redundant Fortinet 200D Firewall, dat in het datacenter in Merelbeke is geplaatst, verbonden aan de Ghelamco Arena via Dark Fiber. Meer informatie over deze verbinding wordt gegeven in het document "Continuity and Security measures", ook onderdeel van ISMS of the ISO27001 certification.

BIJLAGE 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 Cloud Services
Unit4 Global Cloud Services	Microsoft Azure	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure and Services
	Microsoft Dynamics	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Software Services, in het bijzonder Microsoft Dynamics (en cloud infrastructure).
	Microsoft	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van software tooling en Office
	Sungard	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	Digital Realty	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	Amazon Web Services	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	Bit Data Center	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	IBM Softlayer	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services
	NGD	Zoals vermeld in Bijlage 1, paragraaf 5.	Verlenen van Cloud Infrastructure en Services

Unit4 Global Cloud Services – Intuo SaaS	Amazon Web Services	Frankfurt, Germany	Providing solution - Suite
	Freshdesk	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	LogDNA	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Mandrill	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)

	Mixpanel	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Pingdom	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Productboard	European Economic Area and United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Providing solution - Learn (SCORM only) (privacy shield link: Link)
	Sentry	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Slack	United States of America (Privacy Policy)	Providing solution – Perform (privacy shield link: Link)
	Skylight	United States of America (Privacy Policy)	Providing solution – Suite
	Stripe	Countries in which Stripe operates (Privacy Policy)	Providing solution – Learn (privacy shield link: Link)
	Wistia	United States of America (Privacy Policy)	Providing solution – Learn (privacy shield link: Link)
People Platform Services ("**PPS**") (generally) including IDS and Wanda (together with any supporting services)	Microsoft Azure	Zoals vermeld hierboven in Bijlage 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 2.

BIJLAGE 4 – EU STANDARD CONTRACTUAL CLAUSES

Deze bijlage is van toepassing in het geval van verwerkingen door de Verwerker of Sub-Verwerker buiten de EER waarvoor de Europese Commissie geen besluit tot adequate beveiliging heeft gegeven.

Deze tabel bevat de informatie die benodigd is voor de EU Standard Contractual Clauses:

Parties	The data exporter is the Controller whose details appear in an Order Form (as Customer) in the Agreement between Controller and Processor. The data importer is the Processor whose details appear in an Order Form (as Customer) in the Agreement between Controller and Processor, which enters into these Standard Contractual Clauses on behalf of each of any Sub-Processors that are located in a country outside of the European Economic Area for which the European Commission has not issued an adequacy decision.
Clause 9 and 11(3)	The data exporter is based in the Territory specified in the Agreement.
Appendix 1	The information required to complete this Appendix is set out in Schedule 1 and Schedule 3 of these Data Processing Terms
Appendix 2	The information required to complete this Appendix is set out in Schedule 2 of these Data Processing Terms

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Parties
Name of the data exporting organisation: …
Address: …
Tel. …; fax …; e-mail: …
Other information needed to identify the organisation
…
(the data **exporter**)
And
Name of the data importing organisation: …
Address: …
Tel. …; fax …; e-mail: …
Other information needed to identify the organisation:
…
(the data **importer**)
each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]);

b) 'the data exporter' means the controller who transfers the personal data;

c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d) 'the sub-processor' means any data processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a controller in the Member State in which the data exporter is established;

f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing

services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer ([2])

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

   i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

   ii. any accidental or unauthorised access; and

   iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

4. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

    b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([3]). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

The parties agree that these Standard Contractual Clauses become binding on the entering into an order form for services between the parties, which form an agreement.

([1]) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

([2]) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

([3]) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):
See Schedule 1 of the Data Processing Terms (above).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):
See Schedule 1 of the Data Processing Terms (above).

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
See Schedule 1 of the Data Processing Terms (above).

Categories of data

The personal data transferred concern the following categories of data (please specify):
See Schedule 1 of the Data Processing Terms (above).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
See Schedule 1 of the Data Processing Terms (above).

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
See Schedule 1 of the Data Processing Terms (above).

Appendix 2

to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Schedule 2 of the Data Processing Terms (above).