Unit4 Information Om Personuppgiftsbehandling (Inklusive EUS Standardavtalsklausuler)

AVSNITT 1 – BESKRIVNING AV BEHANDLINGEN AV PERSONUPPGIFTER

1. PERSONUPPGIFTER SOM KOMMER ATT BEHANDLAS:

Produkt	De Personuppgifter som kan komma att behandlas kan inkludera:	Vem dessa Personuppgifter avser:
Unit4 ERP x	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; personnummer, nationellt försäkringsnummer, sjukförsäkringsnummer eller ID-kortsnummer; civilstånd; socialförsäkringsinformation för socialförsäkringar; kön; anställningsinformation (inklusive: lön; befattning; lönetrappa; lönesteg; erfarenheter och personliga anteckningar; skatteinformation; förmånspaket; medlemskap i fackförening; närmaste anhöriga (namn; adress; födelsedatum; telefonnummer, kontaktuppgifter i nödsituation); dag för anställnings början och upphörande; bankkonto eller kreditkortsuppgifter; uppgifter om enskild firma (namn; registreringsnummer och registreringskontor); styrelseuppdrag; mervärdesskatteregistreringar; dokument (skriftliga eller elektroniska) som innehåller någon av ovanstående information.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och • Arbetssökande och potentiella arbetstagare.
Unit4 ERP 7	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; personnummer, nationellt försäkringsnummer, sjukförsäkringsnummer eller ID-kortsnummer; civilstånd; socialförsäkringsinformation för socialförsäkringar; kön; anställningsinformation (inklusive: lön; befattning; lönetrappa; lönesteg; erfarenheter och personliga anteckningar; skatteinformation; förmånspaket; medlemskap i fackförening; närmaste anhöriga (namn; adress; födelsedatum; telefonnummer, kontaktuppgifter i nödsituation); dag för anställnings början och upphörande; bankkonto eller kreditkortsuppgifter; uppgifter om enskild firma (namn; registreringsnummer och registreringskontor); styrelseuppdrag; mervärdesskatteregistreringar; dokument (skriftliga eller elektroniska) som innehåller någon av ovanstående information.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och • Arbetssökande och potentiella arbetstagare.
Unit4 Financials	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; personnummer, nationellt försäkringsnummer, sjukförsäkringsnummer eller ID-kortsnummer; civilstånd; socialförsäkringsinformation för socialförsäkringar; kön; anställningsinformation (inklusive: lön; befattning; lönetrappa; lönesteg; erfarenheter och personliga anteckningar; skatteinformation; förmånspaket; medlemskap i fackförening; närmaste anhöriga (namn; adress; födelsedatum; telefonnummer, kontaktuppgifter i nödsituation); dag för anställnings början och upphörande; bankkonto eller kreditkortsuppgifter; uppgifter om enskild firma (namn; registreringsnummer och registreringskontor); styrelseuppdrag; mervärdesskatteregistreringar; dokument (skriftliga eller elektroniska) som innehåller någon av ovanstående information.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och • Arbetssökande och potentiella arbetstagare.
Unit4 Student Management	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; personnummer, nationellt försäkringsnummer, sjukförsäkringsnummer eller ID-kortsnummer; civilstånd; socialförsäkringsinformation för socialförsäkringar; kön; anställningsinformation (inklusive: lön; befattning; lönetrappa; lönesteg; erfarenheter och personliga anteckningar; skatteinformation; förmånspaket; medlemskap i fackförening; närmaste anhöriga (namn; adress; födelsedatum; telefonnummer, kontaktuppgifter i nödsituation); dag för anställnings början och upphörande; bankkonto eller kreditkortsuppgifter; uppgifter om enskild firma (namn; registreringsnummer och registreringskontor); styrelseuppdrag; mervärdesskatteregistreringar; dokument (skriftliga eller elektroniska) som innehåller någon av ovanstående information. Ytterligare Personuppgifter avseende före detta och nuvarande anställda: personaltyp (t.ex. fakultet, rådgivare, studenthemsföreståndare); akademisk avdelning; rekryteringsstatus; anställningsstatus; arbets-mängd; fakultetsranking; publikationer; mätning av arbetsstatus; utbildningsinformation och kvalificerings-information. Ytterligare Personuppgifter avseende före detta och nuvarande sökande: information om tidigare utbildning; betyg och/eller testresultat; fysisk hälsostatus; arbetsintyg från tidigare arbetsgivare; och arbetsplatsinformation. Ytterligare Personuppgifter avseende före detta och nuvarande studenter: akademiska meriter inklusive resultat och mål; inskrivningsinformation; information om akademisk utveckling (inklusive betyg); akademiska resultat; akademiska eller arbetsrelaterade placeringar; information om kursplanering; avgifts- och betalningshistorik; boendepreferenser och -historik; information om finansiellt stöd; hälsouppgifter (inklusive vaccinationer, allergier, medicinska tillstånd), försäkringsinformation och hälsodokumentation.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika slag), agenter eller befattnings-havare; • Arbetssökande och potentiella arbetstagare; och • Nuvarande, för detta, och potentiella studenter.
Unit4 FP&A	Namn; adresser; telefonnummer (inklusive mobiltelefonnummer); e-postadresser; annan kontaktinformation. Andra typer av Personuppgifter behöver inte lagras eller behandlas för att uppnå ändamålen med Produkten (enligt vad som anges nedan), men andra typer av Personuppgifter kan lagras eller behandlas av Produkten om den konfigurerats för att göra detta (exempelvis försäljningsinformation) eller om den läggs in i Produkten av Kunden.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare.
Unit4 Assistance PSA Suite	Namn; adresser; telefonnummer (inklusive mobiltelefonnummer); e-postadresser; annan kontaktinformation. Andra typer av Personuppgifter behöver inte lagras eller behandlas för att uppnå ändamålen med Produkten (enligt vad som anges nedan), men andra typer av Personuppgifter kan lagras eller behandlas av Produkten om den konfigurerats för att göra detta eller om den läggs in i Produkten av Kunden.	• Nuvarande och före detta anställda; • Konsulter och underkonsulter (av olika

		slag), agenter eller befattningshavare; • Varje person som är medlem av ett projektteam (inklusive icke-anställda) • Arbetssökande och potentiella arbetstagare; och • Kundens kontaktpersoner hos kunder och leverantörer
Unit4 Talent Management	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation (gatuadress och land); födelsedatum; arbetstitel; avdelning. Genom användning av Learn-modulen: deltagande i kurser; deltagande i sessioner; frågesportsresultat- och genomgång; data avseende videodeltagande; data avseende bilddeltagande; data avseende textdeltagande; utmärkelser; certifieringar. Genom att använda Perform-modulen: incheckningsdata, OKR (Objectives and Key Results) data; återkoppling och beröm. Genom att använda Engage-modulen: svar och återkoppling på frågor avseende engagemang.	• Nuvarande och före detta anställda; • Nuvarande och före detta jobbkandidater • Konsulter eller underkonsulter (av olika slag), agenter eller befattningshavare; och • Arbetssökande och potentiella arbetstagare.
People Platform Services (“**PPS**”), Lokaliseringstjänster och Appar	Eftersom PPS, Lokaliseringstjänster och Appar är tjänster som används tillsammans med, och har gränssnitt mot, Unit4s övriga Produkter och Tjänster, kan de Behandla alla typer av Personuppgifter som anges i denna tabell med avseende på angivna Produkter och Tjänster. Dessutom kan Wanda Behandla: Unit4Id (som identifierar en användare av IDS); alla typer av Personuppgifter eller information som en användare kan tillföra en programvara till vilken Wanda är kopplad (sådan information behandlas eller lagras såvida inte Användaren väljer att radera den); andra konversationer eller dialogdata; metadata som kan hänföras till en individ; och Application Insights Logs (en Microsoft tjänst som används för att utföra diagnostik.	Alla kategorier av personer som anges i denna tabell. Beroende på vilken programvara eller tjänst som Wanda är kopplad till, kan PPS potentiellt Behandla Personuppgifter avseende alla individer som en Användare väljer att införa.
Unit4 Property Management	Namn; adresser; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); webbsideadress; personnummer, nationellt försäkringsnummer, sjukförsäkringsnummer eller ID-kortsnummer; födelsedatum; kundidentitet; språk; markering om skyddad identitet; markering om dödsbo; mervärdesskattenummer; kontaktinformation (inklusive: titel/befattning, intressen); bankkontouppgifter; anställningsinformation (inklusive: arbetsgivare, adressuppgifter); ansökningsuppgifter (inklusive: yrke, årsinkomst, anställningsår, antal personer i hushållet, tidigare hyresvärd, bedömning av kreditbedömning, datum för kreditbedömning); ansökande och andra egenskaper (definierade av den Personuppgiftsansvarige; könummer; medlemskap (inklusive: medlemsnummer, status, startdag och slutdag för medlemskap, anledning till ansökan/avslut av medlemskap, första dag för anteckning om uppgifter, huvudmedlemskap, relaterade medlemskap, kö-/hyrespoäng, poäng för bostadssparande); roller/personkategorier; Användare (användar-ID, typ av användare, signatur); hyresavtal och uppgifter om hyrestagare och bostadsrättsinnehavare (inklusive: identitet på mottagare av e-faktura, information om autogirobetalare, borgensåtaganden, garantier); ärendehanteringsinformation; uppdragstagare (för utskick om uppdragsarbeten); anteckningar (som registreras av den Personuppgiftsansvarige); dokument (skrivna eller elektroniska) som innehåller något av ovanstående.	• Nuvarande och före detta anställda; • Uppdragstagare eller underleverantörer (av olika slag), agenter eller befattningshavare; • Arbetssökande och potentiella arbetstagare; och • konsumenter (exempelvis hyressökande, hyresgäster och bostadsrättsinnehavare) avseende förvaltningstjänster.

2. BEHANDLINGENS ART OCH ÄNDAMÅL

Generellt består Personuppgiftsbiträdets Behandling enbart av de åtgärder som är nödvändiga för att Personuppgiftsbiträdet ska utföra sina åtaganden och utöva sina rättigheter under Avtalet, inklusive (i förhållande till Personuppgifter) insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Ändamålet med Behandlingen är utförandet av Personuppgiftsbiträdets åtaganden och utövande av dess rättigheter under Avtalet, inklusive utförandet av funktioner som krävs eller begärs av den Personuppgiftsansvarige för att den Personuppgiftsansvarige ska uppfylla sina lagliga och/eller kontraktuella skyldigheter. Personuppgiftsbiträdet kommer också att Behandla Kundens Personuppgifter för att förbättra sina produkter och tjänster (exempelvis för produktförbättring genom artificiell intelligens, maskininlärning etc.) eller dataanalyser.

Med avseende på, och beroende av, respektive Produkt eller Tjänst, kommer Behandlingen att inkludera följande:

Produkt	Behandlingens art och ändamål
Unit4 ERP x	Personuppgifter kommer att registreras i Unit4 ERP 8 för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Reseansökningar; • Hantering av utlägg; • Behandling av tidrapporter; • Frånvarohantering; • HR & lönerelaterade processer: • Lön; • Inskrivning på kurser; • Kompetenshantering; • Omdömen; • Lönerevision; • Registrering av arbetssökande; • Genomförande av betalningar; • Fakturering; • Köprekvisitioner;

	• Personal/projektplanering. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 ERP 8 som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
Unit4 ERP 7	Personuppgifter kommer att registreras i Unit4 ERP 7 för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Reseansökningar; • Hantering av utlägg; • Behandling av tidrapporter; • Frånvarohantering; • HR & lönerelaterade processer: • Lön; • Inskrivning på kurser; • Kompetenshantering; • Omdömen; • Lönerevision; • Registrering av arbetssökande; • Genomförande av betalningar; • Fakturering; • Köprekvisitioner; • Personal/projektplanering. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 ERP 7 som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden. och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
Unit4 Financials	Personuppgifter kommer att registreras i Unit4 Financials för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Registrering av kunder/leverantörer/anställda; • Genomförande av betalningar; • Fakturering; • Hantering av utlägg; • Reseansökningar; • Köprekvisitioner och beställningar; • Personal/projektplanering; • HR & lönerelaterade processer: • Lön; • Behandling av tidrapporter; • Frånvarohantering; • Inskrivning på kurser; • Kompetenshantering; • Omdömen; • Lönerevision; • Registrering av arbetssökande. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 Financials som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt).

	Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4s Financials Produkt, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
Unit4 Student Management	Personuppgifter kommer att registreras i Unit4 Student Management för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Rekrytera potentiella studenter • Besvarande av förfrågningar om information • Behandling av ansökningar • Hantera den akademiska livscykeln för en student inklusive inledande aktiviteter, kursplanering, akademiska framsteg, rådgivning, boende och andra faciliteter, examen • Planera och schemalägga fakultetspersonal Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 Student Management som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
Unit4 FP&A	Personuppgifter kommer att registreras i FP&A för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Budget; • Finansiell och annan rapportering; • Distribution av rapporter; • Behandling av godkännanden; • Personal/projektplanering. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 FP&A som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
Unit4 Talent Management	Personuppgifter kommer att registreras i Unit4 Talent Management för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Hantering av humankapital • Hantering av arbetstagares prestationer • Talangutveckling • Utvärdering av kandidater • Utbildning • Återkoppling och beröm; • Personanalys och -engagemang Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 Talent Management som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.

Unit4 Assistance PSA Suite	Personuppgifter kommer att registreras i Unit4 Assistance PSA Suite för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • automatisering av en professionell tjänsteorganisation, inklusive finansiell och HR administration (HRM); • daglig tids- och projekthantering; • tidsbokning och utlägg med kvitton; • överflyttning av affärsmöjligheter till projekt, budgetar och estimerade timmar, och planering av projekt och resurser; • mätning av tid och utlägg och genomförande av fakturering; • integrering av projekt i andra applikationer; och • utförande av redovisning för assistans vid integration av finansiella data med andra lösningar. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Unit4 Assistance PSA Suite som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
People Platform Services (“**PPS**”), Lokaliseringstjänster och Appar	Personuppgifter kommer att behandlas av PPS, Lokaliseringstjänsterna och Apparna för att tillåta de angivna syftena med tjänsten enligt vad som anges i den tillämpliga Tjänstebeskrivningen för PPS på www.unit4.com/terms. Dessutom kommer Personuppgifter att införas i Wanda genom användning av valfri tredjepartsprogramvara (tex. Slack Integration, Facebook Messenger eller andra Microsoft applikationer (inklusive Microsoft Teams)). Beroende på vilken Unit4s Produkt eller Tjänst som används av Kunden, kan Wanda hjälpa till att färdigställa administrativa uppgifter för Kundens anställda. Uppgifterna kan innefatta: • Registrering av tidsposter • Registrering av utlägg • Reseansökningar • Förfrågningar om lönebesked • Registrering av frånvaro • Balansförfrågningar • Köprekvisitioner. Behandlingen kommer att involvera: **Produkt (programvarulösning)** Wanda som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt). Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 PPS, Lokaliseringstjänster och Appar, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden. Åtkomst till Personuppgifter för produktutveckling via AI maskininlärning eller dataanalys.
Unit4 Property Management	Personuppgifter kommer att registreras i Unit4 Property Management för att möjliggöra för Kunden att organisera och hantera processer som är relaterade till dess verksamhetsfunktioner och lednings- och/eller administrativa processer inom dess interna verksamhet. Processerna kan innefatta: • Registrering av sökande • Hantering av uthyrningar • Hantering av hyresavtal • Hantering av bostadsrättsinnehavare • Hantering av elektronisk avtalssignering • Fakturering inklusive fakturautskrifter • Hantering av betalningar • Hantering av indrivning av fordringar • Hyresförändringar **Produkt (programvarulösning)** Unit4 Property Management som exekverar programmerbar programvarukod för att tillse att de aktiviteter som anges ovan kan utföras. Detta kan involvera överföring av data till eller från tredjepartslösningar som inte är under Personuppgiftsbiträdets kontroll, genom integrationer. **Tjänster** Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Tjänster enligt vad som anges närmare i Tjänstebeskrivningen, eller i Tjänstebeskrivningen för People Platform (enligt vad som är tillämpligt).

	Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kundanpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.

3. BESKRIVNING AV BEHANDLINGEN OCH MEDLEN FÖR DENNA:

Personuppgiftsbiträdet ska Behandla Personuppgifterna i samband med följande aktiviteter (nedan aktiviteter omnämns som exempel endast):

Typ av Behandling	Beskrivning	Medel och resurser
Unit4 SaaS (Allmänt)	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i Unit4s Tjänstebeskrivningar.	Personal Unit4 Cloud Services Operations har personal i länder inom EU/EES (inklusive, men inte begränsat till Polen, Sverige, Norge, Nederländerna, Spanien och Portugal), Storbritannien, USA, Kanada, Malaysia och Singapore. Denna personal hos Personuppgiftsbiträdet driftar Unit4 SaaS. Tillgångar och infrastruktur Unit4 använder hostade infrastukturtjänster från tredje part för att tillhandahålla Unit4 SaaS, och nyttjar andra programvarusystem för drift och förvaltning. Se avsnitt 3.
U4 Talent Management SaaS	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i tillämplig Tjänstebeskrivning.	Personal Unit4s Talent Management Cloud Services Operations har personal huvudsakligen i Belgien och i vissa andra EU/EES-länder. Denna personal hos Personuppgiftsbiträdet driftar Unit4 Talent Management SaaS. Tillgångar och infrastruktur Unit4 använder hostade infrastukturtjänster från tredje part för att tillhandahålla Unit4 Talent Management SaaS, och nyttjar andra programvarusystem för drift och förvaltning. Se avsnitt 3.
Supporttjänster	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i Unit4s Supportvillkor.	Personal Unit4 Kundsupport har personal i länder inom EU/EES (inklusive, men inte begränsat till Polen, Sverige, Norge, Tyskland, Irland, Nederländerna, Spanien och Portugal), Storbritannien, USA, Kanada (och sådana andra platser som behövs för att stödja Unit4s affärsbehov). Denna personal hos Personuppgiftsbiträdet tillhandahåller Unit4s Supporttjänster (som anges i Unit4s Supportvillkor). Tillgångar och infrastruktur Unit4 nyttjar andra programvarusystem för drift, leverans och förvaltning av dessa tjänster.
Konsulttjänster	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i mer detaljerad projektdokumentation eller uppdragsbeskrivningar som överenskommes mellan Parterna när Projektet inleds.	Personal Unit4s konsultverksamhet har personal i alla länder där Unit4 har ett registrerat bolag, inklusive Storbritannien, Irland, Polen, Portugal, Norge, Spanien, Frankrike, Tyskland, Sverige, USA, Kanada, Malaysia och Singapore (och sådana andra platser som behövs för att stödja Unit4s affärsbehov. Denna personal hos Personuppgiftsbiträdet tillhandahåller Unit4s Konsulttjänster. Tillgångar och infrastruktur Unit4 nyttjar andra programvarusystem för drift, leverans och förvaltning av dessa tjänster.
Unit4 Konsulttjänster (om underkonsult anlitas)	Personuppgiftsbiträdet och dess Underbiträden ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och (om tillämpligt) tredje parts kontrakts- och tjänstedokumentation som tillhandahålls som en del av Avtalet. För ytterligare detaljer, se avsnitt 3. Personuppgiftsbiträdet ska ingå ett skriftligt avtal med Underbiträdet, som ska vara i enlighet med Dataskyddslagstiftningen och Avtalet. Vidare har den Personuppgiftsansvarige medgett att Personuppgiftsbiträdet anlitar de tillämpliga Underbiträden som finns angivna i avsnitt 3 genom att ingå Avtalet.	Se avsnitt 3 eller tillämpligt Orderformulär.
Tredjepartsprodukter och Tredjeparts-tjänster	Personuppgiftsbiträdet och dess Underbiträden ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och Tredjepartsleverantörens kontrakts- och tjänstedokumentation som tillhandahålls som en del av Avtalet.	Se avsnitt 3 eller tillämpligt Orderformulär, och eventuella kompletterande villkor i ytterligare bilagor till denna Information om Personuppgiftsbehandling, om detta krävs av Tredjepartsleverantören eller enligt Tillämplig Lag.
People Platform Services (“**PPS**”),	I tillägg till vad som anges för Unit4 SaaS, kommer PPS, Lokaliseringstjänster och Appar att (där så är tillämpligt) Behandla	Personal

Lokaliseringstjänster och Appar	Personuppgifter i enlighet med en integritetspolicy som presenteras för slutanvändaren, som ombeds lämna sitt samtycke, där sådana Personuppgifter Behandlas.	Unit4 Cloud Services Operations, som driftar PPS, Lokaliseringstjänster och/eller Appar, har personal i länder inom EU/EES (inklusive, men inte begränsat till Polen, Sverige, Norge, Nederländerna, Spanien och Portugal), Storbritannien, USA, Kanada, Malaysia och Singapore. Denna personal hos Personuppgiftsbiträdet driftar Unit4 SaaS.
		
		Tillgångar och infrastruktur
		
		Unit4 nyttjar sina egna och tredje parts (delade) infrastrukturtjänster för att tillhandahålla PPS, Lokaliseringstjänster och/eller Appar. Detta inkluderar tredjepartssystem (s.k. collaboration apps), över vilka Unit4 inte har någon kontroll. PPS, inklusive Wanda, Lokaliseringstjänster och/eller Appar, använder ett antal olika produkter och tjänster från Microsoft, enligt följande:
		
		• Kognitiva tjänster:
		  ○ LUIS Cognitive Service – språkförståelse
		  ○ Text Translator API –*textöversättning*
		  ○ QnA Maker Cognitive service – *tillhandahåller en frågor och svar-tjänst*
		• Bot ramverkskopplingar – tillhandahåller kopplingar mellan *Wanda och supporterade sociala kanaler*.
		• Traffic manager – *används för katastrofåterställning och reservsystem om den primära regionen är instabil*
		• Web apps / web jobs – *hostar webb APIer och långvariga webbaserade processer*
		• Service bus – *tillhandahåller intern kommunikation i Wandas ekosystem*
		• Storage accounts – *används för att lagra konversationstillstånd och användarinställningar*
		• Cosmos DB –*tillhandahåller lagring*
		• Functions – *tillhandahåller logiska algoritmer för utökningar*
		• Event grid – *tillhandahåller kommunikation*
		• API management – *hanterar APIer*
		• Service Plans – *Linux och dynamiska tjänsteplaner för att köra Tjänsten*
		• Storage accounts – *används för lagring*
		• Key vault – *lagrar konfidentiell data som används för att kommunicera med Microsofts tjänster och för interna tjänster*
		• Redis cache – *tillhandahåller cachningsmöjligheter*
		• Application Insights – *Övervakning av system, inclusive telemetri och loggning*
		• *SQL server – tillhandahåller lagring*
		• Kubernetes – *open source container*
		
		Ytterligare information och detaljer avseende dessa Microsoftprodukter och -tjänster återfinns här: https://azure.microsoft.com/en-us/services/.
		
		Förutom detta använder sig PPS, Lokaliseringstjänster och/eller Appar av:
		
		Twilio – sendgrid – för att skicka e-postmeddelanden.

4. LAGRINGSPERIOD

Personuppgiftsbiträdet ska behålla Personuppgifterna **under Avtalets avtalstid.**

Efter den avtalade lagringstiden, ska Personuppgiftsbiträdet återlämna Personuppgifterna till den Personuppgiftsansvarige, i ett migreringsbart format som bestäms av Personuppgiftsbiträdet **eller** omedelbart radera Personuppgifterna utan att behålla en kopia, enligt den Personuppgiftsansvariges begäran.

5. INFORMATION OM LAND (ELLER PLATS) FÖR BEHANDLING AV PERSONUPPGIFTER

<table>
<tr><td>Produkt – Lokal Installationsmiljö (On-premises)</td><td colspan="4">Datan lagras på den Personuppgiftsansvariges servrar på dess huvudsakliga verksamhetsort eller registrerade säte, enligt vad som meddelas Unit4 från tid till annan.</td></tr>
<tr><td>Produkt - Unit4 SaaS</td><td colspan="4">Unit4 SaaS tillhandahålls från ett antal datacenter, inklusive på världsvid basis genom Microsoft Azure. Unit4 kommer att placera Kunden i den mest logiska lokaliseringen beroende på var Kunden är lokaliserad (enligt vad som anges i Orderformuläret). Alla Kundens data kommer att lagras enbart i den valda geopolitiska zonen, och kommer inte att flyttas utanför denna utan uttryckligt medgivande från Kunden.
<table>
<tr><th>TYP AV MOLNTJÄNST</th><th>GEOPOLITISK ZON</th><th>PLATS FÖR DATACENTER</th><th>ANLÄGGNING ELLER PARTNERSKAP</th></tr>
<tr><td>SAAS CLOUD</td><td>EU</td><td>DUBLIN / AMSTERDAM</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>USA</td><td>FLERTAL PLATSER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>KANADA</td><td>TORONTO / QUEBEC CITY</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>STORBRITANNIEN</td><td>LONDON / CARDIFF</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>ASIEN</td><td>SINGAPORE / HONG KONG</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>AUSTRALIEN</td><td>VICTORIA / NEW SOUTH WALES</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>NORGE</td><td>OSLO / STAVANGER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>SVERIGE (NORDEN)</td><td>SÄTRA OCH SOLLENTUNA</td><td>CONAPTO</td></tr>
</table></td></tr>
<tr><td>Produkt – Talent Management SaaS</td><td colspan="4">Talent Management SaaS driftas i Microsoft Azure, som täcker de båda geopolitiska zonerna för EU och Storbritannien (enligt ovan), varvid den geopolitiska zon som allokeras beror på var Kunden finns lokaliserad. All Kundens Data, förutom vid delning med utvalda underbiträden i avsnitt 3, kommer att lagras enbart i den valda geopolitiska zonen, och kommer inte att flyttas utanför den utan uttryckligt medgivande från Kunden.</td></tr>
</table>

<table>
<tr><td>Unit4 Support – Standardsupport och andra standardiserade supporttjänster</td><td colspan="4">Unit4 Support använder tredjepartsprogramvara (såsom salesforce / ServiceNow) för att registrera och hantera Ärenden. Dessa Ärenden är åtkomliga för alla Unit4s anställda som har åtkomst till tredjepartsprogramvaran, såsom supporttekniker, molntjänsttekniker, konsulter och tjänsteförvaltare. Åtkomsten kontrolleras genom intern kontroll och organisatoriska processer, för att tillse att inte Personuppgifter är åtkomliga för konsulter eller tekniker på platser där åtkomst inte ska finnas till information om specifika kunder.

Kundens lokalisering | Support tillhandahålls primärt från (men kan inkludera andra EU-länder):
Storbritannien och Irland | Storbritannien, Irland, Portugal och Polen.
Sverige, Norge, Danmark, Finland och Island | Polen, Portugal, Norge och Sverige.
USA och Kanada | Polen, Portugal, USA och Kanada.
Övriga Europa | Polen, Portugal och Tyskland.
APAC | Polen, Portugal och Singapore/ Malaysia.</td></tr>
<tr><td>Unit4 Support – 24/7 Support</td><td colspan="4">Genom att använda en ”följ med solen”-metodik, kan 24/7 Support för Kundens Ärenden tillhandahållas från vilken som helst av de platser för support som anges ovan, liksom från Nederländerna, Spanien och sådana andra platser som behövs för att stödja Unit4s affärsbehov).</td></tr>
<tr><td>Unit4 Support – Enbart EU-Support</td><td colspan="4">Om Enbart EU-Support har valts, supporteras Ärenden enbart från de platser inom EU som anges ovan för Standardsupport (under Kontorstid).</td></tr>
<tr><td>People Platform Services (“PPS”), Lokaliserings-tjänster och Appar</td><td colspan="4">PPS är molntjänster som använder delad infrastruktur och tredjepartstjänster som inte kan garantera geopolitisk isolering. Nedan ges en översikt över PPS och de länder (eller platser) för Behandling av Personuppgifter som använder den tjänsten.

Tjänst | Geopolitisk zon | Var Tjänsten lagrar eller behandlar data | Support tillhandahålls primärt från:
Wanda | Vilken som helst | Huvudsakligen inom EU, men kan även ske var som helst globalt där det finns ett Microsoft Azure datacenter (exempelvis USA). | Eu-lädner inklusive Irland, Polen och Spanien; USA och andra platser för globala supportcenter där så krävs.
PPS, Lokaliserings-tjänster och Appar | Beror på var molntjänsten tagits i produktion | Tjänsten tillhandahålls och data lagras i den valda geopolitiska zonen. | Enligt ovan för Unit4 SaaS.</td></tr>
<tr><td>Unit4 Konsulttjänster och Unit4s Customer Success funktion</td><td colspan="4">Ämnesområde | Konsulttjänster och Customer Success tillhandahålls från:
Implementation och andra projekttjänster | I Territoriet eller där Kunden har sitt registrerade säte/huvudsakliga verksamhetsort (enligt vad som är tillämpligt) och/eller Portugal, beroende på vad som avtalats mellan Parterna i projektdokumentationen eller en uppdragsbeskrivning (om tillämpligt).
Datamigrering | I Territoriet eller där Kunden har sitt registrerade säte/huvudsakliga verksamhetsort (enligt vad som är tillämpligt) och/eller Portugal, beroende på vad som avtalats mellan Parterna i projektdokumentationen eller en uppdragsbeskrivning (om tillämpligt).
Felsökning | På tillämpliga platser för Unit4s Supporttjänster och Portugal.
Customer Success | På tillämpliga platser för Unit4s Supporttjänster och Portugal.</td></tr>
</table>

6. KONTAKTUPPGIFTER

Frågor eller kommentarer avseende denna Information om Personuppgiftsbehandling kan riktas till följande kontaktpersoner:

Personuppgiftsbiträdet: Genom brev (skickat till Global Data Protection Officer, kopia till Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, Nederländerna, eller genom e-post till privacy@unit4.com eller till den Unit4 adress som anges för meddelanden i Avtalet.

Personuppgiftsansvarig: Den adress till den Personuppgiftsansvarige som anges i Avtalet.

AVSNITT 2 – SÄKERHETSÅTGÄRDER

I enlighet med vad som anges i punkt 6 i Personuppgiftsbiträdesvillkoren, anges de tekniska och organisatoriska säkerhetsåtgärderna i detta avsnitt, och ska kompletteras eller ändras om nödvändigt. Den personuppgiftsansvarige anser att dessa säkerhetsåtgärder är lämpliga för behandlingen av Personuppgifterna.

Unit4s säkerhetsåtgärder för dess egen verksamhet (Sammanfattning avseende intern affärsverksamhet)

Beskrivning (generell) av de tekniska och organisatoriska säkerhetsåtgärderna som implementeras av Personuppgiftsbiträdet i dess egen organisation:

Fysisk säkerhet:

- Fysisk åtkomstkontroll hanteras av Unit4s faciliteter.
- Alla kontor har säkerhetssystem på plats avseende kontroll av åtkomst genom barriärer, exempelvis ingångsportar, bemannade receptionsdiskar, larmade branddörrar, system för intrångsövervakning, och låsbara kontor.
- Unit4 upprätthåller åtkomstkontroller baserat på vad personer vet, såsom lösenord eller åtkomstkod; eller baserat på vad personer bär med sig, såsom säkerhetskort.
- Serverrum på platsen (om tillämpligt) har ytterligare fysiska kontroller.
- Tillgång till säkrade områden eller känslig information begränsas genom att förhindra obehörig åtkomst av besökare/obehörig personal (genom låsbara kontor eller låsbara skåp) och upprätthålla policys om rena skrivbord där så är lämpligt.
- Besökare till Unit4 kontrolleras i receptionen (genom en särskild receptionist eller annan personal)
- Dokumentförstörare eller andra lämpliga metoder för att förstöra känsliga dokument används.

Virtuell och datorsäkerhet:

- Den ansvarige linjechefen ska tillse att anställda och uppdragstagare återlämnar all Unit4s egendom i deras besittning vid upphörandet av anställningen eller uppdragsavtalet. Dokumentation avseende denna återlämning av egendom finns sparad.
- Unit4 strävar efter att klassificera information som antingen offentlig, konfidentiell, innehavd med ensamrätt, eller känslig. Informationen kommer därefter att skyddas i enlighet med denna klassificering.
- Media (inklusive hårddiskar) kommer att avyttras på ett säkert sätt när de inte längre behövs. Allt känsligt material (hårddiskar, disketter etc). tas bort genom programvara för garanterad borttagning (och inte genom att formateras om eller raderas) innan de kastas eller fysiskt förstörs.
- Antivirusskydd – Unit4 använder den senaste versionen av industristandardlösningar för att tillhandahålla skydd mot virus och skadlig kod.
- Vidare nyttjar Unit4:
- Kontroll av givna behörigheter;
- Loggning och åtkomstkontroll för system;
- Åtgärder för återhämtning;
- Förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna; och
- Förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident.
- Kontinuitetsplan och katastrofåterställningsplan har tagits fram, som inkluderar överväganden om informationssäkerhet.

Säkerhetspolicys och dokumentation:

- Unit4s globala ledningsteam och/eller Unit4s respektive lokala ledningsteam har översyn över både globala och lokala informationshanterings- och säkerhetsplaner, inklusive informationssäkerhetspolicys som svarar mot identifierade informationssäkerhetsrisker och stödjer affärsmålen.
- Ansvaret för informationssäkerhet- och hantering har på global nivå till delats Uni4s globala informationssäkerhetsansvarige (Chief Information Security Officer) och Unit4s globala dataskyddsombud (Global Data Protection Officer), som hanterar resurserna för att tillhandahålla strategisk och övergripande uppfyllelse av informationssäkerhetspolicys- och processer.
- Unit4 har implementerat säkerhetspolicys som uppdateras och justeras regelbundet för att överensstämma med god industristandard.
- Unit4 har en integritetspolicy och en handlingsplan för GDPR som är publicerad på www.unit4.com/terms.
- Unit4 ingår sekretessavtal med tredje parter när konfidentiell information om dess verksamhet delas.
- Unit4 säkerställer att alla anställda och uppdragstagare har standardmässiga sekretessklausuler i sina avtal.
- Unit4 tillhandahåller utbildning åt alla anställda avseende: dataskydd, säkerhet och Unit4s kärnvärden för verksamheten.

Ytterligare element avseende Unit4 SaaS på Microsoft Azure (sammanfattning)

Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna som implementeras av Personuppgiftsbiträdet avseende tillhandahållandet av Unit4 SaaS:

Dataskydd

Unit4 SaaS använder flera olika mekanismer för att skydda Personuppgifter i molnet. Nedan ges en sammanfattande översikt över de kontroller som tillämpas.

Säkerhetsåtgärder, processer och protokoll för nätverk

- Säker dataöverföring över öppna nätverk – all trafik säkras genom användning av protokoll enligt industristandard såsom SSL/TLS och HTTPS.
- Systemsäkerhet – Logisk autentisering och behörighetsmekanismer på plats
- Brandväggar – nästa generations brandväggar för att säkerställa att ingående och utgående trafik kontrolleras.

Säkerhetsåtgärder, processer och protokoll för databaser

- Säkerhet för data – Logisk autentisering och behörighetsmekanismer på plats
- Säkerhet för databaser – varje kund har sin egen säkra databas, vilket betyder att partitionering av databaser inte krävs och att kunders data inte sammanblandas. Resultaten blir att kundens data aldrig delas med andra parter av misstag.
- Säkerhetskopior av databaser är krypterade genom användning av krypteringsteknologi för hela databasen såsom Transparent Database Encryption.
- Icke-transaktionsdata och -filer kommer att skyddas genom standardiserad symmetrisk kryptering (AES).
- Unit4 använder Azure Key Vault för att upprätthålla kontroll över nycklar som används av molnapplikationer och molntjänster för att kryptera data.

Kontinuerligt testad och vidareutvecklad säkerhet

För att kunna upptäcka oförutsedda säkerhetsbrister och förfina våra möjligheter till upptäckt och hantering, arbetar vi kontinuerligt på att förbättra vårt säkerhetsläge för att kunna försvara mot potentiella intrång. Unit4s Cloud Services Operations team, som noggrant övervakar och säkerställer driften av Unit4 SaaS (molninfrastruktur, molntjänster, produkter, enheter och interna resurser), gör penetrationstester och förbättrar vår förmåga att skydda, upptäcka och återhämta från cyberhot.

Upptäckt, begränsning och bemötande av hot

I takt med att antalet, variationen och allvarlighetsgraden för cyberhot har ökat, så har också våra ansträngningar när det gäller upptäckt och bemötande av hot. Centraliserade övervakningssystem tillhandahåller kontinuerlig synlighet och varningar i tid. Frekvent tillämpning av säkerhetspatchar och uppgraderingar skyddar system från kända säkerhetsbrister. System för upptäckt av intrång och skadliga program är designade för att upptäcka och begränsa riskerna för attacker utifrån. I händelse av skadlig aktivitet, följer vårt team för incidenthantering väl etablerade processor för hantering, kommunikation och återställning avseende incidenter. Teamet använder best practice inom industrin för all varna både interna team och kunder. Slutligen övervakar säkerhetsrapporter mönster för åtkomst för att proaktivt hjälpa till att identifiera och begränsa potentiella hot.

Datasegregering

Data är den digitala ekonomins valuta, och vi tar mycket seriöst på vårt ansvar för att skydda kundens data. Både tekniska säkerhetsåtgärder, såsom krypterad kommunikation, och organisatoriska processer ser till att kundens data är säker. I molnet kan data från ett flertal kunder lagras på samma IT-resurser. Unit4 använder logisk isolering för att segregera varje kunds data från andra kunders data.

Unit4 SaaS är designad för att motverka risker i en multitenant miljö. Datalagring och behandling är logiskt separerad mellan kunderna och har separata databasinstanser för alla Unit4s kunder.

Datakryptering

Unit4 tillhandahåller, som standard, säker tillgång till alla sina tjänster genom att kryptera all data i transit som överförs genom öppna nätverk. Detta görs genom att använda enbart säkra protokoll, som HTTPS över TLS, med användning av de senaste säkerhetsalgoritmerna. Mekanismen som används är en transparent kryptering av hela databasen – TDE. Microsoft Azure kunder som använder Public SaaS får TDE kryptering av vilande data som standard.

Åtkomstkontroll

Kunder som använder Unit4s produkter i molnet har full rätt att genomföra front-end åtkomstkontroller för deras applikationer. Detta innebär att ansvaret för att skapa nya konton, stänga ner konton och förnya konton för Unit4s applikationer ligger hos kunden.

Unit4 kommer att behålla begränsad back-end åtkomst till kunddatan (genom en direkt databaskoppling). Åtkomst av Unit4 till Personuppgifter ska vara strikt begränsad till de aktiviteter som är nödvändiga för att installera, implementera, underhålla, reparera, felsöka eller uppgradera lösningen. All åtkomst loggas och är begränsad till en liten grupp av molntjänsttekniker och supportkonsulter. Åtkomstloggar sparas i den centraliserade övervakningslösningen under 365 dagar. I händelse av dataintrång, kan Unit4 tillhandahålla åtkomstloggen på begäran.

Underrättelse om personuppgiftsincidenter

Unit4 ska underrätta Kunden utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident. Kunden bör tillse att alla kontaktuppgifter som anges i Unit4s Supportportal är uppdaterade, eftersom dessa kommer att användas för all kommunikation.

Dataskydd och inbyggt säkerhetsskydd

Unit4s molntjänstplattform har designats från start med datasäkerhet och dataskydd i åtanke. Unit4s förbättrar kontinuerligt säkerheten för lösningen, genom att applicera lärdomar från årliga penetrationstester och revisioner.

Unit4 och operatörerna av datacenter innehar ett antal olika säkerhetscertifieringar. För närmare detaljer se den tillämpliga Tjänstebeskrivningen.

Ytterligare element avseende Unit4s People Platform Services (sammanfattning)

Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna som implementeras av Personuppgiftsbiträdet avseende tillhandahållandet av Unit4 People Platform Services (molntjänster enbart):

Dataskydd

Unit4 People Platform Services använder flera olika mekanismer för att skydda Personuppgifter i molnet. Nedan ges en sammanfattande översikt över de kontroller som tillämpas.

Säkerhetsåtgärder, processer och protokoll för nätverk

- Säker dataöverföring över öppna nätverk – all trafik säkras genom användning av protokoll enligt industristandard såsom SSL/TLS och HTTPS.

Autentisering

- Alla tjänster följer principen om lägsta privilegienivå (least privilege) och autentisering mot tjänster, och deras APIer säkras genom användning av mekanismer enligt industristandard. OpenID Connect och det underliggande oAuth 2.0 protokollet används för att göra säker autentisering av användare och/eller klienttjänster med betrodda parter och validera identitet och åtkomst med användning av kravbaserade bevis.
- HMAC (Hash-based Message Authentication) används som en alternativ metod för att säkra kommunikation mellan tjänster.

Säkerhetsåtgärder, processer och protokoll för databaser

- All data som lagras i lagringskonton krypteras.
- Alla lagringskonton kräver säker överföring – all trafik säkras genom användning av protokoll enligt industristandard såsom SSL/TLS och HTTPS.
- All data som lagras I Azure Cosmos DB krypteras både i vila och i transit
- Alla Azure SQL servrar är aktiverade med Transparent Data Encryption (TDE).
- Alla Azure SQL servrar körs med Threat spårning och granskning aktiverad.
- Azure KeyVault används för att säkra särskilt känslig information som inloggningsuppgifter för tjänsteansvariga.

Säkerhetsåtgärder, processer och protokoll för meddelanden

- All data som lagras i Azure Service Bus instanser krypteras i vila.
- All trafik (i transit) genom Azure Service Bus säkras genom användning av protokoll enligt industristandard såsom SSL.

Mer detaljer om säkerhetspolicyn och säkerhetsprogram återfinns på www.unit4.com/terms.

Datakryptering

Unit4s People Platform Services tillhandahåller, som standard, säker tillgång till alla sina tjänster genom att kryptera all data i transit som överförs genom öppna nätverk. Detta görs genom att använda enbart säkra protokoll, som HTTPS över TLS (1.2), med användning av de senaste säkerhetsalgoritmerna. All data som lagras krypteras.

Underättelse om personuppgiftsincidenter

Unit4 ska underrätta Kunden utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident. Kunden bör tillse att alla kontaktuppgifter som anges i Unit4s Supportportal är uppdaterade, eftersom dessa kommer att användas för all kommunikation.

Dataskydd och inbyggt säkerhetsskydd

Unit4s People Platform Services har designats från start med datasäkerhet och dataskydd i åtanke. Unit4s förbättrar kontinuerligt säkerheten för lösningen, genom att applicera lärdomar från årliga penetrationstester och revisioner.

AVSNITT 3 – UNIT4s UNDERBITRÄDEN

Tjänster	**Underbiträde** (bolagsnamn, lokalisering etc.)	**Plats för Behandling**	**Typ av tjänster som utförs av Underbiträdet**
Unit4 Konsulttjänster (om underkonsult anlitas)	Enligt vad som specificeras i Avtalet.	Enligt vad som specificeras i Avtalet.	Enligt vad som anges i Orderformuläret eller överenskommes skriftligen med Kunden.
Tredjepartsprodukter och Tredjepartstjänster, enbart om dessa köps av Kunden	Enligt vad som specificeras i Avtalet.	Enligt vad som anges i Avtalet, eller i ytterligare bilagor eller tillägg till Avtalet som hänvisar till behandling avseende Tredjepartsleverantörer.	Programvarutjänster och/eller supporttjänster och/eller molntjänster.
Unit4 SaaS	Microsoft Azure	Enligt vad som anges i avsnitt 1, punkt 5.	Tillhandahåller molninfrastruktur och molntjänster.
	Microsoft Dynamics	Enligt vad som anges i avsnitt 1, punkt 5.	Tillhandahåller program-varutjänster, särskilt Microsoft Dynamics (inklusive viss molninfrastruktur).
	Microsoft	Enligt vad som anges i avsnitt 1, punkt 5.	Tillhandahåller programvaruverktyg och Office
	Conapto	Enligt vad som anges i avsnitt 1, punkt 5.	Tillhandahåller molninfrastruktur och molntjänster.
	Twilio – Sendgrid	United States of America (Privacy Policy)	Skickar e-postmeddelanden (EUs standardavtalsklausuler – se avsnitt 4)
Unit4 SaaS – Talent Management	Microsoft Azure	Dublin, Irland	Tillhandahåller lösning - Suite
	LogDNA	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (EUs standardavtalsklausuler – se avsnitt 4)
	Mandrill	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (EUs standardavtalsklausuler – se avsnitt 4)
	Mixpanel	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (EUs standardavtalsklausuler – se avsnitt 4)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Tillhandahåller lösning - Learn (enbart SCORM) (EUs standardavtalsklausuler – se avsnitt 4)
	Sentry	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (EUs standardavtalsklausuler – se avsnitt 4)
	Slack	United States of America (Privacy Policy)	Tillhandahåller lösning - Perform (EUs standardavtalsklausuler – se avsnitt 4)
	Wistia	United States of America (Privacy Policy)	Tillhandahåller lösning - Learn (EUs standardavtalsklausuler – se avsnitt 4)
People Platform Services (“**PPS**”) (generellt) inklusive IDS och Wanda (tillsammans med eventuella stödtjänster)	Microsoft Azure	Enligt vad som anges i avsnitt 1, punkt 5, och enligt vad som anges av Microsoft här: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.	Tillhandahåller molninfrastruktur och plattformstjänster (enligt vad som anges ovan i avsnitt 1, punkt 2).
	Twilio – Sendgrid	United States of America (Privacy Policy)	Skickar e-postmeddelanden (EUs standardavtalsklausuler – se avsnitt 4)

AVSNITT 4 – EUs STANDARDAVTALSKLAUSULER

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2021/914 av den 4 juni 2021

om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679

STANDARDAVTALSKLAUSULER

Personuppgiftsansvarig till personuppgiftsbiträde

Unit4 är personuppgiftsbiträde / uppgiftsinförare

Kunden är personuppgiftsansvarig / uppgiftsutförare

I relationen mellan parterna är det MODUL TVÅ (Överföring från personuppgiftsansvarig till personuppgiftsbiträde) i standardavtalsklausulerna som gäller.

Dessa standardavtalsklausuler gäller endast i det fall då överföring av personuppgifter görs av personuppgiftsansvarig från inom EES till personuppgiftsbiträde som finns utanför EES (i ett s.k. tredje land) och i det fall då beslut om tillämplighet finns.

AVSNITT I

Klausul 1

Syfte och tillämpningsområde

a) Syftet med dessa standardavtalsklausuler är att säkerställa överensstämmelse med kraven i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning) ([1]) vid överföring av personuppgifter till ett tredjeland.

b) Parterna:

i) den eller de fysiska eller juridiska personer, den eller de offentliga myndigheter, den eller de byråer eller andra organ (*enheterna*) som överför personuppgifter enligt förteckningen i bilaga I.A. (*uppgiftsutföraren*), och

ii) den eller de enheter i ett tredjeland som tar emot personuppgifter från uppgiftsutföraren, direkt eller indirekt via en annan enhet som också är part i dessa klausuler, enligt förteckningen i bilaga I.A. (*uppgiftsinföraren*)

har kommit överens om dessa standardavtalsklausuler (*klausulerna*).

c) Dessa klausuler är tillämpliga med avseende på överföring av personuppgifter enligt vad som anges i bilaga I.B.

d) Det tillägg till dessa klausuler som innehåller de bilagor som det hänvisas till utgör en integrerad del av dessa klausuler.

Klausul 2

Klausulernas verkan och beständighet

a) Genom dessa klausuler fastställs lämpliga skyddsåtgärder, däribland verkställbara rättigheter och effektiva rättsmedel för de registrerade enligt artikel 46.1 och artikel 46.2 c i förordning (EU) 2016/679 och, när det gäller överföring av personuppgifter från personuppgiftsansvariga till personuppgiftsbiträden och/eller från personuppgiftsbiträden till personuppgiftsbiträden, standardavtalsklausuler enligt artikel 28.7 i förordning (EU) 2016/679, under förutsättning att de inte ändras, förutom för att välja en eller flera lämpliga moduler eller lägga till eller uppdatera informationen i tillägget. Detta hindrar inte parterna från att inbegripa de standardavtalsklausuler som fastställs i dessa klausuler i ett mer övergripande avtal och/eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med dessa klausuler eller påverkar de registrerades grundläggande rättigheter eller friheter.

b) Dessa klausuler påverkar inte de skyldigheter som uppgiftsutföraren omfattas av med stöd av förordning (EU) 2016/679.

Klausul 3

Berättigade tredje parter

a) Registrerade personer får åberopa och verkställa dessa klausuler, i egenskap av berättigade tredje parter, gentemot uppgiftsutföraren och/eller uppgiftsinföraren, med följande undantag:

i) Klausul 1, klausul 2, klausul 3, klausul 6, klausul 7.

ii) Klausul 8 – modul ett: klausul 8.5 e och klausul 8.9 b; modul två: klausul 8.1 b, 8.9 a, c, d och e; modul tre: klausul 8.1 a, c och d och klausul 8.9 a, c, d, e, f och g; modul fyra: klausul 8.1 b och klausul 8.3 b.

iii) Klausul 9 – modul två: klausul 9 a, c, d och e; modul tre: klausul 9 a, c, d och e.

iv) Klausul 12 – modul ett: klausul 12 a och d; modulerna två och tre: klausul 12 a, d och f.

v) Klausul 13.

vi) Klausul 15.1 c, d och e.

vii) Klausul 16 e.

viii) Klausul 18 – modulerna ett, två och tre: klausul 18 a och b; modul fyra: klausul 18.

b) Led a påverkar inte de registrerades rättigheter enligt förordning (EU) 2016/679.

Klausul 4

Tolkning

a) Om begrepp som definieras i förordning (EU) 2016/679 används i dessa klausuler ska begreppen ha samma betydelse som i den förordningen.

b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.

c) Dessa klausuler ska inte tolkas på ett sätt som står i strid med de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679.

Klausul 5

Hierarki

Om en konflikt uppstår mellan dessa klausuler och bestämmelserna i de överenskommelser mellan parterna som gäller vid den tidpunkt då dessa klausuler överenskoms eller därefter träder i kraft, ska dessa klausuler ha företräde.

Klausul 6

Beskrivning av överföringen eller överföringarna

Närmare uppgifter om överföringen eller överföringarna, och i synnerhet de kategorier av personuppgifter som överförs och det eller de ändamål för vilka de överförs, anges i bilaga I.B.

Klausul 7 – Valfri

Dockningsklausul

a) En enhet som inte är part i dessa klausuler får, efter överenskommelse med parterna, när som helst ansluta sig till dessa klausuler, antingen som uppgiftsutförare eller uppgiftsinförare, genom att fylla i tillägget och underteckna bilaga I.A.

b) När den anslutande enheten har fyllt i tillägget och undertecknat bilaga I.A ska den bli en part i dessa klausuler och ha samma rättigheter och skyldigheter som en uppgiftsutförare eller uppgiftsinförare i enlighet med dess beteckning i bilaga I.A.

c) Den anslutande enheten ska inte ha några rättigheter eller skyldigheter enligt dessa klausuler från perioden innan enheten blev en part.

AVSNITT II – PARTERNAS SKYLDIGHETER

Klausul 8

Skyddsåtgärder för uppgifter

Uppgiftsutföraren garanterar att han eller hon har gjort rimliga ansträngningar för att se till att uppgiftsinföraren, genom genomförandet av lämpliga tekniska och organisatoriska åtgärder, kan fullgöra sina skyldigheter enligt dessa klausuler.

8.1 Instruktioner

a) Uppgiftsinföraren ska endast behandla personuppgifterna enligt dokumenterade instruktioner från uppgiftsutföraren. Uppgiftsutföraren får ge sådana instruktioner under hela avtalets giltighetstid.

b) Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren om han eller hon inte kan följa dessa instruktioner.

8.2 Ändamålsbegränsning

Uppgiftsinföraren ska endast behandla personuppgifterna för det eller de specifika ändamålen med överföringen, enligt vad som fastställs i bilaga I.B, såvida inte uppgiftsutföraren har gett andra instruktioner.

8.3 Öppenhet

På begäran ska uppgiftsutföraren tillhandahålla en kopia av dessa klausuler, inklusive tillägget när det har fyllts i av parterna, till den registrerade utan kostnad. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive de åtgärder som beskrivs i bilaga II och personuppgifter, får uppgiftsutföraren redigera delar av texten i tillägget till dessa klausuler innan en kopia tillhandahålls, men han eller hon måste bifoga en meningsfull sammanfattning om den registrerade annars inte skulle kunna förstå dess innehåll eller utöva sina rättigheter. På begäran ska parterna tillhandahålla skälen till redigeringen till den registrerade, i möjligaste mån utan att avslöja de redigerade uppgifterna. Denna klausul påverkar inte uppgiftsutförarens skyldigheter enligt artiklarna 13 och 14 i förordning (EU) 2016/679.

8.4 Korrekthet

Om uppgiftsinföraren får kännedom om att de personuppgifter som han eller hon har tagit emot är felaktiga, eller har blivit inaktuella, ska han eller hon informera uppgiftsutföraren utan onödigt dröjsmål. I sådana fall ska uppgiftsinföraren samarbeta med uppgiftsutföraren för att radera eller rätta uppgifterna.

8.5 Behandlingens varaktighet och radering eller återlämnande av uppgifter

Uppgiftsinförarens behandling ska endast äga rum under den period som anges i bilaga I.B. När tillhandahållandet av behandlingstjänsterna har avslutats ska uppgiftsinföraren, enligt uppgiftsutförarens val, radera alla personuppgifter som behandlats på uppdrag av uppgiftsutföraren och intyga för uppgiftsutföraren att detta har skett, eller till uppgiftsutföraren återlämna alla personuppgifter som har behandlats på uppdrag av uppgiftsutföraren och radera befintliga kopior. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen. Detta påverkar inte klausul 14, i synnerhet kravet enligt klausul 14 e att uppgiftsinföraren under hela avtalets giltighetstid ska meddela uppgiftsutföraren om han eller hon har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i klausul 14 a.

8.6 Säkerhet vid behandling

a) Uppgiftsinföraren, och under överföring även uppgiftsutföraren, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa uppgifternas säkerhet, däribland genom skydd mot säkerhetsbrott som skulle leda till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande eller obehörig åtkomst till uppgifterna (*personuppgiftsincident*). Vid bedömning av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till de senaste rönen, kostnaderna för genomförandet, behandlingens karaktär, omfattning, sammanhang och ändamål samt riskerna för de registrerade i samband med behandlingen. Parterna ska i synnerhet överväga att använda kryptering eller pseudonymisering, även under överföringen, om ändamålet med behandlingen kan uppfyllas på detta sätt. Vid användning av pseudonymisering ska uppgiftsutföraren om möjligt behålla sin fullständiga kontroll över den ytterligare information som krävs för att knyta personuppgifterna till en viss registrerad. För att fullgöra sina skyldigheter enligt denna punkt ska uppgiftsinföraren åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga II. Uppgiftsinföraren ska göra regelbundna kontroller för att säkerställa att dessa åtgärder även fortsättningsvis ger en lämplig säkerhetsnivå.

b) Uppgiftsinföraren ska endast ge sin personal tillgång till personuppgifterna i den utsträckning det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Uppgiftsinföraren ska säkerställa att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

c) I händelse av en personuppgiftsincident som gäller uppgifter som har behandlats av uppgiftsinföraren enligt dessa klausuler ska uppgiftsinföraren vidta lämpliga åtgärder för att hantera incidenten, däribland åtgärder för att mildra dess negativa konsekvenser. Uppgiftsinföraren ska även meddela uppgiftsutföraren utan onödigt dröjsmål efter att ha fått kännedom om incidenten. Meddelandet ska innehålla uppgifter om en kontaktpunkt som kan lämna mer information, en beskrivning av incidentens karaktär (inbegripet, om möjligt, vilka kategorier och det ungefärliga antalet registrerade och personuppgiftsregister som berörs), dess sannolika konsekvenser samt vilka åtgärder som har vidtagits eller föreslagits för att hantera incidenten, däribland, i tillämpliga fall, åtgärder för att mildra dess möjliga negativa konsekvenser. Om, och i den mån, det inte är möjligt att tillhandahålla all information vid samma tillfälle ska det inledande meddelandet innehålla den information som då finns tillgänglig, varefter ytterligare information ska tillhandahållas utan onödigt dröjsmål efterhand som den blir tillgänglig.

d) Uppgiftsinföraren ska samarbeta med och bistå uppgiftsutföraren så att uppgiftsutföraren kan fullgöra sina skyldigheter enligt förordning (EU) 2016/679, framför allt att meddela den behöriga tillsynsmyndigheten och de berörda registrerade, med beaktande av behandlingens karaktär och den information som finns tillgänglig för uppgiftsinföraren.

8.7 Känsliga uppgifter

Om överföringen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar och lagöverträdelser (*känsliga uppgifter*) ska uppgiftsinföraren tillämpa de särskilda begränsningar och/eller de ytterligare skyddsåtgärder som beskrivs i bilaga I.B.

8.8 Vidare överföringar

Uppgiftsinföraren ska endast lämna ut personuppgifter till en tredje part enligt dokumenterade instruktioner från uppgiftsutföraren. Dessutom får uppgifterna endast lämnas ut till en tredje part utanför Europeiska unionen ([4]) (i samma land som uppgiftsinföraren eller i ett annat tredjeland, nedan kallat *vidare överföring*), om den tredje parten är eller samtycker till att vara bunden av dessa klausuler i motsvarande modul, eller

i) om den vidare överföringen sker till ett land som omfattas av ett beslut om adekvat skyddsnivå enligt artikel 45 i förordning (EU) 2016/679 som täcker den vidare överföringen,

ii) om den tredje parten på annat sätt säkerställer lämpliga skyddsåtgärder enligt artikel 46 eller 47 i förordning (EU) 2016/679 med avseende på behandlingen i fråga,

iii) om den vidare överföringen är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk i samband med särskilda administrativa, tillsynsrelaterade eller rättsliga förfaranden, eller

iv) om den vidare överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

Vid varje vidare överföring måste uppgiftsinföraren uppfylla kraven för alla andra skyddsåtgärder i dessa klausuler, i synnerhet ändamålsbegränsning.

8.9 Dokumentation och efterlevnad

a) Uppgiftsinföraren ska skyndsamt och på ett lämpligt sätt hantera förfrågningar från uppgiftsutföraren angående behandlingen enligt dessa klausuler.

b) Parterna ska kunna visa att de uppfyller kraven i dessa klausuler. Framför allt ska uppgiftsinföraren föra lämplig dokumentation över den behandling som utförts på uppdrag av uppgiftsutföraren.

c) Uppgiftsinföraren ska se till att uppgiftsutföraren har tillgång till all information som behövs för att visa att de skyldigheter som fastställs i dessa klausuler har fullgjorts och, på uppgiftsutförarens begäran, möjliggöra och bidra till revisioner av den behandling som omfattas av dessa klausuler med rimliga mellanrum eller om det finns indikationer på bristande efterlevnad. När beslut fattas om en granskning eller revision får uppgiftsutföraren ta hänsyn till relevanta intyg som innehas av uppgiftsinföraren.

d) Uppgiftsutföraren får välja att utföra revisionen själv eller anlita en oberoende revisor. Revisionerna får omfatta inspektioner i uppgiftsinförarens lokaler eller fysiska anläggningar och ska, om så är lämpligt, utföras med rimligt varsel.

e) Parterna ska se till att den information som avses i leden b och c, inklusive resultaten av eventuella revisioner, finns tillgänglig för den behöriga tillsynsmyndigheten på begäran.

Klausul 9

Användning av underentreprenörer

a) ALLMÄNT SKRIFTLIGT TILLSTÅND Uppgiftsinföraren har uppgiftsutförarens allmänna tillstånd att anlita en eller flera underentreprenörer i en överenskommen förteckning. Uppgiftsinföraren ska informera uppgiftsutföraren skriftligen om alla planerade ändringar av förteckningen genom tillägg eller ersättning av underentreprenörer minst 30 dagar i förväg, så att uppgiftsutföraren har tillräckligt med tid för att invända mot sådana ändringar före anlitandet av underentreprenören(-erna). Uppgiftsinföraren ska ge uppgiftsutföraren all information som behövs för att uppgiftsutföraren ska kunna utöva sin rätt att göra invändningar.

b) Om uppgiftsinföraren anlitar en underentreprenör för att utföra särskilda behandlingar (på uppdrag av uppgiftsutföraren) ska han eller hon göra detta genom ett skriftligt avtal som, i sak, innehåller samma skyldigheter i fråga om dataskydd som de avtal som är bindande för uppgiftsinföraren enligt dessa klausuler, däribland vad gäller de registrerades rättigheter som berättigade tredje parter ([8]). Parterna är överens om att uppgiftsinföraren, genom att uppfylla kraven i denna klausul, fullgör sina skyldigheter enligt klausul 8.8. Uppgiftsinföraren ska säkerställa att underentreprenören fullgör de skyldigheter som uppgiftsinföraren omfattas av enligt dessa klausuler.

c) Uppgiftsinföraren ska, på uppgiftsutförarens begäran, tillhandahålla en kopia av avtalet med underentreprenören och eventuella senare ändringar till uppgiftsutföraren. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsinföraren redigera texten i avtalet innan en kopia tillhandahålls.

d) Uppgiftsinföraren ska fortsatt vara fullt ansvarig inför uppgiftsutföraren för fullgörandet av underentreprenörens skyldigheter inom ramen för dennes avtal med uppgiftsinföraren. Uppgiftsinföraren ska meddela uppgiftsutföraren om underentreprenören underlåter att fullgöra sina skyldigheter inom ramen för avtalet.

e) Uppgiftsinföraren ska komma överens om en klausul om tredjepartsberättigande med underentreprenören, varigenom uppgiftsutföraren – om uppgiftsinföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp avtalet med underentreprenören och beordra underentreprenören att radera eller återlämna personuppgifterna.

Klausul 10

De registrerades rättigheter

a) Uppgiftsinföraren ska skyndsamt meddela uppgiftsutföraren om varje begäran från en registrerad. Uppgiftsinföraren ska inte själv besvara begäran, såvida inte han eller hon har fått tillstånd att göra detta av uppgiftsutföraren.

b) Uppgiftsinföraren ska bistå uppgiftsutföraren med att fullgöra dennes skyldigheter att tillgodose de registrerades begäranden om att utöva sina rättigheter enligt förordning (EU) 2016/679. I detta avseende ska parterna fastställa lämpliga tekniska och organisatoriska åtgärder i bilaga II, med beaktande av behandlingens karaktär, genom vilka biståndet ska tillhandahållas, såväl som tillämpningsområdet för och omfattningen av det bistånd som begärs.

c) När uppgiftsinföraren fullgör sina skyldigheter enligt leden a och b ska han eller hon följa uppgiftsutförarens instruktioner.

Klausul 11

Tillgång till prövning

a) Uppgiftsinföraren ska informera de registrerade i ett öppet och lättillgängligt format, genom enskilda meddelanden eller på sin webbplats, om en kontaktpunkt som har tillstånd att hantera klagomål. Uppgiftsinföraren ska skyndsamt hantera varje klagomål som tas emot från en registrerad.

[ALTERNATIV: Uppgiftsinföraren samtycker till att registrerade även får inge klagomål till ett oberoende tvistlösningsorgan ([11]) utan kostnad för den registrerade. Uppgiftsinföraren ska informera de registrerade, på det sätt som anges i led a, om denna mekanism för prövning och om att de inte måste använda den eller följa en viss ordning när de begär prövning.]

b) Om en tvist uppstår mellan en registrerad och en av parterna när det gäller efterlevnaden av dessa klausuler ska den parten göra sitt yttersta för att lösa tvisten i godo på ett skyndsamt sätt. Parterna ska informera varandra om sådana tvister och, i tillämpliga fall, samarbeta för att lösa dem.

c) Om den registrerade åberopar en rättighet som berättigad tredje part enligt klausul 3 ska uppgiftsinföraren godta den registrerades beslut att

i) inge ett klagomål till tillsynsmyndigheten i den medlemsstat där han/hon är stadigvarande bosatt eller har sin arbetsplats, eller till den behöriga tillsynsmyndigheten enligt klausul 13,

ii) hänskjuta tvisten till de behöriga domstolarna i den mening som avses i klausul 18.

d) Parterna godtar att den registrerade får företrädas av ett organ, en organisation eller sammanslutning utan vinstsyfte enligt de villkor som fastställs i artikel 80.1 i förordning (EU) 2016/679.

e) Uppgiftsinföraren ska följa ett beslut som är bindande enligt tillämplig lagstiftning i EU eller medlemsstaterna.

f) Uppgiftsinföraren är införstådd med att det val som gjorts av den registrerade inte kommer att påverka hans/hennes materiella och processuella rättigheter att begära prövning i enlighet med tillämplig lagstiftning.

Klausul 12

Ansvarsskyldighet

a) Varje part ska vara ansvarig inför den andra parten eller de andra parterna för eventuella skador den orsakar den andra parten eller de andra parterna genom överträdelse av dessa klausuler.

b) Uppgiftsinföraren ska vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsinföraren eller dess underentreprenör orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler.

c) Utan att det påverkar led b ska uppgiftsutföraren vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsutföraren eller uppgiftsinföraren (eller dess underentreprenör) orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler. Detta påverkar inte uppgiftsutförarens ansvarsskyldighet eller, om uppgiftsutföraren är ett personuppgiftsbiträde som agerar på uppdrag av en personuppgiftsansvarig, den personuppgiftsansvariges ansvarsskyldighet enligt förordning (EU) 2016/679 eller förordning (EU) 2018/1725, enligt vad som är tillämpligt.

d) Parterna är överens om att en uppgiftsutförare som enligt led c hålls ansvarig för skada som orsakats av uppgiftsinföraren (eller dess underentreprenör) ska ha rätt att återkräva den del av ersättningen från uppgiftsinföraren som motsvarar dennes ansvarsskyldighet för skadan.

e) Om fler än en part är ansvariga för eventuell skada som orsakats den registrerade till följd av en överträdelse av dessa klausuler ska alla ansvarsskyldiga parter vara solidariskt ansvariga, och den registrerade ska ha rätt att väcka talan i domstol mot var och en av dessa parter.

f) Parterna är överens om att en part som hålls ansvarig enligt led e ska ha rätt att återkräva från den andra parten eller de andra parterna den del av ersättningen som motsvarar dess/deras ansvarsskyldighet för skadan.

g) Uppgiftsinföraren får inte åberopa en underentreprenörs uppförande för att undvika sitt eget ansvar.

Klausul 13

Tillsyn

a) [Om uppgiftsutföraren är etablerad i en av EU:s medlemsstater:] Den tillsynsmyndighet som har ansvar för att säkerställa uppgiftsutförarens efterlevnad av förordning (EU) 2016/679 när det gäller överföring av uppgifter, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet.

[Om uppgiftsutföraren inte är etablerad i en av EU:s medlemsstater, men omfattas av det territoriella tillämpningsområdet för förordning (EU) 2016/679 i enlighet med artikel 3.2 i den förordningen, och har utsett en företrädare enligt artikel 27.1 i förordning (EU) 2016/679:] Tillsynsmyndigheten i den medlemsstat i vilken företrädaren i den mening som avses i artikel 27.1 i förordning (EU) 2016/679 är etablerad, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet.

[Om uppgiftsutföraren inte är etablerad i en av EU:s medlemsstater, men omfattas av det territoriella tillämpningsområdet för förordning (EU) 2016/679 i enlighet med artikel 3.2 i den förordningen, dock utan att vara skyldig att utse en företrädare enligt artikel 27.2 i förordning (EU) 2016/679:] Tillsynsmyndigheten i en av de medlemsstater i vilken de registrerade vars personuppgifter överförs enligt dessa klausuler befinner sig i samband med

utbjudandet av varor eller tjänster till dem, eller i samband med att deras beteende övervakas, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet.

b) Uppgiftsinföraren samtycker till att godta den behöriga tillsynsmyndighetens behörighet och samarbeta med den i varje förfarande som syftar till att säkerställa efterlevnaden av dessa klausuler. Uppgiftsinföraren samtycker i synnerhet till att svara på förfrågningar, gå med på revisioner och iaktta de åtgärder som antagits av tillsynsmyndigheten, inbegripet korrigerande och kompenserade åtgärder. Uppgiftsinföraren ska ge tillsynsmyndigheten en skriftlig bekräftelse på att nödvändiga åtgärder har vidtagits.

Klausul 14

Lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna

a) Parterna garanterar att de inte har någon anledning att misstänka att de lagar och förfaranden i det mottagande tredjelandet som är tillämpliga på uppgiftsinförarens behandling av personuppgifter, däribland eventuella krav på att lämna ut personuppgifter eller åtgärder för att bevilja åtkomst för offentliga myndigheter, hindrar uppgiftsinföraren från att fullgöra sina skyldigheter enligt dessa klausuler. Detta bygger på förutsättningen att lagar och förfaranden som är förenliga med andemeningen i de grundläggande rättigheterna och friheterna, och som inte går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda de ändamål som anges i artikel 23.1 i förordning (EU) 2016/679, inte strider mot dessa klausuler.

b) Genom att tillhandahålla den garanti som avses i led a intygar parterna att de har tagit vederbörlig hänsyn till särskilt följande aspekter:

i) De särskilda omständigheterna kring överföringen, däribland behandlingskedjans längd, antalet inblandade aktörer och vilka överföringskanaler som använts; planerade vidare överföringar; typen av mottagare; ändamålet med behandlingen; de överförda personuppgifternas kategorier och format; den ekonomiska sektor inom vilken överföringen äger rum; platsen för lagring av de överförda uppgifterna.

ii) De lagar och förfaranden i det mottagande tredjelandet – inbegripet krav på att lämna ut uppgifterna till offentliga myndigheter eller att ge sådana myndigheter åtkomst till uppgifterna – som är relevanta mot bakgrund av överföringens särskilda omständigheter samt tillämpliga begränsningar och skyddsåtgärder ([12]).

iii) Alla relevanta avtalsenliga, tekniska eller organisatoriska skyddsåtgärder som införts för att komplettera skyddsåtgärderna enligt dessa klausuler, inbegripet åtgärder som tillämpats under överföringen och vid behandlingen av personuppgifterna i det mottagande tredjelandet.

c) Uppgiftsinföraren garanterar att han eller hon, i samband med den bedömning som avses i led b, har gjort sitt yttersta för att ge uppgiftsutföraren relevant information, och samtycker till att fortsätta att samarbeta med uppgiftsutföraren för att säkerställa efterlevnaden av dessa klausuler.

d) Parterna är överens om att dokumentera den bedömning som avses i led b och att på begäran göra den tillgänglig för den behöriga tillsynsmyndigheten.

e) Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren om han eller hon, efter att ha godkänt dessa klausuler och under hela avtalets giltighetstid, har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i led a, däribland efter en ändring i lagarna i tredjelandet eller en åtgärd (såsom en begäran om utlämnande av uppgifter) som antyder att en tillämpning av sådana lagar i praktiken inte stämmer överens med kraven i led a. [För modul tre: Uppgiftsutföraren ska vidarebefordra meddelandet till den personuppgiftsansvarige.]

f) Efter att ha tagit emot ett meddelande i enlighet med led e, eller om uppgiftsutföraren har andra anledningar att misstänka att uppgiftsinföraren inte längre kan fullgöra sina skyldigheter enligt dessa klausuler, ska uppgiftsutföraren skyndsamt fastställa lämpliga åtgärder (t.ex. tekniska eller organisatoriska åtgärder för att säkerställa säkerhet och konfidentialitet) som ska antas av uppgiftsutföraren och/eller uppgiftsinföraren för att hantera situationen [för modul tre:, i tillämpliga fall efter samråd med den personuppgiftsansvarige]. Uppgiftsutföraren ska avbryta överföringen av uppgifter om han eller hon anser att inga lämpliga skyddsåtgärder kan säkerställas för överföringen, eller efter att ha fått instruktioner från [för modul tre: den personuppgiftsansvarige eller] den behöriga tillsynsmyndigheten att göra det. I sådana fall ska uppgiftsutföraren ha rätt att säga upp avtalet i den mån det gäller behandling av personuppgifter enligt dessa klausuler. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat. Om avtalet sägs upp enligt denna klausul ska klausul 16 d och e tillämpas.

Klausul 15

Uppgiftsinförarens skyldigheter vid åtkomst av offentliga myndigheter

15.1 Meddelanden

a) Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren och, om så är möjligt, den registrerade (vid behov med hjälp av uppgiftsutföraren) om han eller hon

i) får en rättsligt bindande begäran från en offentlig myndighet, inbegripet en rättslig myndighet, i enlighet med det mottagande landets lagstiftning om att personuppgifter som överförts enligt dessa klausuler ska lämnas ut; meddelandet ska innehålla information om de begärda personuppgifterna, den begärande myndigheten, den rättsliga grunden för begäran och det svar som lämnats, eller

ii) får kännedom om att offentliga myndigheter har haft direkt tillgång till enligt dessa klausuler överförda personuppgifter i enlighet med det mottagande landets lagstiftning; meddelandet ska innehålla all information som uppgiftsinföraren har tillgång till.

[För modul tre: Uppgiftsutföraren ska vidarebefordra meddelandet till den personuppgiftsansvarige.]

b) Om uppgiftsinföraren är förbjuden att meddela uppgiftsutföraren och/eller den registrerade enligt det mottagande landets lagstiftning samtycker uppgiftsinföraren till att göra sitt yttersta för att få till stånd ett undantag från förbudet, för att kunna tillhandahålla så mycket information som möjligt inom kortast möjliga tid. Uppgiftsinföraren samtycker till att dokumentera sina ansträngningar för att kunna bekräfta dem på begäran av uppgiftsutföraren.

c) Om det är tillåtet enligt det mottagande landets lagstiftning samtycker uppgiftsinföraren till att, med jämna mellanrum under hela avtalets giltighetstid, ge uppgiftsutföraren så mycket relevant information som möjligt om de begäranden som tagits emot (i synnerhet antalet begäranden, vilken typ av uppgifter som begärts, den eller de begärande myndigheterna, om begärandena har bestridits och resultaten av bestridandena etc.). [För modul tre: Uppgiftsutföraren ska vidarebefordra informationen till den personuppgiftsansvarige.]

d) Uppgiftsinföraren samtycker till att lagra den information som avses i leden a–c under hela avtalets giltighetstid och göra den tillgänglig för den behöriga tillsynsmyndigheten på begäran.

e) Leden a–c påverkar inte uppgiftsinförarens skyldighet enligt klausul 14 e och klausul 16 att skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler.

15.2 Granskning av laglighet och uppgiftsminimering

a) Uppgiftsinföraren samtycker till att granska lagligheten i begäran om utlämnande av uppgifter, särskilt om begäran omfattas av de befogenheter som har beviljats den begärande offentliga myndigheten, och att bestrida begäran om han eller hon, efter noggrann bedömning, drar slutsatsen att det finns rimliga

skäl att betrakta begäran som olaglig enligt det mottagande landets lagstiftning, tillämpliga skyldigheter enligt internationell rätt och principen om internationell hövlighet. Uppgiftsinföraren ska, enligt samma villkor, fullfölja möjligheterna att överklaga. Om uppgiftsinföraren bestrider en begäran ska han eller hon vidta provisoriska åtgärder för att upphäva konsekvenserna av begäran tills den behöriga rättsliga myndigheten har fattat beslut i frågan. Uppgiftsinföraren får inte lämna ut de begärda personuppgifterna förrän han eller hon är skyldig att göra detta enligt tillämpliga förfaranderegler. Dessa krav påverkar inte uppgiftsinförarens skyldigheter enligt klausul 14 e.

b) Uppgiftsinföraren samtycker till att dokumentera sin rättsliga bedömning och varje bestridande av begäran om utlämnande av uppgifter och, i den mån det är tillåtet enligt det mottagande landets lagstiftning, göra dokumentationen tillgänglig för uppgiftsutföraren. Uppgiftsinföraren ska även göra dokumentationen tillgänglig för den behöriga tillsynsmyndigheten på begäran. [För modul tre: Uppgiftsutföraren ska se till att den personuppgiftsansvarige får tillgång till bedömningen.]

c) Uppgiftsinföraren samtycker till att tillhandahålla den minsta tillåtna mängden information när han eller hon besvarar en begäran om utlämnande av uppgifter, baserat på en rimlig tolkning av begäran.

AVSNITT IV – SLUTBESTÄMMELSER

Klausul 16

Bristande efterlevnad av klausulerna och avtalets uppsägning

a) Uppgiftsinföraren ska skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler, oavsett orsak.

b) Om uppgiftsinföraren bryter mot dessa klausuler eller inte kan uppfylla kraven i dessa klausuler ska uppgiftsutföraren avbryta överföringen av personuppgifter till uppgiftsinföraren tills efterlevnaden åter har säkerställts eller avtalet har sagts upp. Detta påverkar inte tillämpningen av klausul 14 f.

c) Uppgiftsutföraren ska ha rätt att säga upp avtalet i den mån det gäller behandlingen av personuppgifter enligt dessa klausuler om

i) uppgiftsutföraren har avbrutit överföringen av personuppgifter till uppgiftsinföraren enligt led b och om efterlevnaden av dessa klausuler inte har återupprättats inom en rimlig tidsperiod, under alla omständigheter inom en månad efter avbrytandet,

ii) uppgiftsinföraren gör sig skyldig till allvarliga eller upprepade överträdelser av dessa klausuler, eller

iii) uppgiftsinföraren inte följer ett bindande beslut av en behörig domstol eller tillsynsmyndighet angående hans eller hennes skyldigheter enligt dessa klausuler.

I sådana fall ska uppgiftsutföraren informera den behöriga tillsynsmyndigheten [för modul tre: och den personuppgiftsansvarige] om denna bristande efterlevnad. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat.

d) [För modulerna ett, två och tre: Personuppgifter som överförts före uppsägningen av avtalet i enlighet med led c ska efter uppgiftsutförarens eget val omedelbart återlämnas till uppgiftsutföraren eller raderas i sin helhet. Detsamma ska gälla för eventuella kopior av uppgifterna.] [För modul fyra: Personuppgifter som samlats in av uppgiftsutföraren i EU och som överförts före uppsägningen av avtalet enligt led c ska omedelbart raderas i sin helhet, inklusive eventuella kopior.] Uppgiftsinföraren ska intyga för uppgiftsutföraren att uppgifterna har raderats. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av de överförda personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen.

e) Endera parten får återkalla sin överenskommelse om att vara bunden av dessa klausuler om i) Europeiska kommissionen antar ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679 som omfattar den överföring av personuppgifter som dessa klausuler gäller för, eller ii) förordning (EU) 2016/679 blir en del av den rättsliga ramen i det land till vilket personuppgifterna överförs. Detta påverkar inte övriga skyldigheter som är tillämpliga på behandlingen i fråga enligt förordning (EU) 2016/679.

Klausul 17

Tillämplig lag

Dessa klausuler ska regleras genom lagstiftningen i en av EU:s medlemsstater, under förutsättning att lagstiftningen omfattar rättigheter för berättigade tredje parter. Parterna är överens om att detta ska vara i överensstämmelse med lagen som reglerar Avtalet.

Klausul 18

Val av forum och jurisdiktion

a) Varje tvist som uppstår på grund av dessa klausuler ska lösas av domstolarna i en medlemsstat i EU.

b) Parterna är överens om att dessa ska vara domstolarna ska vara den domstol som styr Avtalet.

c) En registrerad får även inleda rättsliga förfaranden mot uppgiftsutföraren och/eller uppgiftsinföraren vid domstolarna i den medlemsstat där han/hon har sin stadigvarande vistelseort.

d) Parterna är överens om att underkasta sig sådana domstolars jurisdiktion.

---

(1) Om uppgiftsutföraren är ett personuppgiftsbiträde som omfattas av förordning (EU) 2016/679 och som agerar på uppdrag av en unionsinstitution eller ett unionsorgan som personuppgiftsansvarig, säkerställer användningen av dessa klausuler vid anlitande av ett annat personuppgiftsbiträde (som underentreprenör) som inte omfattas av förordning (EU) 2016/679 även överensstämmelse med artikel 29.4 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39), i den utsträckning som dessa klausuler och de skyldigheter i fråga om uppgiftsskydd som fastställs i avtalet eller en annan rättsakt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i enlighet med artikel 29.3 i förordning (EU) 2018/1725 har samordnats. Detta kommer särskilt att vara fallet om den personuppgiftsansvarige och personuppgiftsbiträdet använder de standardavtalsklausuler som ingår i beslut 2021/915.

(2) Detta kräver att uppgifterna görs anonyma på ett sätt som gör att den enskilda individen inte längre kan identifieras av någon annan, i linje med skäl 26 i förordning (EU) 2016/679, och att denna process är oåterkallelig.

(3) Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till

avtalet. Om uppgiftsinföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

(4) Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till avtalet. Om uppgiftsinföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

(5) Se artikel 28.4 i förordning (EU) 2016/679 och, om den personuppgiftsansvarige är en EU-institution eller ett EU-organ, artikel 29.4 i förordning (EU) 2018/1725.

(6) Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till avtalet. Om uppgiftsinföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

(7) Detta omfattar huruvida överföringen och den efterföljande behandlingen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar eller lagöverträdelser.

(8) Detta krav får uppfyllas av den underentreprenör som anslutit sig till dessa klausuler inom ramen för den tillämpliga modulen i enlighet med klausul 7.

(9) Detta krav får uppfyllas av den underentreprenör som anslutit sig till dessa klausuler inom ramen för den tillämpliga modulen i enlighet med klausul 7.

(10) Denna period får förlängas med högst två ytterligare månader i den mån det är nödvändigt med beaktande av begärandenas komplexitet och antal. Uppgiftsinföraren ska skyndsamt och på vederbörligt sätt informera den registrerade om sådana förlängningar.

(11) Uppgiftsinföraren får endast erbjuda oberoende tvistlösning genom en skiljedomstol om han eller hon är etablerad i ett land som har ratificerat New York-konventionen om verkställighet av skiljedomar.

(12) När det gäller konsekvenserna av sådana lagar och förfaranden för efterlevnaden av dessa klausuler kan olika aspekter anses utgöra en del av den övergripande bedömningen. Sådana aspekter kan omfatta relevant och dokumenterad praktisk erfarenhet av tidigare begäranden om utlämning av uppgifter från offentliga myndigheter, eller avsaknad av sådana begäranden, som täcker en tillräckligt representativ tidsram. Detta gäller särskilt interna register eller annan dokumentation som upprättats kontinuerligt i enlighet med tillbörlig aktsamhet och som godkänts på ledningsnivå, under förutsättning att denna information kan delas med tredje parter på ett lagligt sätt. Om denna praktiska erfarenhet används som grund för slutsatsen att uppgiftsinföraren inte kommer att hindras från att uppfylla kraven i dessa klausuler måste den stödjas av andra relevanta, objektiva aspekter, och parterna måste noggrant överväga huruvida dessa aspekter tillsammans har tillräckligt stor vikt, vad gäller deras tillförlitlighet och representativitet, för att underbygga denna slutsats. Parterna måste i synnerhet ta hänsyn till huruvida deras praktiska erfarenhet bekräftas och inte motsägs av offentligt tillgänglig eller på annat sätt åtkomlig och tillförlitlig information om förekomst eller avsaknad av begäranden inom samma sektor och/eller av tillämpningen av lagstiftningen i praktiken, t.ex. rättspraxis och rapporter från oberoende tillsynsorgan.

TILLÄGG

FÖRKLARANDE ANMÄRKNINGAR:

Det måste vara möjligt att tydligt urskilja den information som är tillämplig på varje överföring eller kategori av överföringar och, i detta avseende, fastställa parternas respektive roller som uppgiftsutförare och/eller uppgiftsinförare. Detta innebär inte nödvändigtvis att separata tillägg måste fyllas i och undertecknas för varje överföring/kategori av överföringar och/eller avtalsförhållande, om denna öppenhet kan uppnås genom ett tillägg. Separata tillägg bör emellertid användas om det är nödvändigt för att säkerställa tillräcklig klarhet.

BILAGA I

A. FÖRTECKNING ÖVER PARTER

Uppgiftsutförare: [*Uppgiftsutförarens/uppgiftsutförarnas identitet och kontaktuppgifter och, i tillämpliga fall, uppgifter om hans/hennes eller deras dataskyddsombud och/eller företrädare i Europeiska unionen]*

i enlighet med Avtalet

Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler

i enlighet med Avtalet

Roll (personuppgiftsansvarig/personuppgiftsbiträde)

i enlighet med Avtalet

Uppgiftsinförare: [*Uppgiftsinförarens/uppgiftsinförarnas identitet och kontaktuppgifter, inklusive eventuella kontaktpersoner med ansvar för dataskydd]*

i enlighet med Avtalet

Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler

i enlighet med Avtalet

Roll (personuppgiftsansvarig/personuppgiftsbiträde)

i enlighet med Avtalet

B. BESKRIVNING AV ÖVERFÖRINGEN

Kategorier av registrerade vars personuppgifter överförs

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Kategorier av personuppgifter som överförs

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Känsliga uppgifter som överförs (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder där full hänsyn tas till uppgifternas karaktär och de medföljande riskerna, till exempel strikt ändamålsbegränsning, åtkomstbegränsningar (däribland åtkomst endast för personal som har specialutbildning), registrering av åtkomst till uppgifterna, begränsningar av vidare överföringar eller ytterligare säkerhetsåtgärder.

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Frekvens för överföringen (t.ex. om uppgifterna överförs vid ett engångstillfälle eller kontinuerligt).

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Behandlingens karaktär

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Ändamålet/ändamålen med överföringen av uppgifter och den efterföljande behandlingen

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

Vid överföringar till personuppgiftsbiträden/underentreprenörer, ange även föremålet för behandlingen liksom dess karaktär och varaktighet

Som beskrivs i sektionerna 1 och 3 i Unit4 Information om Personuppgiftsbehandling

C. BEHÖRIG TILLSYNSMYNDIGHET

Ange den eller de behöriga tillsynsmyndigheterna i enlighet med klausul 13

Den behöriga tillsynsmyndigheten skall vara (såvida inte annat anges i klausul 13) den nederländska “De Autoriteit Persoonsgegevens (AP)”.

BILAGA II

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INKLUSIVE TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA UPPGIFTERNAS SÄKERHET

FÖRKLARANDE ANMÄRKNINGAR:

De tekniska och organisatoriska åtgärderna måste beskrivas i specifika (och inte allmänna) ordalag. Se även den allmänna kommentaren på den första sidan av tillägget, i synnerhet om behovet av att tydligt ange vilka åtgärder som är tillämpliga på varje överföring/uppsättning av överföringar.

Beskrivning av de tekniska och organisatoriska åtgärder som genomförts av uppgiftsinföraren/uppgiftsinförarna (inklusive relevanta tillstånd) för att säkerställa en lämplig säkerhetsnivå, med hänsyn till behandlingens karaktär, omfattning, sammanhang och ändamål, och riskerna för fysiska personers rättigheter och friheter.

Vid överföringar till personuppgiftsbiträden/underentreprenörer, beskriv även de särskilda tekniska och organisatoriska åtgärder som ska vidtas av personuppgiftsbiträdet/underentreprenören för att kunna bistå den personuppgiftsansvarige och, vid överföringar från ett personuppgiftsbiträde till en underentreprenör, uppgiftsutföraren

Som beskrivs i sektion 2 i Unit4 Information om Personuppgiftsbehandling

---

BILAGA III

FÖRTECKNING ÖVER UNDERENTREPRENÖRER

FÖRKLARANDE ANMÄRKNINGAR:

Denna bilaga måste fyllas i för modulerna två och tre i samband med utfärdandet av ett särskilt tillstånd för underentreprenörer (klausul 9 a, alternativ 1).

Ej tillämpligt.