

1. TILLÄMPNINGSSOMRÅDET FÖR DESSA PERSONUPPGIFTSBITRÄDESVILLKOR

- 1.1 Kunden (hädanefter kallad "**Personuppgiftsansvarig**"), är den Part som (ensam eller tillsammans med andra) bestämmer ändamålen och medlen för Behandlingen av Personuppgifter.
- 1.2 Unit4 och dess Koncernbolag (hädanefter kallad "**Personuppgiftsbiträdet**"), är den Part som agerar för den Personuppgiftsansvariges räkning, utan att stå direkt under den Personuppgiftsansvariges ansvar.
- 1.3 Personuppgiftsbiträdet ska Behandla Personuppgifterna åt den Personuppgiftsansvarige (och den Personuppgiftsansvarige godkänner detta) i enlighet med Dataskyddslagstiftningen och dessa Personuppgiftsbiträdesvillkor inklusive dess bilagor.
- 1.4 I Bilaga 1 beskrivs, utan begränsning, ändamålen och medlen med Behandlingen, kategorierna av Personuppgifter som ska Behandlas, lagringstiden för sådana Personuppgifter och landet/länderna (eller platsen/platserna) där Personuppgifterna ska Behandlas.
- 1.5 Bilaga 2 anger de tillämpliga säkerhetsåtgärder som implementerats av Personuppgiftsbiträdet, och som den Personuppgiftsansvarige bekräftar är adekvata.
- 1.6 Bilaga 3 anger uppgifter avseende eventuella Underbiträden.
- 1.7 Bilaga 4 innehåller EU:s standardavtalsklausuler, som är tillämpliga om det sker en överföring av Personuppgifter från den Personuppgiftsansvarige, lokaliserad i ett land inom EES, till Personuppgiftsbiträdet, som är lokaliserad i ett land utanför EES, enligt vad som beskrivs närmare i punkt 2.3 nedan.
- 1.8 Bilagorna till dessa Personuppgiftsbiträdesvillkor ska uppdateras från tid till annan under avtalstiden för dessa Personuppgiftsbiträdesvillkor, om nödvändigt.

2. BEHANDLING

- 2.1 Personuppgiftsbiträdet och den Personuppgiftsansvarige ska i god tid tillhandahålla varandra all nödvändig information som krävs för korrekt efterlevnad av Dataskyddslagstiftningen.
- 2.2 Behandlingen av Personuppgifter utförs i det land/på den plats, eller de länder/de platser, som anges i Bilaga 1. Den Personuppgiftsansvarige lämnar härmed sitt uttryckliga godkännande till Behandling av Personuppgifterna i de länder/platser som anges i Bilaga 1. Om Behandling kommer att ske i ett annat land/på annan plats, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige härmed.
- 2.3 Om Personuppgifterna ska Behandlas i ett land utanför Europeiska unionen (EU)/Europeiska Ekonomiska Samarbetsområdet (EES), för vilket EU-kommissionen inte utfärdat ett beslut om att det aktuella landet säkerställer en adekvat skyddsnivå, får Behandling endast ske om lämpliga skyddsåtgärder har vidtagits för att säkerställa en adekvat skyddsnivå för Personuppgifterna. I sådant fall ska Parterna, för att säkerställa att sådana lämpliga avtalade skyddsåtgärder föreligger, efterleva sina respektive åtaganden och skyldigheter i EU:s standardavtalsklausuler som bifogats i Bilaga 4 till dessa Personuppgiftsbiträdesvillkor (eller uppfylla sådana andra lämpliga skyddsåtgärder som Tillsynsmyndigheten eller en behörig lagstiftare anger uppfyller villkoren för en adekvat skyddsnivå för dataskydd), och den Personuppgiftsansvarige medger härmed, och instruerar Personuppgiftsbiträdet att utföra sådan Behandling.

3. PERSONUPPGIFTSBITRÄDETS SKYLDIGHETER

- 3.1 Personuppgiftsbiträdet ska Behandla Personuppgifter på ett korrekt och omsorgsfullt sätt i enlighet med villkoren i dessa Personuppgiftsbiträdesvillkor och ska säkerställa efterlevnaden av Dataskyddslagstiftningen till skydd för Personuppgifter.
- 3.2 Personuppgiftsbiträdet ska enbart Behandla Personuppgifterna i samband med fullgörandet av Avtalet och den Personuppgiftsansvariges skriftliga instruktioner, såvida inte Personuppgiftsbiträdet är skyldig enligt lag att Behandla uppgifterna för andra ändamål. Om en sådan skyldighet föreligger ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om den relevanta lagbestämmelsen och Personuppgiftsbiträdets skyldighet.
- 3.3 Personuppgiftsbiträdet ska endast Behandla Personuppgifterna för de ändamål som anges i de mottagna instruktionerna och i syfte att fullgöra skyldigheterna enligt dessa Personuppgiftsbiträdesvillkor. Personuppgiftsbiträdet har inte rätt att använda Personuppgifterna för andra ändamål.
- 3.4 Personuppgiftsbiträdet får inte överföra Personuppgifterna till en Tredje part (annat än till den Registrerade eller till person som är godkänd av den Personuppgiftsansvarige eller Personuppgiftsbiträdet att Behandla Personuppgifterna), såvida inte en sådan överföring sker på instruktion från den Personuppgiftsansvarige eller i samband med fullgörandet av Avtalet och dessa Personuppgiftsbiträdesvillkor (inklusive respektive bilagor) eller när det är nödvändigt för att uppfylla en skyldighet enligt lag eller domstolsbeslut.
- 3.5 Personuppgiftsbiträdet får inte ändra Personuppgifterna, såvida inte den Personuppgiftsansvarige instruerar om en sådan ändring.
- 3.6 Personuppgiftsbiträdet ska hjälpa den Personuppgiftsansvarige i rimlig omfattning för att hantera en begäran från en Registrerad om utövande av sina rättigheter enligt Dataskyddslagstiftningen, innefattande men inte begränsat till att (i) säkerställa att de Registrerade får tillgång till sina Personuppgifter, (ii) på den Registrerades förfrågan, rätta eller radera Personuppgifter, (iii) på den Registrerades förfrågan, tillhandahålla dokumentation som utvisar att rättelse eller radering skett, (iv) på den Registrerades förfrågan, tillhandahålla de Personuppgifter som den Registrerade har lämnat till den Personuppgiftsansvarige och som den Personuppgiftsansvarige har lämnat till Personuppgiftsbiträdet, och (v) på den Registrerades förfrågan, överföra Personuppgifter till en annan personuppgiftsansvarig (dataportabilitet). Personuppgiftsbiträdet ska tillhandahålla Personuppgifterna i ett strukturerat, allmänt använt och maskinläsbart format i händelse av en begäran om återlämning eller utlämnande av Personuppgifterna.
- 3.7 Om Personuppgiftsbiträdet mottager en förfrågan eller invändning från en Registrerad (vilket kan innefatta (men inte är begränsat till) en förfrågan om information, tillgång, rättelse, dataöverföring, begränsning av behandling, eller överföring av Personuppgifter) ska Personuppgiftsbiträdet omedelbart vidarebefordra förfrågan till den Personuppgiftsansvarige.
- 3.8 Personuppgiftsbiträdet ska föra ett register över alla kategorier av Behandlingar som görs för den Personuppgiftsansvariges räkning, i enlighet med kraven i Dataskyddslagstiftningen. Personuppgiftsansvarig ska tillhandahålla Personuppgiftsbiträdet all nödvändig information som behövs för detta syfte.
- 3.9 Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige med uppfyllelse av legala informationsskyldigheter i förhållande till Tillsynsmyndigheter och Registrerade, och om nödvändigt och om det rör Personuppgiftsbiträdets teknologi, bistå den Personuppgiftsansvarige om en konsekvensbedömning avseende dataskydd krävs enligt Dataskyddslagstiftningen.
- 3.10 Om den Personuppgiftsansvarige är föremål för en specifik begäran om information från en Registrerad eller annan tredje part (annat än den Registrerade eller person som är behörig att Behandla Personuppgifterna under den Personuppgiftsansvariges eller Personuppgiftsbiträdets direkta ansvar), som är berättigad att framställa en sådan begäran, ska Personuppgiftsbiträdet bistå den Personuppgiftsansvarige därmed. Personuppgiftsbiträdet ska inte vidta några åtgärder avseende förfrågningar från Registrerade eller tredje parter (annat än den Registrerade eller till person som är godkänd av den Personuppgiftsansvarige eller Personuppgiftsbiträdet att Behandla Personuppgifterna), såvida inte den Personuppgiftsansvarige har instruerat Personuppgiftsbiträdet därom på förhand. Om en Registrerad kontaktar Personuppgiftsbiträdet för att utöva sina rättigheter enligt Tillämplig Lag ska Personuppgiftsbiträdet omedelbart vidarebefordra en sådan förfrågan till den Personuppgiftsansvarige.

4 DEN PERSONUPPGIFTSANSVARIGES SKYLDIGHETER

- 4.1 Den Personuppgiftsansvarige ansvarar för lagligheten av Behandlingen av Personuppgifterna, och uppfyllelse av legala krav enligt Dataskyddslagstiftningen, inklusive, men inte begränsat till, skyddet för de Registrerades rättigheter.
- 4.2 Den Personuppgiftsansvarige ansvarar självständigt för att bestämma ändamålen och medlen för Behandlingen av Personuppgifter.
- 4.3 Den Personuppgiftsansvarige ansvarar för att informera de Registrerade och garantera att de Registrerade kan utöva sina rättigheter enligt Dataskyddslagstiftningen och annan tillämplig lagstiftning och regelverk till skydd för personuppgifter, och för kommunikation med de Registrerade.
- 4.4 Den Personuppgiftsansvarige garanterar att de insamlade Personuppgifterna är adekvata, relevanta och inte för omfattande i relation till de ändamål för vilka Personuppgifterna överförs och (på annat sätt) Behandlas.
- 4.5 Den Personuppgiftsansvarige ska, i god tid och enlighet med det överenskomna format som anges i Bilaga 1, tillhandahålla all information som Personuppgiftsbiträdet kan behöva för Behandlingen.
- 4.6 Den Personuppgiftsansvarige ansvarar för (i förhållandet mellan Parterna, och i förhållande till de Registrerade och Tillsynsmyndigheten att: (i) tillse att de Registrerade har lämnat erforderliga samtycken för Behandlingen (av Personuppgiftsbiträdet och av eventuella Underbiträden) och/eller att annan laglig grund för Behandlingen föreligger; och (ii) alla krav och klagomål som härrör från Personuppgiftsbitrådets åtgärder, i den utsträckning som sådana åtgärder är ett resultat av den Personuppgiftsansvariges instruktioner.

5 UNDERBITRÄDEN

- 5.1 Personuppgiftsbiträdet kommer att anlita de Underbiträden som finns angivna i Bilaga 3 eller i ett Orderformulär.
- 5.2 Den Personuppgiftsansvarige godkänner härmed att ändringar får ske avseende Underbiträden. Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige skriftligen i förväg vid planerade förändringar, såsom vid byte av Underbiträden. Den Personuppgiftsansvarige kan skriftligen invända mot sådana förändringar inom sju (7) dagar efter mottagande av den skriftliga underrättelsen om sådan förändring.
- 5.3 Personuppgiftsbitrådets anlåtande av ett Underbiträde påverkar inte på något sätt de skyldigheter Personuppgiftsbiträdet har gentemot den Personuppgiftsansvarige. Underbiträdet får endast ges tillgång till de relevanta Personuppgifterna när Underbiträdet uppfyller (eller säkerställer uppfyllelse av) skyldigheterna enligt dessa Personuppgiftsbiträdesvillkor i alla väsentliga avseenden. Personuppgiftsbiträdet ska ingå ett skriftligt avtal med varje Underbiträde avseende behandlingen av Personuppgifter, som ska uppfylla kraven i Dataskyddslagstiftningen, och där så är praktiskt genomförbart, vara på väsentligen samma villkor som de som anges i dessa Personuppgiftsbiträdesvillkor.
- 5.4 Bilaga 3 anger nuvarande Underbiträden, geografisk plats för Behandlingen och beskrivning av de tjänster som tillhandahålls av respektive Underbiträde. Personuppgiftsbiträdet ska, om nödvändigt och inom skälig tid efter en förändring, uppdatera denna Bilaga under avtalstiden för Avtalet.
- 5.5 Om Personuppgiftsbiträdet har underkontrakterat skyldigheter till ett Underbiträde som har godkänts av den Personuppgiftsansvarige (under Avtalet, eller enligt senare lämnat godkännande), ska Personuppgiftsbiträdet vara ansvarig under dessa Personuppgiftsbiträdesvillkor för alla åtgärder som vidtas av sådant Underbiträde.
- 5.6 Om Personuppgiftsbiträdet har underkontrakterat skyldigheter till ett Underbiträde, kan den Personuppgiftsansvarige (under vissa omständigheter) lämna instruktioner till Underbiträdet avseende Behandlingen av den Personuppgiftsansvariges Personuppgifter av Underbiträdet. Under sådana omständigheter är inte Personuppgiftsbiträdet ansvarigt för ett brott mot dessa Personuppgiftsbiträdesvillkor som uppkommer till följd av att Underbiträdet agerar i enlighet med den Personuppgiftsansvariges instruktioner, oavsett om Personuppgiftsbiträdet är medvetna om dessa eller ej.

6 SÄKERHET OCH PERSONUPPGIFTSINCIDENTER

- 6.1 Personuppgiftsbiträdet ska vidta sådana tekniska och organisatoriska säkerhetsåtgärder, i enlighet med Dataskyddslagstiftningen och god branschstandard, som är nödvändiga för att säkerställa tillgänglighet, integritet och sekretess i förhållande till Personuppgifterna och för att skydda Personuppgifterna mot förlust eller olaglig Behandling. För att kunna uppfylla dessa krav, ska den Personuppgiftsansvarige informera Personuppgiftsbiträdet om de säkerhetskrav som gäller för Personuppgifterna och, vid förändringar i Behandlingen av Personuppgifter, i god tid tillhandahålla den information som krävs.
- 6.2 De tekniska och organisatoriska säkerhetsåtgärderna finns beskrivna i Bilaga 2 och överensstämmer med allmänt godtagbara säkerhetsstandarder. Den Personuppgiftsansvarige bekräftar att denne är införstådd med att de arrangemang som framgår av Bilaga 2 är tillräckliga för att säkerställa en lämplig säkerhetsnivå för Personuppgifterna, i enlighet med Dataskyddslagstiftningen.
- 6.3 Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en Personuppgiftsincident.
- 6.4 Den underrättelse som avses i punkt 6.3 ska åtminstone innehålla:
 - 6.4.1 en beskrivning av Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet Registrerade som berörs samt de kategorier av och det ungefärliga antalet Personuppgifter som berörs;
 - 6.4.2 namnet på och kontaktuppgifterna för Dataskyddsombudet eller annan kontaktperson från vilken mer information kan erhållas;
 - 6.4.3 en beskrivning av de sannolika konsekvenserna av Personuppgiftsincidenten; och
 - 6.4.4 en beskrivning av de åtgärder som Personuppgiftsbiträdet har vidtagit för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
- 6.5 Vid en Personuppgiftsincident ska Personuppgiftsbiträdet bistå den Personuppgiftsansvarige med att fullgöra dennes lagstadgade informationsskyldighet gentemot Tillsynsmyndigheter och/eller de Registrerade.
- 6.6 Om Personuppgiftsbiträdet anser att en instruktion från den Personuppgiftsansvarige avseende Behandling strider mot Dataskyddslagstiftningen, ska denne omedelbart informera den Personuppgiftsansvarige därom.

7 YTTERLIGARE SEKRETESSBESTÄMMELSER

- 7.1 Personuppgiftsbiträdet ska behandla alla Personuppgifter som Behandlas under Avtalet med sekretess, och ska vidta alla nödvändiga åtgärder för att upprätthålla sekretessen för Personuppgifterna. Personuppgiftsbiträdet ska också tillse att sådan sekretess gäller för dess anställda och anlitad personal som har tillgång till Personuppgifterna.
- 7.2 Sekretessskyldigheten som hänvisas till i denna punkt ska inte gälla om den Personuppgiftsansvarige har lämnat skriftligt tillstånd att lämna ut Personuppgifterna till en tredje part, eller är skyldig enligt lag att lämna ut Personuppgifterna till en tredje part.

8 REVISIONER

- 8.1 Personuppgiftsbiträdet ger den Personuppgiftsansvarige möjlighet att kontrollera Personuppgiftsbitrådets efterlevnad av dessa Personuppgiftsbitrådesvillkor, eller medger en revision som görs av oberoende revisorer, på den Personuppgiftsansvariges bekostnad, utan användning av den Personuppgiftsbitrådets konfidentiella information och utan att störa Personuppgiftsbitrådets verksamhet. Om revisionen visar att Personuppgiftsbiträdet inte fullgör sina åtaganden enligt dessa Personuppgiftsbitrådesvillkor ska Personuppgiftsbiträdet åtgärda sådana brister så snart är praktiskt möjligt. I sådant fall ska Personuppgiftsbiträdet betala skäligen och verifierade kostnader för revisorn (betalning sker endast mot uppvisande av en giltig faktura från revisorerna för sådana kostnader).
- 8.2 Revision får äga rum högst en gång per år, såvida det inte finns påvisbara omständigheter som utvisar att Personuppgiftsbiträdet inte fullgör sina åtaganden enligt dessa Personuppgiftsbitrådesvillkor. Personuppgiftsbiträdet ska tillhandahålla all information som rimligen är nödvändig för att utföra revisionen.
- 8.3 Vid en inspektion av en Tillsynsmyndighet eller av en annan behörig myndighet (en "Myndighet"), ska Personuppgiftsbiträdet samarbeta i den utsträckning som rimligen krävs och informera den Personuppgiftsansvarige därom så snart som möjligt.
- 8.4 Personuppgiftsbiträdet ska utse en kontaktperson som assisterar den Personuppgiftsansvarige fullgörande av informationsskyldigheter som uppkommer till följd av Behandlingen, och Personuppgiftsbiträdet ska informera den Personuppgiftsansvarige om kontaktpersonerna till kontaktpersonen.

9 ÄNDRINGAR

- 9.1 För det fall förändringar av åtaganden och skyldigheter enligt Avtalet kan medföra väsentliga konsekvenser för Behandlingen av Personuppgifter, ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige en underrättelse om de föreslagna ändringarna till dessa Personuppgiftsbitrådesvillkor (vilket kan ske via e-post eller via Unit4 Community). Den Personuppgiftsansvarige ska meddela eventuella invändningar avseende sådana väsentliga konsekvenser inom 7 dagar från mottagandet av underrättelsen, och om invändning ej görs, ska den Personuppgiftsansvarige anses ha accepterat ändringarna och den uppdaterade versionen ska anses gälla från angiven dag.
- 9.2 Ändringar av bilagorna till dessa Personuppgiftsbitrådesvillkor kan göras av Personuppgiftsbiträdet från tid till annan och publiceras på dess webbsida. Dessa ändringar ska meddelas den Personuppgiftsansvarige (sådan meddelande kan ske genom e-post eller via Unit4 Community), varvid versionsnummer och datum för den uppdaterade versionen ska anges. Väsentliga ändringar av bilagorna kommer inte att göras utan att den Personuppgiftsansvarige fått möjlighet att invända däremot.

10 ÖMSESIDIG SKADESLÖSHETSFÖRBINDELSE

- 10.1 Personuppgiftsbiträdet ska hålla den Personuppgiftsansvarige skadeslös från böter och/eller sanktionsavgifter som Tillsynsmyndigheten, eller annan på Tillsynsmyndighetens vägnar, påför den Personuppgiftsansvarige, och från krav på skadestånd från Registrerade, om det har fastställts att sådana böter och/eller sanktionsavgifter eller skadeståndsanspråk är en direkt följd av att Personuppgiftsbiträdet har Behandlat Personuppgifter i strid med sådana skyldigheter som åligger Personuppgiftsbiträdet enligt Dataskyddslagstiftningen eller annan tillämplig lagstiftning för dataskydd.

För att kunna tillgodogöra sig skadeslöshetsåtagandet i denna punkt 10.1 ska den Personuppgiftsansvarige:

- (i) omedelbart skriftligen informera Personuppgiftsbiträdet om existensen av och innehållet i ett ersättningsanspråk från en Registrerad eller en utredning eller annan instruktion som kan leda till att Tillsynsmyndigheten avser att fatta, eller fattar, ett beslut om påförande av böter/sanktionsavgift;
 - (ii) agera i samråd med Personuppgiftsbiträdet avseende åtgärder och kommunikation med Tillsynsmyndigheten eller den Registrerade;
 - (iii) om det finns skäl, invända mot och/eller överklaga påförda böter/sanktionsavgifter; och
 - (iv) låta Personuppgiftsbiträdet självständigt hantera ärendet, inklusive förlikningar. För detta syfte ska den Personuppgiftsansvarige samarbeta med och tillhandahålla nödvändiga fullmakter och information till Personuppgiftsbiträdet, för att Personuppgiftsbiträdet ska kunna tillvarata sin rätt i förhållande till de legala åtgärderna och, om nödvändigt, agera i den Personuppgiftsansvariges namn.
- 10.2 Den Personuppgiftsansvarige ska hålla Personuppgiftsbiträdet skadeslös från böter och/eller sanktionsavgifter som Tillsynsmyndigheten, eller annan på Tillsynsmyndighetens vägnar, påför den Personuppgiftsbiträdet, och från krav på skadestånd från Registrerade, om det har fastställts att sådana böter och/eller sanktionsavgifter eller skadeståndsanspråk är en följd av att den Personuppgiftsansvarige har brutit mot sina skyldigheter enligt Dataskyddslagstiftningen eller annan tillämplig lagstiftning för dataskydd.

För att kunna tillgodogöra sig skadeslöshetsåtagandet i denna punkt 10.2 ska Personuppgiftsbiträdet:

- (i) omedelbart skriftligen informera den Personuppgiftsansvarige om existensen av och innehållet i ett ersättningsanspråk från en Registrerad eller en utredning eller annan instruktion som kan leda till att Tillsynsmyndigheten avser att fatta, eller fattar, ett beslut om påförande av böter/sanktionsavgift;
 - (ii) agera i samråd med den Personuppgiftsansvarige avseende åtgärder och kommunikation med Tillsynsmyndigheten eller den Registrerade;
 - (iii) om det finns skäl, invända mot och/eller överklaga påförda böter/sanktionsavgifter; och
 - (iv) låta den Personuppgiftsansvarige självständigt hantera ärendet, inklusive förlikningar. För detta syfte ska Personuppgiftsbiträdet samarbeta med och tillhandahålla nödvändiga fullmakter och information till den Personuppgiftsansvarige, för att den Personuppgiftsansvarige ska kunna tillvarata sin rätt i förhållande till de legala åtgärderna och, om nödvändigt, agera i Personuppgiftsbitrådets namn.
- 10.3 Om Parterna är gemensamt ansvariga (vare sig solidariskt ansvariga eller på annat sätt) gentemot tredje parter, inklusive berörda Registrerade, eller blir gemensamt påförda en sanktionsavgift från Tillsynsmyndigheten, ska respektive Part ansvara gentemot varandra enligt punkt 10.1 och 10.2 ovan för en sådan andel av skadeståndet eller böterna/sanktionsavgiften som är proportionerlig mot respektive Parts skuld till den händelse som orsakat ansvaret, med hänsyn tagen till beslut eller dom från domstol eller annan tvistlösningsinstans, eller Tillsynsmyndigheten, och i vilken utsträckning Parts brott mot sina åtaganden enligt dessa Personuppgiftsbitrådesvillkor bidragit till ansvaret.

11 AVTALSTID OCH UPPSÄGNING

- 11.1 Dessa Personuppgiftsbitrådesvillkor ska träda i kraft när båda Parter undertecknat Avtalet.
- 11.2 När Avtalet upphör att gälla ska Personuppgiftsbiträdet överföra – eller på den Personuppgiftsansvariges begäran förstöra – Personuppgifterna på det sätt som anges i Bilaga 1. För det fall Personuppgifter lagras i ett datorsystem eller i en annan form som inte skäligen kan överföras till den Personuppgiftsansvarige ska Personuppgiftsbiträdet omedelbart radera Personuppgifterna från sina system, såvida inte annat överenskommit skriftligen.

Bilagor:

Bilaga 1: Beskrivning av Behandlingen av Personuppgifter

Bilaga 2: Säkerhetsåtgärder

Bilaga 3: Underbiträden

Bilaga 4: EU:s standardavtalsklausuler

BILAGA 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 7	Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; nationellt försäkringsnummer eller sjukförsäkringsnummer eller ID-kortsnummer; civilstånd; socialförsäkringsinformation under 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.	<ul style="list-style-type: none"> Nuvarande och före detta anställda; Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och Arbetsökande 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; nationellt försäkringsnummer eller 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.	<ul style="list-style-type: none"> Nuvarande och före detta anställda; Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och Arbetsökande och potentiella arbetstagare.
Unit4 Student Management	<p>Namn; adresser; avtalsuppgifter; telefonnummer (inklusive mobiltelefonnummer); e-postadress(er); annan kontaktinformation; födelsedatum; ålder; födelseplats; nationalitet eller medborgarskap; hemort; legal hemvist; talade språk; passnummer; nationellt försäkringsnummer eller 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.</p> <p>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.</p> <p>Ytterligare Personuppgifter avseende före detta och nuvarande sökande: information om tidigare utbildning; betyg och/eller testresultat; fysisk hälsostatus; arbetsintyg från tidigare arbetsgivare; och arbetsplatsinformation.</p> <p>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.</p>	<ul style="list-style-type: none"> Nuvarande och före detta anställda; Konsulter och underkonsulter (av olika slag), agenter eller befattningshavare; och and Arbetsökande 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 <u>inte</u> 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.	<ul style="list-style-type: none"> 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 <u>inte</u> 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.	<ul style="list-style-type: none"> 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) Arbetsökande och potentiella arbetstagare. 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.	<ul style="list-style-type: none"> Nuvarande och före detta anställda; Nuvarande och före detta jobbkandidater

	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.	Konsulter eller underkonsulter (av olika slag), agenter eller befattningshavare; och Arbetssökande och potentiella arbetstagare.
People Platform Services ("PPS") (generellt) inklusive IDS och Wanda (tillsammans med eventuella stödtjänster)	Eftersom PPS 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.

2. BEHANDLINGENS ART OCH ÄNDAMÅL

Generellt består Personuppgiftsbitrådets Behandling enbart av de åtgärder som är nödvändiga för att Personuppgiftsbitrådet 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 Personuppgiftsbitrådets åtaganden och utövande av dess rättigheter under dessa Personuppgiftsbitrådesvillkor, inklusive utförandet av funktioner som krävs eller begärs av den Personuppgiftsansvarige för att den Personuppgiftsansvarige ska uppfylla sina lagliga och/eller kontraktuella skyldigheter. Med avseende på, och beroende av, respektive Produkt eller Tjänst, kommer Behandlingen att inkludera följande:

Produkt	Behandlingens art och ändamål
Unit4 ERP 7	<p>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:</p> <ul style="list-style-type: none"> • Reseansökningar; • Hantering av utlägg; • Behandling av tidrapporter; • Frånvarohantering; • HR & lönerelaterade processer: <ul style="list-style-type: none"> ○ Lön; ○ Inskrivning på kurser; ○ Kompetenshantering; ○ Omdömen; ○ Lönerrevision; ○ Registrering av arbetssökande; • Genomförande av betalningar; • Fakturering; • Köprekvisitioner; • Personal/projektplanering. <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 ERP 7 Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. <p>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.</p>
Unit4 Financials	<p>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:</p> <ul style="list-style-type: none"> • Registrering av kunder/leverantörer/anställda; • Genomförande av betalningar; • Fakturering; • Hantering av utlägg; • Expense claim processing; • Reseansökningar; • Köprekvisitioner och beställningar; • Personal/projektplanering; • HR & lönerelaterade processer: <ul style="list-style-type: none"> ○ Lön; ○ Behandling av tidrapporter; ○ Frånvarohantering; ○ Inskrivning på kurser;

	<ul style="list-style-type: none"> ○ Kompetenshantering; ○ Omdömen; ○ Lönerrevision; ○ Registrering av arbetssökande. <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • 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. <p>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.</p>
Unit4 Student Management	<p>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:</p> <ul style="list-style-type: none"> • 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 <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Student Management Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. <p>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.</p>
Unit4 FP&A	<p>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:</p> <ul style="list-style-type: none"> • Budget; • Finansiell och annan rapportering; • Distribution av rapporter; • Behandling av godkännanden; • Personal/projektplanering. <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4s FP&A Produkt, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. <p>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.</p>
Unit4 Talent Management	<p>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:</p> <ul style="list-style-type: none"> • Hantering av humankapital • Hantering av arbetstagares prestationer • Talangutveckling • Utvärdering av kandidater

	<ul style="list-style-type: none"> • Utbildning • Återkoppling och beröm; • Personanalys och -engagemang <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 Talent Management SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Talent Management molntjänst. • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 Talent Management Produkten, och assistera Kunden i samband med drift av lösningen enligt vad som anges närmare i Unit4s Supportvillkor. <p>Åtkomst till Personuppgifter för att tillhandahålla konfiguration och/eller kund Anpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.</p>
Unit4 Assistance PSA Suite	<p>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:</p> <ul style="list-style-type: none"> • 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; • integration av projekt i andra applikationer; • utförande av redovisning för assistans vid integration av finansiella data med andra lösningar. <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4s Unit4 Assistance PSA Suite 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 kund Anpassning och/eller datamigrering (t.ex. från äldre system) och/eller andra Konsulttjänster som köps av Kunden.
People Platform Services ("PPS") (generellt) inklusive IDS och Wanda (tillsammans med eventuella stöd tjänster)	<p>Personuppgifter kommer att behandlas av PPS för att tillåta de angivna syftena med tjänsten enligt vad som anges i den tillämpliga Tjänstebeskrivningen för PPS på www.unit4.com/terms.</p> <p>Dessutom kommer Personuppgifter att införas i Wanda genom användning av valfria 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:</p> <ul style="list-style-type: none"> • Registrering av tidsposter • Registrering av utlägg • Reseansökningar • Förfrågningar om lönebesked • Registrering av frånvaro • Balansförfrågningar • Köprekvitioner. <p>Behandlingen kommer att involvera:</p> <p>Produkt (programvarulösning)</p> <ul style="list-style-type: none"> • 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 Personuppgiftsbitrådets kontroll, genom integrationer. <p>Tjänster</p> <ul style="list-style-type: none"> • Överföring och lagring av Personuppgifter för att tillhandahålla ytterligare Unit4 SaaS enligt vad som anges närmare i Unit4s Tjänstebeskrivning för Unit4 SaaS, eller People Platform Services (enligt vad som anges närmare i tillämplig Tjänstebeskrivning för People Platform Services). • Åtkomst till Personuppgifter för att tillhandahålla support och underhåll för Unit4 PPS 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 kund Anpassning 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 för molntjänsterna.	<u>Personal</u> Unit4 Cloud Services Operations har personal i Polen, Sverige, Norge, Storbritannien, USA, Kanada, Malaysia och Singapore. Denna personal hos Personuppgiftsbiträdet driver Unit4 SaaS. <u>Tillgångar och infrastruktur</u> Unit4 använder hostade infrastukturtjänster från tredje part för att tillhandahålla Unit4 SaaS, och nyttjar andra programvarusystem för drift och förvaltning. Se Bilaga 3.
U4 Talent Management SaaS	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i Unit4s Tjänstebeskrivning för Talent Management SaaS.	<u>Personal</u> Unit4s Talent Management Cloud Services Operations har personal huvudsakligen i Belgien och i vissa andra EES-länder. Denna personal hos Personuppgiftsbiträdet driver Unit4 Talent Management SaaS. <u>Tillgångar och infrastruktur</u> Unit4 använder hostade infrastukturtjänster från tredje part för att tillhandahålla Unit4 Talent Management SaaS, och nyttjar andra programvarusystem för drift och förvaltning. Se Bilaga 3.
Supporttjänster	Personuppgiftsbiträdet ska Behandla Personuppgifterna i enlighet med de aktiviteter som beskrivs i Avtalet, och mer specifikt i Unit4s Supportvillkor.	<u>Personal</u> Unit4 Kundsupport har personal i Polen, Sverige, Norge, Storbritannien, Tyskland, Portugal, 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 i avsnitt B i SLA). <u>Tillgångar och infrastruktur</u> 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.	<u>Personal</u> 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. <u>Tillgångar och infrastruktur</u> 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 Bilaga 3. Personuppgiftsbiträdet ska ingå ett skriftligt avtal med Underbiträdet, som ska vara i enlighet med Dataskyddslagstiftningen och dessa Personuppgiftsbiträdes-villkor. Vidare har den Personuppgiftsansvarige medgett att Personuppgiftsbiträdet anlitar de tillämpliga Underbiträden som finns angivna i Bilaga 3 genom att ingå dessa Personuppgifts-biträdesvillkor.	Se Bilaga 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 tjänste-dokumentation som tillhandahålls som en del av Avtalet.	Se Bilaga 3 eller tillämpligt Orderformulär, och eventuella kompletterande villkor i ytterligare bilagor till dessa Personuppgiftsbiträdesvillkor, om detta krävs av Tredjepartsleverantören eller enligt Tillämplig Lag.
People Platform Services ("PPS") (generellt) inklusive IDS och Wanda (tillsammans med eventuella stödtjänster)	I tillägg till vad som anges för Unit4 SaaS, kommer PPS att (där så är tillämpligt) Behandla Personuppgifter i enlighet med en integritetspolicy som presenteras för slutanvändaren, som ombeds lämna sitt samtycke, där sådana Personuppgifter Behandlas.	<u>Personal</u> Unit4 Cloud Services Operations, som driver PPS, har personal i Polen, Sverige, Norge, Storbritannien, USA, Kanada, Malaysia och Singapore. Denna personal hos Personuppgiftsbiträdet driver Unit4 SaaS. <u>Tillgångar och infrastruktur</u>

	<p>Unit4 nyttjar sina egna och tredje parts (delade) infrastrukturtjänster för att tillhandahålla Unit4s People Platform tjänster. Detta inkluderar tredjepartssystem (s.k. collaboration apps), över vilka Unit4 inte har någon kontroll. PPS, inklusive Wanda, använder ett antal olika produkter och tjänster från Microsoft, enligt följande:</p> <ul style="list-style-type: none"> • Kognitiva tjänster: <ul style="list-style-type: none"> ◦ 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 supporteade sociala kanaler. • Traffic manager – används för katastrofåterställning och reservsystem om den primära regionen är instabil • Web apps / web jobs – hostar webb APler 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 • 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, inklusive telemetri och loggning • SQL server – tillhandahåller lagring • Kubernetes – open source container <p>Ytterligare information och detaljer avseende dessa Microsoftprodukter och -tjänster återfinns här: https://azure.microsoft.com/en-us/services/.</p>
--	---

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

Produkt – Lokal Installationsmiljö (On-premises)	Datan lagras på den Personuppgiftsansvariges servrar på dess huvudsakliga verksamhetsort eller registrerade säte, enligt vad som meddelas Unit4 från tid till annan.			
Produkt - Unit4 SaaS	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.			
	TYP AV MOLNTJÄNST	GEOPOLITISK ZON	PLATS FÖR DATACENTER	ANLÄGGNING ELLER PARTNERSKAP
	SAAS CLOUD	EU	DUBLIN / AMSTERDAM	MICROSOFT AZURE
	SAAS CLOUD	USA	FLERTAL PLATSER	MICROSOFT AZURE
	SAAS CLOUD	KANADA	TORONTO / QUEBEC CITY	MICROSOFT AZURE
	SAAS CLOUD	STORBRIANNIEN	LONDON / CARDIFF	MICROSOFT AZURE
	SAAS CLOUD	ASIEN	SINGAPORE / HONG KONG	MICROSOFT AZURE
	SAAS CLOUD	AUSTRALIEN	VICTORIA / NEW SOUTH WALES	MICROSOFT AZURE
	SAAS CLOUD	NORGE	OSLO / STAVANGER	MICROSOFT AZURE
SAAS CLOUD	SVERIGE (NORDEN)	SÅTRA OCH SOLLENTUNA	CONAPTO	
Produkt – Talent Management SaaS	Talent Management SaaS tillhandahålls från Amazon Web Services (ABW) datacenter i Frankfurt. All Kundens Data, förutom vid delning med utvalda underbiträden i Bilaga 3, kommer att lagras enbart i den valda geopolitiska zonen, och kommer inte att flyttas utanför den utan uttryckligt medgivande från Kunden.			
Unit4 Support – Standardsupport och andra standardiserade supporttjänster	Unit4 Support använder tredjepartsprogramvara (såsom salesforce / ServiceNow) för att registrera och hantera Årenden. Dessa Årenden är åtkomliga för alla Unit4s anställda som har åtkomst till tredjepartsprogramvaran, såsom supporttekniker, molntjänstekniker, 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:	
	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.		

Unit4 Support – 24/7 Support (För Kunder som har Utökad Support och Premiumsupport)	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.			
Unit4 Support – Enbart EU-Support	Om Enbart EU-Support har valts, supporteras Ärenden enbart från de platser inom EU som anges ovan för Standardsupport (under Kontorstid).			
People Platform Services ("PPS") (generellt) inklusive IDS och Wanda (tillsammans med eventuella stödtjänster)	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 utanför EU.	Irland, USA och andra globala supportcenter där så krävs
	IDS	Beror på var molntjänsten tagits i produktion	Enligt ovan för Unit4 SaaS.	Enligt ovan för Unit4 SaaS.
Unit4 Konsulttjänster och Unit4s Customer Success funktion	Ämnesområde	Konsulttjänster och Customer Success tillhandahålls från:		
	Implementation och andra projektjänster	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.		

6. KONTAKTUPPGIFTER

Frågor eller kommentarer avseende dessa Personuppgiftsvillkor eller dess Bilagor ställs till följande kontaktpersoner:

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

Personuppgiftsbiträdet: Genom brev (skickat till Global Data Privacy 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.

BILAGA 2 – SÄKERHETSÅTGÄRDER

I enlighet med vad som anges i punkt 6 i Personuppgiftsbiträdesvillkoren, anges de tekniska och organisatoriska säkerhetsåtgärderna i denna Bilaga, 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 inträngsovervakning, 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 i ärendehanteringssystemet.
- 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.
- Antiviruskydd – 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 (Global Information Security Manager) och Unit4s globala dataskyddsombud (Global Data Privacy 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 är krypterade genom att använda krypteringsteknologi för hela databasen såsom Transparent Database Encryption. Azure Storage Service Encryption används för att kryptera alla data som placeras i kundens lagringskonto.
- 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 förfinas 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 processer 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 med användning av exempelvis Dedicated Accounts och genom att ha separata databasinstanser för alla Unit4s kunder.

Nätverksisolering på flera punkter:

- Varje dedikerad utplacering (deployment) är isolerad från andra utplaceringar och kommunicerar genom privata IP-adresser.
- Kundens virtuella maskiner (VM) kan bara kommunicera med andra virtuella maskiner som ägs eller kontrolleras av samma kund, och med ändpunkter för infrastruktur tjänster som är avsedda för offentlig kommunikation.
- Trafik mellan virtuella maskiner överförs alltid genom pålitliga paketfilter.

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

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. Kryptering av vilande data kan beställas som en tilläggstjänst av kunden. 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 kunddata (genom en direkt databaskoppling). Åtkomst av Unit4 till personlig information 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.

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 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.

Som bevis för säker design och drift, innehar Unit4 Cloud Services SaaS Ops ISO 27001:2013 certifiering och ISAE3402 (SOC1) rapport. Unit4 och operatörerna av datacenter innehar ett antal olika säkerhetscertifieringar, för närmare detaljer se tjänstebeskrivningen för Unit4 SaaS.

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 (1.2) 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 säkerhetspolicy och säkerhetsprogram återfinns på www.unit4.com/terms.

Dataskryptering

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.

Ytterligare element avseende Unit4 SaaS – Talent Management (sammanfattning)

Talent Management SaaS är ISO27001-certifierad och har genomgått en ISO27001 (fas 1 & 2) och GDPR granskning. Den mest relevanta informationen inkluderas i tabellen nedan, och ytterligare dokumentation eller information finns tillgänglig på begäran.

Domän	Hantering
Informationssäkerhet – hantering och styrning	Talent Management SaaS har implementerat ett hanteringssystem för informationssäkerhet (Information Security Management System, ISMS) under ISO27001. Detta innehåller, men är inte begränsat till, en informationssäkerhetspolicy för alla anställda. Denna policy kan tillhandahållas på begäran. Dessutom, för att tillhandahålla informationssäkerhet, implementeras hanteringsåtgärder som reducerar risker. Dessa risker, och sannolikheten för att de ska inträffa, inkluderas i ISMS (ISO 27001).
Personalsäkerhet	Tillhandahållandet av Talent Management SaaS regleras genom att alla konfidentiella data finns i ett HRIS (Human Resource Information System) och uppfyller ISO27001, för vilket informationssäkerhetsavdelningen är ansvarig.
Hantering av tillgångar	Tillgångar (både digitala och icke-digitala) hanteras inom ramen för en policy för dataklassificering.
Åtkomstkontroll för information	Det finns flera policys, som fungerar i enlighet med principen för lägsta privilegienivå (least privilege), både för tillhandahållna applikationer, allmän information och egen data. Tillgång till egna system, som hostas av Amazon (AWS) är begränsad till de specifikt identifierade individerna, och användning av lösenord är strikt förbjuden. Enbart publika/privata nyckelpar används för autentisering med servrar. Åtkomsträttigheterna per användare bestäms i enlighet med den fastställda åtkomstpolicyen. Specifika frågor om informationsåtkomst och dess policys kan sändas till informationssäkerhet.
Driftssäkerhet	Detta faller inom ramen för vår ISMS (ISO 27001).
Kommunikations-säkerhet	All kommunikation faller under en policy för dataklassificering. All nätverkstrafik sker över SSL/HTTPS, det mest vanliga och betrodda kommunikationsprotokollet över Internet. Intern infrastruktur isoleras genom användning av strikta brandväggar och nätverksåtkomstlistor. Varje system designas till en brandväggssäkerhetsgrupp beroende på funktion. Grundläget är att all åtkomst nekas och enbart uttryckligen tillåtna portar är öppna. Uthållighetsskikt och lagringsskikt krypteras (också i vila) och säkras bakom VPN & VPC brandväggar. Kontor använder ett nätverk som skydds genom en redundant Fotrinet 200D brandvägg, placerad i datacentret i Merelbeke, som är uppkopplad till Ghelamco-området genom mörk fiber. Mer information om denna uppkoppling ges i dokumentet "Continuity och Security Measures", som också är en del av ISMS (ISO 27001).

BILAGA 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 Tredjepartsleve-rantörer.	Programvarutjänster och/eller supporttjänster och/eller molntjänster.
Unit4 SaaS	Microsoft Azure	Enligt vad som anges i Bilaga 1, punkt 5.	Tillhandahåller molninfrastruktur och molntjänster.
	Microsoft Dynamics	Enligt vad som anges i Bilaga 1, punkt 5.	Tillhandahåller program-varutjänster, särskilt Microsoft Dynamics (inklusive viss molninfrastruktur).
	Microsoft	Enligt vad som anges i Bilaga 1, punkt 5.	Tillhandahåller programvaruverktyg och Office
	Conapto	Enligt vad som anges i Bilaga 1, punkt 5.	Tillhandahåller molninfrastruktur och molntjänster.
Unit4 SaaS – Talent Management	Amazon Web Services	Frankfurt, Tyskland	Tillhandahåller lösning - Suite
	Freshdesk	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	LogDNA	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Mandrill	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Mixpanel	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Pingdom	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Productboard	European Economic Area and United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Tillhandahåller lösning - Learn (enbart SCORM) (privacy shield link: Link)
	Sentry	United States of America (Privacy Policy)	Tillhandahåller lösning - Suite (privacy shield link: Link)
	Slack	United States of America (Privacy Policy)	Tillhandahåller lösning - Perform (privacy shield link: Link)
	Stripe	Countries in which Stripe operates (Privacy Policy)	Tillhandahåller lösning - Learn (privacy shield link: Link)
	Wistia	United States of America (Privacy Policy)	Tillhandahåller lösning - Learn (privacy shield link: Link)
People Platform Services ("PPS") (generellt) inklusive IDS och Wanda (tillsammans med eventuella stöd-tjänster)	Microsoft Azure	Enligt vad som anges i Bilaga 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 Bilaga 1, punkt 2).

BILAGA 4 – EUs STANDARDAVTALSCLAUSULER

Denna tabell innehåller den information som behöver införas i EU:s standardavtalsklausuler, som bifogas nedan.

Parter	Uppgiftsutföranden är den Personuppgiftsansvarige, som specificeras i ett Orderformulär (som Kund) i Avtalet mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet. Uppgiftsinföranden är Personuppgiftsbiträdet som specificeras i ett Orderformulär (som Unit4) i Avtalet mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet.
Punkt 9 och 11(3)	Uppgiftsutföranden är baserad i det Territorium som anges i Avtalet.
Bilaga 1	Den information som krävs för att färdigställa denna Bilaga finns angiven i Bilaga 1 och Bilaga 2 till dessa Personuppgiftsbiträdesvillkor.
Bilaga 2	Den information som krävs för att färdigställa denna Bilaga finns angiven i Bilaga 2 till dessa Personuppgiftsbiträdesvillkor.

STANDARDAVTALSCLAUSULER ("registerföreare")

Standardavtalsklausuler enligt artikel 26.2 i direktiv 95/46/EG för överföring av personuppgifter till registerföreare i tredjeländer med otillräckligt uppgiftsskydd

Parter

Namn på den uppgiftsutförande organisationen:

Adress: ...

Tel.; Fax; e-postadress: ...

Övriga uppgifter som krävs för att identifiera organisationen:

("Uppgiftsutföraren")

Och

Namn på den uppgiftsinförande organisationen:

Adress: ...

Tel.; Fax; e-postadress: ...

Övriga uppgifter som krävs för att identifiera organisationen:

("Uppgiftsinföraren")

var och en "part", tillsammans "parterna".

HAR ENATS om följande avtalsklausuler ("klausulerna") för att säkerställa ett adekvat skydd för privatliv och grundläggande rättigheter och friheter för enskilda i samband med överföring från uppgiftsutföraren till uppgiftsinföraren av sådana personuppgifter som anges i tillägg 1.

Klausul 1

Definitioner

I dessa klausuler gäller följande definitioner:

- personuppgifter, särskilda kategorier av uppgifter, behandling, registeransvarig, registerföreare, registrerad och tillsynsmyndighet: samma innebörd som i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter;¹
- uppgiftsutförare: den registeransvarige som överför personuppgifterna;
- uppgiftsinförare: den registerföreare som går med på att från uppgiftsutföraren ta emot personuppgifter för vidare behandling i enlighet med uppgiftsutförarens instruktioner och villkoren i klausulerna, och som inte omfattas av ett system i tredjeländ som garanterar ett adekvat skydd i den mening som avses i artikel 25.1 i direktiv 95/46/EG;
- underentreprenör: registerföreare som anlitas av uppgiftsinföraren eller av en annan av uppgiftsinförarens underentreprenörer och som går med på att från uppgiftsinföraren eller en annan av uppgiftsinförarens underentreprenörer ta emot personuppgifter i den enda avsikten att efter överföringen behandla personuppgifter för uppgiftsutförarens räkning i enlighet med uppgiftsutförandens instruktioner, villkoren i klausulerna samt villkoren i det skriftliga underentreprenörsavtalet;
- tillämplig uppgiftsskyddslagstiftning: sådan lagstiftning som avser att skydda personers grundläggande fri- och rättigheter, särskilt deras personliga integritet i samband med behandling av personuppgifter, och som är tillämplig på registeransvariga i den medlemsstat där uppgiftsutföraren är etablerad;
- tekniska och organisatoriska säkerhetsåtgärder: åtgärder avsedda att skydda personuppgifter mot oavsiktlig eller olaglig utplåning, oavsiktlig förlust, ändring, otillåtet utlämnande eller otillåten åtkomst, i synnerhet när behandlingen inbegriper överföring av uppgifter över ett nät, och mot varje annan form av olaglig behandling.

Klausul 2

Information om överföringen

Information om överföringen, och i förekommande fall om särskilda kategorier av personuppgifter, anges i tillägg 1, vilket utgör en integrerad del av klausulerna.

Klausul 3

Tredjepartsberättigande

¹ Parterna kan här återge definitionerna och betydelseerna i direktiv 95/46/EG, om de anser det lämpligare att avtalet fungerar självständigt.

1. Den registrerade kan i egenskap av berättigad tredje part åberopa denna klausul och klausulerna 4 b–i, 5 a–e och 5 g–j, 6.1–2, 7, 8.2 samt klausulerna 9–12 gentemot uppgiftsutföraren.
2. Den registrerade kan gentemot uppgiftsinföraren åberopa denna klausul, klausulerna 5 a–e och 5 g, klausulerna 6, 7, 8.2 samt klausulerna 9–12 i sådana fall där uppgiftsutföraren har upphört att existera i faktisk eller rättslig mening, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsutförarens rättsliga skyldigheter, och som en följd av detta påtar sig uppgiftsutförarens rättigheter och skyldigheter, i vilket fall den registrerade kan åberopa de ovannämnda klausulerna gentemot denna.
3. Den registrerade kan gentemot underentreprenören åberopa denna klausul, klausulerna 5 a–e och 5 g, 6, 7, 8.2 samt klausulerna 9–12 i de fall där uppgiftsutföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsutförarens rättsliga skyldigheter, och som en följd av detta övertar uppgiftsutförarens rättigheter och skyldigheter, i vilket fall den registrerade kan åberopa de ovannämnda klausulerna gentemot denna enhet. Skadeståndsansvaret ska i sådana fall vara begränsat till underentreprenörens egen behandling av uppgifter enligt klausulerna.
4. Parterna har inget att invända mot att en registrerad företrädare av sammanslutningar eller andra organ om denne uttryckligen så önskar och i den mån det är tillåtet enligt nationell rätt.

Klausul 4

Uppgiftsutförarens skyldigheter

Uppgiftsutföraren godtar och garanterar

- a) att behandlingen, inbegripet själva överföringen, av personuppgifterna har skett och även i fortsättningen kommer att ske i enlighet med tillämplig uppgiftsskyddslagstiftning (och i förekommande fall anmäls till behöriga myndigheter i den medlemsstat där uppgiftsutföraren är etablerad) och inte strider mot gällande lagar eller andra författningar i den medlemsstaten;
- b) att han instruerat och under behandlingen av personuppgifter kommer att instruera uppgiftsinföraren att behandla de överförda personuppgifterna endast för uppgiftsutförarens räkning och i enlighet med tillämplig uppgiftsskyddslagstiftning och klausulerna;
- c) att uppgiftsinföraren kommer att ge tillräckliga garantier vad gäller de tekniska och organisatoriska säkerhetsåtgärder som anges i tillägg 2 till detta avtal;
- d) att han, mot bakgrund av tillämplig uppgiftsskyddslagstiftning, har funnit säkerhetsåtgärderna lämpliga för att skydda personuppgifter mot oavsiktlig eller olaglig utplåning, oavsiktlig förlust, ändring, otillåtet utlämnande eller otillåten åtkomst, i synnerhet när behandlingen inbegriper överföring av uppgifter över ett nät, och mot varje annan form av olaglig behandling, med hänsyn tagen till teknikens ståndpunkt, kostnaden för vidtagande av åtgärderna och de risker behandlingen innebär och karaktären hos de uppgifter som ska behandlas;
- e) att han kommer att se till att säkerhetsåtgärderna följs;
- f) att, om överföringen avser särskilda kategorier av uppgifter, de registrerade har informerats eller informeras senast när överföringen sker eller så snart som möjligt därefter om att deras uppgifter kan komma att överföras till ett tredjeland som inte tillhandahåller adekvat skydd i den mening som avses i direktiv 95/46/EG;
- g) att vidarebefordra anmälningar från uppgiftsinföraren eller eventuella underentreprenörer i enlighet med klausul 5 b och klausul 8.3 till tillsynsmyndigheten om uppgiftsutföraren beslutar att fortsätta överföringen eller häva avbrottet;
- h) att på begäran tillhandahålla de registrerade en kopia av klausulerna, med undantag för tillägg 2, och en sammanfattande beskrivning av säkerhetsåtgärderna, samt en kopia av eventuella underentreprenörsavtal som måste ingås enligt klausulerna, såvida inte klausulerna eller avtalet innehåller affärsinformation;
- i) att uppgiftsbehandlingen vid en eventuell utläggning på entreprenad utförs i enlighet med klausul 11 av en underentreprenör som tillhandahåller åtminstone samma skyddsnivå för personuppgifter och den registrerades rättigheter som uppgiftsinföraren ska göra enligt klausulerna, och
- j) att han kommer att se till att klausul 4 a–i följs.

Klausul 5

Uppgiftsinförarens skyldigheter²

Uppgiftsinföraren godtar och garanterar

- a) att behandla personuppgifter för uppgiftsutförarens räkning och enlighet med dennes instruktioner samt dessa klausuler; om han av något skäl inte kan fullgöra detta krav går han med på att omedelbart informera uppgiftsutföraren om detta, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet;
- b) att han inte har anledning att förmoda att den lagstiftning som är tillämplig på honom hindrar honom från att fullfölja uppdragsutförarens instruktioner och sina skyldigheter enligt detta avtal; om lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som klausulerna innebär, ska han anmäla ändringen till uppgiftsutföraren, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet;
- c) att han har vidtagit de tekniska och organisatoriska säkerhetsåtgärder som anges i tillägg 2 innan de överförda personuppgifterna behandlas;
- d) att han utan dröjsmål kommer att underrätta uppgiftsutföraren om
 - i) varje rättsligt bindande begäran från rättsliga myndigheter om utlämnande av personuppgifterna, om inte detta är förbjudet på grund av exempelvis ett straffrättsligt förbud som syftar till att bevara sekretessen vid brottsutredningar,
 - ii) varje oavsiktlig eller otillåten åtkomst, och

² Standardavtalsklausulerna är inte oförenliga med obligatoriska krav i den nationella lagstiftning som är tillämplig på uppgiftsinföraren, förutsatt att kraven inte går utöver vad som är nödvändigt i ett demokratiskt samhälle på någon av de grunder som anges i artikel 13.1 i direktiv 95/46/EG, dvs. om det är en nödvändig åtgärd med hänsyn till statens säkerhet, försvaret, den allmänna säkerheten, förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelse av etiska regler som gäller för lagreglerade yrken, ett för staten viktigt ekonomiskt eller finansiellt intresse eller skydd av den registrerades eller andras fri- och rättigheter. Exempel på sådana obligatoriska krav som inte går utöver vad som krävs i ett demokratiskt samhälle är internationellt erkända sanktioner, krav på skatterapportering eller upplysningsplikt när det gäller bekämpning av penningtvätt.

- iii) varje förfrågan direkt från de registrerade, utan att svara på dem om han inte givits tillstånd till det.
- e) att utan dröjsmål och korrekt handlägga alla frågor från uppgiftsföraren om behandling av sådana personuppgifter som överförs och att rätta sig efter tillsynsmyndighetens rekommendationer med avseende på behandlingen av de uppgifter som överförs;
- f) att på uppgiftsförarens begäran ställa sin databehandlingsutrustning till förfogande för granskning av den uppgiftsbehandling som dessa klausuler avser; granskningen ska genomföras av uppgiftsföraren eller av ett inspektionsorgan med oberoende och sakkunniga ledamöter; de av tystnadsplikt bundna ledamöterna utses av uppgiftsföraren, i förekommande fall enligt överenskommelse med tillsynsmyndigheten;
- g) att på begäran förse de registrerade med en kopia av klausulerna eller av eventuella befintliga underentreprenörsavtal, såvida inte klausulerna eller kontraktet innehåller känslig affärsinformation; i vilket fall uppgiftsföraren kan ta bort dessa uppgifter; denna skyldighet omfattar dock inte tillägg 2, som ska ersättas av en sammanfattande beskrivning av säkerhetsåtgärderna i de fall där den registrerade inte kan erhålla en kopia från uppgiftsföraren,
- h) att han, om uppgiftsbehandlingen läggs ut på entreprenad, i förväg har underrättat uppgiftsföraren och utverkat skriftligt förhandstillstånd från denne;
- i) att den uppgiftsbehandling som utförs av underentreprenören utförs i enlighet med klausul 11;
- j) att omedelbart översända en kopia av eventuella underentreprenörsavtal som ingåtts enligt klausulerna till uppgiftsföraren.

Klausul 6

Ansvar

1. Parterna är överens om att en registrerad som lidit skada till följd av att en part eller en parts underentreprenör brutit mot de skyldigheter som avses i klausul 3 eller klausul 11 har rätt till ersättning från uppgiftsföraren.
2. Om den registrerade, i situationer där uppgiftsföraren eller dennes underentreprenör bryter mot någon av sina skyldigheter enligt klausulerna 3 eller 11, inte kan rikta skadeståndsanspråk mot uppgiftsföraren i enlighet med punkt 1 på grund av att uppgiftsföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, ska uppgiftsföraren godta att den registrerade kan rikta ett skadeståndsanspråk mot uppgiftsföraren som om denne var uppgiftsföraren, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsförarens rättsliga skyldigheter, i vilket fall den registrerade kan göra sina rättigheter gällande gentemot denna enhet. Uppgiftsföraren kan inte åberopa att en underentreprenör har brutit i sina skyldigheter för att undvika eget ansvar.
3. Om en registrerad, i situationer där en underentreprenör har brutit mot någon av sina skyldigheter enligt klausulerna 3 eller 11, inte kan rikta ett skadeståndsanspråk mot uppgiftsföraren eller uppgiftsföraren i enlighet med punkt 1 och 2 på grund av att såväl uppgiftsföraren som uppgiftsföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, ska underentreprenören godta att den registrerade kan rikta ett skadeståndsanspråk mot underentreprenören, med avseende på dennes egen behandling av personuppgifter i enlighet med klausulerna, som om denne var uppgiftsföraren eller uppgiftsföraren, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsförarens eller uppgiftsförarens rättsliga skyldigheter, i vilket fall den registrerade kan göra sina rättigheter gällande gentemot denna enhet. Skadeståndsansvaret ska i sådana fall vara begränsat till underentreprenörens egen behandling av uppgifter enligt klausulerna.

Klausul 7

Medling och forum

1. Uppgiftsföraren samtycker till att, om den registrerade åberopar tredje parts rättigheter och/eller kräver ersättning för skador i enlighet med klausulerna, godta den registrerades beslut att
 - a) inleda medling av tredje part eller, i tillämpliga fall, av tillsynsmyndigheten
 - b) hänskjuta tvisten till domstol i den medlemsstat där uppgiftsföraren är etablerad.
2. Parterna är överens om att den registrerades val inte påverkar dennes materiella eller processuella rätt att söka gottgörelse i enlighet med andra bestämmelser i nationell eller internationell lagstiftning.

Klausul 8

Samarbetet med tillsynsmyndigheterna

1. Uppgiftsföraren åtar sig att deponera ett exemplar av detta avtal hos tillsynsmyndigheten, om så föreskrivs i tillämplig uppgiftsskyddslagstiftning eller om tillsynsmyndigheten begär det.
2. Parterna är överens om att tillsynsmyndigheten har rätt att genomföra inspektioner hos uppgiftsföraren och uppgiftsförarens eventuella underentreprenörer i samma omfattning och på samma villkor som skulle gälla för en revision hos uppgiftsföraren enligt tillämplig uppgiftsskyddslagstiftning.
3. Uppgiftsföraren ska omedelbart underrätta uppgiftsföraren om uppgiftsföraren och dennes eventuella underentreprenörer omfattas av lagstiftning som förhindrar att de blir föremål för inspektion i enlighet med punkt 2. I sådant fall ska uppgiftsföraren ha rätt att vidta de åtgärder som anges i klausul 5 b.

Klausul 9

Tillämplig lag

Klausulerna omfattas av lagen i den medlemsstat där uppgiftsföraren är etablerad, nämligen Sverige.

Klausul 10

Ändring av avtalet

Parterna åtar sig att inte ändra klausulerna. Detta hindrar inte parterna från att om nödvändigt lägga till klausuler om affärsrelaterade frågor, så länge dessa inte står i strid med någon klausul.

Klausul 11

Utläggning på entreprenad

1. Uppgiftsföraren får inte utan uppgiftsförarens föregående samtycke på entreprenad lägga ut någon del av den behandling som uppgiftsföraren utför för uppgiftsförarens räkning i enlighet med klausulerna. Om uppgiftsföraren, med uppgiftsförarens samtycke, lägger över sina skyldigheter enligt dessa klausuler på en underentreprenör, får detta endast ske genom ingående av ett skriftligt avtal med underentreprenören, varigenom denne

åläggs samma skyldigheter som enligt klausulerna åligger uppgiftsföraren.³ Om underentreprenören inte uppfyller sina skyldigheter i fråga om uppgiftsbehandling enligt ett sådant avtal ska uppgiftsföraren förbli fullt ansvarig gentemot uppgiftsutföraren för under-entreprenörens uppfyllande av sina skyldigheter enligt avtalet.

2. Det på förhand ingångna skriftliga avtalet mellan uppgiftsutföraren och uppgiftsföraren ska även inbegripa en bestämmelse om berättigad tredje part i enlighet med klausul 3 i sådana fall där den registrerade inte kan rikta skadeståndsanspråk i enlighet med klausul 6.1 mot uppgiftsutföraren eller uppgiftsföraren, eftersom dessa har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, och ingen annan enhet har till fullo övertagit uppgiftsutförarens eller uppgiftsförarens rättsliga skyldigheter enligt avtal eller lag. Skadeståndsansvaret ska i sådana fall vara begränsat till underentreprenörens egen behandling av uppgifter enligt klausulerna.
3. Bestämmelserna om uppgiftsskyddsaspekter vid utläggning på entreprenad av det kontrakt som avses i punkt 1 på en underentreprenör ska omfattas av lagen i den medlemsstat där uppgiftsutföraren är etablerad, nämligen Sverige.
4. Uppgiftsutföraren ska föra en förteckning över entreprenadavtal som ingåtts enligt klausulerna och anmälts av uppgiftsföraren i enlighet med klausul 5 j. Förteckningen ska uppdateras minst en gång om året. Förteckningen ska vara tillgänglig för uppgiftsutförarens dataskyddsmyndighet.

Klausul 12

Skyldigheter efter det att behandlingen av personuppgifter har upphört

1. Parterna är överens om att uppgiftsföraren och eventuella underentreprenörer efter behandlingens upphörande och beroende på vad uppgiftsutföraren beslutar antingen ska återlämna alla överförda personuppgifter och kopior av dessa till uppgiftsutföraren, eller förstöra alla personuppgifter och intyga för uppgiftsutföraren att så skett, såvida inte den på uppgiftsföraren tillämpliga lagstiftningen helt eller delvis hindrar honom från att återlämna eller förstöra de överförda personuppgifterna. I så fall ska uppgiftsföraren garantera att denne kommer att bevara sekretessen hos de överförda personuppgifterna och inte aktivt behandla de överförda personuppgifterna ytterligare.
2. Uppgiftsföraren och underentreprenören garanterar att de på uppgiftsutförarens och/eller tillsynsmyndighetens begäran kommer att ställa sin databehandlingsutrustning till förfogande för en granskning av de åtgärder som anges i punkt 1.

Parterna överenskommer att dessa Standardavtalsklausuler ska bli bindande mellan Parterna vid ingående av ett orderformulär för tillhandahållande av tjänster, som utgör ett avtal.

Bilaga 1

Till Standardavtalsklausulerna

Denna Bilaga utgör en del av Standardavtalsklausulerna och måste färdigställas och undertecknas av Parterna.

EU:s medlemsstater kan komplettera eller specificera, i enlighet med nationella procedurer, krav på eventuell ytterligare information som ska införas i denna Bilaga.

Uppgiftsutföraren

Uppgiftsutföraren är (vänligen specificera era aktiviteter som är relevanta för överföringen:

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Uppgiftsföraren

Uppgiftsutföraren är (vänligen specificera era aktiviteter som är relevanta för överföringen:

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Registrerade

De personuppgifter som ska överföras avser följande kategorier av registrerade (vänligen specificera):

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Typ av personuppgifter

De personuppgifter som ska överföras avser följande kategorier av personuppgifter (vänligen specificera):

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Särskilda kategorier av personuppgifter (om tillämpligt)

De personuppgifter som ska överföras avser följande särskilda kategorier av personuppgifter (vänligen specificera):

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Typ av behandling

De personuppgifter som ska överföras omfattas av följande typer av behandling (vänligen specificera):

Se Bilaga 1 till Personuppgiftsbiträdesvillkoren (ovan).

Bilaga 2

Till Standardavtalsklausulerna

Beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som implementerats av uppgiftsföraren i enlighet med punkt 4(d) och 5(c) (eller se bifogat dokument/lagstiftning:

Se Bilaga 2 till Personuppgiftsbiträdesvillkoren (ovan).

³ Detta krav kan uppfyllas genom att även underentreprenören undertecknar det avtal som ingåtts mellan uppgiftsutföraren och uppgiftsföraren enligt detta beslut.