Unit4 Databehandlingsinformasjon som inkorporerer EUs standard personvernbestemmelser

DEL 1 – BESKRIVELSE AV BEHANDLINGEN AV PERSONOPPLYSNINGER

1. PERSONOPPLYSNINGER SOM VIL BLI BEHANDLET:

Produkt	Personopplysninger som vil kunne bli behandlet kan omfatte:	Til den dette måtte tilhøre:
Unit4 ERP x	Navn; adresser; kontraktsdetaljer; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon; fødselsdato; alder; fødested; nasjonalitet eller statsborgerskap; oppholdsted; bosted; talespråk; passnummer; fødselsnummer eller personnummer eller referansenummer på ID-kort; sivilstatus; trygdeinformasjon under trygdeordninger; kjønn; informasjon om arbeidsforhold (inkludert: lønn; stilling; lønnstariff; lønnstrinn; kompetanse og personlige notater); skatteinformasjon; forsikringsinformasjon; fagforeningsmedlemskap; nærmeste pårørende (navn; adresse; fødselsdato; telefonnummer; kontaktinformasjon for nødstilfeller); start- og sluttdato for arbeidsforhold; bankkonto- eller bankkortdetaljer; informasjon om eget firma (navn, registreringsnummer og forretningskontor); styreverv, organisasjonsnummer; dokumenter (skriftlig eller elektronisk) som inneholder noe av informasjonen som nevnt ovenfor.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere; og søkere eller potensielle ansatte.
Unit4 ERP 7	Navn; adresser; kontraktsdetaljer; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon; fødselsdato; alder; fødested; nasjonalitet eller statsborgerskap; oppholdsted; bosted; talespråk; passnummer; fødselsnummer eller personnummer eller referansenummer på ID-kort; sivilstatus; trygdeinformasjon under trygdeordninger; kjønn; informasjon om arbeidsforhold (inkludert: lønn; stilling; lønnstariff; lønnstrinn; kompetanse og personlige notater); skatteinformasjon; forsikringsinformasjon; fagforeningsmedlemskap; nærmeste pårørende (navn; adresse; fødselsdato; telefonnummer; kontaktinformasjon for nødstilfeller); start- og sluttdato for arbeidsforhold; bankkonto- eller bankkortdetaljer; informasjon om eget firma (navn, registreringsnummer og forretningskontor); styreverv, organisasjonsnummer; dokumenter (skriftlig eller elektronisk) som inneholder noe av informasjonen som nevnt ovenfor.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere; og søkere eller potensielle ansatte.
Unit4 Financials	Navn; adresser; kontraktsdetaljer; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon; fødselsdato; alder; fødested; nasjonalitet eller statsborgerskap; oppholdsted; bosted; talespråk; passnummer; fødselsnummer eller personnummer eller referansenummer på ID-kort; sivilstatus; trygdeinformasjon under trygdeordninger; kjønn; informasjon om arbeidsforhold (inkludert: lønn; stilling; lønnstariff; lønnstrinn; kompetanse og personlige notater); skatteinformasjon; forsikringsinformasjon; fagforeningsmedlemskap; nærmeste pårørende (navn; adresse; fødselsdato; telefonnummer; kontaktinformasjon for nødstilfeller); start- og sluttdato for arbeidsforhold; bankkonto- eller bankkortdetaljer; informasjon om eget firma (navn, registreringsnummer og forretningskontor); styreverv, organisasjonsnummer; dokumenter (skriftlig eller elektronisk) som inneholder noe av informasjonen som nevnt ovenfor.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere; og søkere eller potensielle ansatte.
Unit4 Student Management	Navn; adresser; kontraktsdetaljer; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon; fødselsdato; alder; fødested; nasjonalitet eller statsborgerskap; oppholdsted; bosted; talespråk; passnummer; fødselsnummer eller personnummer eller referansenummer på ID-kort; sivilstatus; trygdeinformasjon under trygdeordninger; kjønn; informasjon om arbeidsforhold (inkludert: lønn; stilling; lønnstariff; lønnstrinn; kompetanse og personlige notater); skatteinformasjon; forsikringsinformasjon; fagforeningsmedlemskap; nærmeste pårørende (navn; adresse; fødselsdato; telefonnummer; kontaktinformasjon for nødstilfeller); start- og sluttdato for arbeidsforhold; bankkonto- eller bankkortdetaljer; informasjon om eget firma (navn, registreringsnummer og forretningskontor); styreverv, organisasjonsnummer; dokumenter (skriftlig eller elektronisk) som inneholder noe av informasjonen som nevnt ovenfor. Ytterligere Personopplysninger for tidligere og nåværende ansatte: type personale (f.eks. fakultet, rådgiver, bestyrer av studentbolig (housing director); akademisk avdeling, rekrutteringsstatus; ansettelsesstatus; arbeidsmengde; fakultetsrangering; publikasjoner; måling av arbeidsstatus; informasjon om utdanning og kvalifikasjoner. Ytterligere Personopplysninger for tidligere og nåværende søkere: informasjon om tidligere utdanning; karakterutskrift og/eller (supplerende) testresultater; fysisk helsetilstand; referanser fra tidligere arbeidsgiver; og informasjon om arbeidssted. Ytterligere Personopplysninger for tidligere og nåværende studenter: karakterutskrift inkludert resultater og mål; informasjon om immatrikulering; informasjon om akademisk progresjon (inkludert karakterer); akademiske utmerkelser; akademiske eller arbeidsrelaterte utplasseinger; informasjon om studieforløp; faktura- og betalingshistorikk; boligpreferanser og –historikk; informasjon om studiestøtte; helsejournal (inkludert vaksiner, allergier, helsetilstand), informasjon om forsikring og helsedokumentasjon.	Nåværende eller tidligere ansatte (inkludert eventuelle fakultetsansatte eller personale); Leverandører eller underleverandører (av noe slag); agenter eller ledere; og Søkere eller potensielle ansatte; og nåværende, tidligere og potensielle studenter.
Unit4 FP&A	Navn; adresser; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon. Andre Personopplysninger behøver ikke å lagres eller behandles for å oppnå formålet med Produktet (som fremgår nedenfor), men andre Personopplysninger vil kunne lagres eller behandles av Produktet dersom det er konfigurert til å gjøre det eller det blir matet inn i Produktet av Kunden.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere.
Unit4 Assistance PSA Suite	Navn; adresser; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon. Andre Personopplysninger behøver ikke å lagres eller behandles for å oppnå formålet med Produktet (som fremgår nedenfor), men andre Personopplysninger vil kunne lagres eller behandles av Produktet dersom det er konfigurert til å gjøre det eller det blir matet inn i Produktet av Kunden.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere; Enhver annen som deltar i et prosjektteam (inkludert ikke-ansatte), søkerer eller potensielle ansatte. Kundens kundedetaljer og leverandørdetaljer.

Unit4 Talent Management	Navn; adresser; kontraktsdetaljer; telefonnummer (inkludert mobil); e-postadresse(r); annen kontaktinformasjon (gateadresse og land); fødselsdato; alder; fødested; arbeidstittel; avdeling. Ved å bruke Learn-modulen: påmelding til kurs; påmelding til sesjoner; prøveresultater og gjennomgang; data angående videobruk; data angående lysbildebruk; data angående tekstbruk; utmerkelser; sertifiseringer. Ved å bruke Perform-modulen: innsjekkingsdata; OKR (Objectives and Key Results) data; tilbakemeldinger og ros. Ved å benytte Engage-modulen: svar og tilbakemeldinger på spørsmål angående engasjement.	Nåværende eller tidligere ansatte; Nåværemde eller tidligere jobbkandidater; Leverandører eller Underleverandører (av noe slag), agenter eller ledere; og Søkere eller potensielle ansatte.
People Platform Services ("**PPS**"), Lokaliserings-tjenester og Unit 4 Applikasjoner	Ettersom PPS, Lokaliseringstjenester og/eller Unit4 Applikasjoner er tjenester som arbeider sammen med og har grensesnitt mot øvrige Unit4-produkter og -tjenester, vil de kunne behandle alle typer Personopplysninger som angis i denne tabellen angående de opplistede Produktene og Tjenestene. I tillegg vil Wanda kunne behandle: Unit4ID (som identifiserer brukere av IDS); alle Personopplysninger eller informasjon som blir inngitt av en bruker til en programvare som Wanda kan kobles til (slik informasjon blir behandlet eller lagret med mindre Bruker beslutter at det skal slettes); alle andre opplysninger om samtaler eller dialoger; metadata som kan anvises til en enkeltperson; og Application Insights Logs (en Microsoft-tjeneste som benyttes for å utføre diagnostikk).	Alle kategorier av personer som er listet opp i denne tabellen. Avhengig av programvaren eller tjenesten som Wanda er koblet til, kan PPS potensielt Behandle Personopplysninger alle personer som Brukeren velger å inngi.
Unit4 Eiendoms-håndtering	Navn; addresser; telefonnummer (inkludert mobil), e-postadresse, adresse til hjemmeside, fødselsnummer eller personnummer eller referansenummer på ID-kort; fødselsdato, kundeidentitet, språk, kjennetegn for hemmelig identitet, kjennetegn for eiendom, MVA-nummer, informasjon om kontaktpersoner (inkludert: tittel/stilling, interesser); bankkontodetaljer, informasjon om arbeidsforhold (inkludert: arbeidsgiver, adresseinformasjon); søkerdetaljer (inkludert: yrke, årlig inntekt, år for ansettelse, antall personer i husholdningen, tidligere utleier, vurdering av kredittopplysninger, dato for kredittvurdering); søker og andre kjennetegn (definert av Behandlingsansvarlig); køposisjon, medlemskap (inkludert: medlemsnummer, status, medlemskapets start- og sluttdato, begrunnelse for innmelding/avslutning, dato for første inntreden, hovedmedlemskap, relaterte medlemskap, leietakerpoeng, boligsparingspoeng); roller/kateogier av personer; brukere (bruker-ID, type bruker, signatur); leieavtale og detaljer om leieboer i henhold til kontrakten (inkludert: identiteten til mottaker for e-faktura, informasjon om fullmektig, depositum, kausjon, garanti); informasjon om sakshåndtering; leverandør (anvisning for forsendeler); notater (registrert av Behandlingsansvarlig); dokumenter (skriftlig eller elektronisk) som inneholder noe av informasjonen som nevnt ovenfor.	Nåværende eller tidligere ansatte; Leverandører eller underleverandører (av noe slag); agenter eller ledere; Søkere eller potensielle ansatte; og kunder av forvaltningstjenester (f.eks. eiendomssøkere og leietakere).

2. BEHANDLINGENS ART OG FORMÅL:

Generelt vil Databehandlerens Behandling utelukkende være av en slik art som er nødvendig for å gjøre Databehandleren i stand til å overholde sine forpliktelser og utøve sine rettigheter under Avtalen, inkludert (når det gjelder Personopplysninger) innsamling, registrering, organisering, strukturering, lagring, tilpassing eller endring, gjenfinnelse, konsultasjon, bruk, fremvisning, spredning eller tilgjengeliggjøring på annen måte, justering eller sammenføyelse, begrensning, sletting, eller destruering. Hensikten eller formålet med Behandlingen er uførelsen av Databehandlerens forpliktelser og utøvelsen av sine rettigheter under Avtalen, inkludert utførelsen av de funksjoner som kreves eller anmodes av Behandlingsansvarlig for at Databehandleren skal oppfylle sine lovbestemte og/eller kontraktsmessige forpliktelser. Databehandler vil også behandle dine personopplysninger for å forbedre sine produkter og tjenester (f.eks. for produktforbedring via kunstig intelligens, maskinlæring, osv.) eller til dataanalyse.

I sammenheng med, og avhengig av, Produktet eller Tjenesten, vil Behandlingen inkludere følgende:

Produkt	Behandlingens art og formål
Unit4 ERP x	Personopplysninger blir registrert i Unit4 ERP 8 for å sette Kunden i stand til å organisere og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Reiseutgifter; • Håndtering av utlegg; • Håndtering av timelister; • Fraværshåndtering; • HR og lønnsrelaterte prosesser; • Lønn; • Kurspåmelding; • Kompetansehåndtering; • Omdømme; • Lønnsrevisjon; • Registrering av søkere; • Gjennomføring av betalinger; • Fakturering; • Innkjøp; • Personal/prosjektplanlegging: Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 ERP 8 utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig.

	Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s Produkt og hjelp til Kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 ERP 7	Personopplysninger vil registreres i Unit4 ERP 7 for å sette Kunden i stand til å organisere og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Reiseforespørsler; • Håndtering av utleggskrav • Håndtering av timeliser • Fraværshåndtering • HR og lønnsrelaterte prosesser: • Lønn; • Kurspåmelding; • Kompetansehåndtering; • Omdømme; • Lønnsrevisjon; • Registrering av søkere; • Gjennomføring av betalinger; • Fakturering; • Innkjøpsrekvisisjoner • Personal/prosjektplanlegging Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 ERP 7 utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis (ovenfor) kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4-produkter og hjelp til Kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 Financials	Personopplysninger vil registreres i Unit4 Financials for å sette Kunden i stand til å organisere og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Registrering av Kunder/Leverandører/Ansatte • Gjennomføring av betalinger; • Fakturering; • Håndtering av utleggskrav; • Reiseforespørsler; • Innkjøp og bestillinger; • Personal/prosjektplanlegging; • HR og lønnsrelaterte prosesser: • Lønn; • Håndtering av timeliser • Fraværshåndtering • Kurspåmelding; • Kompetansehåndtering; • Omdømme; • Lønnsrevisjon; • Registrering av søkere; Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 Financials utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis (som nærmere beskrevet ovenfor) kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4-produkter og hjelp til Kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 Student Management	Personopplysninger vil registreres i Unit4 Student Management for å sette Kunden i stand til å organisre og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere:

	• Rekruttering av potensielle studenter; • Besvare anmodninger om informasjon; • Behandle søknader; • Håndtere den akademiske livssyklusen til en student, inludert innledende aktiviterer, kursplanlegging, akademisk progresjon, rådgivning, bolig og andre fasiliteter, uteksaminering • Planlegge og beramme fakultetspersonale Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 Student Managment utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4-produktet og hjelp til kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 FP&A	Personopplysninger vil registreres i Unit4 FP&A for å sette Kunden i stand til å organisre og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Budsjettering; • Finansiell og annen rapportering; • Distribusjon av rapporter; • Behandling av godkjennelser; • Personal/prosjektplanlegging. Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 FP&A utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet Beskrivelse av tjenesten for eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4produktet og hjelp til kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 Talent Management	Personopplysninger vil registreres i Unit4 Talent Management for å sette Kunden i stand til å organisre og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Håndtering av menneskelig kapital; • Håndtering av arbeidstakeres prestasjoner; • Talentutvikling; • Vurdering av kandidater; • Læring; • Tilbakemelding og ros; og • Personanalyse og –engasjement. Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 Talent Management utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4-produktet og hjelp til kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
Unit4 Assistance PSA Suite	Personopplysninger vil registreres i Unit4 Assistance PSA Suite for å sette Kunden i stand til å organisre og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • automatisering av en profesjonell tjenesteorganisasjon, inkludert finansiell og HR adminstrasjon (HRM); • daglig tids- og prosjekthåndtering; • booking av tid og utgifter med kvitteringer; • overføring av forretningsmuligheter til prosjekter, busjett og estimerte timer, og planlegging av prosjekter og ressurser; • oversikt over tid og utgifter og gjennomføring av fakturering; • integrasjon av prosjekter inn i andre applikasjoner; og • utførelse av regnskapsføring til hjelp for integrasjon av finansielle data inn i andre løsninger.

	Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 Assistance PSA Suite utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å tilby ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4-produktet og hjelp til kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.
People Platform Services ("**PPS**"), Lokaliseringer og Applikasjoner	Personopplysninger vil bli behandlet av PPS, Lokaliseringstjenester og/eller Applikasjoner for å tillate de angitte formålene med tjenesten som angitt i gjeldende Beskrivelse for tjeneste for PPS på www.unit4.com/terms. I tillegg vil Personopplysninger innføres i Wanda gjennom å anvende en valgfri tredjepartsprogramvare (f.eks. Slack Integration eller andre Microsoft-applikasjoner (inkludert Microsoft Teams)). Avhengig av Unit4-produktet eller -tjenesten som benyttes av Kunden, vil Wanda kunne hjelpe til med å ferdigstille administrative oppgaver for Kundens ansatte. Oppgaver kan inkludere: • Registrering i timelister • Registrering av utgifter • Reiseforespørsler • Spørsmål om lønnsslipper • Registrering av fravær • Spørsmål om balanse • Innkjøp Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Wanda utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s PPS, Lokaliseringstjenester og/eller Applikasjoner og hjelp til kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt. Tilgang til Personopplysninger for produktutvikling via AI maskinlæring eller dataanalyse.
Unit4 Eiendoms-håndtering	Personopplysninger vil registreres i Unit4 Eiendomshåndtering for å sette Kunden i stand til å organisre og håndtere prosesser relatert til virksomhetsfunksjoner og ledelse og/eller administrative prosesser i deres interne virksomhet. Prosessene kan inkludere: • Registrering søkere • Utleiehåndtering • Prosesser i forbindelse med leieavtaler • Prosesser i forbindelse med leieboere • Behandling av elektroniske signaturer • Debitering, inkludert fakturautskrift • Hådntere betaling • Håndtere pengeinnkreving • Endringer i leien Behandlingen vil omfatte: ***Produkt (programvareløsning)*** Unit4 Eiendomshåndtering utferdiger programmerbar programvarekode for å tilse at de aktiviteter som angis ovenfor kan finne sted. Dette kan omfatte overføring av data til eller fra en tredjepartsløsning som ikke er under Databehandlers kontroll, gjennom integrasjoner. ***Tjenester*** Overføring og lagring av Personopplysninger for å gi ytterligere Tjenester som nærmere beskrevet i Beskrivelse av tjenesten eller People Platform Beskrivelse av tjenesten, der anvendelig. Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s-produktet og hjelp til Kunden i forbindelse med drift av løsningen som nærmere beskrevet i Unit4 Vilkår for kundestøtte. Tilgang til Personopplysninger for å konfigurere og/eller tilpasse og/eller flytte om på data (f.eks. fra dets systemarv) og/eller andre Profesjonelle tjenester som Kunden har kjøpt.

3. BESKRIVELSE AV BEHANDLINGEN OG MIDLENE FOR DENNE:

Databehandler vil Behandle forannevnte Personopplysninger i forbindelse med følgende aktiviteter (aktivitetene under er kun angitt som eksempler):

Type behandling	Beskrivelse	Midler og ressurser
Unit4 SaaS (General)	Databehandler skal Behandle Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og mer spesifikt i Unit4s Beskrivelse av tjenesten.	Personale Unit4s driftsteam har personale i land i EU (inludert, men ikke begrenset til, Polen, Sverige, Norge, Nederland, Spania og Portugal), Storbritannia, USA, Canada, Malaysia og Singapore. Dette Databehandler-personale drifter Unit4 SaaS. Verdier og infrastruktur Unit4 anvender infrastrukturtjenester levert fra tredjepart for å tilby Unit4 SaaS og benytter andre programvaresystem for drift og håndtering. Se Del 3.
Unit4 Talent Management SaaS	Databehandler skal Behandle Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og mer spesifikt i den anvendelige Beskrivelsen av tjenesten.	Personale Unit4 Talent Management SaaS operations team har personale hovedsakelig i Belgia og noen andre EØS-land. Datahas personnel predominantly in Belgium and some other EEA countries. Dette Databehandler-personale drifter Unit4 Talent Management SaaS Tjenesten. Verdier og infrastruktur Unit4 anvender hostingtjenester for infrastruktur fra tredjeparter for å tilby Unit4 SaaS og benytter andre programvaresystem for drift og håndtering. Se Del 3.
Kundestøtte	Databehandler skal Behandle Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og mer spesifikt i Unit4 Vilkår for kundestøtte.	Personale Unit4s Kundestøtte har personale i land i EU (inludert, men ikke begrenset til, Polen, Sverige, Norge, Tyskland, Irland, Nederland, Spania og Portugal), Storbritannia, Canda (og øvrige steder som er påkrevet for å støtte Unit4s virksomhetsbehov). Dette Databehandler-personale drifter Unit4s Kundestøtte (som beskrevet i Unit4 Vilkår for kundestøtte i avsnitt B i SLA). Verdier og infrastruktur Unit4 anvender andre programvaresystemer for drift, levering og håndtering av disse tjenestene.
Profesjonelle tjenester og/eller konsultasjon	Databehandler skal Behandle Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og mer spesifikt i mer detaljert prosjektdokumetnasjon eller Arbeidsbeskrivelser som er avtalt Partene i mellom når Prosjektet innledes.	Personale Unit4s team for Profesjonelle tjenester har personale i alle land hvor Unit4 har et registrert selskap, inkludert Storbritannia, Irland, Polen, Portugal, Norge, Spania, Frankrike, Tyskland, Sverige, USA, Canada, Singapore/Malaysia (og øvrige steder som er påkrevet for å støtte Unit4s virksomhetsbehov). Dette Databehadler-personale drifter Unit4s Profesjonelle tjenester. Verdier og infrastruktur Unit4 anvender andre programvaresystemer for drift, levering og håndtering av disse tjenestene.
Unit4 Profesjonelle tjenester (om under-databehandlere benyttes)	Databehandler og dens underdatabehandlere skal Behandle de tidligere nevnte Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og (om aktuelt) tredjeparts avtale- og tjenestedokumentasjon som gis som en del av Avtalen. For nærmere detaljer, se Del 3. Databehandler skal inngå en skriftlig avtale med Underdatabehandler(e), som skal være i overenstemmelse med relevante lover og regler, samt denne Avtalen. Videre har Behandlingsansvarlig gitt Databehandler tillatelse til å engasjere de Underdatabehandler(e) som er angitt i Del 3 ved å inngå Avtalen.	Se Del 3 eller det anvendelige Ordreskjema.
Tredjeparts-produkter og Tredjeparts-tjenester	Databehandler og dens underdatabehandlere skal Behandle de tidligere nevnte Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og tredjeparts avtale- og tjenestedokumentasjon som gis som en del av Avtalen.	Se Del 3 eller det anvendelige Ordreskjema og eventuelle ytterligere bestemmelser som er gitt i øvrige bilag til denne Informasjon om databehandling, om påkrevet av Tredjepartsleverandøren eller Gjeldende lover og regler.
People Platform Services ("**PPS**"), Lokaliserings-tjenester og/eller Applikasjoner	I tillegg til Unit4 SaaS, vil PPS, Lokaliseringstjenester og/eller Applikasjoner (der det er aktuelt) Behandle Personopplysninger i forbindelse med en personvernerkløring som blir presentert for sluttbrukeren, som bes om å avgi samtykke, i de tilfelle slike Personopplysninger behandles.	Personale Unit4s driftsteam, som drifter PPS, Lokaliseringstjenester og/eller Applikasjoner har personale i land i EU (inkludert, men ikke begrenset til, Polen, Sverige, Norge, Nederland, Spania og Portugal), Storbritannia, USA, Canada, Malaysia og Singapore. Dette Databehandler-personale drifter Unit4s SaaS. Verdier og infrastruktur Unit4 benytter sine egne og tredjeparters (delte) infrastrukturtjenester for å yte Unit4s PPS, Lokaliseringstjenester og/eller Applikasjoner. Dette inkluderer tredjepartsystemer (m.a.o. samarbeidsapplikasjoner), som Unit4 ikke har noen kontroll over. PPS, inkludert Wanda,

		Lokaliseringstjenester og/eller Applikasjoner benytter flere av Microsofts produkter og tjenester, herunder:
		• Kognitive tjenester:
		  ○ LUIS Cognitive Service - *språkforståelse*
		  ○ Text Translator API – *tekstoversettelse*
		  ○ QnA Maker Cognitive service – *tilbyr en tjeneste for spørsmål og svar*
		• Bot framework connectors – *åpner opp for å koble Wanda til de sosiale kanaler som støttes*
		• Traffic manager – *brukes til katastrofegjenoppretting og reservesystem om den primære regionen ikke er frisk*
		• Web apps / web jobs – *hoster web APIer og langvarige web-baserte prosesser*
		• Service bus – *tilbyr internkommunikasjon i Wandas ekosystem*
		• Storage accounts – *brukes for å lagre samtalestatus og brukerinnstillinger*
		• Cosmos DB – *tilbyr lagring*
		• Functions – *tilbyr logiske algoritmer for utvidelser*
		• Event grid – *tilbyr kommunikasjon*
		• API management – for å håndtere API-er
		• Service Plans – *Linux og dynamiske tjenesteplaner for å kjøre Tjenesten i*
		• Storage accounts – *brukes til lagring*
		• Key vault – *lagrer konfidensiell data som brukes for å kommunisere med Microsoft-tjenester og for interne tjenester*
		• Redis cache – *tilby caching-muligheter*
		• Application Insights – *Overvåkningssystem, inkludert fjernmåling og loggføring*
		• SQL server – *tilbyr lagring*
		• Kubernetes – *åpen kontainer for dataklynger*
		Further information and details relating to those Microsoft products and services can be found here: https://azure.microsoft.com/en-us/services/.
		I tillegg benytter PPS, Unit 4 Lokaliseringstjenester og/eller Unit4 Applikasjoner:
		Twilio – sendgrid – *for å sende e-poster*

4. LAGRINGSPERIODE

Databehandler vil beholde Personopplysninger **under Avtalens gyldighetstid.**

Etter den avtale lagringstiden skal Databehandler returnere Personopplysningene til Behandlingsansvarlig, i et format som er kompatibelt for migrasjon, bestemt av Databehandler **eller** umiddelbart destruere Personopplysningene uten å beholde en kopi, først på Behandlingsansvarliges anmodning.

5. INFORMASJON OM LAND (ELLER STED) FOR BEHANDLING AV PERSONOPPLYSNINGER

<table>
<tr><td>Produkt – Lokal installasjon (On premises)</td><td colspan="4">Data lagres på Behandlingsansvarliges server på deres hovedkontor eller registrerte kontor, som kan meddeles til Unit4 til enhver tid.</td></tr>
<tr><td>Produkt - Unit4 SaaS</td><td colspan="4">Unit4 SaaS driftes i flere datasentre, inkludert på verdensomspennende basis Microsoft Azure. Unit4 vil innsette kunden på den mest logiske plasseringen, avhengig av hvor Kunden bor (som angitt i Ordreskjema). Alle Kundedata vil bare bli lagret i den valgte geo-politiske sonen og vil ikke bli flyttet ut av den uten uttrykkelig samtykke fra kunden.
<table>
<tr><th>SKYMODELL</th><th>GEO-POLITISK SONE</th><th>PLASSERING AV DATASENTER</th><th>FASILITET ELLER PARTNERSKAP</th></tr>
<tr><td>SAAS CLOUD</td><td>EU</td><td>DUBLIN / AMSTERDAM</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>USA</td><td>FLERE LOKASJONER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>CANADA</td><td>TORONTO / QUEBEC BY</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>STORBRITANNIA</td><td>LONDON / CARDIFF</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>ASIA</td><td>SINGAPORE / HONG KONG</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>AUSTRALIA</td><td>VICTORIA / NEW SOUTH WALES</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>NORGE</td><td>OSLO / STAVANGER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>SVERIGE (NORDEN)</td><td>SÄTRA OG SOLLENTUNA</td><td>CONAPTO</td></tr>
</table></td></tr>
<tr><td>Produkt – Talent Management SaaS</td><td colspan="4">Talent Management SaaS driftes i Microsoft Azure, som dekker både EU og Storbritannia som geo-politiske soner (ovenfor), hvor sonen blir allokert på bakgrunn av Kundens plassering. All Kundedata, utenom ved deling med utvalgte underdatabehandlere i Del 3, vil bare bli lagret i den valgte geo-politiske sonen og vil ikke bli flyttet ut av den uten uttrykkelig samtykke fra kunden.</td></tr>
<tr><td>Unit4 Kundestøtte – Standard kundestøtte og andre standard kundestøtte-tjenester</td><td colspan="4">Unit4 Kundestøtte anvender tredjepartsprogramvare (slik som SalesForce/ServiceNow) for å registrere og håndtere Saker. Disse Sakene er tilgjengelige for enhver Unit4-ansatt som har fått tilgang til tredjepartsprogramvare slik som ingeniører for kundestøtte og skytjenester, samt konsulenter for Profesjonelle tjenester og tjenestehåndtering. Tilgang kontrolleres gjennom interne håndterings- og organiseringsprosesser, for å sikre at Personopplysninger ikke er tilgjengelige for konsulenter eller teknikere på lokasjoner som ikke burde ha tilgang til spesifikke Kundedetaljer.
<table>
<tr><th>Kundens lokalisering</th><th>Primær Kundestøtte gis fra (men kan inkludere andre EU-land):</th></tr>
<tr><td>Storbritannia og Irland</td><td>Storbritannia, Irland, Portugal og Polen</td></tr>
<tr><td>Sverige, Norge, Danmark, Finland og Island</td><td>Polen, Portugal, Norge og Sverige.</td></tr>
<tr><td>USA & Canada</td><td>Polen, Portugal, USA og Canada.</td></tr>
<tr><td>Resten av Europa</td><td>Polen, Portugal og Tyskland.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td colspan="2">APAC</td><td>Polen, Portugal og Singapore/ Malaysia.</td></tr>
<tr><td>Unit4 Kundestøtte – 24/7 Kundestøtte</td><td colspan="3">Gjennom å benytte en «følg solen»-metodikk kan kundestøtte i Kundesaker skje 24/7 på enhver lokasjon angitt ovenfor, samt i Nedeland, Spania og slike andre lokasjoner som er nødvendig for å støtte Unit4s virksomhetsbehov.</td></tr>
<tr><td>Unit4 Kundestøtte – Utelukkende EU Kundestøtte</td><td colspan="3">Dersom Utelukkende EU Kundestøtte er valgt, vil det kun gis Kundestøtte i Saker innen EU-lokasjonene angitt ovenfor for standard kundestøtte (i kontortiden).</td></tr>
<tr><td rowspan="4">People platform services (“PPS”) (generelt) inkludert IDS og Wanda (sammen med støtte-tjenester), Lokaliserings-tjenester og/eller Applikasjoner</td><td colspan="3">PPS er skytjenester som benytter delt infrastruktur og tredjepartstjenester som ikke kan garantere isolasjon i den geopolitiske sonen. Under gis en oversikt over PPS og landet (eller stedet) for Behandling av Personopplysninger som benytter den tjenesten.</td></tr>
<tr><td>Tjeneste</td><td>Geo-politisk sone</td><td>Hvor Tjenester Behandler eller lagrer Data</td><td>Primær Kundestøtte gis fra:</td></tr>
<tr><td>Wanda</td><td>Hvilken som helst</td><td>Hovedsakelig innen EU, men kan være hvor som helst der hvor det er et Azure datasenter (f.eks. USA).</td><td>EU-land, inkludert Irland, Polen og Spania, USA og andre globale kundestøttesentre hvor det er påkrevet.</td></tr>
<tr><td>PPS, Lokaliserings-tjenester og/eller Applikasjoner</td><td>Beror på hvor skytjenesten tas i bruk</td><td>Tjenesten tilbys og data lagres i den valgte geo-politiske sonen.</td><td>Som ovenfor for Unit4 SaaS</td></tr>
<tr><td rowspan="5">Unit4 Profesjonelle tjenester og Unit4 Customer Success-funksjon</td><td>Emne</td><td colspan="2">Profesjonelle tjenester og Customer Success gis fra:</td></tr>
<tr><td>Implementering andre prosjekttjenester</td><td colspan="2">I Territoriet eller stedet hvor Kunden har sitt registrete kontor/hovedsete (hvilket som er anvendelig) og/eller Portugal avhengig av hva som er avtalt mellom Partene i prosjektdokumetnasjonen eller Arbeidsbeskrivelsen (om anvendelig).</td></tr>
<tr><td>Datamigrasjon</td><td colspan="2">I Territoriet eller stedet hvor Kunden har sitt registrete kontor/hovedsete (hvilket som er anvendelig) og/eller Portugal avhengig av hva som er avtalt mellom Partene i prosjektdokumetnasjonen eller Arbeidsbeskrivelsen (om anvendelig).</td></tr>
<tr><td>Feilsøking</td><td colspan="2">I anvendelig lokasjon for Unit4 Kundestøtte og Portugal.</td></tr>
<tr><td>Customer Success</td><td colspan="2">I anvendelig lokasjon for Unit4 Kundestøtte og Portugal.</td></tr>
</table>

6. KONTAKTINFORMASJON

For spørsmål eller kommentarer til denne Informasjonen om databehandling er følgende kontaktpersoner:

Databehandler: Ved brev (addressert til Global Data Protection Officer, kopi til Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, Nederland, eller på e-post til privacy@unit4.com eller til Unit4-adressen for meddelelser som er angitt i Avtalen.

Behandlingsansvarlig: Adressen som angis for Behandlingsansvarlig i Avtalen.

DEL 2 – SIKKERHETSTILTAK

Som angitt i avsnitt 6 i Databehandlingsvilkårene, er de tekniske og organisatoriske sikkerhetstiltakene listet opp i denne delen og vil suppleres eller endres hvis nødvendig. Den Behandlingsansvarlige anser disse tiltakene å være egnede for behandlingen av Personopplysninger.

Unit4s forretningsmessige sikkerhetstiltak (sammendrag av intern forretningsvirksomhet)

Beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene implementert av Databehandleren innen dens organisasjon (generelt):

Fysisk sikkerhet:

- Fysisk adgangskontroll er håndtert av Unit4s fasiliteter.
- Alle kontorer har sikkerhetssystemer når det gjelder kontroll av tilgang gjennom barrierer, for eksempel inngangsporter, bemannede resepsjoner, alarmerte branndører, systemer for oppdagelse av inntrengere og/eller låsbare kontorer.
- Unit4 håndterer adgangskontroll ved hjelp av det personer vet, slik som passord eller personlig adgangskode, eller ved hjelp av hva personer har med seg, slik som adgangspass.
- På-stedet serverrom (når relevant) har ekstra fysiske kontroller.
- Tilgang til sikre områder eller sensitiv informasjon er begrenset for å hindre at besøkende/uautorisert personale får uautorisert tilgang (gjennom låsbare kontorer eller låsbare skap) og gjennomføring av retningslinjer for ren kontorplass der det er passende.
- Besøkende hos Unit4 kontrolleres i resepsjonen (enten av en resepsjonist eller annet medlem av personalet).
- Makuleringsmaskiner eller annen egnet metode for sikker fjerning av sensitive dokumenter brukes.

Virtuell- og databehandlingssikkerhet:

- Den ansvarlige linjelederen vil sikre at ansatte og leverandører returnerer alle eiendeler tilhørende Unit4 de er i besittelse av etter terminering av deres arbeidsforhold eller leverandøravtale. Det føres register over slik returnering av eiendeler.
- Unit4 sikter på å klassifisere informasjon som enten offentlig, konfidensiell, beskyttet eller sensitiv. Informasjon vil deretter beskyttes i henhold til denne klassifiseringen.
- Medium (inkludert harddisker) blir kastet sikkert og trygt når det ikke lenger er behov for dem. Alt sensitivt materiale (harddisker, disketter, etc.) fjernes ved bruk av programvare som garanterer fjerning (ikke gjennom reformatering eller sletting), før det kastes eller fysisk ødelegges.
- Antivirusprogram – vi benytter den siste versjonen av løsninger som er industristandard for å gi beskyttelse mot virus og ondsinnet programvare (anti-malware).
- Videre anvender Unit4:
- kontroll av tildelte rettigheter
- registrering og kontrollering av tilgang til systemet
- gjenopprettingstiltak
- evnen til å sikre Behandlings-systemer og -tjenesters kontinuerlige konfidensialitet, integritet, tilgjengelighet og robusthet, og
- systemer og prosesser for å tillate gjenoppretting av tilgjengeligheten og tilgangen til Personopplysninger til rett tid ved en fysisk eller teknisk hendelse.
- planer for forretningskontinuitet og Katastrofegjenoppretting som omfatter informasjonssikkerhetsbetraktninger har blitt utarbeidet.

Retningslinjer for sikkerhet og dokumentasjon:

- Unit4s globale lederteam og/eller dets respektive lokale lederteam fører tilsyn med både global og lokal informasjonshåndtering og sikkerhetsplaner, inkludert retningslinjer for informasjonssikkerhet som møter identifisert informasjonssikkerhetsrisiko og støtter forretningsmålene.
- Informasjonssikkerhet og administrasjon er tildelt globalt til den globale informasjonssikkerhetslederen (Chief Information Security Officer) og global personvernombud (Global Data Protection Officer), som administrerer ressurser for å levere strategisk og samlet overholdelse av informasjonssikkerhetsretningslinjer og –prosess.
- Unit4 har implementert sikkerhetsretningslinjer som er oppdatert og endret regelmessig for å overholde god industripraksis.
- Unit4 har en personvernerklæring og white paper på GDPR publisert på www.unit4.com/terms.
- Unit4 inngår konfidensialitetsavtaler med tredjeparter når konfidensiell informasjon deles i forbindelse med dets virksomhet.
- Unit4 sikrer at alle ansatte og leverandører inngår standard konfidensialitetsbestemmelser i sine kontrakter.
- Unit4 gir alle ansatte opplæring relatert til: personvern, sikkerhet og dets kjerneprinsipper som angitt over.

Tilleggselementer for Unit4 SaaS på Microsoft Azure (sammendrag)

Beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene som er implementert av Databehandleren i forbindelse med levering av Unit4 SaaS:

Datasikkerhet

Unit4 SaaS benytter flere mekanismer for å beskytte Personopplysninger i skyen. Under er en omfattende oversikt over anvendte kontrolltiltak.

Sikkerhetsegenskaper på nettverksnivå, prosess og protokoller

- Sikker dataoverføring over offentlige nettverk - all trafikk er sikret ved bruk av protokoller som er industristandard, slik som SSL/TLS og HTTPS.
- Systemsikkerhet – logisk autentisering og autorisasjonsmekanismer er på plass
- Brannmurer – neste generasjon brannmurteknologi for å sikre at inngående og utgående trafikk er kontrollert.

Sikkerhetsegenskaper på databasenivå, prosess og protokoller

- Datasikkerhet - logisk autentisering og autorisasjonsmekanismer er på plass.
- Databasesikkerhet – Hver kunde har sin egen sikre database, hvilket betyr at å skille mellom databaser ikke er påkrevet og kundedata ikke sammenblandes. Resultatet er at en kundes data aldri feilaktig deles med andre.
- Sikkerhetskopier av databaser er kryptert ved bruk av teknologi som krypterer hele databasen, slik som Transparent Database Encryption.
- Ikke-transaksjonell data og filer vil bli sikret ved standard symmetrisk kryptering (AES).
- Unit4 bruker Azure Key Vault for å ha kontroll over nøkler brukt av skyapplikasjoner og tjenester for kryperting av data.

Kontinuerlig testet og utviklet sikkerhet

For å avdekke uforutsette sårbarheter og raffinere våre evner til å oppdage og respondere, undersøker vi kontinuerlig hvordan vi kan forbedre sikkerhetsstillingen (security posture) vår for å forsvare mot potensielle brudd. Unit4s team for drift av sky (Cloud operations team) som fører nært tilsyn med og sikrer Unit4s drift av sky (skyinfrastruktur, skytjenester, produkter, enheter og interne ressurser) – tester penetrering og forbedrer vår evne til å beskytte, oppdage og gjenopprette etter cybertrusler.

Avdekke, minimere og respondere på trusler

Siden antallet, variasjonen og alvorligheten av cybertrusler har økt, har også vår aktsomhet når det gjelder å avdekke og respondere på trusler økt. Sentraliserte overvåkningssystem gir fortløpende synlighet og betimelige varsler. Hyppig bruk av sikkerhetsrettelser (security patches) og –oppdateringer bidrar til å beskytte systemet fra kjente sårbarheter. Systemer for oppdagelse av inntrengeroppkopling og ondsinnet programvare er konstruert for å oppdage og minimere risiko fra angrep fra utsiden. I tilfelle ondsinnet aktivitet vil vårt team for respons på hendelser følge etablerte prosedyrer for hendelseshåndtering, kommunikasjon og gjenoppretting. Teamet bruker beste praksis i industrien til å varsle både interne team og kunder. Til slutt, sikkerhetsrapporter overvåker adgangsmønster for å bidra til å proaktivt identifisere og minimere potensielle trusler.

Datasegregering

Data er valutaen i den digitale økonomien og vi tar ansvaret for å beskytte kundedata veldig alvorlig. Både teknologiske sikkerhetsanordninger, slik som kryptert kommunikasjon, og operasjonelle prosesser bidrar til å holde kundedata sikret. Data fra flere kunder kan være lagret på samme IT-ressurser i skyen. Unit4 bruker logisk isolasjon til å segregere hver kundes data fra andres. Unit4 SaaS er designet for å motvirke risikoer iboende i et miljø for flere leietakere (multitenant environment). Datalagring og –behandling er logisk separert blant kunder ved å ha separate databaseinstanser for alle våre kunder.

Datakryptering

Unit4 leverer, som en standard, sikker tilgang til alle sine tjenester ved kryptering av all data i transitt som overføres på offentlige nettverk. Dette gjøres ved å kun bruke sikre protokoller, som HTTPS over TLS, som bruker siste sikkerhetschiffer. Mekanismen som brukes er en transparent kryptering av hele databasen – TDE. Kunder av Microsoft Azures Public SaaS får TDE kryptering av inaktive data som en standard.

Adgangskontroll

Kunder som bruker Unit4-produkter i skyen har full mulighet til å utøve front-end adgangskontroller til sin applikasjon. Dette betyr at ansvaret for å opprette nye kontoer, avslutte kontoer og kontogjennomgang for Unit4s applikasjoner ligger hos kunden.

Unit4 vil beholde begrenset back-end tilgang til kundedata (gjennom direkteforbindelse til database). Unit4s tilgang til personopplysninger skal være strengt begrenset til aktiviteter som er nødvendige for installering implementering, vedlikehold, reparasjon, feilsøking eller oppdatering av løsningen. All tilgang registreres og er begrenset til en liten gruppe skyingeniører og kundestøttekonsulenter. Tilgangslogger er lagret i det sentraliserte overvåkningssystemet i 365 dager. I tilfelle Datasikkerhetsbrudd, vil Unit4 kunne fremlegge tilgangslogg ved forespørsel.

Varsel om datasikkerhetsbrudd

Unit4 skal varsle Kunden uten ugrunnet opphold etter å ha blitt kjent med et Datasikkerhetsbrudd. Kunder skal påse at kontaktene opplistet i Unit4 Community alltid er oppdaterte, siden de vil bli brukt for all kommunikasjon.

Innebygd personvern og datasikkerhet

Unit4s skyplattform ble designet fra bunnen av, med datasikkerhet og personvern i tankene. Unit4 forbedrer løsningens sikkerhet kontinuerlig, ved å anvende kunnskap opparbeidet gjennom årlige penetrasjonstester og revisjoner.

Unit4 og operatørene av datasentrene har ulike sikkerhetssertifiseringer, vennligst se den aktuelle Beskrivelsen av tjenesten.

Tilleggselementer for Unit4 People Platform Services (sammendrag)

Beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene som er implementert av Databehandleren i forbindelse med leveranse av Unit4 People Platform Services (kun for sky):

Datasikkerhet

Unit4 People Platform benytter flere mekanismer for å beskytte personopplysninger i skyen. Under er en omfattende oversikt over anvendte kontrolltiltak.

Sikkerhetsegenskaper på nettverksnivå, prosess og protokoller

- Sikker dataoverføring over offentlige nettverk - all trafikk er sikret ved bruk av protokoller som er industristandard, slik som SSL/TLS og HTTPS.

Autentisering

- Alle tjenester følger prinsippet om minste privilegium og autentisering mot tjenester og deres APIer er sikret gjennom bruk av mekanismer som er industristandard. OpenID Connect og den underliggende oAuth 2.0 protokollen er brukt til å sikkert utføre autentisering av brukere og/eller klienttjenester med betrodde parter og vil bekrefte identitet og tilgang ved bruk av kravsbaserte symboler (tokens).
- HMAC (Hash-based Message Authentication) brukes som alternativ metode for å sikre kommunikasjon mellom tjenester.

Sikkerhetsegenskaper på databasenivå, prosess og protokoller

- All data lagret i lagrinskontoer krypteres inaktivt (at rest).
- Alle lagringskontoer krever sikker overføring – all trafikk er sikret gjennom bruk av protokoller som er industristandard, slik som SSL/TLS and HTTPS.
- All data lagret i Azure Cosmos DB krypteres inaktivt (at rest) og under transport.
- Alle Azure SQL-servere er aktivert med Transparent Data Encryption (TDE).
- Alle Azure SQL-servere kjører med trusselavdekking og revisjon aktivert.
- Azure KeyVault brukes for å sikre særlig sensitiv informasjon som tjenesteansvarlig berettigelsesbevis (service principal credentials).

Sikkerhetsegenskaper på meldingsnivå, prosess og protokoller

- All data lagret av Azure Service Bus instanser krypteres inaktivt (at rest).
- All trafikk (i transitt) på Azure Service Bus sikres ved bruk av protokoller som er industristandard slik som SSL.

Mer informasjon om sikkerhetsretningslinjene og sikkerhetsprogrammet er tilgjengelig på www.unit4.com/terms.

Datakryptering

Unit4 People Platform Services leverer, som en standard, sikker tilgang til alle sine tjenester ved kryptering av all data i transitt som overføres på offentlige nettverk. Dette gjøres ved å kun bruke sikre protokoller, som HTTPS over TLS (1.2), som bruker siste sikkerhetschiffer. All data som lagres er kryptert.

Varsel om datasikkerhetsbrudd

Unit4 skal varsle Kunden uten ugrunnet opphold etter å ha blitt kjent med et Datasikkerhetsbrudd. Kunder skal påse at kontaktene opplistet i Unit4 Community alltid er oppdaterte, siden de vil bli brukt for all kommunikasjon.

Innebygd personvern og datasikkerhet

Unit4 People Platform Services ble designet fra bunnen av, med datasikkerhet og personvern i tankene. Unit4 forbedrer løsningens sikkerhet kontinuerlig, ved å anvende kunnskap opparbeidet gjennom årlige penetrasjonstester og revisjoner.

DEL 3 – UNIT4S UNDERDATABEHANDLERE

Tjeneste	**Underdatabehandler** (selskapsnavn, sted etc.)	**Sted for Behandling**	**Type tjeneste som utføres av Underdatabehandler / Modul brukt med**
Unit4s Profesjonelle tjenester (hvis fremkontrahert til en leveransepartner)	Som spesifisert i Avtalen.	Som spesifisert i Avtalen.	Som spesifisert i Ordreskjema eller avtalt skriftlig med Kunden.
Tredjepartsprodukter og Tredjepartstjenester, kun relevant når kjøpt av kunden.	Som spesifisert i Avtalen.	Som angitt i Avtalen eller i andre bilag eller vedlegg til Avtalen relatert til Tredjepartsleverandørs behandling.	Programvare og/eller kundestøtte og/eller skytjenester.
Unit4 SaaS	Microsoft Azure	Som angitt over i Del 2, punkt 5.	Leverer skyinfrastruktur og -tjenester.
	Microsoft Dynamics	Som angitt over i Del 2, punkt 5.	Leverer programvaretjenester, særlig Microsoft Dynamics (inkludert noe skyinfrastruktur).
	Microsoft	Som angitt over i Del 2, punkt 5.	Leverer programmeringsverktøy (software tooling) og Office
	Conapto	Som angitt over i Del 2, punkt 5.	Leverer skyinfrastruktur og -tjenester.
	Twilio – Sendgrid	USA (Privacy Policy)	Sende e-post (EUs standard personvernbestemmelser – se Del 4)
Unit4 SaaS – Talent Management	Microsoft Azure	Dublin, Irland	Leverer løsning - Suite
	LogDNA	USA (Privacy Policy)	Leverer løsning – Suite (EUs standard personvernbestemmelser – se Del 4)
	Mandrill	USA (Privacy Policy)	Leverer løsning – Suite (EUs standard personvernbestemmelser – se Del 4)
	Mixpanel	USA (Privacy Policy)	Leverer løsning – Suite (EUs standard personvernbestemmelser – se Del 4)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Leverer løsning - Learn (kun SCORM) (EUs standard personvernbestemmelser – se Del 4)
	Sentry	USA (Privacy Policy)	Leverer løsning – Suite (EUs standard personvernbestemmelser – se Del 4)
	Slack	USA (Privacy Policy)	Leverer løsning – Perform (EUs standard personvernbestemmelser – se Del 4)
	Wistia	USA (Privacy Policy)	Leverer løsning – Learn (EUs standard personvernbestemmelser – se Del 4)
People Platform Services ("**PPS**") (generelt) inkludert IDS og Wanda (sammen med eventuelle støttetjenester)	Microsoft Azure	Som angitt i Del 1, punkt 5 og som gitt av Microsoft her: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.	Leverer skyinfrastruktur og plattformtjenester (som angitt over) i Del 1.
	Twilio – Sendgrid	USA (Privacy Policy)	Sende e-post (EUs standard personvernbestemmelser – se Del 4)

DEL 4 – EUS STANDARD PERSONVERNBESTEMMELSER

STANDARD CONTRACTUAL CLAUSES ("SCC")

Controller to Processor

Unit4 is the Processor/data importer

Customer is the Controller/data exporter

In the relation between Parties, Module Two (Transfer controller to processor) of the SCC is applicable.

These SCC only apply where there is any transfer by the Controller of Personal Data from inside the EEA to the Processor located outside the EEA, also known as a third country, and where no adequacy decision applies.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([i]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, **as listed in the Agreement ("Customer")** and as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, **as listed in the Agreement ("Unit4")** and as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([ii]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([iii]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([iv]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) **[Where the data exporter is established in an EU Member State:]** The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:]** The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (v);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and

confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be in accordance with, the law that govern the Agreement.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the law that govern the Agreement.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.**APPENDIX**

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

As listed in the Agreement

Activities relevant to the data transferred under these Clauses:

As described in the Agreement

2. Role (controller/processor):
As described in the Agreement

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

As listed in the Agreement.

Activities relevant to the data transferred under these Clauses:

As described in the Agreement

2. Role (controller/processor):

As described in the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in Section 1 and 3 of the Data Processing Information.

Categories of personal data transferred

As described in Section 1 and 3 of the Data Processing Information.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As described in Section 1 and 3 of the Data Processing Information.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As described in Section 1 and 3 of the Data Processing Information.

Nature of the processing

As described in Section 1 and 3 of the Data Processing Information.

Purpose(s) of the data transfer and further processing

As described in Section 1 and 3 of the Data Processing Information.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described in Section 1 and 3 of the Data Processing Information.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Section 1 and 3 of the Data Processing Information.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority will be the authority of The Netherlands:

"De Autoriteit Persoonsgegevens".

(Unless otherwise required under clause 13).

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As described in Section 2 of the Data Processing Information

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), **Option 1).**

N/A

---

[i] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[ii] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[iii] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[iv] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[v] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.