Vedlegg A(i) – Unit4 Databehandlingsvilkår

1. ANVENDELSESOMRÅDET FOR DISSE DATABEHANDLINGSVILKÅRENE

1.1 Kunden (heretter omtalt som «**Behandlingsansvarlig**») er den Part som (alene eller sammen med andre) bestemmer formålet med, samt hvilke midler man skal ta i bruk ved, Behandlingen av Personopplysninger.

1.2 Unit4 og dets Tilknyttede selskaper (heretter omtalt som «**Databehandler**») er den Part som opptrer på vegne av Behandlingsansvarlig, uten å være gjenstand for dennes direkte kontroll.

1.3 Databehandler vil behandle Personopplysninger på vegne av Behandlingsansvarlig (og Behandlingsansvarlig samtykker til dette), i henhold til gjeldende lover og regler, samt disse Databehandlingsvilkårene, med vedlegg.

1.4 Bilag 1 beskriver, blant annet, midlene og målene ved Behandlingen, kategoriene av Personopplysninger som skal Behandles, lagringstiden for slike Personopplysninger, samt hvilke(t) land (eller sted(er)) Personopplysningene skal Behandles.

1.5 Bilag 2 beskriver de gjeldende sikkerhetstiltak som Databehandler har implementert, og som Behandlingsansvarlig bekrefter at er adekvate.

1.6 Bilag 3 angir nærmere informasjon om eventuelle Underdatabehandlere.

1.7 Bilag 4 inneholder EUs standard personvernbestemmelser , som får anvendelse i ethvert tilfelle hvor Behandlingsansvarlig overfører Personopplysninger innenfor EØS-området til Databehandler utenfor EØS-området, som nærmere beskrevet i punkt 2.3 nedenfor.

1.8 Bilagene kan oppdateres til enhver tid under Databehandlingsvilkårenes avtaleperiode, om nødvendig.

2 BEHANDLING

2.1 Databehandler og Behandlingsansvarlig skal gi hverandre all informasjon som er nødvendig for å sikre korrekt etterlevelse av Personvernregelverket, uten unødig opphold.

2.2 Behandlingen av Personopplysninger foregår i det eller de landene, eller på det eller de stedene, som angis i Bilag 1. Behandlingsansvarlig gir sitt uttrykkelige samtykke til Behandling av Personopplysninger i de landene/på de stedene som er angitt i Bilag 1. Dersom Behandlingen skal foregå i et eller flere andre land, eller på et eller flere andre steder, skal Databehandler informere Behandlingsansvarlig om dette.

2.3 Dersom Personopplysninger Behandles i et land utenfor det europeiske økonomiske samarbeidsområdet (EØS) og EU-kommisjonen ikke har foretatt noen beslutning om at det aktuelle landet anses å inneha et adekvat beskyttelsesnivå, skal Behandlingen kun finne sted dersom det er implementert egnede sikkerhetstiltak som sikrer et adekvat beskyttelsesnivå for Personopplysninger. I slike tilfeller, for å sikre at egnede beskyttelsestiltak er avtalt, skal Partene oppfylle sine respektive forpliktelser i EUs standard personvernbestemmelser inntatt i Bilag 4 til disse Databehandlingsvilkårene (eller slike egnede beskyttelsestiltak som Tilsynsmyndigheten for personvern eller en annen kompetent myndighet («**Myndigheten**») beslutter at oppfyller vilkårene for et adekvat beskyttelsesnivå) og Behandlingsansvarlig godtar herved, og instruerer Databehandler til å utføre slik Behandling.

3 DATABEHANDLERS ANSVAR

3.1 Databehandler vil Behandle Personopplysninger på en korrekt og hensynsfull måte i samsvar med disse Databehandlingsvilkårene, og skal etterleve Personvernregelverket.

3.2 Databehandler vil kun Behandle Personopplysninger i samsvar med oppfyllelsen av Avtalen og de skriftlige instrukser som er gitt av Behandlingsansvarlig, med mindre Databehandler er juridisk forpliktet til å Behandle Personopplysninger på en måte som strider mot dette. I sistnevnte tilfelle skal Databehandler informere Behandlingsansvarlig om den eller de relevante lovbestemmelsene og pliktene i henhold til disse.

3.3 Databehandler vil kun Behandle Personopplysninger for de formål som er angitt i mottatte instrukser, og for å oppfylle forpliktelsene i henhold til disse Databehandlingsvilkårene. Databehandler skal ikke bruke Personopplysninger til andre formål.

3.4 Databehandler vil ikke utlevere Personopplysninger til tredjeparter (utenom til den Registrerte eller andre personer som er godkjent av Behandlingsansvarlig eller Databehandler til å Behandle Personopplysninger), med mindre en slik utlevering skjer i henhold til Behandlingsansvarliges instrukser eller i sammenheng med oppfyllelsen av Avtalen, disse Databehandlingsvilkårene (inkludert de respektive Bilagene) eller når det er nødvendig for å oppfylle en lovbestemt plikt eller rettslig avgjørelse.

3.5 Databehandler vil ikke endre, redigere, korrigere eller på annen måte forandre Personopplysningene uten at Behandlingsansvarlig har instruert om dette.

3.6 Databehandler skal i rimelig utstrekning bistå Behandlingsansvarlig med å imøtekomme anmodninger fra den Registrerte i forbindelse med utøvelsen av sine rettigheter under Personvernregelverket, herunder, men ikke begrenset til, å (i) gi den Registrerte tilgang til sine Personopplysninger; (ii) rette eller slette Personopplysninger på anmodning fra den Registrerte; (iii) fremlegge bevis for at Personopplysninger har blitt rettet eller slettet; (iv) fremlegge de Personopplysninger som den Registrerte har gitt til Behandlingsansvarlig og som Behandlingsansvarlig har gitt til Databehandler og; (v) overføre alle Personopplysninger som tilhører den Registrerte til en annen Behandlingsansvarlig (dataportabilitet). Dersom det fremsettes en anmodning om å returnere eller fremlegge en kopi av Personopplysninger, skal Databehandler skal utlevere denne i et strukturert, alminnelig anvendt og i maskinlesbart format.

3.7 Dersom Databehandler mottar en anmodning eller en protest fra den Registrerte (som kan innebære (men er ikke begrenset til) en anmodning om informasjon, tilgang, retting, dataoverføring, begrensing av behandling, eller overføring av Personopplysninger), skal Databehandler umiddelbart videresende anmodningen til Behandlingsansvarlig.

3.8 Databehandler skal føre protokoll over alle kategorier av Behandlingsaktiviteter som utføres på vegne av Behandlingsansvarlig, i samsvar med Personvernregelverket. Databehandler skal gi Behandlingsansvarlig all nødvending informasjon som knytter seg til dette.

3.9 Databehandler skal bistå Behandlingsansvarlig med å overholde de juridiske informasjonspliktene overfor Myndigheten og den Registrerte. Databehandler skal, om nødvendig, og dersom det angår Databehandlerens teknologi, bistå Behandlingsansvarlig der hvor en vurdering av personvernkonsekvensene anses nødvendig etter Personvernregelverket.

3.10 Dersom Behandlingsansvarlig er gjenstand for en særskilt anmodning om informasjon fra den Registrerte eller en tredjepart (utenom den Registrerte eller andre personer som er godkjent av Behandlingsansvarlig eller Databehandler til å Behandle Personopplysninger) som er berettiget til å fremsette en slik anmodning, skal Databehandler bistå Behandlingsansvarlig med dette. Databehandler skal ikke foreta seg noe som helst med tanke på eventuell anmodning fra den Registrerte eller en tredjepart (utenom den Registrerte eller andre personer som er godkjent av Behandlingsansvarlig eller Databehandler til å Behandle Personopplysninger), for så vidt ikke Behandlingsansvarlig har instruert Databehandler om dette på forhånd. Dersom den Registrerte kontakter Databehandler for å utøve sine rettigheter etter Personvernregelverket, skal Databehandler umiddelbart videresende denne anmodningen til Behandlingsansvarlig.

4 BEHANDLINGSANSVARLIGES ANSVAR

4.1 Behandlingsansvarlig er ansvarlig for lovligheten av Behandlingen av Personopplysninger og at den er i samsvar med Personvernregelverket, inkludert, men ikke begrenset til, å sikre rettighetene til de Registrerte.

4.2 Behandlingsansvarlig er alene ansvarlig for å bestemme formålet med og midlene for Behandlingen av Personopplysninger.

4.3 Behandlingsansvarlig er ansvarlig for å informere den Registrerte og å garantere for den Registrertes rettigheter etter Personvernregelverket og annen personvernlovgivning, og for kommunikasjon med de Registrerte.

4.4 Behandlingsansvarlig garanterer at de innsamlede Personopplysninger er adekvate, relevante og begrenset til det som er nødvendig for formålene de overføres og (på annen måte) Behandles.

4.5 Behandlingsansvarlig skal innen rimelig tid og i et omforent format som angitt i Bilag 1, gjøre tilgjengelig all informasjon som Databehandler vil kunne behøve for Behandlingen.

4.6 Behandlingsansvarlig er ansvarlig for (i forholdet partene i mellom og overfor de Registrerte og Myndigheten): (i) å påse at de Registrerte har avgitt gyldig samtykke til Behandlingen (enten gjennom Databehandler eller en eventuell Underdatabehandler) og/eller sikre at de har gyldig behandlingsgrunnlag til å utføre Behandlingen; og (ii) alle krav eller klager som oppstår som følge av Databehandlers handlinger, i den grad handlingene er et resultat av Behandlingsansvarliges instrukser.

5 UNDERDATABEHANDLERE

5.1 Ved inngåelse av Avtalen vil Databehandler engasjere Underdatabehandleren(e) som angitt i Bilag 3 eller i Ordreskjema.

5.2 Behandlingsansvarlig samtykker herved til endringer i Underdatabehandlere. Databehandler skal skriftlig informere Behandlingsansvarlig forut for enhver planlagt endring, for eksempel når det gjelder utskiftning av en Underdatabehandler. Behandlingsansvarlig gis mulighet til å protestere mot slike endringer skriftlig, innen 7 dager fra skriftlig meddelelse om slik endring.

5.3 Databehandlers engasjement av en Underdatabehandler påvirker ikke på noen som helst måte ansvaret Databehandler har overfor Behandlingsansvarlig. Underdatabehandler kan bare gis tilgang til de relevante Personopplysninger når Underdatabehandler oppfyller (eller forsikrer oppfyllelse av) forpliktelsene etter disse Databehandlingsvilkårene i alle vesentlige aspekter. Databehandler skal inngå en skriftlig avtale med hver Underdatabehandler om Behandlingen av Personopplysninger, som skal oppfylle kravene i Personvernregelverket, og, hvor det er praktisk mulig, være på vesentlige samme vilkår som angis i disse Databehandlingsvilkårene.

5.4 Bilag 3 angir nåværende Underdatabehandlere, hvor Behandlingen finner sted og en beskrivelse av arbeidet. Databehandler vil, om nødvendig og innen rimelig tid etter en endring, oppdatere dette Bilaget under Avtalens gyldighetstid.

5.5 Der Databehandler engasjerer en Underdatabehandler (etter Avtalen eller på annen måte ved etterfølgende godkjenning) til å utføre enkelte av sine forpliktelser, skal Databehandler være ansvarlig under disse Databehandlingsvilkårene for alle handlinger som Underdatabehandlerne utfører.

5.6 Der Databehandler engasjerer en Underdatabehandler kan Behandlingsansvarlig (under visse omstendigheter) gi instrukser til Underdatabehandler i forbindelse med Underdatabehandlerens Behandling av Personopplysninger. Under slike omstendigheter er Databehandler ikke ansvarlig for brudd på disse Databehandlingsvilkårene som er en følge av at Underdatabehandleren handler etter instrukser fra Behandlingsansvarlig, uten hensyn til om Databehandler er klar over dette eller ikke.

6 PERSONOPPLYSNINGSSIKKERHET OG DATASIKKERHETSBRUDD

6.1 Databehandler skal implementere de tekniske og organisatoriske sikkerhetstiltak, i samsvar med Personvernregelverket og god forretningsskikk, som er nødvendige for å sikre tilgjengelighet, integritet og konfidensialitet til Personopplysningene og for å beskytte Personopplysningene mot tap eller ulovlig Behandling. For å kunne oppfylle disse kravene, skal Behandlingsansvarlig informere Databehandler om ethvert sikkerhetskrav som får anvendelse på Behandlingen og ved anmodning om endringer i sikkerhetskravene for Behandling av Personopplysninger, i god tid gi all nødvendig informasjon.

6.2 De tekniske og organisatoriske sikkerhetstiltakene er beskrevet i Bilag 2 og samsvarer med allment aksepterte sikkerhetsstandarder. Behandlingsansvarlig bekrefter at de prosedyrer som er beskrevet i Bilag 2 er tilstrekkelige for å oppnå et adekvat beskyttelsesnivå for Personopplysninger, i samsvar med Personvernregelverket.

6.3 Databehandler skal varsle Behandlingsansvarlig uten unødig opphold etter at Databehandler får kjennskap til et Datasikkerhetsbrudd.

6.4 Varselet nevnt i avsnitt 6.3 skal minst inneholde:

6.4.1 Datasikkerhetsbruddets art, inkludert, om mulig, de kategorier av og et omtrentlig antall av Registrerte som berøres, og kategorier av og et omtrentlig antall av Personopplysninger som berøres;

6.4.2 navnet og kontaktinformasjonen til Personvernombudet eller en annen kontaktperson hvor mer informasjon kan tilveiebringes;

6.4.3 sannsynlige konsekvenser av Datasikkerhetsbruddet; og

6.4.4 tiltakene som er vedtatt eller som er foreslått vedtatt av Databehandler for å takle Datasikkerhetsbruddet, inkludert, hvor det anses hensiktsmessig, tiltak for å dempe dets potensielle negative virkninger.

6.5 Ved Datasikkerhetsbrudd skal Databehandler bistå Behandlingsansvarlig med å oppfylle dennes lovpålagte informasjonsplikter overfor tilsynsmyndighetene og/eller de Registrerte.

6.6 Dersom Databehandler anser at en instruks fra Behandlingsansvarlig for Behandling av Personopplysninger strider mot Personvernregelverket, skal Databehandler umiddelbart informere Behandlingsansvarlig.

7 SUPPLERENDE KONFIDENSIALITETSBESTEMMELSER

7.1 Databehandler skal behandle alle Personopplysninger som den Behandler under Avtalen konfidensielt, og skal treffe alle nødvendige tiltak for å sikre konfidensialitet til Personopplysningene. Databehandlerens personale og andre personer som den engasjerer, og som får tilgang til Personopplysninger, skal også pålegges konfidensialitetsforpliktelser.

7.2 Konfidensialitetsforpliktelsene som det henvises til i dette avsnittet gjelder ikke dersom Behandlingsansvarlig har gitt skriftlig tillatelse til å gi Personopplysningene til en tredjepart, eller dersom det foreligger en lovbestemt plikt til å gi Personopplysningene til en tredjepart.

8 REVISJONER

8.1 Databehandler gir Behandlingsansvarlig mulighet til å kontrollere Databehandlers etterlevelse av disse Databehandlingsvilkårene, eller gir tillatelse til en revisjon utført av uavhengige revisorer, for Behandlingsansvarliges regning, uten å benytte noe av Databehandlers selskapssensitive informasjon og uten å forstyrre Databehandlers drift. Dersom inspeksjonen avdekker at Databehandler ikke etterlever sine forpliktelser under disse Databehandlingsvilkårene skal Databehandler avhjelpe eller rette disse feilene så snart som mulig. I et slikt tilfelle skal Databehandler dekke rimelige og verifiserte kostnader til revisor (betaling utføres kun mot fremvisning av gyldig faktura fra revisorene for slike kostnader).

8.2 Revisjon kan finne sted høyst en gang i året, med mindre det finnes tilstrekkelig bevis til å påvise at Databehandler ikke overholder sine forpliktelser etter disse Databehandlingsvilkårene. Databehandler skal gi Behandlingsansvarlig all informasjon som med rimelighet anses nødvendig for å foreta revisjonen.

8.3 Ved inspeksjon av Myndigheten, skal Databehandler samarbeide i den utstrekning som med rimelighet kreves og informere Behandlingsansvarlig snarest mulig.

8.4 Databehandler skal utpeke en person som kontaktpunkt, som vil bistå Behandlingsansvarlig ved oppfyllelse av informasjonsplikter som oppstår ved Behandling, og Databehandler skal informere Behandlingsansvarlig om kontaktinformasjonen til kontaktpunktet.

9 ENDRINGER

9.1 Dersom endringer i forpliktelsene etter Avtalen kan få vesentlige konsekvenser for Behandlingen av Personopplysninger, vil Databehandler gi Behandlingsansvarlig et varsel om de foreslåtte endringene til disse Databehandlingsvilkårene (slikt varsel kan være på e-post, eller via Unit4 Community). Behandlingsansvarlig må protestere, bare med hensyn til vesentlige endringer, mot de endrede vilkårene innen 7 dager etter mottakelse (av varsel). Dersom Behandlingsansvarlig ikke protesterer, anses Behandlingsanvarlig for å ha akseptert endringene og den oppdaterte versjonen vil gjelde fra angitt ikrafttredelsesdato.

9.2 Databehandler vil til enhver tid kunne foreta endringer til bilagene til disse Databehandlingsvilkårene og disse vil publiseres på Databehandlers nettside. Behandlingsansvarlig vil bli varslet om disse endringene (slikt varsel kan være på e-post, eller via Unit4 Community), hvor versjonsnummer og dato for ikrafttredelse for den oppdaterte versjonen skal angis. Vesentlige endringer til bilagene vil ikke bli foretatt uten at Behandlingsansvarlig gis mulighet til å protestere.

10 GJENSIDIG SKADESLØSHOLDELSE

10.1 Databehandler skal holde Behandlingsansvarlig skadesløs for bøter og/eller straff som Behandlingsansvarlig blir pålagt av eller på vegne av Myndigheten, og for krav som følge av tap eller skade som den Registrerte påføres, om det kan slås fast at disse straffene og/eller bøtene eller kravene er en direkte følge av at Databehandler har Behandlet Personopplysninger i strid med Personvernregelverket eller annen personvernlovgivning.

For å benytte seg av denne skadesløsholdelsesklausulen i punkt 10.1 må Behandlingsansvarlig:

(i) umiddelbart informere Databehandler skriftlig om eksistensen og innholdet i kravet fra den Registrerte eller om enhver etterforskning eller annen instruks som fører til at Myndigheten får til hensikt, eller bestemmer seg for, å ilegge straff eller bot;

(ii) opptre i samråd med Databehandler angående tiltak og kommunikasjon med Myndigheten eller den Registrerte;

(iii) om det finnes grunnlag for å gjøre det, protestere og/eller påklage ilagte bøter; og

(iv) overlate til Databehandler å selvstendig håndtere saken, inkludert forhandlinger. I dette henseende skal Behandlingsansvarlig samarbeide med og gi de nødvendige fullmakter og informasjon, for at Databehandler skal kunne forsvare seg i de rettslige prosessene, om nødvendig i Behandlingsansvarliges navn.

10.2 Behandlingsansvarlig skal holde Databehandler skadesløs for bøter og/eller straff som Databehandler blir pålagt av eller på vegne av Myndigheten, og for krav i forbindelse med tap eller skade som den Registrerte påføres, om det kan slås fast at disse straffene og/eller bøtene eller kravene er en direkte følge av at Behandlingsansvarlig ikke har opptrådt i samsvar med Personvernregelverket eller annen personvernlovgivning.

For å benytte seg av denne skadesløsholdelsesklausulen i punkt 10.2 må Databehandler:

(i) umiddelbart informere Behandlingsansvarlig skriftlig om eksistensen og innholdet i kravet fra den Registrerte eller om enhver etterforskning eller annen instruks som fører til at Myndigheten får til hensikt, eller bestemmer seg for, å ilegge straff eller bot;

(ii) opptre i samråd med Behandlingsansvarlig angående tiltak og kommunikasjon med Myndigheten eller den Registrerte;

(iii) om det finnes grunnlag for å gjøre det, protestere og/eller påklage ilagte bøter; og

(iv) overlate til Behandlingsansvarlig å selvstendig håndtere saken, inkludert forhandlinger. I dette henseende skal Databehandler samarbeide med og gi de nødvendige fullmakter og informasjon, for at Behandlingsansvarlig skal kunne forsvare seg i de rettslige prosessene, om nødvendig i Databehandlers navn.

10.3 Dersom partene er felles ansvarlige (enten ved solidaransvar eller på annen måte) overfor tredjeparter, inkludert de(n) Registrerte, eller blir ilagt en felles bot av Myndigheten, skal Partene forbli ansvarlig overfor hverandre i henhold til punkt 10.1 og 10.2 for en slik del av erstatningsansvaret eller boten/bøtene som er proporsjonal i forhold til graden av skyld i hendelsen som førte til et slikt ansvar. Det skal videre tas hensyn til avgjørelsen til en eventuell domstol eller kompetent nemnd, eller Myndigheten, og i hvilken grad Partens brudd på sine forpliktelser under disse Databehandlingsvilkårene har bidratt til ansvaret.

11 VARIGHET OG OPPHØR

11.1 Disse Databehandlingsvilkårene trer i kraft på Avtalens dato.

11.2 Ved Avtalens opphør skal Databehandler returnere, eller på anmodning fra Behandlingsansvarlig enten desturere eller lagre Personopplysningene, slik som angitt i Bilag 1. Dersom Personopplysningene oppbevares eller lagres i et datasystem eller i et format som ikke med rimelighet kan overrekkes til Behandlingsansvarlig, skal Databehandler umiddelbart destruere Personopplysningene i sine systemer, med mindre Partene på annen måte blir enige skriftlig.

Bilag:

Bilag 1: Beskrivelse av Behandlingen av Personopplysninger

Bilag 2: Sikkerhetstiltak

Bilag 3: Underdatabehandlere

Bilag 4: EUs standard personvernbestemmelser

BILAG 1 – BESKRIVELSE AV BEHANDLINGEN AV PERSONOPPLYSNINGER

1. PERSONLIGE DATA SOM VIL BLI BEHANDLET:

Produkt	Personopplysninger som vil kunne bli behandlet kan omfatte:	Til den dette måtte tilhøre:
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	Ettersom PPS 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	Alle kategorier av personer som er listet opp

Services (“**PPS**”) (generelt) inkludert IDS og Wanda (sammen med eventuelle støttetjenester)	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).	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.

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 disse Databehandlingsvilkårene, inkludert utførelsen av de funksjoner som kreves eller anmodes av Behandlingsansvarlig for at Databehandleren skal oppfylle sine lovbestemte og/eller kontraktsmessige forpliktelser. I sammenheng med, og avhengig av, Produktet eller Tjenesten, vil Behandlingen inkludere følgende:

Produkt	Behandlingens art og formål
Unit4 ERP 7	Personopplysninger blir registrert 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: • 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 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 Unit4 SaaS som nærmere beskrevet i Beskrivelse av tjeneste for Unit4 SaaS eller PPS (som beskrevet i gjeldende Beskrivelse av tjeneste for PPS) Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s ERP 7 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 Financials	Personopplysninger vil registreres i Unit4 Financials 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 av Kunder/Leverandører/Ansatte;
	• Gjennomføring av betalinger;
	• Fakturering;
	• Håndtering av utleggskrav;
	• Reiseforespørsler;
	• Innkjøp og bestillinger;
	• Personal/prosjektplanlegging;
	• HR og lønnsrelaterte prosesser:
	  ○ Lønn;
	  ○ Håndtering av timelister;
	  ○ 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 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 Unit4 SaaS som nærmere beskrevet i Beskrivelse av tjeneste for Unit4 SaaS eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS). Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s Financials 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 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 Unit4 SaaS som nærmere beskrevet i Beskrivelse av tjeneste for Unit4 SaaS eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS) Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s Student Management 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 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 Unit4 SaaS som nærmere beskrevet Beskrivelse av tjeneste for Unit4 SaaS eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS) Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s FP&A 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 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 Unit4 Talent Management SaaS som nærmere beskrevet i Beskrivelse av tjeneste for Unit4 SaaS eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS) Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s Talent Managment 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 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 Unit4 Global SaaS som nærmere beskrevet i Beskrivelse av tjenesten eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS). Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s Assistance PSA Suite 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.
People Platform Services ("**PPS**") (generelt) inkludert IDS og Wanda (sammen med eventuelle støttetjenester)	Personopplysninger vil bli behandlet av PPS 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, Facebook Messenger 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 Unit4 SaaS som nærmere beskrevet i Beskrivelse av tjeneste for Unit4 Global SaaS eller PPS (som beskrevet i gjeldende Beskrivelse for tjeneste for PPS) Tilgang til Personopplysninger for å gi støtte og vedlikehold av Unit4s PPS 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.

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 Beskrivelse av tjeneste for Unit4 SaaS.	<u>Personale</u> Unit4 SaaS driftsteam har personale i Polen, Sverige, Norge, Storbritannia, USA, Canada, Malaysia og Singapore. Dette Databehandler-personale drifter Unit4 SaaS. <u>Verdier og infrastruktur</u> Unit4 anvender infrastrukturtjenester levert fra tredjepart for å tilby Unit4 SaaS og benytter andre programvaresystem for drift og håndtering. Se Bilag 3.
Unit4 Talent Management SaaS	Databehandler skal Behandle Personopplysninger i forbindelse med de aktiviteter som er beskrevet i Avtalen og mer spesifikt i Beskrivelse av tjeneste for	<u>Personale</u> 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

	Unit4 Talent Management SaaS.	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 Bilag 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 Storbritannia, Polen, Portugal, Norge, Tyskland, Sverige, USA, Canda (og øvrige steder som er påkrevet for å støtte Unit4s virksomhetsbehov). Dette Databehadler-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 Bilag 3. Databehandler skal inngå en skriftlig avtale med Underdatabehandler(e), som skal være i overenstemmelse med relevante lover og regler, samt disse Databehandlingsvilkår. Videre har Behandlingsansvarlig gitt Databehandler tillatelse til å engasjere de Underdatabehandler(e) som er angitt i Bilag 3 ved å inngå Avtalen.	Se Bilag 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 Bilag 3 eller det anvendelige Ordreskjema og eventuelle ytterligere bestemmelser som er gitt i øvrige bilag til disse Databehandlingsvilkårene, om påkrevet av Tredjepartsleverandøren eller Gjeldende lover og regler.

People Platform Services ("**PPS**") (generelt) inkludert IDS og Wanda (sammen med eventuelle støttetjenester)	I tillegg til Unit4 SaaS, vil PPS (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
		
		Unit4 SaaS driftsteam, som drifter PPS, har personale i Polen, Sverige, Norge, 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. Dette inkluderer tredjepartsystemer (m.a.o. samarbeidsapplikasjoner), som Unit4 ikke har noen kontroll over. PPS, inkludert Wanda, benytter flere av Microsofts produkter og tjenester, herunder:
		
		• Kognitive tjenester:
		  o LUIS Cognitive Service - *språkforståelse*
		  o Text Translator API – *tekstoversettelse*
		  o 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*
		• 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/.

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 Amazon Web Services (AWS) datasenteret i Frankfurt. All Kundedata, utenom ved deling med utvalgte underdatabehandlere i Bilag 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:</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>
<tr><td>APAC</td><td>Polen, Portugal og Singapore/ Malaysia.</td></tr>
</table></td></tr>
<tr><td>Unit4 Kundestøtte – 24/7 Kundestøtte

(For Kunder som har Utivdet Kundestøtte og Premium Kundestøtte)</td><td colspan="4">Gjennom å benytte en «følg solen»-metodikk kan kundestøtte i Kundesaker skje 24/7 på enhver lokasjon angitt ovenfor.</td></tr>
<tr><td>Unit4 Kundestøtte – Utelukkende EU Kundestøtte</td><td colspan="4">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>People platform services (“PPS”) (generelt) inkludert IDS og Wanda (sammen med</td><td colspan="4">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.
<table>
<tr><th>Tjeneste</th><th>Geo-politisk sone</th><th>Hvor Tjenester Behandler eller lagrer Data</th><th>Primær Kundestøtte gis fra:</th></tr>
<tr><td>Wanda</td><td>Hvilken som helst</td><td>Hovedsakelig innen EU, men kan være andre steder.</td><td>Irland, USA og andre globale kundestøttesenter hvor det er påkrevet.</td></tr>
</table></td></tr>
</table>

støtte-tjenester)	IDS	Beror på hvor skytjenesten tas i bruk	Som ovenfor for Unit4 SaaS	Som ovenfor for Unit4 SaaS
Unit4 Profesjonelle tjenester og Unit4 Customer Success-funksjon	**Emne**	**Profesjonelle tjenester og Customer Success gis fra:**		
	Implementering andre prosjekttjenester	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).		
	Datamigrasjon	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).		
	Feilsøking	I anvendelig lokasjon for Unit4 Kundestøtte og Portugal.		
	Customer Success	I anvendelig lokasjon for Unit4 Kundestøtte og Portugal.		

6. KONTAKTINFORMASJON

For spørsmål eller kommentarer til disse Databehandlingsvilkårene er følgende kontaktpersoner:

Databehandler: Ved brev (addressert til Global Data Privacy 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.

BILAG 2 – SIKKERHETSTILTAK

Som angitt i avsnitt 6 i Databehandlingsvilkårene, er de tekniske og organisatoriske sikkerhetstiltakene listet opp i dette bilaget 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 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. Register over slik returnering av eiendeler er ført i saksbehandlingssystemet (ticketing system).
- 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 (Global Information Security Manager) og global personvernombud (Global Data Privacy 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 er kryptert ved bruk av teknologi som krypterer hele databasen, slik som Transparent Database Encryption. Azure Storage Service Encryption krypterer all data plassert i en kundes lagringskonto.
- 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 som for eksempel bruker Dedicated Accounts og ved å ha separate databaseinstanser for alle våre kunder.

Nettverksisolering på flere punkter:

- Hver dedikerte aktivering (deployment) er isolert fra andre aktiveringer og kommuniserer gjennom private IP-adresser.
- Kunders VMer kan bare kommunisere med andre VMer eid eller kontrollert av same Kunde og med infrastrukturtjenesteendepunkter ment for offentlig kommunikasjon.
- Trafikk mellom VMer går alltid over betrodde pakkefiltre.

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

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. Kunden kan velge å bestille kryptering av inaktive data (data at rest). 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 personlig informasjon 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.

Som et bevis på sikkert design og drift har Unit4 Cloud Services SaaS Ops ISO 27001:2013 sertifisering og ISAE3402 (SOC1) rapport. Unit4 og operatørene av datasentrene har ulike sikkerhetssertifiseringer, vennligst se Beskrivelse av tjeneste for Unit4 SaaS.

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.

Tilleggselementer for Unit4 Talent Management SaaS (sammendrag)

Talent Management SaaS er ISO27001 sertifisert og har gjennomgått en ISO27001 (fase 1 & 2) og GDPR revisjon. Den mest relevante informasjonen fremgår av tabellen, og ekstra dokumentasjon eller informasjon er tilgjengelig på forespørsel.

Domene	Praksis
Håndtering og styring av informasjonssikkerhet	Talent Management SaaS Service har implementert et system for håndtering av informasjonssikkerhet (ISMS) under ISO27001. Dette inneholder, men er ikke begrenset til, retningslinjer for informasjonssikkerhet for alle ansatte. Retningslinjene kan bli fremlagt på forespørsel. I tillegg, for å kunne levere informasjonssikkerhet, er håndteringstiltak implementert for å redusere risikoene. Disse risikoene og sannsynligheten for at de inntreffer er inkludert i ISO27001 ISMS.
Personalsikkerhet	Leveringen av Talent Management SaaS-tjenesten innebærer at all konfidensiell data blir holdt i en HRIS og overholder ISO27001, som informasjonssikkerhetsavdelingen er ansvarlig for.
Håndtering av verdier	Verdier (både digitale and ikke-digitale) forvaltes under retningslinjer for dataklassifisering.
Tilgangskontroll for informasjon	Det er flere retningslinjer som opererer i henhold til prinsippet om minste privilegium, både for leverte applikasjoner, generell informasjon og egen data. Tilgang til egne systemer, driftet med Amazon (AWS), er begrenset til de spesifikt identifiserte individene og bruk av passord er uttrykkelig forbudt. Kun offentlige/private nøkkelpar brukes til å autentifisere med servere. Tilgangsrettighetene per bruker bestemmes i henhold til de etablerte retningslinjene for tilgang. Konkrete spørsmål om tilgang til informasjon og retningslinjer kan bli stilt til informasjonsikkerhet.
Driftssikkerhet	Dette faller inn under omfanget til vår ISMS (ISO27001).
Kommunikasjonssikkerhet	All kommunikasjon er underlagt en retningslinje for dataklassifisering. All nettverkstrafikk kjøres over SSL/HTTPS, den mest vanlige og betrodde kommunikasjonsprotokollen på internett. Intern infrastruktur er isolert ved bruk av strenge brannmurer og lister over nettverkstilgang. Hvert system er tildelt til en gruppe for brannmursikkerhet etter sin funksjon. Som standardinnstilling nektes all tilgang og kun eksplisitt godtatte porter er eksponert. Persistens- og lagringslag er krypterte (også inaktive) og sikret bak VPN & VPC brannmurer. Kontorer bruker et nettverk som er beskyttet av en redundant Fortinet 200D brannmur, plassert i datasenteret i Merelbeke, tilkoblet Ghelamco Arenaen via mørk fiber. Mer informasjon om denne tilkoblingen er gitt i dokumentet "Continuity and Security measures", som også er del av ISMS av ISO27001 sertifiseringen.

BILAG 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 Bilag 2, punkt 5.	Leverer skyinfrastruktur og -tjenester.
	Microsoft Dynamics	Som angitt over i Bilag 2, punkt 5.	Leverer programvaretjenester, særlig Microsoft Dynamics (inkludert noe skyinfrastruktur).
	Microsoft	Som angitt over i Bilag 2, punkt 5.	Leverer programmeringsverktøy (software tooling) og Office
	Conapto	Som angitt over i Bilag 2, punkt 5.	Leverer skyinfrastruktur og -tjenester.
Unit4 SaaS – Talent Management	Amazon Web Services	Frankfurt, Tyskland	Leverer løsning - Suite
	Freshdesk	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	LogDNA	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Mandrill	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Mixpanel	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Pingdom	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Productboard	EU og USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Leverer løsning - Learn (kun SCORM) (privacy shield link: Link)
	Sentry	USA (Privacy Policy)	Leverer løsning – Suite (privacy shield link: Link)
	Slack	USA (Privacy Policy)	Leverer løsning – Perform (privacy shield link: Link)
	Stripe	Land som Stripe opererer i (Privacy Policy)	Leverer løsning – Learn (privacy shield link: Link)
	Wistia	USA (Privacy Policy)	Leverer løsning – Learn (privacy shield link: Link)
People Platform Services ("**PPS**") (generelt) inkludert IDS og Wanda (sammen med eventuelle støttetjenester)	Microsoft Azure	Som angitt i Bilag 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 2.

BILAG 4 – EUS STANDARD PERSONVERNBESTEMMELSER

This table contains the information that is required to be inserted into the EU Standard Contractual Clauses that are set out below this table:

Parties	The data exporter is the Controller whose details appear in an Order Form (as Customer) in the Agreement between Controller and Processor. The data importer is the Processor whose details appear in an Order Form (as Unit4) in the Agreement between Controller and Processor.
Clause 9 and 11(3)	The data exporter is based in the Territory specified in the Agreement.
Appendix 1	The information required to complete this Appendix is set out in Schedule 1 and Schedule 3 of these Data Processing Terms
Appendix 2	The information required to complete this Appendix is set out in Schedule 2 of these Data Processing Terms

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Parties

Name of the data exporting organisation: …

Address: …

Tel. …; fax …; e-mail: …

Other information needed to identify the organisation

…

(the data **exporter**)

And

Name of the data importing organisation: …

Address: …

Tel. …; fax …; e-mail: …

Other information needed to identify the organisation:

…

(the data **importer**)

each a 'party'; together 'the parties',

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer ([2])

The data importer agrees and warrants:

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

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

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

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

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

ii. any accidental or unauthorised access; and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

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

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

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

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

Clause 12

Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that

case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

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

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

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

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

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

See Schedule 1 of the Data Processing Terms (above).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

See Schedule 1 of the Data Processing Terms (above).

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

See Schedule 1 of the Data Processing Terms (above).

Categories of data

The personal data transferred concern the following categories of data (please specify):

See Schedule 1 of the Data Processing Terms (above).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

See Schedule 1 of the Data Processing Terms (above).

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

See Schedule 1 of the Data Processing Terms (above).

Appendix 2

to the Standard Contractual Clauses

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

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