

# DATABEHANDLERAVTALE

## Standardavtalevilkår

i henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (personvernforordningen) med henblikk på databehandlerens behandling av personopplysninger

mellom

[NAVN]

Org.nr. [ORGANISASJONSNUMMER]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

heretter «den behandlingsansvarlige»

og

Adminkit AS

Org.nr. 924 690 496

Rådhusgata 15

3211 Sandefjord

Norge

heretter «databehandleren»

som hver for seg er en «part» og sammen utgjør «partene»

HAR AVTALT følgende standardavtalevilkår (Vilkårene) med henblikk på å overholde personvernforordningen og sikre beskyttelse av fysiske personers grunnleggende rettigheter og friheter

**1. Innhold**

2. Innledning .....	3
3. Den behandlingsansvarliges rettigheter og plikter .....	3
4. Databehandleren handler etter instruks .....	4
5. Konfidensialitet .....	4
6. Sikkerhet ved behandlingen .....	4
7. Bruk av underdatabehandlere .....	5
8. Overføring til tredjeland eller internasjonale organisasjoner .....	6
9. Bistand til den behandlingsansvarlige .....	7
10. Underretning om brudd på personopplysningssikkerheten .....	8
11. Sletting og returnering av opplysninger .....	8
12. Revisjon, herunder inspeksjon .....	8
13. Partenes avtale om andre forhold .....	9
14. Ikrafttredelse og opphør .....	9
15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren .....	10
Vedlegg A Opplysninger om behandlingen .....	11
Vedlegg B Underdatabehandlere .....	12
Vedlegg C Instruks for behandling av personopplysninger .....	13
Vedlegg D Partenes regulering av andre forhold .....	<b>Feil! Bokmerke er ikke definert.</b>

1. Disse Vilklårene fastsetter den behandlingsansvarlige og databehandlerens rettigheter og plikter når databehandleren utfører behandling av personopplysninger på vegne av den behandlingsansvarlige.
2. Disse Vilklårene er utformet med for å sikre partenes etterlevelse av artikkel 28 nummer 3 i Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen).
3. I forbindelse med leveringingen av Adminkit-tjenesten behandler databehandleren personopplysninger på vegne av den behandlingsansvarlige i overensstemmelse med disse Vilklårene.
4. Vilklårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.
5. Det er fire vedlegg til disse Vilklårene, og vedleggene utgjør en integrert del av Vilklårene.
6. Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder om behandlingens formål og art, typen av personopplysninger, kategoriene av registrerte og behandlingens varighet.
7. Vedlegg B inneholder den behandlingsansvarliges betingelser for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som den behandlingsansvarlige har godkjent.
8. Vedlegg C inneholder den behandlingsansvarliges instruks når det gjelder databehandlerens behandling av personopplysninger, en beskrivelse av de sikkerhetstiltakene som databehandleren som minimum skal gjennomføre, og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal utføres.
9. Vedlegg D inneholder bestemmelser om andre aktiviteter som ikke er omfattet av Vilklårene.
10. Vilklårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.
11. Disse Vilklårene fritar ikke databehandleren fra plikter som databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

## 3. Den behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernforordningen (se personvernfor-

ordningen artikkel 24), gjeldende personopplysningsvern-bestemmelser i unionsretten eller medlemsstatenes<sup>1</sup> nasjonale rett og disse Vilklårene.

Side 4 av 15

2. Den behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
3. Den behandlingsansvarlige er ansvarlig for, blant annet, å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om å gjøre.

#### **4. Databehandleren handler etter instruks**

1. Databehandleren skal bare behandle personopplysninger etter dokumenterte instruks fra den behandlingsansvarlige, med mindre noe annet kreves av unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Disse instruksene skal være spesifisert i vedlegg A og C. Etterfølgende instruks kan også gis av den behandlingsansvarlige mens det skjer behandling av personopplysninger, men instruksene skal alltid være dokumenterte og oppbevares skriftlig, herunder elektronisk, sammen med disse Vilklårene.
2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige, etter databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsvern-bestemmelser i unionsretten eller medlemsstatenes nasjonale rett.

#### **5. Konfidensialitet**

1. Databehandleren kan bare gi tilgang til personopplysninger som behandles på den behandlingsansvarliges vegne til personer underlagt databehandlerens instruksjonsmyndighet som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i det nødvendige omfang. Listen av personer som har fått tilgang skal gjennomgås fortløpende. På bakgrunn av en slik gjennomgang kan tilgangen til personopplysninger stenges, dersom den ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelig for disse personene.
2. Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de aktuelle personene underlagt databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

#### **6. Sikkerhet ved behandlingen**

1. Personvernforordningen artikkel 32 fastslår at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

---

<sup>1</sup> Henvisninger til «medlemsstater» i disse Vilklårene skal forstås som en henvisning til stater som er del av det europeiske økonomiske samarbeidsområdet (EØS-stater).

Den behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av relevans omfatter tiltakene:

Side 5 av 15

- a. Evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, gjennom arkitektur i programvaren, fokus på konfidensialitet, testing og bruk av velutprøvde teknologier og systemer.
  - b. Evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse, gjennom back-up og redundans av produksjonssystemer.
  - c. En prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er, gjennom pliktig sikkerhetstrening for it-ansatte, tilgangskontroll, passordskifte rutiner, samt jevnlig sikkerhetstesting av systemene, både applikasjon og infrastruktur og eventuell utbedring/forbedring.
2. Ifølge personvernforordningen artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå risikoene. Med henblikk på denne vurderingen skal den behandlingsansvarlige stille den nødvendige informasjonen til rådighet for databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.
  3. Databehandleren skal også bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges plikter etter personvernforordningen artikkel 32, ved blant annet å stille til den behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sine plikter etter personvernforordningen artikkel 32.

Hvis imøtegåelse av de identifiserte risikoene – etter den behandlingsansvarliges vurdering – krever at det gjennomføres ytterligere tiltak enn det databehandleren allerede har gjennomført, skal den behandlingsansvarlige angi disse tiltakene i vedlegg C.

## **7. Bruk av underdatabehandlere**

1. Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 nummer 2 og nummer 4 for å gjøre bruk av en annen databehandler (en underdatabehandler).
2. Dersom vi finner det nødvendig å endre underleverandører vil dette fremkomme i vår personvernerklæring på denne databehandleravtalen som igjen er linket inn i tjenesteavtalen.  
Dersom du har en spesifikk underleverandør hvor et bytte vil få større betydning for deg som vår kunde vil du få en skriftlig redegjørelse for dette og retten til å påvirke dette byttet.

3. Databehandleren har den behandlingsansvarliges generelle godkjenning til å benytte underdatabehandlere. Listen over underdatabehandlere som den behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.
4. Når databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal underleverandøren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilklårene, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning.

Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som minimum overholder databehandlerens forpliktelser etter disse Vilklårene og personvernforordningen.

5. En kopi av slik underdatabehandleravtale og eventuelle etterfølgende endringer skal – ved den behandlingsansvarliges anmodning – sendes til den behandlingsansvarlige, som på denne måten har mulighet for å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilklårene. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den behandlingsansvarlige.
6. Databehandleren skal i underdatabehandleravtalen inkludere den behandlingsansvarlige som begunstiget tredjepart i tilfelle databehandleren går konkurs, slik at den behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakeføre personopplysningene.
7. Hvis databehandleren ikke oppfyller sine personopplysningsvernforpliktelser blir databehandleren fullt ut ansvarlig overfor den behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen – særlig de nedfestet i personvernforordningen artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

## **8. Overføring til tredjeland eller internasjonale organisasjoner**

1. Adminkit vil benytte seg av leverandører utenfor EU, her også USA. Dette er nødvendig for å kunne levere tjenesten. Vi vil i disse tilfellene benytte oss hovedsakelig av land med advekansbeslutninger og/eller selskaper som kan fremvise en SCC. Gjennom godkjenning av denne avtalen godkjenner du også at Adminkit er autorisert til å sørge for gyldig rettslig grunnlag for overføringen av personopplysninger utenfor EU på vegne av deg som behandlingsansvarlig. Har du innvendinger eller spørsmål til dette kontakt [tbk@adminkit.no](mailto:tbk@adminkit.no)
2. Den behandlingsansvarliges instruks når det gjelder overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningen kapittel V som overføringen er basert på, skal angis i vedlegg C.6.

1. Databehandleren bistår, idet det tas hensyn til behandlingens art og i den grad det er mulig, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommende sin plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

Dette innebærer at databehandleren så langt det er mulig skal bistå den behandlingsansvarlige i den behandlingsansvarlige oppfyllelse av:

- a. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
  - b. opplysningsplikten dersom personopplysninger ikke er blitt samlet inn fra den registrerte
  - c. den registrertes rett til innsyn
  - d. retten til retting
  - e. retten til sletting («retten til å bli glemt»)
  - f. retten til begrensning av behandling
  - g. underretningsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
  - h. retten til dataportabilitet
  - i. retten til å protestere
  - j. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering
2. I tillegg til databehandlerens forpliktelse til å bistå den behandlingsansvarlige i henhold til Vilkårene 6.3., bistår databehandleren også, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, den behandlingsansvarlige med:
    - a. den behandlingsansvarliges forpliktelse ved brudd på personopplysningssikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningssikkerheten til den kompetente tilsynsmyndigheten, det norske datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter
    - b. den behandlingsansvarliges forpliktelse til uten ugrunnet opphold å underrette den registrerte om bruddet på personopplysningssikkerheten når det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter
    - c. den behandlingsansvarliges forpliktelse til før behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (vurdering av personvernkonsekvenser)
    - d. den behandlingsansvarliges forpliktelse til å rådføre seg med den kompetente tilsynsmyndigheten, det norske datatilsynet, før behandlingen dersom en vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

- Partene skal i vedlegg C oppgi de egnede tekniske og organisatoriske tiltakene gjennom hvilke databehandleren skal bistå den behandlingsansvarlige, samt omfanget og utstrekningen av den påkrevde bistanden. Dette gjelder for forpliktelsene som følger av Vilkårene 9.1. og 9.2.

## 10. Underretning om brudd på personopplysningssikkerheten

- Ved brudd på personopplysningssikkerheten skal databehandleren underrette den behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.
- Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje innen 72 timer etter at databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, slik at den behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.
- I overensstemmelse med Vilkår 9 nummer 2 bokstav a skal databehandleren bistå den behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Det innebærer at databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 nummer 3 skal fremgå av den behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndigheten:
  - arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt
  - de sannsynlige konsekvenser av bruddet på personopplysningssikkerheten
  - de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.
- Partene skal i vedlegg C oppgi all informasjon som databehandleren skal fremskaffe når vedkommende bistår den behandlingsansvarlige med å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

## 11. Sletting og returnering av opplysninger

Ved opphør av databehandlertjenestene skal databehandleren slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige innen rimelig tid med mindre unionsretten eller medlemsstatenes nasjonale rett krever oppbevaring av personopplysningene.

## 12. Revisjon, herunder inspeksjon



1. Databehandleren skal stille til den behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og disse Vilklårene. Videre skal databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor som er bemyndiget av den behandlingsansvarlige.
2. Prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av databehandleren og underdatabehandlere er spesifisert i vedlegg C.7 og C.8.
3. Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens lokaler, eller representanter som opptrer på slike tilsynsmyndigheters vegne, adgang til databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

### 13. Partenes avtale om andre forhold

1. Partene kan avtale andre bestemmelser som gjelder databehandlertjenestene, f.eks. erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot disse Vilklårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

### 14. Ikrafttredelse og opphør

1. Vilklårene trer i kraft på datoen for begge partenes godkjenning/aksept av avtalen.
2. Begge partene kan kreve Vilklårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilklårene gir grunn til dette.
3. Vilklårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilklårene ikke sies opp, med mindre partene avtaler andre vilkår som regulerer levering av databehandlertjenestene.
4. Hvis leveringen av databehandlertjenestene opphører, og personopplysningene er slettet eller returnert til den behandlingsansvarlige i overensstemmelse med Vilklårene 11.1 og vedlegg C.4, kan Vilklårene sies opp med skriftlig varsel av begge partene.
5. Underskrift

På vegne av den behandlingsansvarlige

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-postadresse	[E-POST]
Dato	[DATO]
Underskrift	_____

På vegne av databehandleren

Navn	Pål R. Bredvei
------	----------------

Stilling CEO  
Telefonnummer +47 911 02 868  
E-postadresse pal.bredvei@adminkit.no  
Dato  
Underskrift \_\_\_\_\_

## 15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren

1. Partene kan kontakte hverandre via nedenstående kontaktpersoner.
2. Partene forplikter seg til å orientere hverandre løpende om endringer som gjelder kontaktpersoner.

### Behandlingsansvarlige

Navn [NAVN]  
Stilling [STILLING]  
Telefonnummer [TELEFONNUMMER]  
E-postadresse [E-MAIL]

### Databehandleren

Navn Morten Høyseth  
Stilling CTO  
Telefonnummer +47 924 92 017  
E-postadresse morten.hoyseth@adminkit.no

### A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

Ha oversikt og relevant informasjon om tidligere/kommende/eksisterende ansatte. Herunder vil tjenesten gjennom side moduler kunne lagre informasjon om eksempelvis disse områdene:

- Personalregister – personalia om ansatte, tilgangskontroll, meldingsarkiv og organisasjonsoversikt.
- Dokumentarkiv felles for de ansatte/bedriften og på personalkort. Herunder også dokumenter, som advarsler, oppsigelser, kompetanser og lignende relevant for arbeidsforholdet.
- Digital signering av dokumenter – for eksempel arbeidsavtaler.
- Ferie registrering og oversikt, samt fravær av ulike årsaker.
- Kompetanse – Informasjon om ansattes kompetanse.
- Visning av bursdagsdatoer og jubileum for ansatte.
- Tilby informasjon og handlinger rund relevante tjenester knyttet til arbeidsplassen (i hovedsak til bedriftsleder)
- Prosesser i bedriften – for eksempel on/off boarding.
- Arbeidsavtaler – Informasjon knyttet til arbeidsavtaler i bedriften.
- Prosess og hjelp rundt håndtering av medarbeidersamtaler og utviklingssamtaler
- Varslingstjenester til de ansatte

### A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal primært dreie seg om (behandlingens art):

Oppbevare og kunne oppdatere informasjon om de ansatte, som er relevant for den ansatte og ansettelsesforholdet eller et kommende/tidligere ansettelsesforhold.

### A.3. Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

Navn, e-postadresse, telefonnummer, adresse, fødselsnummer, lønn, kontonummer for lønn, pårørende, allergier, t-skjortestørrelse, førerkort, IP adresse. Utover dette brukernavn og passord til databehandlerens tjeneste, og avtaler og notater knyttet til arbeidsforholdet, herunder informasjon om start/slutt-dato, stilling, avdeling og arbeidssted.

### A.4. Behandlingen omfatter følgende kategorier av registrerte personopplysninger:

- Kontaktinformasjon
- Identifikasjon og autorisering

### A.5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan begynne etter at Vilåårene har trådt i kraft. Behandlingen har følgende varighet:

Behandlingen varer inntil behandlingsansvarlig avslutter avtalen.

**B.1. Godkjente underdatabehandlere**

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

NAVN	ORG. NR. ELLER NETTSIDE	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
Dataverse	EL998682224	Ethnikis Antistasis 131, 55134, Kalamaria, Thessaloniki, GREECE	Utvikling av programvare, it drift og relatert.
Komveo IT	UK 9807550	Humat House, 160 London Road Barking UNITED KINGDOM, IG11 8BB	Utvikling av programvare, it drift og relatert.
Auth0	Se <a href="http://www.auth0.com">www.auth0.com</a>	Auth0, Inc. 10800 NE 8th Street, Suite 600 Bellevue, WA 98004, U.S.A.	Håndterer autentisering av brukere ved innlogging
Scrive	Se <a href="http://www.scrive.com">www.scrive.com</a>	Grev Turegatan 11A 114 46 Stockholm, Sverige	Håndterer digital signering av dokumenter
Microsoft Data center Azure	<a href="http://www.microsoft.com">www.microsoft.com</a>	North Europe (p.t.Leopardstown, Dublin, Ireland)	Hosting/skytjenste
SendGrid Inc.	<a href="http://www.sendgrid.com">www.sendgrid.com</a>	Twilio Inc 375 Beale Street, Suite 300, San Francisco, CA 94105 U.S.A.	E-post utsending
Fenerum ApS	DK-40430989	Viby Ringvej 11, 1 8260 Viby J Denmark	Fakturering
Hubspot	<a href="http://www.hubspot.com">www.hubspot.com</a>	Sir John Rogerson's Quay, Dublin	Kunderegistrering
Slack	<a href="http://www.slack.com">www.slack.com</a>	500 Howard Street San Francisco	Kommunikasjon og integrasjon

Ved Vilkårenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. Alle endringer

## **Vedlegg C Instruks for behandling av personopplysninger**

### **C.1. Behandlingens gjenstand/instruks for behandlingen**

Behandlingen omfatter primært personopplysninger knyttet til den ansatte og som er nødvendig for ansettelsesforholdet.

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

- Lagrer/viser frem/tillater redigering av informasjon som behandlingsansvarlig legger inn om de ansatte i bedriften.
- Lagrer filer som behandlingsansvarlige legger inn
- Lagrer informasjon relatert til pålogging

### **C.2. Informasjonssikkerhet**

Behandlingen omfatter personopplysninger knyttet til den ansatte og som er nødvendig for ansettelsesforholdet. Databehandler fokuserer på sikkerhet i applikasjon og behandling av informasjon.

Databehandleren har heretter rett og plikt til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige (og avtalte) sikkerhetsnivået.

Databehandleren skal likevel – under enhver omstendighet og som minimum – gjennomføre følgende tiltak, som er avtalt med den behandlingsansvarlige:

- Personopplysninger skal ikke eksistere på annet enn databehandlerens produksjonssystem og back-up av dette, f.eks. skal ikke kunde/personopplysninger eksistere på testsystemer eller lignende.
- Det er ikke mulig for databehandler å logge seg inn på kundens konto, for slik å se personopplysninger, uten samtykke fra kunde.
- Det er kun en navngitt liste med personer hos databehandler, som har tilgang til produksjonsdatabasen.
- Testing av systemet gjennomføres av databehandler hver 1-2 uke.
- Sikkerhet er en del av utviklingssyklusen hos databehandler; de ansatte på IT gjennomgår årlig pliktig kursing i datasikkerhet og trusselbilder.
- Det gjennomføres jevnlig sikkerhetstesting av applikasjonen av ekstern part, og eventuelle funn blir prioritert og utbedret. Ekstern part har/får ikke tilgang til kunde/personopplysninger.
- Tilgang/autorisasjon til programvaren databehandler stiller til rådighet, styres gjennom tredjepart (se vedlegg B) for å sikre gode, robuste autoriseringsmekanismer.
- Informasjonen som overføres bruker transportkryptering, SSL/TLS.
- Det benyttes datasenter i Europa, drevet av Microsoft, med den strenge tilgangskontrollen dette datasenteret har.

- Lokasjoner hvor de ansatte hos databehandler har kontor seg, er fysisk tilgangsbegrenset med lås/adgangskontroll. Personopplysninger oppbevares ikke på ansattes maskiner eller lignende, disse eksisterer kun i datasenteret. Tilgang til passord for å logge seg inn i produksjonsdatabasen, er kun tilgjengelig for en kort, navngitt liste med personer. Passord lagres ikke lokalt på maskiner eller enheter.
- Databehandler loggfører endringer gjort på brukere/personopplysninger.

### **C.3 Bistand til den behandlingsansvarlige**

Databehandleren skal i den grad det er mulig – i det nedenfor beskrevne omfang og utstrekning – bistå den behandlingsansvarlige i samsvar med Vilklårene 9.1 og 9.2 ved å gjennomføre følgende tekniske og organisatoriske tiltak:

Databehandler gir behandlingsansvarlig informasjon om hvilken informasjon som lagres, og kan innenfor rimelighetens grenser utdype lagringsform, sted og f.eks. sletting ved opphør. Dette gjøres ved at rett kompetanse hos databehandler, svarer – i muntlig eller skriftlig form – på spørsmål fra behandlingsansvarlig, og eventuelt fremlegger dokumentasjon der det er relevant og tilgjengelig.

### **C.4 Oppbevaringsperiode/sletteprosedyrer**

Informasjonen oppbevares så lenge behandlingsansvarlig er bruker, eventuelt til behandlingsansvarlig gir beskjed om at personinformasjon skal slettes.

Ved avtaleoppheør slettes personinformasjon automatisk innen rimelig tid. Skulle den enkelte bruker hos behandlingsansvarlig, ønske å beholde sine personopplysninger etter avtaleoppheør med behandlingsansvarlig, kan dette lagres videre uavhengig av avtalen med behandlingsansvarlig, gitt den enkelte brukers ønske og samtykke.

### **C.5 Lokasjon for behandling**

Behandling av personopplysninger som omfattes av Vilklårene kan ikke, uten den behandlingsansvarliges skriftlige forhåndsgodkjenning, finne sted på andre lokasjoner enn følgende:

- Microsoft sitt driftssenter/datasenter innenfor Europa. P.t. er den fysiske lokasjonen «North Europe», som er lokalisert i Irland. Se vedlegg B.

### **C.6 Instruks for overføring av personopplysninger til tredjeland**

Personopplysninger overføres ikke til tredjeland utover det som er beskrevet i vedlegg B, og med de plikter og føringer som gjelder for endringer i vedlegg B.

Hvis ikke den behandlingsansvarlige i Vilklårene eller etterfølgende gir en dokumentert instruks som gjelder overføring av personopplysninger til et tredjeland eller internasjonal organisasjon, kan ikke databehandleren, innen rammene av Vilklårene, gjennomføre slike overføringer.

## **C.7 Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren**

Databehandleren kan årlig for den behandlingsansvarliges regning innhente en revisjonsrapport eller inspeksjonsrapport fra en uavhengig tredjepart som gjelder databehandlerens overholdelse av personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene. Dette kun etter gjensidig avtale mellom - og samtykke fra – både behandlingsansvarlig og databehandler.

Partene er enig om at følgende typer av rapport kan benyttes i samsvar med Vilklårene:

- Gjennomføres kun etter gjensidig avtale mellom - og samtykke fra – både behandlingsansvarlig og databehandler.
- Etter en realistisk tidsplan databehandler og behandlingsansvarlig er enige om
- Innholdet i rapporten er strengt hemmelig og skal kun deles mellom behandlingsansvarlig og databehandler.

Rapporten oversendes uten ugrunnet opphold til den behandlingsansvarlige til orientering. Den behandlingsansvarlige kan bestride omfanget av og/eller metoden i rapporten og kan i slike tilfeller kreve en ny med annet omfang og/eller med en annen metode. Dette etter samme kriterier som (punktliste over) ved utarbeidelse av en rapport.

Basert på resultatene av kan den behandlingsansvarlige kreve at det gjennomføres ytterligere tiltak for å sikre at personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene blir overholdt, innen rimelig tid.

Den behandlingsansvarlige eller den behandlingsansvarliges representant skal dessuten ha adgang til å inspisere, herunder inspisere fysisk, stedene hvor databehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen. Slike inspeksjoner kan gjennomføres på et tidspunkt hvor databehandler og behandlingsansvarlige er enige om. Inspeksjon foretas kun hvis nødvendig og relevant.

Den behandlingsansvarliges eventuelle utgifter i forbindelse med fysisk inspeksjon dekkes av en behandlingsansvarlige selv. Databehandleren skal likevel avsette de ressurser tid som er nødvendig for at den behandlingsansvarlige skal kunne gjennomføre sin inspeksjon.