1 Innhold

Contents

1 Innhold 1
2 Innledning 1
3 Den behandlingsansvarliges rettigheter og plikter 2
4 Databehandleren handler etter instrukser 3
5 Konfidensialitet 3
6 Sikkerhet ved behandlingen 3
7 Bruk av underdatabehandlere 4
8 Overføring til tredjeland eller internasjonale organisasjoner 5
9 Bistand til den behandlingsansvarlige 6
10 Underretning om brudd på personopplysningssikkerheten 7
11 Sletting og returnering av opplysninger 8
12 Revisjon, herunder inspeksjon 8
13 Partenes avtale om andre forhold 8
14 Ikrafttredelse og opphør 8
15 Kontaktpersoner hos den behandlingsansvarlige og databehandleren 9
16 Vedlegg A Opplysninger om behandlingen 11
17 Vedlegg B Underdatabehandlere 12
18 Vedlegg C Instruks for behandling av personopplysninger 13

2 Innledning

1. Disse Vilkårene fastsetter den behandlingsansvarlige og databehandlerens rettig-heter og plikter når databehandleren utfører behandling av personopplysninger på vegne av den behandlingsansvarlige.

2. Disse Vilkårene er utformet 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 leveringen av Culture Intelligence sine tjenester behandler data-behandleren personopplysninger på vegne av den behandlingsansvarlige i overensstemmelse med disse Vilkårene.

4. Vilkårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avta-ler mellom partene.

5. Det er fire vedlegg til disse Vilkårene, og vedleggene utgjør en integrert del av Vil-kårene.

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 databehandle-rens 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 Vilkårene.

10. Vilkårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.

11. Disse Vilkårene fritar ikke databehandleren fra plikter som databehandleren er på-lagt 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 personvernforordningen artikkel

24), gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes[1] nasjonale rett og disse Vilkårene.

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 instrukser

1. Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser 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 instrukser 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 Vilkårene.

2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige, etter databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsvernbestemmelser 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

[1] Henvisninger til «medlemsstater» i disse Vilkårene skal forstås som en henvisning til stater som er del av det europeiske økonomiske samarbeidsområdet (EØS-stater).

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.

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 kan tiltakene omfatte:

a. pseudonymisering og kryptering av personopplysninger

b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene

c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse

d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

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. Databehandleren må således ikke bruke en underdatabehandler for å oppfylle Vilkårene uten på forhånd å ha innhentet en generell skriftlig godkjennelse fra den behandlingsansvarlige.

3. Databehandleren har den behandlingsansvarliges generelle godkjennelse til å benytte underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige

om eventuelle planlagte endringer som gjelder tilføyelse eller utskiftning av underdatabehandlere med minst 1 måned varsel og dermed gi den behandlingsansvarlige mulighet til å motsette seg slike endringer før den eller de beskrevne underdatabehandler(e) engasjeres. Lengre varslingsfrister for spesifikke underdatabehandlertjenester kan angis i vedlegg B. 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 Vilkårene, 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 Vilkårene 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 Vilkårene. 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. Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den behandlingsansvarlige, og slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.

2. Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren

er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumentert instruks fra den behandlingsansvarlige kan databehandleren innenfor rammene av disse Vilkårene således ikke:

    a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon
    b. overlate behandling av personopplysninger til en underdatabehandler i et tredjeland
    c. behandle personopplysningene i et tredjeland

4. 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.
5. Disse Vilkårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 nummer 2 bokstav c og d, og disse Vilkårene kan ikke utgjøre et grunnlag for overføring av personopplysninger under personvernforordningen kapittel V.

9 Bistand til den behandlingsansvarlige

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 vedkommendes 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, 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, 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

1. Ved brudd på personopplysningssikkerheten skal databehandleren underrette den behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.

2. Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje innen 8 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.

3. 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:

    a. 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

    b. de sannsynlige konsekvenser av bruddet på personopplysningssikkerheten

c. 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.

4. 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

1. Ved opphør av databehandlertjenestene skal databehandleren slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet, 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 Vilkårene. 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 Vilkårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

14 Ikrafttredelse og opphør

1. Vilkårene trer i kraft på datoen for begge partenes underskrift.

2. Begge partene kan kreve Vilkårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilkårene gir grunn til dette.

3. Vilkårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilkårene 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 Vilkårene 11.1 og vedlegg C.4, kan Vilkårene sies opp med skriftlig varsel av begge partene.

5. Underskrift

   På vegne av den behandlingsansvarlige

   Underskrevet på webskjema

   På vegne av databehandleren

   Navn Øyvind Tveit

   Stilling CTO, Culture Intelligence

   Telefonnummer +47 90733048

   E-postadresse oyvind@cultureintelligence.io

   Dato [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.

Ref webskjema

Navn Øyvind Tveit

Stilling CTO, Culture Intelligence

Telefonnummer +47 90733048

E-postadresse oyvind@cultureintelligence.io

16 Vedlegg A Opplysninger om behandlingen

Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

Formålet med behandlingen er å kunne tilby analyser og konsulenttjenester tilknyttet den behandlingsansvarliges eller behandlingsansvarliges kunders organisasjonskultur.

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

Typen personopplysninger som behandles er personopplysninger om bedriftstilknytning og kontaktinformasjon, samt personens egne verdiprioriteringer basert på Culture Intelligence sitt elektroniske spørreskjema.

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

Navn, e-post, organisasjonstilknytning samt verdiprioriteringer som er et resultat av utfylt spørreskjema.

A.4. Behandlingen omfatter følgende kategorier av registrerte:

Ikke relevant.

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

Avtalen gjelder så lenge databehandler behandler eller har tilgang til personopplysninger på vegne av behandlingsansvarlig. Den behandlingsansvarlige kan pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

17 Vedlegg B Underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
Microsoft			Office 365 som inkluderer epost og dokumenter
Microsoft Azure med datasentre i EU/EEA	N/A	Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA	Azure er driftstjenestene til Microsoft hvor databehandlerens digitale tjenester driftes. Platform as a service (PaaS). Skyleverandør for webtjenester, operativsystemer, nettverk, lagring og fysisk drift. Dataintegritet i skyen på sitt beste | Microsoft Klareringssenter
Intercom			(SaaS og PaaS) Meldingstjeneste som benyttes i databehandlerens digitale tjeneste. Intercom og GDPR.

Ved Vilkårenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. Databehandleren kan ikke – uten den behandlingsansvarliges eksplisitte skriftlige godkjennelse – benytte en underdatabehandler til en annen behandlingsaktivitet enn den som er avtalt for vedkommende eller bruke en annen underdatabehandler til den beskrevne behandlingsaktiviteten.

B.2. Varsel for godkjennelse av underdatabehandlere

1 måned.

18 Vedlegg C Instruks for behandling av personopplysninger

C.1. Behandlingens gjenstand/instruks for behandlingen

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

Gjennomføre analyse av organisasjonskultur. Dette gjøres ved at databehandleren sender ut et elektronisk spørreskjema til hver enkelt deltager, som er definert av behandlingsansvarlig. Resultatene fra undersøkelsen blir gjort tilgjengelig for behandlingsansvarlig.

Culture Intelligence kan benytte aggregerte, anonymiserte data til å forbedre sine tjenester.

C.2. Informasjonssikkerhet

Sikkerhetsnivået skal gjenspeile:

Behandlingen omfatter personopplysninger, men de er ikke omfattet av personvernforordningen artikkel 9 om 'særlige kategorier av personopplysninger'. De personlige dataene som lagres er som beskrevet i A2. Derfor skal det etableres et 'middels' sikkerhetsnivå.

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:

Personnavn, epost adresse og tilhørende verdiprioriteringer er pseudonymisert i løsningen. Det kreves særskilt autorisasjon for å kunne identifisere en person. Software utviklere og andre tredjeparter skal ikke kunne koble en person til dennes verdiprioriteringer.

Konfidensialitet over tid er sikret slik det er beskrevet over. Ved opphør av tjenesten vil data bli slettet – ref seksjon 11. Det er databehandlers intensjon at data skal være tilgjengelig for

databehandlingsavsvarlig så lenge tjenesten vedvarer. Konfidensialitet, integritet, tilgjengelighet og robusthet er sikret ved bruk av beste praksis design, konfigurasjon og utviklingsmetoder. Systemene kjører utelukkende på plattformer som er anerkjent som en av industriens beste når det gjeldet sikkerhet (Microsoft Azure).

Det gjøres back-up av data som kan gjenopprettes om data skulle være fjernet eller slettet uten den hensikt. Løsningen kjøres i Microsoft Azure og backup er håndtert gjennom Azure SQL Database.

Databehandleren jobber mot en ISO27001 sertifisering og gjør jevnlig evaluering og justering av sikkerhetstiltak.

All kommunikasjon mellom nettleser og web applikasjon er kryptert (https). Tilgang til løsningen er beskyttet med brukernavn og passord. Alle endepunkter (APIer) i Azure har begrenset tilgang for å sikre at ikke uautentiserte tjenester får tilgang (infrastructure hardening).

Kryptert overføring mellom klient og server. I den grad behandlingsansvarlig skal oversende lister av persondata til databehandler (for eksempel Excel ark) så skal det gjøres via sikrede tjenester.

Opplysninger er sikret med brukerautentisering. Data er kryptert “at rest”. Se også databehandleravtale med Microsoft.

Fysisk sikring av personopplysninger er håndtert av underdatabehandler Microsoft.

Samme krav til hjemmekontor som fysisk kontor. Alle PCer er sikret gjennom tjenester levert av Lillevik IT. Alle anbefalte sikkerhets tiltak er gjennomført. Data lagret på PCer er kryptert. Personlige data lagres ikke på PC.

Logging gjøres på to nivåer. Systemnivå for å sikre at webløsningen fungerer som normalt og ikke er utsatt for unødig belastning eller angrep. På brukernivå logges det IP adresse, nettlesertype, tid for innlogging.

Det benyttes standard tjenester fra Microsoft Azure for logging av trafikk mot APIer, databaser o.l.

Det er kun administrator av løsningen som har tilgang til disse loggene.

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 Vilkårene 9.1 og 9.2 ved å gjennomføre følgende tekniske og organisatoriske tiltak:

Databehandleren bistår etter nærmere avtale med oppsett av systemet for gjennomføring av kulturkartlegging.

Databehandleren yter 1 og 2 linje support om nødvendig.

C.4 Oppbevaringsperiode/sletteprosedyrer

Ved opphør av databehandlertjenestene skal databehandleren enten slette eller levere tilbake personopplysningene i overensstemmelse med Vilkårene 11.1.

C.5 Lokasjon for behandling

Azure lagringsressurser er lokalisert i EU / EEA, se B.1.

C.6 Instruks for overføring av personopplysninger til tredjeland

Personopplysninger overføres ikke til tredjeland.

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

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

Den behandlingsansvarlige eller den behandlingsansvarliges representant kan hver 6 mnd utføre en fysisk inspeksjon av stedene hvor databehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen, for å fastslå at databehandleren overholder personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilkårene.

I tillegg til planlagt inspeksjon kan den behandlingsansvarlige gjennomføre en inspeksjon av databehandleren når den behandlingsansvarlige finner det nødvendig.

C.8 Prosedyrer for revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til underdatabehandleren

Databehandleren eller databehandlerens representant kan hver 6 mnd utføre en fysisk inspeksjon av stedene hvor underdatabehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen, for å fastslå at underdatabehandleren overholder personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilkårene.

I tillegg til planlagt inspeksjon kan databehandleren gjennomføre en inspeksjon av underdatabehandleren når databehandleren (eller den behandlingsansvarlige) finner det nødvendig.

Dokumentasjon for slike inspeksjoner 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 inspeksjon med annet omfang og/eller med en annen metode.

Basert på resultatene av inspeksjonen 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 Vilkårene blir overholdt.