DATABEHANDLERAVTALE

I henhold til personopplysningsloven

og EU Personvernforordning 2016/679

mellom

Meland kommune

Org.nr.: 951 549 770

Behandlingsansvarlig

og

Triangel Solutions AS

Org.nr.: 980 814 351

Databehandler

Datert: 20.06.2018

1. Om avtalen

Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Behandlingsansvarlig og Databehandler (heretter omtalt som "partene") etter:

- Lov av 14.april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven);
- Forskrift av 13.desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften);
- EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysningslovgivningen, viker Avtalens regulering.

2. Definisjoner

Begrepene "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler" og "brudd på personopplysningssikkerhet» skal forstås slik de er definert i personvernforordningen § 4, som gjeldende. "Avvik": brudd på opplysningssikkerhet og bruk av informasjonssystemet i strid med fastlagte rutiner.

3. Avtalens bakgrunn og formål

Denne Avtalen er inngått mellom partene og skisserer de generelle vilkårene for den behandling av personopplysninger som Databehandler utfører på vegne av Behandlingsansvarlig.

Formålet med Avtalen er å sikre behandlingen av personopplysninger på vegne av Behandlingsansvarlig slik at personopplysningene ikke brukes urettmessig eller kommer uberettigede i hende.

4. Omfang

Denne Avtalen kommer til anvendelse på all behandling av personopplysninger som Databehandler foretar på grunnlag av Avtale om bruksrett til minVakt (heretter omtalt som "Tjeneste/oppdragsavtalen"). I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Tjenester som inngår i denne Avtalen er de tjenester som inngår i Tjeneste/oppdragsavtalen og som innebærer behandling av personopplysninger.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens virksomhetsperiode og som innebærer at Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

Personopplysninger skal kun benyttes til de formålene som følger av denne Avtalen, Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekomme kravene i avtalene.

PO ØDS

5. Behandlingens formål, opplysninger og behandlinger

Formålet med behandling av personopplysninger er å ha verktøy og informasjon for å foreta arbeidsplanlegging for den enkelte ansatte, registrere fravær/avvik fra den opprinnelige arbeidsplan, generere fraværsoversikt, gi en oversikt over tilgjengelige vikarressurser, samt å generere timelister for variabel lønn.

I henhold til Vedlegg 2 pkt. 3 til Avtalen vil det for ansatte hos Behandlingsansvarlig eller ansatte i samarbeidende firma bli behandlet opplysninger om navn, fødselsnummer, stilling, stillingsprosent, årslønn, adresse, telefon, e-post adresse, kompetanse, stillingsnummer. For tidligere ansatte vil opplysningene være anonymiserte.

I henhold til Vedlegg 2 pkt. 4 til Avtalen vil det for pårørende hos Behandlingsansvarlig bli behandlet opplysninger om navn, beskrivelse, telefon, e-post, adresse.

Eventuelle endringer av formålet eller hvilke personopplysninger som behandles skal avtales skriftlig av partene og inntas som eget vedlegg til Avtalen.

6. Rammene for behandling av personopplysninger

Behandlingsansvarlig har til enhver tid full rådighet over de personopplysningene som databehandler har anledning til å behandle etter denne Avtalen. Databehandler har ikke selvstendig råderett over personopplysningene, og kan ikke behandle disse til egne formål.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles hos Databehandleren

7. Behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, samt denne Avtalen.

8. Databehandlers plikter

8.1. Generelt

Databehandler forplikter seg til å behandle personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Behandlingsansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene. Databehandler skal ikke ved noen handling eller unnlatelse, sette Behandlingsansvarlig i en slik situasjon at Behandlingsansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler skal ikke:

a) behandle personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
b) behandle personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;

c) utlevere, overlate eller overføre personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Behandlingsansvarlig eller Behandlingsansvarlig har godkjent dette skriftlig;
d) samle inn fra eller overføre personopplysninger til en tredjepart;
e) behandle personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Behandlingsansvarlig på annen måte enn hva som er angitt i denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

Databehandler skal:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Behandlingsansvarlig;
b. gi Behandlingsansvarlig tilgang til og innsyn i personopplysninger som behandles hos Databehandleren;
c. føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;
d. treffe alle rimelige tiltak for å sikre at personopplysningene til enhver tid er korrekte og oppdaterte;
e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer;
f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;
g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
h. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;
i. gi Behandlingsansvarlig nødvendig bistand slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
j. samarbeide med og bistå Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;
k. omgående underrette den Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
l. bistå Behandlingsansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Det er Databehandlers plikt å planlegge, treffe, og gjennomføre, alle nødvendige og adekvate tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger.

Databehandleren skal:

a) etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser, herunder kravene etter personvernforordningen artikkel 32.
   Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;
b) ha gode og hensiktsmessige internkontrollrutiner;
c) ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;
d) etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten blant annet rutiner for avviksmelding, og skal på forespørsel gi Behandlingsansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av personopplysninger;
e) avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;
f) ved mistanke om eller konstatering av avvik, omgående varsle Behandlingsansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;
g) dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;
h) omgående varsle Behandlingsansvarlig ved uautorisert utlevering av personopplysninger;
i) registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Behandlingsansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;
j) bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs.:

PG

GDS

- sikkerhet ved behandlingen;
- melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
- underretning av den registrerte om brudd på personopplysningssikkerheten;

k) i forbindelse med sikkerhetsrevisjon som utføres av Behandlingsansvarlig eller en tredjepart utpekt av Behandlingsansvarlig, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

l) varsle Behandlingsansvarlig om alle forhold som medfører endring i risikobildet;

m) innhente godkjenning av Behandlingsansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i Vedlegg 1 (hvis relevant). Ved brudd på denne Avtalen eller på bestemmelsene i personopplysningslovgivningen eller annen relevant lovgivning kan Behandlingsansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Behandlingsansvarlig.

9. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i Vedlegg 2 for de der angitte tjenester og bekrefter at det er ingen andre underleverandører som benyttes.

Databehandler skal:

1. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;
2. sørge for at underleverandører kun behandler personopplysninger i samsvar med denne Avtalen og ikke i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tjenesten som underleverandøren leverer;
3. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i Vedlegg 2. Oppdatert liste skal være tilgjengelig for Behandlingsansvarlig;
4. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Behandlingsansvarliges forespørsel, dele vurderingen med Behandlingsansvarlig;
5. på Behandlingsansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av personopplysninger;
6. underrette Behandlingsansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles i god tid slik at Behandlingsansvarlig gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal Vedlegg 2 oppdateres og oversendes Behandlingsansvarliges kontaktperson;

7. sikre at Behandlingsansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Behandlingsansvarlig har overfor Databehandler etter Avtalens punkt 12;
8. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarlig destruere alle personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene som framgår av Avtalens punkt 13 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandler er til enhver tid fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

Tilgang til personopplysninger for tredjeparter krever konkret avtale utover denne Avtalen mellom partene for alle andre enn Databehandlers underleverandører.

10. Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten. Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

11. Innsyn, verifikasjon og revisjon

Behandlingsansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Behandlingsansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre behandlingsansvarlige som benytter samme tjeneste hos Databehandler.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Behandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere behandlingsansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Behandlingsansvarlig eller tredjepart som Behandlingsansvarlig utpeker. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av personopplysninger slik det følger av relevant lovgivning.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

12. Varighet og opphør

Denne Avtalen gjelder fra den er signert av partene og gjelder til Avtalen og alle gjeldende avtaler mellom partene, som innebærer at Databehandler skal behandle personopplysninger på vegne av Behandlingsansvarlig, er opphørt.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har mottatt og behandlet på vegne av Behandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Behandlingsansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Databehandler skal gi Behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

13. Endring av avtale

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

14. Meddelelser

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Behandlingsansvarlig og Databehandler skal gis skriftlig, eller bekreftes skriftlig til:

Behandlingsansvarlig	Databehandler
Navn: PER-INGE OLSEN Rolle: PERSONVERNOMBUD E-post: per.inge.olsen@melaud.kommune.no	Navn: Robert Marken Rolle: Personvernombud E-post: robert.marken@triangel.no

15. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Romsdal tingrett som verneting. Dette gjelder også etter opphør av Avtalen.

16. Undertegning

Denne Avtalen foreligger i to originaler, hvorav partene beholder et eksemplar hver.

11. Vedlegg

Vedlegg 1: Tjeneste/oppdragsavtalen. Jmf. tidligere signert kontrakt.

Vedlegg 2: Tillegg til tjeneste/oppdragsavtale.

Sted og dato: Fvetkang 13/8-18 Sted og dato: Molde 19/6-2018

Behandlingsansvarlig	Databehandler
Navn:	Navn: Geir D. Sylte

Vedlegg 2
Tillegg til tjeneste/oppdragsavtale

1. Avtalens behandlinger

Avtalen omhandler produktet **minVakt** med følgende tjenester:

- Turnusplanlegging/Arbeidsplan
- Registrering av fravær/avvik fra plan
- Vikarhåndtering
- Avspasering
- Timelister for variabel lønn
- Internkommunikasjon:
  Meldingsutveksling mellom ansatte og administrasjonen. Meldinger kan sendes som internmeldinger i minVakt, epost eller SMS.
- SMS:
  minVakt har sømløs funksjon for SMS trafikk. Løsningen har sporbar logg for sendte og mottatte meldinger.

2. Rammene for databehandlers håndtering av personopplysninger

Personopplysningene skal benyttes til:

- Foreta arbeidsplanlegging for den enkelte ansatte
- Registrere fravær/avvik fra den opprinnelige arbeidsplan
- Generere fraværsoversikt
- Gi oversikt over tilgjengelige vikarressurser
- Generere timelister for variabel lønn

3. Personopplysninger i løsningen

Obligatoriske felt:

- Navn
- Fødselsnummer
- Stilling
- Stillingsprosent
- Årslønn

Ikke obligatoriske felt:

- Adresse
- Telefon (Mobilnummer/privat/arbeid)
- E-post adresse
- Kompetanse
- Stillingsnummer

Kategorier av registrerte:

- Ansattdata
- Tidligere ansatte
- Ansatte i samarbeidende firma
- Pårørende

4. Annen personopplysning i løsningen

Pårørende:

- Navn
- Beskrivelse
- Telefon (mobil/arbeid/privat)
- E-post
- Adresse

5. Underleverandør

Triangel Solutions AS benytter seg av to underleverandører som gjelder alle tjenester/produkter som leveres til kunde:

- Tafjord Marked, organisasjonsnummer 982 267 005, Ålesund som leverer internettadgang og tilhørende infrastruktur for kommunikasjon mellom våre systemer og kundens system(er). Dette er ren infrastruktur og ingen data lagres/behandles, samt at uautorisert tilgang til datatrafikk hindres ved bruk av kryptering mellom våre systemer og kundens system(er).
- Link Mobility, organisasjonsnummer 992 434 643, Oslo leverer tekstmeldingstjenester for mobiltelefon (SMS) for kommunikasjon mellom våre systemer og den enkelte brukers mobiltelefon. Link Mobility lagrer informasjon om tidspunkt, avsender telefonnummer, mottakers telefonnummer, leveringsstatus og leveringstidspunkt for tekstmeldinger. Selve innholdet i meldingen lagres ikke. Tekstmeldinger er uansett dårlig sikret mot uautorisert tilgang, så man kan ikke sende eller motta sensitive opplysninger gjennom denne leverandøren. Data lagres innen EU/EØS området.
- Microsoft Azure leverer driftstjenester som består av database og sikkerhetskopi. Denne tjenesten benyttes i tillegg til lokal sikkerhetskopi og data lagres i Nederland.

6. Sikkerhet jmf. pkt 8.2 i Databehandleravtale

Webtjenester:
Våre tjenester benytter webteknologi som er tilgjengelig over internett med kryptering i nettleseren til den enkelte bruker. Alle forespørsler og svar fra web-tjenester logges fortløpende og oppbevares inntil ett år på sikkerhetskopi. Loggen inneholder tidspunkt, IP-adresse og navn på forespurt web-side. Innholdet logges ikke på web-tjener. Mer detaljert logging og flere kontrollmekanismer ligger innenfor de ulike produktene (applikasjonene).

Webtjenestene er lokalisert bak brannmur og underliggende databaser er utilgjengelig for ekstern kommunikasjon. Programvare og operativsystemer holdes kontinuerlig oppdatert med sikkerhetsoppdateringer fra leverandørene.

Systemene overvåkes for å oppdage nedetid, skadeverk og uautorisert tilgang. Denne overvåkingen er en kombinasjon av automatisk varsling og manuelt vedlikehold.

Fysiske sikringstiltak:
Utstyr og maskinvare for drift av tjenestene er lokalisert i eget rom med separat adgangskontroll. Dette for å unngå at uautoriserte personer har fysisk tilgang til utstyr og maskinvare. Rommet har egen strømforsyning med dieseldrevet nødstrømsaggregat og batteridrift samt kjøleaggregat for stabil temperatur. Bygningen har også adgangskontroll og alarmsystem.

Sikkerhetskopi blir gjort hver kveld og blir oppbevart utenfor bygningen i tilfelle brann o.l. Sikkerhetskopi kjøres også mot ekstern reservedrift. Våre tjenester kan midlertidig driftes via reservedrifts løsning ved totalhavari i vårt driftsmiljø.

Daglig drift:
Den daglige driften av tjenestene omfatter både automatisk varsling av nedetid til driftsansvarlige, samt vedlikeholdsrutiner for sikkerhetsoppdateringer og kontroll av systemene. Fast forebyggende vedlikehold gjennomføres hver andre onsdag hver måned. Dette inkluderer sikkerhetsoppdateringer fra leverandører. I tillegg kommer vedlikehold utløst av behov som oppstår i den daglige driften.

Nødvendig tilgjengelighet og oppetid til systemene sikres av databehandleren ved hjelp av egen bakvaktsordning.

Detaljerte opplysninger og drift og vedlikehold er forebeholdt IT-drift til databehandleren, men kan gjøres tilgjengelig på forespørsel fra kunde.

Sikkerhetsrevisjoner:
I Dataleverandørens internkontrollsystem basert på ISO 9001 standard, foreligger prosedyre for revisjoner. Hensikten med prosedyren er å gjennomføre kvalitetsrevisjoner for å avdekke om systemet for kvalitetsstyring oppfyller fastsatte krav:

- Kvalitetsmål
- Produkt/kundekrav
- Om systemet er virkningsfullt iverksatt og effektivt vedlikeholdt

Daglig leder er ansvarlig for at revisjonene utføres etter oppsatte revisjonsplaner.

I dokumentasjonen av "Vedlikeholdsprosedyrer" er det beskrevet revisjonsfrekvens og revisjonsarbeide knyttet til:

- Vedlikeholdsprosedyre for Handlingsplan for håndtering av langvarig tidsavbrudd.
- Vedlikeholdsprosedyre for Varslingsinstrukser
- Årsplan vedlikehold

I tillegg foreligger prosedyre for planlegging av tester og øvelser.

7. Oppbevaring av data

Databehandler vil oppbevare historiske data etter avtalens opphør i minst 3 ½ år pluss inneværende regnskapsår. Hvis behandlingsansvarlige vil ha data slettet før den tid og ved evt. utskrift og kopi av innhold i databaser som er omfattet i avtalen, vil dette arbeidet bli fakturert etter faktisk tidsbruk og gjeldene timesats for våre tjenester.

Sletting skjer ved at alle data knyttet til kundens bruk av programvaren fjernes fra databehandlers databaser og sikkerhetskopier.
Data kan bare lagres så lenge det er nødvendig ut fra formålet med behandlingen.