Oppdatert: 27.08.2018

DATABEHANDLERAVTALE

I henhold til personopplysningsloven og

EUs Personvernforordning 2016/679

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");
- Enhver lov, forskrift eller annet regelverk som erstatter disse.

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

2. 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.

3. Omfang

Denne Avtalen kommer til anvendelse på all behandling av personopplysninger som Databehandler foretar på grunnlag av oppsett og drift av websider på vegne av Behandlingsansvarlig. 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.

4. Behandlingens formål, opplysninger og behandlinger

Formålet med og varigheten av behandling av personopplysninger, hvilke personopplysninger som behandles, og behandlingens art er angitt i **Vedlegg 1.**

Nærmere beskrivelse av behandlingen, behandlingens formål og hvilke personopplysninger som omfattes fremgår av Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene [hvis relevant].

5. 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.

6. Behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, samt denne Avtalen og forplikter seg dermed til at det ivaretas et behandlingsgrunnlag for personopplysningene som behandles i databehandlers løsninger, og at de aktuelle behandlingene er i overensstemmelse med gjeldende lovgivning.

7. Databehandlers plikter

7.1. 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 utover det som er nødvendig for feilsøking i forbindelse med Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
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. gi Behandlingsansvarlig tilgang til og innsyn i personopplysninger som behandles hos Databehandleren;
b. 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;
c. ha teknisk mulighet til å slette den registrertes personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;
d. 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;
e. gi Behandlingsansvarlig nødvendig bistand slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
f. 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;

g. omgående underrette den Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

h. bistå Behandlingsansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

7.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige 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. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Databehandler gi Behandlingsansvarlig tilgang til relevant sikkerhetsdokumentasjon for systemene som benyttes for behandling av personopplysninger;

d. loggføre og dokumentere forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;

e. ved konstatering av avvik, varsle Behandlingsansvarlig. I varselet opplyses avviket så godt det lar seg gjøre 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, kontaktopplysningene til kontaktpersonen hos Databehandler der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;

f. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

g. varsle Behandlingsansvarlig ved uautorisert utlevering av personopplysninger;

h. registrere all tilgang til informasjon. Alle oppslag som gjøres registreres slik at de så godt det lar seg gjøre kan spores til den enkelte bruker. Loggene skal

oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;

i. bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;

j. i forbindelse med sikkerhetsrevisjon som utføres av Behandlingsansvarlig eller en tredjepart utpekt av Behandlingsansvarlig, framlegge alle relevante dokumenter av betydning for revisjonen;

k. varsle Behandlingsansvarlig om alle forhold som medfører varig endring i risikobildet;

Nærmere oversikt over Databehandlerens informasjonssikkerhet er angitt i **Vedlegg 2 - SIKKERHETSARKITEKTUR**.

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.

8. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i **Vedlegg 3**

Databehandler skal:

a. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;

b. 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;

c. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i **Vedlegg 3**. Oppdatert liste skal på forespørsel gjøres tilgjengelig for Behandlingsansvarlig;

d. 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;

e. informere Behandlingsansvarlig om skifte eller innføring av nye underleverandører og oppdatere og publiseres **Vedlegg 3** på Databehandlers websider;

g. sikre at Behandlingsansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Behandlingsansvarlig har overfor Databehandler;

h. ved opphør av Avtalen, sikre at underleverandører sletter eller forsvarlig destruerer alle personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene 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.

9. Overføring av personopplysninger til utlandet

Partene i denne Avtalen er enige om at ingen av personopplysningene som behandles under denne Avtalen skal overføres til land utenfor EU/EØS eller USA (under Privacy Shield sertifisering), med mindre det er spesifisert i denne avtalen eller særskilt avtalt mellom partene.

Underleverandører utenfor EU, og som ikke tilbyr lagring av data innenfor EU, har erklært overholdelse av, EU-US Privacy Shield-rammeavtalen og U.S.-Swiss Safe Harbor-rammeavtalen som er fastsatt av det amerikanske handelsdepartementet, og forplikter seg til å underlegge alle personopplysninger fra EU-medlemsland den tilliten rammeavtalene gir, ifølge rammeavtalens gjeldende prinsipper.

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, 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

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig, frem til den dato levering av tjenesten opphører eller databehandleravtalen sies opp.

Ved brudd på denne avtale, personopplysningsloven eller GDPR kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

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 Avtalen oppdateres tilsvarende.

14. Meddelelser

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

Databehandler: post@bysant.no

Behandlingsansvarlig: E-post adressen til kontaktpersonen som er oppgitt ved inngåelse av kundeforholdet, evnt. til adresse spesifisert av behandlingsansvarlig.

15. Lovvalg og verneting

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

VEDLEGG 1 – PERSONOPPLYSNINGER BEHANDLET I WEBPUBLISH

Alle websider logger ip-adressene for samtlige besøkende av sikkerhetshensyn. Loggene oppbevares maksimalt i et år.

Kontaktskjema:

Informasjon sendes på e-post og lagres lokalt i en loggfil i et år.

- Navn
- E-post

Ordremodulen:

Informasjon lagres så lenge løsningen er aktiv. Manuell sletting eller sletting ved hevne intervaller kan aktiveres ved å kontakte Bysant.

- Ip adresse
- Dato for kjøp
- Ordrenummer
- Kobling til brukerkonto
- Leveringsmetode
- Benyttet rabatt-/verdikode
- Produktinformasjon
- Kjøpesummer
- Betalingsreferanse (kortinformasjon lagres kun hos Nets)
- Sporingskoder
- Kommentarer
- Leverings og Faktura adresser med følgende underfelt:
    - Fullt navn
    - E-post
    - Firmanavn
    - Organisasjonsnummer
    - Telefonnummer
    - Adresse
    - Postnummer
    - Sted
    - Land

Brukermodulen:

Informasjonen lagres frem til brukerkontoen slettes.

- E-post
- Kryptert passord
- Fullt navn
- Firmanavn
- Organisasjonsnummer
- Telefonnummer
- Adresse
- Postnummer
- Sted

- Land

Nyhetsbrevsmodulen:

E-post adresse og tidspunkt for påmelding lagres en gang pr interesseliste og slettes ved avmelding. Oppføring i blokkliste (spesifikt ønske om ikke å motta noen markedsføring nå eller i fremtiden) lagres videre selv om alle påmeldinger tas bort så lenge ikke blokkeringen også spesifikt fjernes. Standard påmeldingsskjemaet for nyhetsbrev lar brukerne selv styre oppføringer i interesselister (så lenge administrator ikke skjuler valgene) og krever aktiv påmelding.

Nyhetsbrevmodulen logger også utsendelser, svar fra mottakers e-post server og registrerer i mange tilfelle når en e-post er lest (bilder lastet) og når lenker i e-posten blir klikket på. Denne informasjon lagres så lenge løsningen er aktiv. Manuell sletting eller sletting ved hevne intervaller kan aktiveres ved å kontakte Bysant.

VEDLEGG 2 – SIKKERHETSARKITEKTUR

Nr.	Tema	Krav
1.	Sikring av data	Databehandler sikrer data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet
2.	Kryptering	Alle bærbare arbeidsstasjoner krypteres med BitLocker kryptering
3.	Autentisering	Ved tilgang til data ved tjenstlig behov benyttes brukernavn med passord
4.	Brannmur	Underleverandør for hosting drifter nettverk og brannmur
5.	Tjenestenektangrep	Underleverandør for hosting sikrer nettverket mot tjenestenektangrep
6.	Logging og sporbarhet	Alle forespørsler til webserverne logges for å spore autoriserte og ikke autoriserte innloggingsforsøk
7.	Testdata	Ingen reelle personopplysninger benyttes som testdata ved generell utvikling
8.	Lagringstid	E-post oppbevares så lenge kontoen er aktiv. Logging av autoriserte og uautoriserte påloggingsforsøk slettes automatisk etter maksimalt 365 dager, eller slettes i sin helhet ved opphør av avtalen
9.	Backup og restore	Backup oppbevares i opptil ett år før den slettes automatisk

VEDLEGG 3 – UNDERLEVERANDØRER

Underleverandør	Leveranseområde	Stedlig plassering
IspHuset	Datasenter, hosting	Drammen, Norge
Digital Garden	Datasenter, hosting	Oslo, Norge
Amazon	Backup	Irland
Office 365	E-post	EU (Østerrike, Finland, Irland, Nederland)
Dropbox	Fillagring	USA (Privacy Shield sertifisert)