Utlendingsdirektoratet
Norwegian Directorate
of Immigration

Avtale om behandling og sikring av personopplysninger

mellom Utlendingsdirektoratet og XX (sett inn navn på databehandleren)

Oslo xx.xx.20xx
For Utlendingsdirektoratet

Oslo xx.xx.20xx
For XX (sett inn navn på databehandleren)

Denne avtalen er undertegnet i to eksemplarer. Hver part beholder ett eksemplar.

Innhold

1 Avtalens parter og formål

1.1 Parter

Denne avtalen er inngått mellom Utlendingsdirektoratet (UDI) som behandlingsansvarlig og xx som databehandler.

1.2 Avtalens formål

Denne avtalen skal sikre at roller, ansvar og oppgaver for UDI som behandlingsansvarlig og XX som databehandler utføres i henhold til (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger (personvernforordningen) og personopplysningsloven.

Partene skal, i sin behandling av personopplysninger, ivareta fysiske personers grunnleggende rettigheter og friheter i tråd med prinsippene i personvernforordningen artikkel 5.

Avtalen består av en hovedavtale og tre bilag.

1.3 Databehandlerens håndtering av personopplysninger

Xx skal kun behandle personopplysninger til følgende formål:

- gi tilbud om innkvartering til asylsøkere
- behandling av økonomiske ytelser til beboere i mottak
- tilrettelegge for utlendinger med oppfølgingsbehov i mottak
- behandling av opplysninger om retur, herunder assistert retur
- registrering av opplysninger og samhandling med beboere i bosettingsforberedende arbeid
- kontrollere og verifisere opplysninger
- rapportere om saksbehandlingen etter pålegg fra overordnet myndighet (Bistå ved oppfyllelse av UDIs rapporteringskrav)

I arbeidet på disse områdene skal følgende typer av personopplysninger behandles:

- identitet (fødselsdato, fødested, kjønn, statsborgerskap, passnummer)
- oppholdssted og kontaktinformasjon (postadresse, bostedsadresse, e-postadresse og telefonnummer)
- relasjoner til andre (familie, vertsfamilie, arbeidsgiver, studiested)
- økonomiske forhold (inntekt, økonomisk støtte fra det offentlige, formue)
- helsemessige og sosiale forhold som har betydning for tilrettelegging for beboere med oppfølgingsbehov

Rutiner og systemer som xx anvender i oppgaveløsningen til overnevnte formål skal overholde de kravene oppsatt i personvernforordningen, personopplysningsloven, denne avtalen og tilhørende bilag.

Dette innebærer bl.a. at det ikke kan finne sted viderebehandling av opplysninger til andre formål uten at det er uttrykkelig avtalt med UDI. Dette gjelder også opplysninger om UDIs ansatte og tilhørende metadata.

2 Overordnede krav, roller og ansvar

2.1 Overordnede krav

Oppgavene som denne avtalen omfatter, reguleres av dette avtaledokumentet med tilhørende bilag og de aktuelle rettslige rammebetingelser. Av rettslige rammebetingelser nevnes spesielt; personvernforordningen, personopplysningsloven og forvaltningsloven, i tillegg til særlovgivning som direkte omfatter aktuelle behandlinger som xx utfører og som følger av f.eks. utlendingsloven og utlendingsforskriften.

I tillegg kommer retningslinjer og pålegg som til enhver tid gis for den aktuelle oppgaveløsningen samt de rutiner for de aktuelle behandlingene som er fastsatt av UDI for å sikre riktig saksbehandling.

2.2 Om UDIs rolle og ansvar

UDI er i tråd med definisjonen i personvernforordningen artikkel 4 nr. 7 behandlingsansvarlig for all behandling av personopplysninger som skjer hos databehandleren og som omfattes av denne avtalen. Som behandlingsansvarlig er UDI i henhold til personvernforordningen artikkel 28 ansvarlig for å påse at kravene som stilles i personopplysningsloven og –forordningen er oppfylt ved all behandling av personopplysninger som databehandleren utfører på UDIs vegne.

2.3 Om databehandleren sin rolle og ansvar

xx er i tråd med definisjonen i personvernforordningen artikkel 4 nr. 8 databehandler for de behandlinger av personopplysninger som omfattes av denne avtalen. Xx skal kun behandle personopplysninger i henhold til denne avtalen og utfyllende instrukser gitt av UDI.

2.3.1 Bruk av andre databehandlere/underleverandører

xx kan kun benytte andre databehandlere/underleverandører som er forhåndsgodkjent av UDI. Alle underleverandører på tidspunktet for signering av avtalen skal være opplistet i bilag 3 «Underleverandører».

XX skal varsle UDI om eventuelt nye underleverandører/databehandlere i god tid før de får tilgang til UDIs opplysninger. UDI kan motsette seg xx sin bruk av nye underleverandører/databehandlere, jf. personvernforordningen artikkel 28 nr. 2, men vil ikke nekte slik bruk med mindre det er grunnlag for å frykte at avtalens krav ikke vil bli overholdt. xx er i så fall fullt ut ansvarlig for utførelsen av en underleverandørs oppgaver, på samme måte som om xx selv stod for utførelsen.

Xx og dens databehandlere og underleverandører kan bare behandle personopplysninger, stilt til rådighet av UDI eller som xx får befatning med på vegne av UDI, i henhold til denne avtalen og i tråd med de rammene og føringene som følger av avtalen her, jf. personvernforordningen artikkel 28 nr.4 og artikkel 29. Databehandler plikter å opplyse sine underleverandører om vilkårene i denne avtalen.

3 Behandling av personopplysninger hos databehandleren

3.1 Innsamling og registrering

Personopplysninger skal kun innhentes og registreres når vilkårene for slik innsamling og registrering er tilstede.

Registreringer som gjøres, danner grunnlag for den registrerte sine rettigheter og plikter og for oppgaveløsningen hos alle aktører i utlendingsforvaltningen, herunder de ansvarlige departementene. All behandling (herunder registreringer, sammenstilling, lagring, mv) skal derfor oppfylle de nødvendige kvalitetskravene som følger av lovgivningen.

3.2 Informasjon til den registrerte

I forkant av innsamling og registrering av personopplysninger skal det gis god informasjon på et klart og enkelt språk til den registrerte i tråd med bestemmelsene i personvernforordningens artikler 12 – 15, så lenge unntakene i personopplysningsloven § 16 ikke er til hinder for dette. UDI skal gi anvisning på innhold og omfang av informasjon gjennom avtale, utarbeidede skjema, brosjyrer og/eller rundskriv.

3.3 Innsyn

Begjæringer om innsyn i personopplysninger som xx behandler på vegne av UDI skal videreformidles til UDI. Xx skal om nødvendig bistå UDI, ved hjelp av egnede tekniske eller organisatoriske tiltak, med å besvare anmodningen fra den registrerte, jf. personvernforordningen artikkel 28 nr. 3 bokstav e.

3.4 Retting og sletting av personopplysninger

Begjæringer om retting av personopplysninger som xx behandler på vegne av UDI, og som blir levert inn til xx, skal videreformidles UDI.

Hvis XX oppdager åpenbare feil i registrerte personopplysninger på egenhånd, skal XX rette feilen omgående og varsle UDI om rettingen. UDI skal foreta en vurdering av om den berørte eller andre som har fått tilgang til den aktuelle informasjonen skal informeres om rettingen. Dersom det foreligger tvil om personopplysninger som behandles på vegne av UDI er korrekt, skal UDI varsles omgående slik at videre behandling skjer i samråd med UDI.

3.5 Utlevering

Personopplysninger som XX behandler på vegne av UDI skal ikke overføres til andre eksterne parter nasjonalt eller internasjonalt enn de som følger av lov eller forskrift eller på annen måte er uttrykkelig omtalt i denne avtalen. Eventuell overføring til tredjeland eller internasjonale organisasjoner skal skje etter de særskilte reglene i personvernforordningen artiklene 44 – 46.

4 Taushetsplikt

Partene har taushetsplikt etter til enhver tid gjeldende lover, forskrifter og instrukser. Taushetsplikten omfatter alle opplysninger som behandles om den registrerte.

Partene er enige om å bevare taushet også om sikkerhetsmessige og forretningsmessige forhold eller andre konfidensielle opplysninger som kan, om de kommer på avveie eller blir kjent for andre, skade en av partene. Denne taushetsplikten gjelder enhver kunnskap om den andre parts sikkerhetsrutiner som en part får kjennskap til i forbindelse med inngåelse og oppfyllelse av denne avtalen. Taushetsplikten gjelder partenes ansatte og andre som handler på partenes vegne i forbindelse med gjennomføringen av avtalen. Ansatte og andre som fratrer sin tjeneste hos en av partene skal pålegges taushet om forhold som nevnt over, også etter fratredelse.

Taushetsplikten gjelder også etter avtalens opphør.

Xx må etter anmodning fra UDI kunne dokumentere at alle ansatte og andre som har tilgang til personopplysninger, skriftlig har forpliktet seg til å overholde taushetsplikten før de får tilgang til opplysningene.

Taushetsplikten hindrer ikke oppfyllelse av en lovpålagt opplysningsplikt eller utførelse av nødvendig rapportering til overordnet myndighet.

5 Krav til personopplysningssikkerheten hos databehandleren - sikring av konfidensialitet, integritet, tilgjengelighet og robusthet

5.1 Generelle krav

Xx skal påse at kravene til personopplysningssikkerheten i personvernforordningens artikkel 32 er oppfylt.

Sikkerhetstiltakene skal dokumenteres og gjøres tilgjengelig for den behandlingsansvarlige ved etterspørsel.

5.2 Nærmere beskrivelse av krav til personopplysningssikkerheten

XX skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen skjer i samsvar med akseptabelt risikonivå fastsatt av UDI som behandlingsansvarlig.

XX skal iverksette egnede tiltak for å forebygge eller forhindre unødvendig og ulovlig behandling, herunder tilgang til, bruk eller kopiering av personopplysningene som XX behandler på vegne av UDI etter denne avtalen. UDIs opplysninger skal ikke kopieres eller overføres til andre servere utover det som er nødvendig for tilfredsstillende back-up løsninger.

Tilgangskontroll

xx skal forsikre seg om at alle ansatte i xx og personer relatert til xx som gis tilgang til å benytte personopplysninger regulert i denne avtalen:

- er skikket til å håndtere personopplysningene,

- har tilstrekkelig kompetanse til å bruke systemet på en sikker måte, slik at informasjonen ikke kompromitteres,
- er autorisert for bruk av saksbehandlingsapplikasjoner eller andre verktøy knyttet til behandlingen av personopplysninger
- kun bruker saksbehandlingsapplikasjoner eller andre verktøy med sin egen identitet mot systemet,
- ikke benytter tilgangen utover tjenstlig behov eller til andre formål enn til oppfyllelse av denne avtalen.

Antall personer med tilgang skal være begrenset til det som er nødvendig for en forsvarlig drift.

Det skal foreligge rutiner som sikrer ajourhold av tilgangsrettigheter når den ansatte endrer stillingsinnhold, går i permisjon eller slutter.

Teknisk og fysisk sikring

XX skal teknisk og fysisk sikre sitt utstyr og sine lokaler som benyttes for behandling av personopplysninger som er omfattet av denne avtalen. I den forbindelse skal XX ha forsvarlige rutiner for adgangskontroll.

xx har ansvar for teknisk sikring i informasjonssystem/utstyr som xx eier eller disponerer og som benyttes for behandling av personopplysninger som er omfattet av denne avtalen, jf. personvernforordningen artikkel 32 nr. 1.

Konfidensialitet

xx plikter å ta de forholdsregler som er nødvendig for å sikre at personopplysninger eller andre opplysninger som partene etter avtale plikter å bevare taushet om, ikke blir gjort kjent for uvedkommende i strid med denne avtalen.

Overføring av informasjon stiller krav til hvordan opplysninger blir kommunisert og det presiseres for ordens skyld at dette utelukker bruk av åpen e-post og telefaks for taushetsbelagt informasjon.

Integritet (uautorisert endring av opplysningene)

XX skal sikre opplysningenes integritet. I den grad øvrige forholdsregler ikke sikrer opplysningenes integritet i tilstrekkelig grad, skal det iverksettes egne tiltak som sikrer dette.

Tilgjengelighet og robusthet

xx skal ha:

- konfigurert IKT-utstyr de råder over med nødvendig kapasitet og ressurser, slik at tilgjengeligheten er tilfredsstillende
- tilfredsstillende back-up rutiner for drift hvis det oppstår driftsavvik
- beredskaps- og kontinuitetsplaner tilpasset de foreliggende behov

5.3 Krav til dokumentasjon hos databehandleren – UDIs rett til kontroll og revisjon

Dokumentasjon og rapportering

Partene har plikt til å bistå hverandre ved utarbeidelse og fremskaffelse av dokumentasjon som er nødvendig for å tilfredsstille dokumentasjonskrav etter gjeldende lover og bistand i forbindelse med tilsynsmyndighetenes krav og eventuelle kontroll, jf. personvernforordningen artikkel 30 nr. 2 og artikkel 31.

xx må som databehandler for UDI kunne dokumentere at sikkerheten knyttet til behandling av de aktuelle opplysningene er tilfredsstillende og i samsvar med de dokumentasjonskrav som følger av personvernforordningen. xx skal sikre oppdatert system- og brukerdokumentasjon for egne systemer og/eller løsninger som de benytter i oppgaveløsningen for UDI.

Kontroll og revisjon

UDI har rett til innsyn i relevant sikkerhetsmessig dokumentasjon og til verifikasjon av hvordan løsningene er sikret og at behandlingen av opplysningene skjer i tråd med avtalen.

XX skal for egen regning gjennomføre en sikkerhetsrevisjon av behandlingen, minimum hvert 2. år. Resultatet fra sikkerhetsrevisjonen skal dokumenteres og forelegges UDI. Partene kan avtale at det skal foreligge en sikkerhetsrevisjon fra en uavhengig tredjepart.

UDI kan videre kreve at sikkerhetsbrudd vurderes av en uavhengig part. Vurderingene skal kunne skje straks bruddet inntrer og rapport skal gis uten ugrunnet opphold. Utgiftene til slik vurdering dekkes av UDI. Retten til innsyn, verifikasjon og sikkerhetsrevisjon er begrenset til de behandlinger og sikkerhetsmessige forhold UDI er ansvarlig for.

5.4 Eventuelt opphør

Ved eventuelt opphør av denne avtalen skal xx bruk av tilganger som er gitt til bruk i oppgaveløsningen i henhold til denne avtalen, opphøre jf. personvernforordningen artikkel 28 nr. 3 bokstav g. Alt materiell som UDI er ansvarlig for, skal samtidig leveres tilbake til UDI eller stilles til disposisjon for den som UDI utpeker. Xx skal yte nødvendig bistand i forbindelse med eventuell overføring av oppgaver til en annen enhet/virksomhet. XX skal ved opphør av avtalen slette alle kopier av personopplysninger.

6 Avvikshåndtering og varslingsplikt

Partene skal alltid varsle hverandre om forhold som har betydning for gjennomføring av avtalen. Det samme gjelder dersom en av partene oppdager mangler i eksisterende rutiner.

Det skal etableres løsninger og/eller iverksettes rutiner som gjør det mulig å identifisere sikkerhetsbrudd som omfattes av avtalen. Med sikkerhetsbrudd menes hendelser som er i strid med rettslige rammebetingelser, fastlagte instrukser og det som er nedfelt i avtalen. Slike sikkerhetsbrudd kan for eksempel være uautorisert tilgang til data, misbruk eller tap av data, tyveri, brann eller annen ødeleggelse av personopplysninger.

Ved sikkerhetsbrudd som er relevante for behandlingen av personopplysninger omfattet av avtalen, eller på annen måte relevante for informasjonssikkerheten hos UDI, skal UDI varsles

muntlig uten ugrunnet opphold og det skal straks igangsettes tiltak for å minimere mulig skade for UDI. Aktuelle avvik skal også rapporteres skriftlig så snart som mulig og senest innen 24 timer etter at bruddet er oppdaget.

Den skriftlige rapporten skal inneholde informasjon om

- hva som har inntruffet,
- hvor mange registrerte som er berørt av hendelsen,
- hvor mange personopplysninger bruddet omfatter,
- når og hvor hendelsen inntraff,
- hvilke strakstiltak som ble iverksatt,
- hvilke konsekvenser hendelsen har, og
- hvem som er ansvarlig for videre oppfølging.

Ved sikkerhetsbrudd som omfatter personopplysninger er det UDI som vurderer om Datatilsynet skal varsles jf. Artikkel 33 nr.1.

Kontaktinformasjon se bilag 1.

7 Mislighold

7.1 Beskrivelse av mislighold

Mislighold foreligger dersom en av partene ikke oppfyller sine plikter etter denne avtalen og dette ikke skyldes force majeure, eller forhold som den andre parten har ansvaret eller risikoen for. Brudd på taushetsplikten anses alltid som vesentlig mislighold.

Dersom en av partene ønsker å påberope seg mislighold, skal dette meddeles den andre parten skriftlig uten ugrunnet opphold.

7.2 Sanksjoner ved mislighold

Dersom UDI finner at sikkerheten ikke er tilstrekkelig ivaretatt, kan UDI pålegge utbedring av misligholdet innen den tid som anses nødvendig i forhold til sikkerhetsbruddets karakter. UDI kan også gi pålegg om å stanse behandlingen (herunder registrering og/eller overføring) av personopplysninger, for eksempel ved at tilgangene for en eller flere av xx ansatte stenges dersom sikkerheten ikke er tilfredsstillende. Det samme gjelder hvis UDIs systemer blir angrepet via kommunikasjonen med xx enheter.

I den grad vesentlig mislighold på databehandlers side innebærer erstatningsmessige forpliktelser for UDI, kan UDI kreve erstatning av xx.

8 Avtalens varighet og endringshåndtering

Avtalen trer i kraft når begge parter har signert.

Avtalen skal endres dersom endringer i lovgivningen gjør dette nødvendig. Krav som følger av endringer i lover og/eller forskrifter skal gjennomføres innen de tidsfrister som følger av den aktuelle lov eller forskrift. UDI kan i tillegg ensidig gjøre endringer i instrukser, krav og

retningslinjer, men skal om mulig alltid forelegge endringsbehovet for xx og skal i størst mulig grad bestrebe at det foreligger enighet om de endringer som foretas.

For å sikre at avtalens innhold og utforming er i tråd med de faktiske behov, skal avtalen gjennomgå en revisjon minimum hvert tredje år, beregnet fra dato avtalen er underskrevet av begge parter.

Dersom det finner sted strukturelle endringer hos én eller begge parter som medfører behov for å la andre juridiske personer stå som part i avtalen, forplikter begge parter seg til å bistå hverandre slik at avtalen og ordningen den regulerer, kan opprettholdes.

Avtalen trer i kraft ved signering av driftsavtalen og løper uten tidsbegrensning. Ved et ev. opphør av driftsavtalen vil også denne avtale opphøre.

Alle endringer i avtalen skal fremkomme av endringsloggen, jf. bilag 2.

9 Annet

Hver av partene bærer egne kostnader i forbindelse med avtalen med mindre annet er uttrykkelig avtalt.

Oversikt over bilag:

Bilag 1: Kontaktinformasjon
Bilag 2: Endringslogg
Bilag 3: Eventuelle underleverandører

Databehandleravtalen - Bilag 1 Kontaktinformasjon

1. Kontaktpunkter UDI

Type henvendelse	Kontaktpunkt	Beskrivelse

2. Kontaktpersoner xxx

Type henvendelse	Kontaktpunkt	Beskrivelse

Databehandleravtalen - Bilag 2 Endringslogg

Versjon	Dato	Endring	Ansvarlig/initiert av

Databehandleravtalen - Bilag 3 Underleverandører

Firmanavn	Ansvarsområde	Ev. overføring til tredjeland