**DATABEHANDLERAVTALE MELLOM UTLEIER OG LEVERANDØR**

2. utgave 05/22

VEILEDNING OM BEHANDLING AV PERSONOPPLYSNINGER I FORBINDELSE MED UTLEIE AV FAST EIENDOM

Personopplysningsloven og personvernforordningen (GDPR) treffer svært bredt. Innen eiendomsbransjen vil en lang rekke aktiviteter være omfattet. Enkle eksempler er adgangskontroll og resepsjonstjenester, fordi disse aktivitetene alltid vil medføre en eller annen form for *behandling av personopplysninger*.

Loven regulerer helt eller delvis automatisert behandling av personopplysninger, og ikke-automatisert behandling av personopplysninger som skal inngå i et register.

En *personopplysning* er enhver opplysning om en identifisert eller identifiserbar fysisk person. *Behandling* er enhver operasjon som gjøres med personopplysninger, for eksempel innsamling, lagring, analyse eller utlevering.

Når en virksomhet behandler personopplysninger på vegne av en annen, kreves det at man inngår en databehandleravtale. *Databehandleren* er virksomheten som behandler personopplysninger på vegne av den *behandlingsansvarlige*. Det er den behandlingsansvarlige som har hovedansvaret for å oppfylle lovens krav, og en måte å gjøre dette på er å stille krav i en databehandleravtale til hvordan databehandleren skal opptre.

GDPR artikkel 28 krever at det inngås databehandleravtaler, og har detaljerte krav til hva en databehandleravtale må inneholde. Disse kravene er grunnlaget for bestemmelsene i denne databehandleravtalen.

Denne databehandleravtalen er ment for et typetilfelle, der leietakerne er behandlingsansvarlig, med utleier som databehandler og leverandøren som utleiers underleverandør (underdatabehandler). Det vil normalt være Leietaker som bestemmer at man skal ha adgangskontroll og en resepsjonsfunksjon. Leietaker kan i utgangspunktet (teorien) velge å styre disse funksjonene selv, eller sette de ut til en tjenesteleverandør (i dette tilfelle utleier, som så benytter en tredjeparts leverandør). Da oppstår det en (under)databehandlerrelasjon, fordi leverandøren i forbindelse med disse aktivitetene på oppdrag for utleier vil behandle personopplysninger som leietaker i utgangspunktet har ansvaret for.

Databehandleravtalen kan også med enkle grep benyttes der utleier selv er behandlingsansvarlig.

Nærmere veiledning om enkelte bestemmelser i databehandleravtalen finnes i vedlegg 3. Mer informasjon om reglene for behandling av personopplysninger finnes på Datatilsynets nettsider www.*datatilsynet.no.*

**DATABEHANDLERAVTALE**

**MELLOM**

**UTLEIER OG LEVERANDØR**

# Bakgrunn og formål

[…] **(Utleier**) og […] **(Leverandøren)** har [dato] inngått en avtale (**Avtalen**) som omfatter levering av nærmere angitte tjenesterfor [adresse, gnr. og bnr.] **(Eiendommen).**

Utleier bruker Leverandøren som underleverandør for å levere de ovennevnte tjenestene til leietaker/leietakerne (**Leietaker**) i Eiendommen.

Denne databehandleravtalen regulerer Utleiers og Leverandørens rettigheter og plikter i forbindelse med Leverandørens behandling av personopplysninger på vegne av Leietaker. Leietaker er behandlingsansvarlig, og Utleier er databehandler for behandlingen av slike personopplysninger. Leverandøren, i egenskap av å være Utleiers underleverandør, er såkalt «underdatabehandler» for personopplysningene, og er gjennom denne databehandleravtalen ilagt tilsvarende forpliktelser som Utleier er underlagt i avtalen med Leietaker.

Formålet med behandlingen, behandlingens art, kategorien av registrerte og typer personopplysninger som omfattes er nærmere beskrevet i Vedlegg 1.

# Utleiers plikter

Utleier bekrefter å ha inngått databehandleravtale med Leietaker som oppfyller kravene i GDPR art. 28, og som er dekkende for de behandlinger som Leverandøren skal gjennomføre på vegne av Utleier.

Utleier bekrefter at Leietaker i avtalen med Utleier har bekreftet at:

* Leietaker har rettslig grunnlag for behandlingen av personopplysningene,
* personopplysningene er fullstendige og korrekte slik at Utleier og Leverandøren blir i stand til å oppfylle sine plikter

Utleier skal, i samråd med Leietaker:

* Svare på henvendelser fra de registrerte om behandlingen av personopplysninger.
* Vurdere nødvendigheten av tiltak som angitt i pkt. 3.2.1. og ved behov bestille slike tiltak fra Leverandøren.

Utleier skal ha tilstrekkelige tekniske og organisatoriske tiltak for å sikre overholdelse av relevante krav etter gjeldende personvernlovgivning.

# Leverandørens plikter

## Instruks fra Utleier

Leverandøren skal bare behandle personopplysninger som angitt i denne databehandleravtalen med mindre noe annet avtales gjennom etterfølgende dokumentert instruks fra Utleier.

Dersom Leverandøren likevel må behandle personopplysninger på grunn av ufravikelig lov, skal Leverandøren såfremt det er lovlig underrette Utleier i forkant.

Leverandøren skal varsle Utleier dersom Leverandøren mener at en instruks fra Utleier er i strid med gjeldende lovgivning.

## Informasjonssikkerhet

### Vurdering av tiltak

Leverandøren skal sikre et tilfredsstillende sikkerhetsnivå iht. GDPR art. 32.

Herunder skal Leverandøren sikre at opplysningene ikke blir gjort tilgjengelige for uvedkommende (*konfidensialitet*), at de ikke kan endres utilsiktet eller av uvedkommende (*integritet*), og at de er tilgjengelige for godkjente brukere når disse har behov for det for å kunne utføre sine oppgaver (*tilgjengelighet*).

Ved vurderingen av hvilke tekniske og organisatoriske tiltak som skal tas i bruk, skal Leverandøren i samråd med Utleier vurdere:

* Beste praksis
* Kostnaden
* Karakteren og omfanget av behandlingen
* Konteksten og formålet med behandlingen
* Alvorlighet av den risiko behandlingen av personopplysninger medfører for de registrerte enkeltpersoners rettigheter

Relevant dokumentasjon for sikkerhetstiltakene skal gjøres tilgjengelig for Utleier på forespørsel.

### Bistand til Utleier

Leverandøren skal gi bistand slik at Utleier kan ivareta sitt eget ansvar etter avtalen med Leietaker og gjeldende lovgivning. Herunder skal Leverandøren bistå Utleier med å:

* Få på plass tekniske og organisatoriske tiltak som nevnt ovenfor
* Overholde varslingsplikt til tilsynsmyndigheter og registrerte personer som følge av eventuelle avvik når lovgivningen krever det
* Utføre vurdering av personvernkonsekvenser når lovgivningen krever det
* Utføre forutgående drøftelser med tilsynsmyndigheter når en vurdering av personvernkonsekvenser gjør det nødvendig

Bistanden skal utføres i den utstrekning det er nødvendig ut fra Utleiers behov, karakteren av behandlingen og informasjonen tilgjengelig for Utleier.

### Henvendelser fra registrerte personer

Leverandøren skal ha tekniske og organisatoriske tiltak for kunne bistå Utleier (i samråd med Leietaker) med å svare på henvendelser fra de enkeltpersoner som det er registrert opplysninger om, når disse utøver sine rettigheter etter lovgivningen.

### Kompensasjon for bistand

Bistand som fastsatt i denne databehandleravtalen, samt bistand i forbindelse med særskilte rutiner og instrukser pålagt av Utleier, skal kompenseres av Utleier etter medgått tid i samsvar med Leverandørens vanlige betingelser og timesatser, eller hvis slike ikke finnes; som nærmere avtalt mellom partene.

## Avvik og avviksmeldinger

Enhver bruk av personopplysninger i strid med etablerte rutiner, instrukser fra Utleier eller gjeldende lovgivning, samt eventuelle sikkerhetsbrudd, skal behandles som avvik.

Leverandøren skal ha rutiner og systematiske prosesser for å følge opp avvik. Disse skal omfatte gjenoppretting, tiltak for å lukke avvik og tiltak for å forhindre gjentagelse.

Leverandøren skal uten ugrunnet opphold varsle Utleier om ethvert sikkerhetsbrudd eller annet brudd på denne databehandleravtalen. Leverandøren skal gi Utleier all informasjon som er nødvendig for å sette Utleier og Leietaker i stand til å overholde gjeldende lovgivning og for at det skal være mulig for Leietaker å besvare henvendelser fra Datatilsynet.

## Konfidensialitet

Leverandøren har taushetsplikt om personopplysninger og annen konfidensiell informasjon, herunder, men ikke begrenset til, forretningshemmeligheter. Leverandøren skal sikre at alle som utfører arbeid for Leverandøren og som har tilgang til eller er involvert i behandling av personopplysninger (i) er underlagt taushetsplikt, og (ii) overholder forpliktelsene etter denne databehandleravtalen.

Taushetsplikten gjelder også etter opphør av databehandleravtalen.

## Sikkerhetsrevisjoner

Leverandøren vil jevnlig foreta sikkerhetsrevisjoner og kontroll av at forpliktelser i databehandleravtalen er etterlevd. Utleier skal på forespørsel få tilgang til rapporter som dokumenterer sikkerhetsrevisjoner og etterlevelse.

Leverandøren skal etter nærmere avtale muliggjøre og bidra ved revisjoner som gjennomføres av eller på oppdrag fra Utleier eller Leietaker. Revisjon av eventuelle underleverandører skal skje gjennom Leverandøren med mindre annet er særskilt avtalt.

## Bruk av underleverandører; overføring av personopplysninger utenfor EU/EØS

Enhver underleverandør av Leverandøren skal godkjennes skriftlig av Utleier etter samråd med Leietaker før underleverandøren kan behandle personopplysninger. En liste med godkjente underleverandører på avtaletidspunktet er vedlagt denne databehandleravtalen som vedlegg 2.

Dersom Leverandøren planlegger å skifte ut eller benytte ny underleverandør, skal Leverandøren skriftlig varsle Utleier senest [fire] uker før ny underleverandør starter behandling av personopplysninger. Varselet skal inneholde tilstrekkelig informasjon til at Utleier kan vurdere om godkjenning skal gis eller ikke. Utleier skal senest [fire] uker etter mottak av slikt varsel godkjenne underleverandøren. Godkjenning kan ikke nektes uten saklig og rimelig grunn. Manglende svar på slikt varsel innen fristen, anses som godkjenning. Dersom Utleier motsetter seg endring av underleverandør, vil Leverandøren forsøke å finne en annen løsning på behovet underleverandøren skal oppfylle. Om annen løsning ikke finnes, vil berørte tjenester til Utleier som forutsetter behandling av personopplysninger fra den nye underleverandøren, opphøre fra det tidspunkt den nye underleverandøren er planlagt å starte sin behandling.

Leverandøren kan ikke benytte underleverandør(er) som innebærer overføring av personopplysninger utenfor EU/EØS uten etter særskilt avtale med Utleier. Dersom Utleier og Leietaker godkjenner slik overføring, skal Utleier samarbeide med Leverandøren om å sikre lovligheten av slik overføring.

Dersom Leverandør skal engasjere en annen underdatabehandler for å utføre spesifikke behandlingsaktiviteter for Utleier, skal den andre underdatabehandleren være underlagt de samme forpliktelser og begrensninger som de som er pålagt Leverandøren i henhold til denne databehandleravtalen.

# Avtalebrudd

Ved brudd på denne databehandleravtalen skal de relevante bestemmelser om avtalebrudd i Avtalen gjelde.

# Varighet, avslutning av databehandleravtalen, endringer

Denne databehandleravtalen skal gjelde fra den er signert av begge parter og inntil Avtalen utløper, eller inntil Leverandørens behandling av personopplysninger på vegne av Utleier i henhold til denne databehandleravtalen opphører av annen grunn.

Ved avslutning av denne databehandleravtalen skal personopplysninger returneres i standardisert format på et elektronisk medium. Leverandøren skal først returnere og deretter slette alle personopplysninger. Leverandøren skal umiddelbart stanse behandling av personopplysningene ved utløpet av databehandleravtalen.

Som alternativ til å få returnert personopplysningene kan Utleier velge å instruere Leverandøren om at personopplysningene skal slettes, med mindre ufravikelig lovgivning forhindrer Leverandøren fra slik sletting. Leverandørens sletting skal dokumenteres.

Forpliktelsene etter pkt. 3.4 og 4 skal fortsette å gjelde etter databehandleravtalens opphør.

Partene skal revidere denne databehandleravtalen i den grad det er nødvendig for å tilfredsstille endringer i relevant lovgivning eller pålegg fra offentlig myndighet.

# Tvister og jurisdiksjon

Denne databehandleravtalen skal reguleres av norsk rett.

Avtalt verneting skal være det samme som etter Avtalen.

\*\*\*\*\*

*[sted], [dato]*

for Utleier for Leverandøren

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
[…] […]

[*Det må kontrolleres for hver avtale at disse kategoriene er riktige. Det er et lovkrav at riktige typer data angis i avtalen*.]

1. **Behandlingsaktiviteter og formål**

Leverandøren vil utføre følgende behandlingsaktiviteter for følgende formål:

* Adgangskontroll: Formålet med Leverandørens behandling av personopplysninger på vegne av Utleier er å bistå Leietaker med å sikre at ingen uvedkommende får adgang til Eiendommen, samt utføre driftsteknisk oppfølging og feilretting.
* Resepsjon: Formålet med Leverandørens behandling av personopplysninger på vegne av Utleier er å bistå Leietaker med resepsjonstjenester og registrering av besøkende.
* Parkering: Formålet med Leverandørens behandling av personopplysninger på vegne av Utleier er å bistå Leietaker med å administrere og kontrollere Leietakers parkeringsplasser til bruk for deres ansatte og/eller besøkende.
* Kameraovervåking: Formålet med Leverandørens behandling av personopplysninger på vegne av Utleier er å bistå Leietaker med å ivareta sikkerheten til Leietakers ansatte og besøkende, samt utføre driftsteknisk oppfølging og feilretting.
1. **Typer personopplysninger og kategorier av registrerte personer**

Leverandøren vil for hver opplistede behandlingsaktivitet behandle følgende typer personopplysninger om følgende kategorier av registrerte personer:

* Adgangskontroll:
	+ Ansatte hos Leietaker: Navn, tidspunkt og sted for adgang.
	+ Besøkende til lokalet: Navn, tidspunkt og sted for adgang.
* Resepsjon:
	+ Besøkende i bygget: Navn, telefonnummer, tidspunkt for besøk.
* Parkering:
	+ Ansatte hos Leietaker: Navn, telefonnummer, bilregistreringsnummer, tidspunkt for ankomst og avreise.
	+ Besøkende hos Leietaker: Bilregistreringsnummer, tidspunkt for ankomst og avreise.
* Kameraovervåking:
	+ Ansatte hos Leietaker: Videoopptak, herunder med bilde av person, bevegelser i og i nærheten av Eiendommen, tidspunkt for ankomst og avreise.
	+ Besøkende hos Leietaker: Videoopptak, herunder med bilde av person, bevegelser i og i nærheten av Eiendommen, tidspunkt for ankomst og avreise.
	+ Andre personer som oppholder seg i eller i nærheten av Eiendommen: Videoopptak, herunder med bilde av person, bevegelser i og i nærheten av Eiendommen, tidspunkt for ankomst og avreise.
		1. Godkjente underleverandører

Dette vedlegget spesifiserer hvilke underleverandører Leverandøren kan bruke.

|  |  |  |
| --- | --- | --- |
| Navn på underleverandør (fullt juridisk navn) | Dato for oppstart av bruk av under­leverandør | Lokasjon |
|  | (For eksempel: Fra avtalens oppstart) |  |

**VEILEDNING/KOMMENTARER**

Nedenfor følger veiledende tekst og kommentarer til databehandleravtalen. Formålet med vedlegget er å gi en nærmere forklaring av noen av bestemmelsene, og hjelpe partene med å vurdere tilpasninger av avtalen der det er nødvendig.

**Punkt 1 – Bakgrunn og formål**

I punkt 1 første avsnitt skal partene sette navn på virksomhetene, dato for avtalen, og spesifikasjon av hvilken eiendom avtalen gjelder.

I punkt 1 andre avsnitt beskrives formål og bakgrunn for avtalen. Dette bør justeres dersom beskrivelsen ikke passer fullt ut for den enkelte avtalen. Det gjøres særlig oppmerksom på at beskrivelsen av partenes roller (behandlingsansvarlig og databehandler) må endres dersom det er utleier selv som er behandlingsansvarlig, og ikke leietaker.

**Punkt 2 – Utleiers plikter**

I punkt 2 oppstilles den «opprinnelige» databehandlerens (utleiers) mest sentrale plikter, som utleier i sin avtale med leietaker må sikre at er overholdt. Merk at dette ikke er en komplett oversikt over alle plikter man har etter GDPR. Det er imidlertid de pliktene som er særlig viktig for Leverandør (som underdatabehandler) å vite at er oppfylt. Det anbefales alltid at man både som databehandler og behandlingsansvarlig har et internkontrollsystem og rutiner for å overholde kravene i GDPR.

**Punkt 3.1 – Instruks fra Utleier**

Utgangspunktet er at databehandleren (utleier) kun kan behandle personopplysninger i samsvar med en instruks fra den behandlingsansvarlige (leietaker), og GDPR artikkel 28 krever at dette skal fremgå av databehandleravtalen. Tilsvarende gjelder i forholdet mellom databehandler og underdatabehandler. Unntakene fra dette er først og fremst dersom (under)databehandler er pålagt i lov å gjøre visse aktiviteter, for eksempel å utlevere opplysninger på ordre fra politiet eller en domstol. Det er også viktig å understreke at (under)databehandler skal varsle den behandlingsansvarlige (eventuelt via databehandler), dersom de mottar en ulovlig instruks. Med andre ord kan ikke underdatabehandler uten videre gjemme seg bak at de «bare gjorde som utleier/leietaker sa». Partene bør derfor vurdere behovet for å avtalefeste konsekvensene som kan følge av en mulig ulovlig instruks.

**Punkt 3.2 - Informasjonssikkerhet**

Det er et grunnleggende krav i GDPR at informasjonssikkerheten skal stå i forhold til risikoen. Både den behandlingsansvarlige og (under)databehandleren har ansvar for informasjonssikkerheten. I en standardisert tjeneste er det imidlertid naturlig at (under)databehandleren tar hovedansvar for å vurdere hvilke tiltak som er best egnet til å håndtere risikoen tjenesten innebærer. Likevel må den behandlingsansvarlige ivareta personvernet til sine ansatte, kunder osv., og må derfor kunne vurdere ytterligere tiltak i noen tilfeller (se nærmere om bistand som kan kreves fra utleier i punkt 3.2.2).

Det kan derfor enkelte tilfeller være nødvendig å innta minimumskrav til informasjonssikkerhet som et vedlegg til databehandleravtalen. Dette vil for eksempel være tilfellet der det etter behandlingsansvarlig sin vurdering krever at det iverksettes ytterligere tiltak enn det databehandler har lagt opp til. Dersom slike krav fra behandlingsansvarlig krever økt innsats eller ressursbruk fra databehandlerens side, vil det kunne tas hensyn til i vederlaget.

**Punkt 3.3 - Avvik og avviksmeldinger**

Det er viktig at begge parter har rutiner for å hindre at feil skjer, og rutiner for hva som skal gjøres når feil skjer likevel. Feil i form av *brudd på personopplysningssikkerheten* kan føre til skade og ulempe for de enkeltpersoner som personopplysningene gjelder. Derfor må Leverandør i slike tilfeller gi informasjon til Utleier, slik at Utleier kan vurdere betydningen av bruddet. Det er viktig at leietaker gjør sin risikovurdering, ut fra sin virksomhet. Dersom data om besøksregistrering fra et advokatfirma eller legekontor kommer på avveie, kan det ha en helt annen betydning enn dersom data om besøksregistrering fra et bilverksted kommer på avveie. Det er derfor leietakers ansvar å vurdere om det enkelte brudd betyr at man må varsle Datatilsynet, enkeltpersonene som er berørt, og å foreta selve varslingen, mens databehandler og eventuelt (underdatabehandler) «kun» skal bistå.

**Punkt 3.6 – Bruk av underleverandører; overføring av personopplysninger utenfor EU/EØS**

I utgangspunktet kan ikke en databehandler benytte underdatabehandlere (underleverandører som behandler personopplysninger) uten spesifikk eller generell tillatelse fra den behandlingsansvarlige. For standardiserte tjenester, er det nødvendig med en generell tillatelse. Den behandlingsansvarlige (leietaker) må likevel kunne utøve en viss innflytelse, og i ytterste konsekvens legge ned veto. Derfor skal alltid bytte av underleverandører (som behandler personopplysninger) varsles, og avtalen fastlegger rutinen for å håndtere eventuelle protester.

Fireukers fristen kan tilpasses den enkelte avtale ved behov.

**Vedlegg 1 og 2 – detaljer om avtalen**

Partene bør i fellesskap fylle ut bilagene, og kontrollere at beskrivelsene der blir riktig for den enkelte avtale. Det er viktig at avtalen beskriver alle formålene, typer opplysninger, og hvem det behandles opplysninger om. For standardiserte tjenester, kan gjerne leverandøren ta hovedansvaret for at beskrivelsene blir riktig, siden de ikke kan avvike i stor grad fra kunde til kunde.