DATABEHANDLERAVTALE MELLOM UTLEIER OG LEIETAKER

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 leietaker er den behandlingsansvarlige, og utleier er databehandleren som behandler personopplysninger på vegne av leietaker. 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). Da oppstår det en databehandlerrelasjon, fordi utleier i forbindelse med disse aktivitetene vil behandle personopplysninger som leietaker i utgangspunktet har ansvaret for.

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](http://www.datatilsynet.no).

**BILAG […] TIL STANDARD LEIEAVTALE FOR NÆRINGSLOKALER/-BYGG**

**DATABEHANDLERAVTALE**

**MELLOM**

**UTLEIER OG LEIETAKER**

# Bakgrunn og formål

[…] **(Utleier**) og […] **(Leietaker)** har [dato] inngått avtale (**Leieavtalen**) om leie av [lokaler/bygg] i [adresse, gnr. og bnr.] **(Eiendommen).**

I forbindelse med drift av Eiendommen vil utleier få tilgang til og behandle personopplysninger, for eksempel gjennom adgangskontroll, resepsjonstjenester mv. Dette er personopplysninger som Utleier behandler på vegne av Leietaker. Denne databehandleravtalen regulerer Utleiers og Leietakers rettigheter og plikter i forbindelse med Utleiers behandling av personopplysninger på vegne av Leietaker. Leietaker er behandlingsansvarlig, og Utleier er databehandler for behandlingen av slike personopplysninger.

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

I tilfelle uoverensstemmelse mellom Leieavtalen og Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal Databehandleravtalen gis forrang.

# Leietakers plikter

Leietaker bekrefter at Leietaker:

* Har rettslig grunnlag for behandlingen av personopplysningene
* Har ansvaret for at personopplysningene er fullstendige og korrekte slik at Utleier blir i stand til å oppfylle sine plikter

Leietaker skal:

* + Svare på henvendelser fra de registrerte om behandlingen av personopplysninger
	+ I samråd med utleier vurdere nødvendigheten av tiltak som angitt i pkt. 3.2.1 og ved behov bestille slike tiltak fra Utleier.

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

# Utleiers plikter

## Instruks fra Leietaker

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

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

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

## Informasjonssikkerhet

### Vurdering av tiltak

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

Herunder skal Utleier 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 Utleier i samråd med Leietaker 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 Leietaker på forespørsel.

### Bistand til Leietaker

Utleier skal gi bistand slik at Leietaker kan ivareta sitt eget ansvar etter gjeldende lovgivning. Herunder skal Utleier bistå Leietaker 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 Leietakers behov, karakteren av behandlingen og informasjonen tilgjengelig for Utleier.

### Henvendelser fra registrerte personer

Utleier skal ha tekniske og organisatoriske tiltak for kunne bistå Leietaker med å svare på henvendelser fra de enkeltpersoner som det er registrert opplysninger om, når disse utøver sine rettigheter etter lovgivningen. Utleier skal umiddelbart videresende til Leietaker forespørsler eller klager som Utleier eventuelt mottar fra den registrerte.

### Kompensasjon for bistand

Bistand som fastsatt i denne databehandleravtalen, samt bistand i forbindelse med særskilte rutiner og instrukser pålagt av Leietaker, skal kompenseres av Leietaker etter medgått tid i samsvar med Utleiers 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 Leietaker eller gjeldende lovgivning, samt eventuelle sikkerhetsbrudd, skal behandles som avvik.

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

Utleier skal uten ugrunnet opphold, og senest innen 24 timer, varsle Leietaker om ethvert sikkerhetsbrudd eller annet brudd på denne databehandleravtalen. Utleier skal gi Leietaker all informasjon som er nødvendig for å sette Leietaker i stand til å overholde gjeldende lovgivning og for at det skal være mulig for Leietaker å besvare henvendelser fra Datatilsynet. Ved behov, kan informasjon gis trinnvis.

Det er Leietakers ansvar å melde avvik til Datatilsynet og registrerte personer i henhold til gjeldende lovgivning.

Melding til Leietaker om brudd på personopplysningssikkerheten bør inneholde en beskrivelse av:

* arten av bruddet, herunder kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
* de berørte registrertes identitet,
* navn og kontaktinformasjon til Personvernombudet eller et annet kontaktpunkt hos Utleier for ytterligere innhenting av informasjon,
* de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
* tiltak som er truffet eller foreslått for å håndtere bruddet på personopplysningssikkerheten, herunder tiltak for å redusere eventuelle skadevirkninger,
* annen informasjon som kreves for at Leietaker kan overholde gjeldende personvernregler.

Informasjon som nevnt i punktene ovenfor skal gis uten ugrunnet opphold, men den kan gis trinnvis i den grad det er nødvendig.

## Konfidensialitet

Utleier har taushetsplikt om personopplysninger og annen konfidensiell informasjon, herunder, men ikke begrenset til, forretningshemmeligheter. Utleier skal sikre at alle som utfører arbeid for Utleier 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

Utleier vil jevnlig foreta sikkerhetsrevisjoner og kontroll av at forpliktelser i databehandleravtalen er etterlevd. Utleier skal dokumentere og gjøre tilgjengelig for Leietaker informasjon som er nødvendig for å påvise etterlevelse av databehandleravtalen og gjeldende personvernregler og skal uoppfordret varsle Leietaker om sårbarheter av betydning som avdekkes gjennom sikkerhetsrevisjoner.

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

Hver av partene dekker sine egne kostnader forbundet med en revisjon.

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

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

Dersom Utleier planlegger å skifte ut eller benytte ny underleverandør, skal Utleier skriftlig varsle Leietaker senest 60 dager før ny underleverandør starter behandling av personopplysninger. Varselet skal inneholde tilstrekkelig informasjon til at Leietaker kan vurdere om godkjenning skal gis eller ikke. Leietaker skal senest 60 dager etter mottak av slikt varsel godkjenne underleverandøren. Godkjenning kan ikke nektes uten saklig og rimelig grunn. Manglende svar på slikt varsel innen fristen, anses ikke som godkjenning. Dersom Leietaker motsetter seg endring av underleverandør, vil Utleier forsøke å finne en annen løsning på behovet underleverandøren skal oppfylle. For eksempel, videreføre avtale med eksisterende leverandør, finne alternative leverandører eller undersøke om tekniske eller organisatoriske tiltak kan gjennomføres slik at ny leverandør oppfyller Leietakers krav til personvern. Om annen løsning ikke finnes, vil berørte tjenester til Leietaker som forutsetter behandling av personopplysninger fra den nye underleverandøren, opphøre fra det tidspunkt den nye underleverandøren er planlagt å starte sin behandling.

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

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

# Avtalebrudd

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

# Varighet, avslutning av databehandleravtalen, endringer

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

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

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

\*\*\*\*\*

*[sted], [dato]*

for Utleier for Leietaker

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

[*Det må kontrolleres for hver avtale at disse kategoriene er riktige. Det er et lovkrav at riktige typer data angis i avtalen*. *Aktivitetene under er eksempler og må justeres der det er nødvendig.*]

* **Behandlingsaktiviteter og formål**

Utleier vil utføre følgende behandlingsaktiviteter for følgende formål:

Adgangskontroll:

Beskrivelse av formålet: [Formålet med Utleiers behandling av personopplysninger på vegne av Leietaker er å bistå Leietaker med å sikre at ingen uvedkommende får adgang til Eiendommen, samt utføre driftsteknisk oppfølging og feilretting.]

Beskrivelse av behandlingen: [Hver ansatt har et unikt adgangskort som gir dem tilgang til bestemte soner i bygget. Personopplysninger behandles i forbindelse med produksjon av adgangskort/brikker som er knyttet til enkeltpersoner og ved at det genereres logger over bruk av kortene på ulike passeringspunkter. For vanlig kortbruk innenfor kjernetid slettes logg fortløpende. Kortbruk med kode (typisk utenfor kjernetid) slettes etter maksimalt XX dager. Sletting skjer ved at logger overskrives.]

Besøksregistrering:

Beskrivelse av formålet: [Formålet med Utleiers behandling av personopplysninger på vegne av Leietaker er å bistå med å sikre effektiv besøksavvikling, ivareta ansattes sikkerhet ved å gi Leietaker kontroll på hvem som ferdes i bygget og ivareta besøkenes sikkerhet i tilfelle av brann eller andre hendelser som krever evakuering av bygget.]

Beskrivelse av behandlingen: [Ansatte forhåndsregistreres fra en liste som lastes inn og lagres i besøksregistreringssystemet. Ved ankomst, registrer besøkende seg i informasjonskiosken/resepsjonen og oppgir hvem de besøker. Besøksmottakeren får deretter et varsel om at gjesten har ankommet. Standard rutine er at informasjon om besøket slettes ved midnatt den dagen besøket har funnet sted.]

Kameraovervåking:

Beskrivelse av formålet: [Formålet med Utleiers behandling av personopplysninger på vegne av Leietaker er å bistå Leietaker å kunne avdekke forsøk på og gjennomføring av sikkerhetstruende virksomhet mot Leietakers skjermingsverdige verdier, ansatte og besøkende, samt utføre driftsteknisk oppfølging og feilretting. .]

Beskrivelse av behandlingen: [Bygget har kameraer plassert innenfor begrensede områder. Opptak fra kameraene lagres i en database og blir automatisk slettet etter 7 dager.]

Parkering:

Beskrivelse av formålet: [Formålet med Utleiers behandling av personopplysninger på vegne av Leietaker er å bistå Leietaker i å administrere og kontrollere Leietakers parkeringsplasser til bruk for deres ansatte og/eller besøkende.]

Beskrivelse av behandlingen: [Besøkende registrerer seg i parkeringsappen/resepsjonen. Opplysningene blir automatisk slettet ved midnatt den dagen besøket har funnet sted.]

* **Typer personopplysninger og kategorier av registrerte personer**

Utleier 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.
* Andre med adgang til lokalet: Navn, tidspunkt og sted for adgang.

Besøksregistrering:

* Besøkende i bygget: Navn, telefonnummer, tidspunkt for besøk.
* Ansatte: Navn, Avdeling, telefonnummer/e-postadresse

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.

Parkering:

* + Ansatte hos Leietaker: Navn, telefonnummer, bilregistreringsnummer, tidspunkt for ankomst og avreise.
	+ Besøkende til Leietaker: Bilregistreringsnummer, tidspunkt for ankomst og avreise.
		1. Godkjente underleverandører

Dette vedlegget spesifiserer hvilke underleverandører Utleier kan bruke.

|  |  |  |  |
| --- | --- | --- | --- |
| Navn på underleverandør (fullt juridisk navn) | Dato for oppstart av bruk av under­leverandør | Lokasjon | Beskrivelse av aktivitet/type behandling |
| [Underleverandør AS] | [Avtalens oppstart] | [Sverige] | [leverandør av database, lagrer og behandler video fra kameraovervåkning] |

**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.

**Punkt 2 – Leietakers plikter**

I punkt 2 oppstilles leietakers mest sentrale plikter i rollen som behandlingsansvarlig. 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 utleier (databehandler) å vite at er oppfylt. Det anbefales alltid at man som behandlingsansvarlig har et internkontrollsystem og rutiner for å overholde kravene i GDPR.

**Punkt 3.1 – Instruks fra Leietaker**

Utgangspunktet er at databehandleren kun kan behandle personopplysninger i samsvar med en instruks fra den behandlingsansvarlige, og GDPR artikkel 28 krever at dette skal fremgå av databehandleravtalen. Unntakene fra dette er først og fremst dersom databehandler (utleier) 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 databehandler skal varsle den behandlingsansvarlige, dersom de mottar en ulovlig instruks. Med andre ord kan ikke utleier uten videre gjemme seg bak at de «bare gjorde som 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 databehandleren har ansvar for informasjonssikkerheten. I en standardisert tjeneste er det imidlertid naturlig at 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 utleier i slike tilfeller gi informasjon til leietaker, slik at leietaker kan vurdere betydningen av bruddet for sine ansatte, kunder, gjester, osv. 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.

**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.

**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 utleier ta hovedansvaret for at beskrivelsene blir riktig, siden de ikke kan avvike i stor grad fra leietaker til leietaker.