GDPR
FOR EIENDOMSSELSKAPER

NORSK
EIENDOM

Forord

EUs nye personvernregler (GDPR) stiller strenge krav til alle som håndterer personvernopplysninger. Dette gjelder også bedrifter i eiendomsbransjen. For det første stilles det krav til bedriftens eget internkontrollsystem om å dokumentere hvordan personopplysninger der håndteres. Videre vil det på områder som kundeoppfølging, adgangskontroll i bygg og mannskapslister på byggeplass være nødvendig å dokumentere hvordan personopplysninger i disse aktivitetene håndteres.

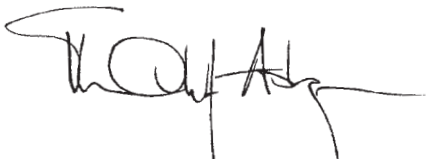
Norsk Eiendom har utarbeidet denne veilederen for å gi en forståelse av hvilke plikter og krav som gjelder for eiendomsbransjen. Vi har også fått utarbeidet ulike maler for nødvendige avtaler som følger av forpliktelsene. Disse ligger tilgjengelig på våre nettsider.

Gjennom økt bruk av sensorer, digitalisering og individuelle, smarte løsninger i vår bransje vil også mengden og type informasjon øke kraftig. Vi må derfor anta at bransjens forpliktelser innenfor personvern vil øke fremover.

Norsk Eiendom kan ikke gå god for at veilederen beskriver alle forhold som omfattes av GDPR. Ut over de forhold som er beskrevet, vil veilederen kunne gi den enkelte bedrift idéer om hva de selv bør sjekke opp mot GDPR.

Veilederen er utarbeidet i samarbeid med Advokatfirmaet Føyen Torkildsen AS.

Majorstuen, mai 2018



Thor Olaf Askjer
Administrerende direktør
Norsk Eiendom

Veileder for GDPR i eiendomsbransjen

1. INTRODUKSJON

Den 25. mai 2018 trådte EUs nye personvernforordning (The General Data Protection Regulation, kjent som «GDPR») i kraft i EU. Det nye regelverket for personvern vil gjennom EØS-avtalen også få virkning i Norge. Den nye personopplysningsloven som vil gjøre GDPR til norsk rett er ventet å tre i kraft i Norge i løpet av juli 2018. Regelverket vil gjelde for alle norske selskaper og vil dermed også gi eiendomsbransjens aktører nye og mer omfattende plikter enn tidligere ved behandling av personopplysninger.

Regelverket vil blant annet få anvendelse på enhver form for registrering og bruk av personopplysninger om selskapers ansatte og andre fysiske personer. Videre må tilbydere av for eksempel adgangskontrollsystemer, og aktører som fører elektroniske mannskapslister, sørge for å innføre nye rutiner for å etterleve kravene i det nye regelverket.

2. SENTRALE BEGREPER

2.1. Personopplysninger

GDPR gjelder når eiendomsaktører påtar seg eller tilbyr tjenester som innebærer behandling av personopplysninger. Med personopplysninger menes all informasjon som direkte eller indirekte kan føres tilbake til enkeltpersoner. Med behandling av personopplysninger menes enhver bruk av opplysningene (registrering, sammenstilling, utlevering osv.).

Eksempler på når behandling av personopplysninger er aktuelt i eiendomsbransjen kan være i forbindelse med forvaltningstjenester som adgangskontroll, nøkkelkort, kantineregistrering, vaktmestertjenester, parkeringstjenester og kameraovervåkning, ved administrasjon av kundeforhold, og ved føring av mannskapslister på byggeplassen. Det er viktig å merke seg at også behandling av personopplysninger om selskapets egne ansatte vil være underlagt GDPR.

2.2. Roller

GDPR opererer med to sentrale begreper; behandlingsansvarlig og databehandler. En behandlingsansvarlig er det selskapet som bestemmer formålet med behandlingen og hvordan personopplysningene skal behandles. Databehandler er «medhjelperen» til behandlingsansvarlig og behandler personopplysninger kun på vegne av behandlingsansvarlig, uten å ha noen selvstendig råderett over personopplysningene.

2.3. Behandlingsgrunnlag

Behandling av personopplysninger krever et gyldig rettslig grunnlag for slik behandling, et såkalt behandlingsgrunnlag. Dette gjelder uavhengig av om man har rollen som behandlingsansvarlig eller databehandler. For behandlingsansvarlige kan et slikt grunnlag være i form av enten samtykke, lov, forfølgning av en berettiget interesse, eller at behandlingen av personopplysninger er nødvendig for å oppfylle en avtale med personen personopplysningen gjelder.

For databehandleren må gyldig grunnlag for behandling av personopplysninger etableres gjennom en såkalt databehandleravtale med den behandlingsansvarlige. Det er den behandlingsansvarliges ansvar å sørge for et gyldig behandlingsgrunnlag mot den enkeltpersonen personopplysningene gjelder.

Det er viktig å merke seg at det ikke er anledning til å behandle personopplysninger i større utstrekning enn det som følger av behandlingsgrunnlaget. I eiendomsbransjen vil behandlingsgrunnlaget i de fleste praktiske tilfeller basere seg på lov eller avtale. Behandlingen av personopplysninger må da begrenses til det som følger av den relevante lovbestemmelsen, eller det som er nødvendig for å oppfylle den aktuelle avtalen.

3. PLIKT TIL INTERNKONTROLL I VIRKSOMHETEN

GDPR vektlegger internkontroll og ansvarlighet hos virksomhetene. Dette betyr at enhver behandlingsansvarlig eller databehandler som behandler personopplysninger plikter å dokumentere hvordan den etterlever kravene i GDPR. Herunder må det dokumenteres at virksomhetene har systemer for å sikre etterlevelse av regelverket. Dokumentasjon av behandlingen av personopplysninger protokolleres gjerne i et internkontrolldokument.

Virksomhetene må etablere slik internkontroll og rutiner for hvordan regelverket og deres forpliktelser etter databehandleravtalene skal etterleves. Dette krever en oversikt over hvor personopplysninger behandles i virksomheten, slik at de forpliktelser virksomheten er underlagt kan identifiseres, og eventuelle avvik kan lukkes.

4. PLIKTER I ULIKE TYPETILFELLER I EIENDOMSBRANSJEN

4.1. Ulike roller

Som nevnt stiller GDPR strengere krav til behandlingen av personopplysninger enn tidligere regelverk. Aktørene i eiendomsbransjen vil ha ulike roller etter GDPR. Dette avhenger av om virksomheten er utbygger, entreprenør, utleier eller forvalter, og om leietaker er næringsdrivende eller en privatperson. Det stilles ulike krav til de forskjellige rollene, men gjennomgående for regelverket er at det stilles strenge krav til ansvarlighet og internkontroll hos virksomheten.

4.2. Føring av kundeopplysninger mv.

Føring av ulike typer kundeopplysninger er relevant for de fleste virksomheter. Ved registrering og bruk av kundeopplysninger som inneholder opplysninger om enkeltpersoner, kommer GDPR til anvendelse. Eksempler kan være registre over kontaktpersoner hos virksomhetens bedriftskunder og offentlige kunder, registre over privatpersoner som er eksisterende eller potensielle kunder, f.eks. interessentlister over potensielle boligkjøpere, osv. GDPR stiller krav til behandlingen av slike personopplysninger. Som nevnt i punkt 2.3 stilles det blant annet krav til at den behandlingsansvarlige eller databehandler har et gyldig behandlingsgrunnlag.

Behandlingsgrunnlaget vil typisk variere avhengig av om den aktuelle kunden er en privatperson eller en virksomhet. Ved behandling av opplysninger om kunder som er privatpersoner, vil det relevante behandlingsgrunnlaget i de fleste tilfeller være innhenting av samtykke fra den det gjelder. For at det skal eksistere et gyldig samtykke og dermed et gyldig behandlingsgrunnlag, må den personopplysningene omhandler ha gitt et uttrykkelig samtykke til hvert formål opplysningene brukes til. Ved utforming av samtykkene er det krav om at det skal fremkomme klart hvem den behandlingsansvarlige er og hva det samtykkes til. Det er i tillegg viktig at den behandlingsansvarlige kan dokumentere at det er gitt et gyldig samtykke fra den det gjelder. Samtykket kan når som helst trekkes tilbake, og i så fall bortfaller samtykket som behandlingsgrunnlag.

Ved behandling av opplysninger om enkeltpersoner tilknyttet en bedriftskunde eller en offentlig kunde, vil det relevante behandlingsgrunnlaget ofte være at behandlingen er nødvendig for å forfølge en berettiget interesse som virksomheten har i det aktuelle tilfellet. Det kan f.eks. dreie seg om registrering av kontaktpersoner oppgitt av en bedrift, og utsendelse av relevant kundeinformasjon til slike kontaktpersoner. Det er ofte upraktisk å innhente samtykke fra disse personene i slike tilfeller, fordi det er virksomheten og ikke enkeltpersonene kundeforholdet relaterer seg til. Grunnlaget om forfølging av en berettiget interesse vil ofte kunne brukes i tilfeller som dette så lenge den aktuelle handlingen ikke går nevneverdig utover personverninteressene til den opplysningene gjelder.

Uavhengig av hva som er behandlingsgrunnlaget stilles det krav til hvor lenge det er anledning til å beholde kundeopplysninger i virksomhetens databaser. Opplysningene kan beholdes så lenge det er nødvendig for å oppfylle formålet opplysningene ble innhentet for, og kun så lenge det fortsatt eksisterer et gyldig behandlingsgrunnlag. Når formålet med behandlingen faller bort, eller når det relevante behandlingsgrunnlaget bortfaller (f.eks. ved at et samtykke trekkes tilbake eller en avtale med behandlingsansvarlig opphører), skal opplysningene slettes. Unntak fra dette gjelder kun dersom virksomheten ved lov er pålagt å beholde opplysningene.

4.3. Særlig om bruk av kundeopplysninger til elektronisk markedsføring

Kundeopplysninger vil ofte være interessante å bruke til utsendelse av ulike typer elektronisk markedsføring via e-post, som f.eks. nyhetsbrev, informasjon om produkter og tjenester osv. Også i disse tilfellene gjelder reglene i GDPR som redegjort for ovenfor.

Reglene i GDPR suppleres i dette tilfellet av reglene i markedsføringsloven. Ved utsendelse av markedsføringshenvendelser til personlige e-postadresser, er det viktig å være klar over at markedsføringsloven i utgangspunktet forbyr å rette markedsføringshenvendelser til fysiske personer uten at mottakeren har gitt forutgående samtykke til dette. Forbudet gjelder enten den personlige e-postadressen er privat eller tilknyttet en virksomhet, så lenge den er knyttet til en enkeltpersons navn. Enhver henvendelse i forbindelse med en næringsdrivendes virksomhet vil være å anse som «markedsføring» i denne sammenheng, selv om den enkelte henvendelse ikke bærer preg av direkte «salgsfremstøt» e.l.

Markedsføringsloven inneholder imidlertid et viktig praktisk unntak fra dette forbudet: Kravet om forhåndssamtykke gjelder ikke i eksisterende kundeforhold der den næringsdrivende avtaleparten har mottatt kundens, eller kundens kontaktpersons, e-postadresse i forbindelse med kundeforholdet. Markedsføringen kan bare gjelde den næringsdrivendes egne varer, tjenester eller andre ytelser tilsvarende dem som kundeforholdet bygger på. Også annen informasjon som er relevant for kundeforholdet vil kunne sendes ut. Når e-postadressen samles inn, og ved hver enkelt senere markedsføringshenvendelse, skal mottakeren enkelt og gebyrfritt gis anledning til å reservere seg mot slike fremtidige henvendelser.

4.4. Føring av mannskapslister

På en byggeplass stilles det eksempelvis krav etter byggherreforskriften om at byggherren skal føre elektroniske oversiktslister (såkalte «mannskapslister») over hvem som oppholder seg på byggeplassen. Siden byggherren er ansvarlig for at slike lister føres, vil byggherren være behandlingsansvarlig for registreringen av personopplysninger som inngår i listene. Dette krever som nevnt et gyldig behandlingsgrunnlag. I dette tilfellet vil det være bestemmelsen i byggherreforskriften som pålegger en slik plikt som utgjør behandlingsgrunnlaget.

Det er imidlertid vanlig bransjepraksis at byggherren viderefører ansvaret for å føre mannskapslister til entreprenøren. Entreprenøren vil da få rollen som databehandler på vegne av byggherren. For at entreprenøren skal kunne registrere disse personopplysningene, må det derfor inngås en databehandleravtale mellom byggherren og entreprenøren. Denne avtalen skal reflektere de kravene som byggherren er underlagt når det gjelder behandling av personopplysningene. Entreprenøren skal kun behandle opplysningene i den utstrekning og på de måter som følger av databehandleravtalen.

4.5. Administrering av adgangskontrollsystemer

Et annet eksempel på et tilfelle hvor GDPR vil påvirke eiendomsbransjen, er i forbindelse med adgangskontrollsystemer til fast eiendom. Hvis det er utleier som benytter adgangskontrollsystemer for å føre egen kontroll med at ikke uvedkommende får tilgang til utleiers eiendom, er utleier å anse som behandlingsansvarlig for de personopplysninger som registreres.

Hvis utleier på den annen side registrerer opplysninger om nøkkelkort som er nødvendige for å gi den enkelte av leietakers ansatte riktig adgang til de lokaler leietaker leier, er utleier å anse som databehandler på vegne av leietaker som behandlingsansvarlig. Avgjørende for skillet er som nevnt hvilken av partene som bestemmer formålet med den aktuelle behandlingen og hvilke hjelpemidler som skal brukes til dette.

Den praktiske hovedregel vil være at utleier opptrer som databehandler for å administrere adgangskontrollsystemet på vegne av leietaker. Leietakeren vil da være behandlingsansvarlig overfor sine ansatte, og utleier må kun behandle de personopplysningene som registreres i henhold til databehandleravtalen som må inngås mellom leietaker og utleier.

Norsk Eiendom har utarbeidet en standard databehandleravtale for bruk av elektroniske nøkkelkort, som følger med som et valgfritt bilag til Norsk Eiendoms standard leieavtale for næringslokaler/-bygg.

I slike tilfeller hvor utleier har tilgang til opplysningene, men begrenset rett til å bruke dem, kan det være at utleier ønsker å benytte seg av personopplysningene til egen bruk. Dette krever i så fall at utleier selv kan ta rollen som behandlingsansvarlig, med selvstendig råderett over personopplysningene.

Et eksempel på dette kan være i bygg med omfattende bruk av sensorløsninger og andre former for overvåkning, hvor utleier har interesse av å benytte slike sensordata for effektivisering av ressursene i bygget. Slike sensordata vil ofte være å anse som personopplysninger. Det blir dermed viktig å kartlegge hvor det behandles personopplysninger og for hvilket formål slik behandling skal skje. Deretter må det kartlegges hvorvidt utleier kan påvise et gyldig behandlingsgrunnlag for slik behandling. Dette vil kreve en konkret vurdering i hvert enkelt tilfelle.

4.6. Norsk Eiendoms standard databehandleravtaler

Norsk Eiendom har utarbeidet følgende standard databehandleravtaler for typetilfellene som er nevnt i pkt. 4.4 og 4.5 ovenfor:

1) Databehandleravtale mellom leietaker og utleier for bruk av elektroniske nøkkelkort. Denne følger med som et valgfritt bilag til Norsk Eiendoms standard leieavtale for næringslokaler/-bygg.

2) Databehandleravtale mellom utleier og underleverandør (f.eks. et vaktselskap) der utleier benytter en underleverandør i forbindelse med bruk av elektroniske nøkkelkort. Denne benyttes for å speile forpliktelsene utleier har etter avtalen ovenfor, videre til underleverandøren.

3) Databehandleravtale mellom byggherre og entreprenør der entreprenøren påtar seg å føre mannskapslister etter byggherreforskriften på byggherrens vegne.

Standardavtalene er tilgjengelige for Norsk Eiendoms medlemmer og kan lastes ned fra Norsk Eiendoms nettsider. Det er viktig å merke seg at standardavtalene kun utgjør maler for de nevnte typetilfeller. Avtalepartene må i hvert enkelt tilfelle kontrollere at beskrivelsene i avtalene treffer, samt fylle ut nærmere beskrivelser der avtalene gir anvisning på det.

5. ØVRIGE PLIKTER

I tillegg til de temaene som hittil er nevnt, er det verdt å merke seg at GDPR også stiller en del øvrige krav som eiendomsaktører må være bevisst på når det gjelder behandling av personopplysninger. Blant annet stilles det krav til hvilken informasjon som skal formidles til enkeltindividene, krav til å gi enkeltindividene rett til å kreve innsyn, retting eller sletting av de opplysninger som er registrert om vedkommende, samt krav til å melde brudd på datasikkerhet til Datatilsynet. Dette er kun noen av de mest sentrale forpliktelsene etter GDPR. Aktørene i eiendomsbransjen må gjøre en konkret vurdering av i hvilken grad disse og øvrige krav etter GDPR vil treffe deres virksomhet.

Foto: Thor Olaf Askjer • Design: www.jensendesign.no

June 2018

NORSK EIENDOM

Kontaktinformasjon:
www.noeiendom.no
Telefon: 23 08 80 00
E-post: firmapost@noeiendom.no

Postadresse:
Norsk Eiendom
Postboks 7185 Majorstuen
0307 Oslo

Besøksadresse:
Næringslivets Hus
Middelthunsgate 27
Majorstuen, Oslo