UTKAST-Bransjenorm for behandling av personopplysninger i eiendomsmeglingsbransjen

INNHOLD

UTKAST

1 INNLEDNING

1.1 BAKGRUNN OG FORMÅL

Eiendomsmegling er en profesjonell prosess for kjøp og salg av eiendom etter gjeldende lover og forskrifter. Eiendomsmeglingsbransjen har en viktig rolle i norsk økonomi og for norske boligeiere. En eiendomsmegler skal sørge for at transaksjonen skjer på en sikker og trygg måte både for selger og kjøper. For å kunne utføre sine oppgaver vil det bli behandlet en rekke personopplysninger, både om kjøper, selger og (mulige) interessenter.
Det er imidlertid viktig at personopplysningene behandles i henhold til gjeldende regelverk og at brukere av eiendomsmeglingstjenester har tillit til at foretakene behandler personopplysninger på en lovlig og trygg måte.

Formålet med denne bransjenormen er å etablere en felles praksis for behandling av personopplysninger i tilknytning til eiendomsmegling, samt sikre at personvernregelverket følges av Eiendom Norges medlemsforetak.

Bransjenormen gjelder all behandling av personopplysninger og informasjon som foretas i forbindelse med kjøp og salg av bolig. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-verktøy er også inkludert.

Bransjenormen omhandler ikke behandling av personopplysninger om ansatte som foregår som en del av personaladministrasjon.

Alle som utfører arbeid på vegne av Eiendom Norges medlemsbedrifter skal gjøre seg kjent med dette dokumentet og etterleve de krav som her er beskrevet. Det er den enkelte ansattes plikt til å gjøre det som ligger innenfor rammene av den enkeltes stilling for å ivareta personvernet til ansatte, kunder og foretakenes samarbeidspartnere.

1.2 DEFINISJONER

Med **personopplysninger** menes enhver opplysning om en identifisert eller identifiserbar fysisk person som direkte eller indirekte kan identifiseres, særlig ved hjelp av identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Med **behandling** menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring

Med **behandlingsansvarlig** menes en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

Med **databehandler** menes en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den

UTKAST

behandlingsansvarlige.

For øvrige definisjoner vises det til vedlegg 1.

2 KRAV OG PLIKTER SOM FØLGE AV BEHANDLING AV PERSONOPPLYSNINGER

Behandling av personopplysninger i eiendomsmeglingsbransjen reguleres av lov om behandling av personopplysninger (personopplysningsloven). Loven er gitt i medhold av EUs personvernforordning, General Data Protection regulation (GDPR). Bestemmelsene i personopplysningsloven gjelder for behandling av personopplysninger, om ikke annet følger av en særskilt lov som regulerer behandlingsmåten. Eiendomsmeglingsbransjen er underlagt følgende særlovgivning som regulerer behandling av personopplysninger[1]:

- Eiendomsmeglingsloven
- Eiendomsmeglingsforskriften
- Regnskapsloven
- Bokføringsloven
- Avhendingslova
- Markedsføringsloven
- Hvitvaskingsloven

2.1 FORHOLDET MELLOM BRANSJENORMEN OG ANDRE REGLER

Bransjenormen er hjemlet i GDPR artikkel 40 og gir veiledning til etterlevelse av regelverket basert på eiendomsmeglingsbransjens særlige utfordringer. Bransjenormen skal styrke personvernet og gjøre det lettere for eiendomsmeglingsvirksomheter å etterleve personvernregelverket. Bransjenormer gir ikke grunnlag for å behandle personopplysninger i strid med norsk rett, herunder GDPR, rettsavgjørelser, vedtak fra Datatilsynet mv.

Denne bransjenormen må videre ses i sammenheng med Bransjenorm for markedsføring av bolig (senere veileder for markedsføring av boliger), samt bransjenorm for direkte markedsføring, som er utarbeidet av Federation of Direct Marketing. Ved eventuell konflikt mellom bransjenormen og norsk lov og forskrift, skal bransjenormen vike.

3 ROLLER OG ANSVAR

Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personopplysninger behandles i henhold til personvernprinsippene slik de følger av GDPR artikkel 5. nr.1, samt at kravene i denne bransjenormen etterleves.

Den behandlingsansvarlige skal påse at det er implementert nødvendig internkontroll etter personvernregelverket og at virksomheten har etablert tilfredsstillende informasjonssikkerhet.

Det avgjørende for vurdering av hvilket selskap som er å anse som behandlingsansvarlig, vil være hvilket selskap som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

[1] Oversikten er ikke uttømmende

UTKAST

I utgangspunktet vil det være det enkelte eiendomsmeglerforetaket (juridisk foretak) som behandler personopplysninger om potensielle kunder, boligkjøper og boligselger som er behandlingsansvarlig for disse personopplysningene.

3.1 SÆRLIG OM BEHANDLINGSANSVAR I KONSERN OG FRANCHISEFORETAK

Dersom et eiendomsmeglerforetak er organisert som et morselskap med flere datterselskap, vil det i utgangspunktet være det enkelte datterselskapet som er behandlingsansvarlig for personopplysninger datterselskapet behandler. Det samme gjelder franchiseforetak hvor man har en franchisegiver og flere franchisetakere.

I enkelte slike tilfeller kan det imidlertid tenkes situasjoner hvor behandlingsansvaret plasseres hos morselskapet eller franchisegiver. Dette må i så fall avtales i et rettslig bindende dokument som får anvendelse på og håndheves av hvert berørte foretak i konsernet/franchisen, herunder deres ansatte. Denne avtalen må også klart regulere hvilke roller og ansvar de ulike foretakene har knyttet til behandlingen av personopplysninger.

Hvert enkelt foretak må ta stilling til hvor behandlingsansvaret er plassert. Dette er viktig ettersom det har en rekke praktiske konsekvenser for plikter for behandlingsansvarlige, og rettighetene til den/de registrerte. Eksempelvis vil en person ha rett til innsyn i opplysninger som en behandlingsansvarlig har registrert. Hvilke opplysninger det da skal gis innsyn i, avhenger av hvem som er behandlingsansvarlig. Videre vil utlevering av personopplysninger fra en behandlingsansvarlig til en annen, kreve at det foreligger et rettslig grunnlag for slik overføring. Dersom behandlingsansvaret er plassert i hvert enkelt foretak, kreves det derfor et rettslig grunnlag dersom andre foretak i konsernet/franchisen, herunder morselskap/franchisegiver, skal få utlevert personopplysningene.

3.2 PERSONVERNOMBUD

Foretakene anbefales å utpeke et personvernombud som kan bistå foretakene og deres kunder i spørsmål om personvern, samt oppfølging av internkontroll.

GDPR åpner for at det i et konsern kan opprettes én personvernrådgiver, forutsatt at alle virksomhetene har enkel tilgang til vedkommende. Personvernrådgiveren kan være ansatt hos foretaket eller leies inn gjennom en tjenesteavtale.

4 GRUNNPRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER I EIENDOMSMEGLINGSBRANSJEN

All behandling av personopplysninger som foretas av eiendomsmeglingsforetakene skal foretas under hensyn til personvernprinsippene slik de fremgår av GDPR artikkel 5:

- Lovlighet, rettferdighet og gjennomsiktighet

Personopplysninger skal behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til den registrerte. Foretakene skal forsikre seg om at de har rettslig grunnlag for alle behandlinger av personopplysninger som foretas. Foretakene skal videre informere alle berørte personer om behandlingen av personopplysninger som foretas, herunder hva

UTKAST

personopplysningene skal brukes til, hvor personopplysningene er hentet fra, og hvor lenge personopplysningene vil bli lagret. De som er registrerte i foretakenes systemer må også informeres om hvilke rettigheter de har, og hvordan de kan gjøre disse rettighetene gjeldende.

- Formålsbegrensning

Personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene. Det er ikke tillatt å samle inn, eller på annen måte behandle personopplysninger uten å ha et formål. Formålet med den aktuelle behandlingen må videre passe inn med det rettslige grunnlaget for behandlingen. Dersom personopplysninger er samlet inn for ett formål, skal de ikke brukes til andre, nye formål, dersom de nye formålene er uforenlige med det opprinnelige formålet. Eksempelvis er det ikke anledning til å bruke visningslister til å ringe de registrerte for å tilby foretakets tjenester. Dersom personopplysninger er samlet inn for å kunne inngå eller oppfylle en avtale som den registrerte er del av, skal personopplysningene ikke benyttes til markedsføringsformål med mindre den registrerte samtykker til dette.

- Dataminimering

Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for. Dersom det ikke er nødvendig å behandle en bestemt type personopplysninger for å oppnå dette aktuelle formålet, vil det heller ikke være lovlig å gjøre det.

- Riktighet

Personopplysninger skal være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller korrigeres.

- Lagringsbegrensning

Personopplysninger skal lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for.

- Integritet og fortrolighet

Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.

5 NÆRMERE OM BEHANDLING AV PERSONOPPLYSNINGER I EIENDOMSMEGLINGSBRANSJEN

Eiendomsmeglingsforetakene skal påse at personopplysninger som behandles har rettslig

UTKAST

grunnlag etter personopplysningsregelverket og at personopplysningene bare brukes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet. Videre skal det påses at personopplysningene som behandles er tilstrekkelige og relevante for formålet med behandlingen, og at de er korrekte og oppdaterte, og ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen.

Eiendomsmeglingsbransjens behandling av personopplysninger kan deles inn i følgende hovedkategorier[2]:

- Behandling av personopplysninger om kunder, potensielle kjøpere og kjøpere for å oppfylle avtaler med kunder om å selge boligen deres.
- Behandling av personopplysninger for å markedsføre foretakets tjenester.
- Behandling av personopplysninger som ledd i eiendomsmeglingsforetakets kontrolltiltak.

De ulike behandlingsaktivitetene reiser imidlertid forskjellige personvernrettslige problemstillinger. I det følgende vil hovedkategoriene av behandlingsaktiviteter, sammen med de spesifikke behandlingene som foretas som ledd i dette, bli presentert, sammen med retningslinjer til hvordan de særskilte personvernrettslige problemstillingene som oppstår skal håndteres.

En mer detaljert oversikt over de ulike typene behandlinger av personopplysninger som foretas av eiendomsmeglerforetak presenteres i vedlegg 2 («Protokoll over behandlingsaktiviteter»).

5.1 BEHANDLING AV PERSONOPPLYSNINGER FOR Å OPPFYLLE AVTALER MED KUNDER OM Å SELGE BOLIGEN DERES

I forbindelse med salg av boliger er det nødvendig å behandle en rekke personopplysninger både om kunden/selger og potensielle kjøpere. Det rettslige grunnlaget for denne behandlingen vil således være at behandlingen er nødvendig for å kunne inngå eller oppfylle en kontrakt som den registrerte er del i.

Følgende behandlingsaktiviteter vil være en naturlig del av et eiendomsmeglingsoppdrag[2]:

5.1.1 Befaring/Verdivurdering

Før det inngås avtale med selger om å selge boligen vil det ofte være naturlig at eiendomsmegler foretar en befaring av eiendommen. Formålet med dette vil blant annet være å vurdere eiendommens antatte verdi, salgsmuligheter, og betingelser for oppdraget. I denne forbindelse vil megleren behandle personopplysninger som oppdragsgivers navn, adresse, opplysninger knyttet til boligens stand og verdi, samt eventuelle andre forhold knyttet til boligen.

Megler vil i den anledning utarbeide notater om boligen. Disse notatene skal lagres på et nærmere angitt område i foretakets sakssystem. Notatene er å anse som interne saksnotater som den potensielle kunden ikke har innsynsrett i.

5.1.2 Oppdragsavtale

[2] Alle foretak vil i tillegg behandle personopplysninger om sine ansatte som ledd i personaladministrasjon, men dette omhandles ikke i denne bransjenormen. Listen er ikke uttømmende

UTKAST

Oppdragsavtalen mellom megler og kunde skal være skriftlig og inneholde de opplysninger som kreves i eiendomsmeglingsloven § 6-4. Dersom oppdragsavtalen skal oversendes pr. e- post må avtalen beskyttes med passord. Passordet skal oppgis til kunden pr. telefon eller SMS. Bakgrunnen for dette er at oppdragsavtalen må inneholde kundens fødselsnummer.

Oppdragsavtalen skal snarest mulig innføres i en oppdragsjournal i foretakets fagsystem i henhold til eiendomsmeglingsforskriften § 3-2.

5.1.3 Takst/tilstandsvurdering

Som hovedregel vil takstmenn være selvstendige behandlingsansvarlige, og har således et selvstendig ansvar for å påse at kravene i personopplysningsregelverket følges. Det er derfor ikke nødvendig å inngå databehandleravtale med takstmenn. Eiendomsmeglingsforetakenes rolle i forbindelse med utarbeidelse av taksrapporten vil i utgangspunktet være begrenset til å oversende navn og adresse til selger/kunden til takstmann for henvisning av oppdrag, samt å ta imot taksten når denne er utarbeidet av takstmann. Når eiendomsmeglingsforetaket har mottatt takstrapporten, er foretaket behandlingsansvarlig for den videre bruken av denne.

Takstrapporten kan i utgangspunktet oversendes på vanlig e-post, men det skal før hver oversendelse foretas en vurdering av hvorvidt det foreligger spesielle omstendigheter ved taksten som gjør at det er en høy risiko for personvernet til den registrerte dersom innholdet i taksten kommer på avveie. I slike tilfeller skal taksten beskyttes med passord.

5.1.4 Salgsoppgaven/Undersøkelsesplikt

Det følger av eiendomsmeglingsloven § 6-7 av eiendomsmegler skal sørge for at kjøper før handel sluttes får opplysninger denne har grunn til å regne med å få og som kan få betydning for avtalen.

Ovennevnte opplysninger hentes inn fra ulike kilder, herunder kunden/selger og offentlige registre, og skal oppgis i salgsoppgaven.

Salgsoppgaven vil normalt sett foreligge i både papir- og elektronisk form. Papirutgaver av salgsoppgaven som er til overs etter at salget er avsluttet skal makuleres innen ett år etter at salget er avsluttet og saken er arkivert. Den elektroniske utgaven av salgsoppgaven skal lagres i foretakets fagsystem i tråd med lovpålagt oppbevaringsplikt.

Dersom tidligere salgsoppgaver skal benyttes i markedsføringsformål må selger orienteres om dette og gis mulighet til å reservere seg mot slik bruk av salgsoppgaven.

Dersom det benyttes en ekstern leverandør til å utarbeide salgsoppgaven må det inngås databehandleravtale med denne.

5.1.5 Fotograf

Dersom det benyttes eksterne fotografer til å ta bilder av boligen vil denne fotografen som hovedregel selv være behandlingsansvarlig og vil således ha et selvstendig ansvar for å påse at kravene i personopplysningsregelverket følges. Det er ikke nødvendig å inngå databehandleravtale med fotografen. Dersom fotografen er ansatt i foretaket vil det være foretaket som er behandlingsansvarlig. Eiendomsmeglerforetaket vil uansett være behandlingsansvarlig for enhver bruk av fotografier i tilknytning til oppdraget.

UTKAST

Ved fotografering av fellesarealer skal det alltid tas hensyn til personvernet til øvrige naboer. Ved fotografering av fasader, felles garasjeanlegg og lekeplasser skal det tilstrebes å ikke få med identifiserbare gjenstander eller personer. Som et eksempel bør registreringsnumre på biler som står parkert i felles garasjeanlegg sladdes. Barn skal under enhver omstendighet ikke tas bilde av uten av foreldrene har samtykket.

Dersom det benyttes droner til å filme eller fotografere eiendommen skal det alltid gjøres en avveining mellom foretakets berettigede interesse i å markedsføre eiendommen, og andre personers krav til personvern. Før opptaket gjøres skal det gis informasjon som nevnt i punkt 10.1 til alle eiere av eiendommer og eventuelt andre personer som vil bli berørt. Dette kan eksempelvis løses gjennom å legge et informasjonsskriv i postkassen til berørte personer. Hver enkelt person som er registrert vil ha rett til å motsette seg filming/fotografier med droner. Informasjon som nevnt ovenfor skal gis innen rimelig tid før opptaket skal finne sted, og senest fire dager før.

Fotografier av eiendommen kan i utgangspunktet oversendes på vanlig e-post, men det bør før hver oversendelse foretas en vurdering av hvorvidt det foreligger spesielle omstendigheter ved fotografiene som gjør at det er en høy risiko for personvernet til den registrerte dersom disse kommer på avveie. I slike tilfeller skal fotografiene beskyttes med passord. Fotografier som benyttes i salgsoppgaven vil bli lagret sammen med denne, mens øvrige fotografier som ikke benyttes i salgsoppgaven skal slettes ett år etter at salget er avsluttet og saken er arkivert.

5.1.6 Stylist

Dersom det benyttes eksterne stylister til å innrede boligen for salg vil disse som hovedregel selv være behandlingsansvarlig og vil således ha et selvstendig ansvar for å påse at kravene i personopplysningsregelverket følges. Det er i disse tilfellene ikke nødvendig å inngå databehandleravtale med stylisten. Dersom stylisten er ansatt i foretaket vil det være foretaket som er behandlingsansvarlig.

5.1.7 Visning/interesselister

Visningslister/interesselister er lister med personer som er interessert i den aktuelle boligen som er til salgs. Formålet med slike lister er at den som står på listen skal bli kontaktet for mulige bud på boligen, få informasjon om innkomne bud, samt for å korrigere eventuelle feilopplysninger og/eller gi nye, relevante opplysninger om boligen. Visningslisten skal kun inneholde eiendommens registerbetegnelse og adresse, samt interessentens navn, telefonnummer, og eventuelt e-postadresse.

Informasjonen som fremgår av visningslister skal kun benyttes til det aktuelle formålet. Dersom megler ønsker å bruke visningslister til andre formål, herunder kontakte de registrerte for å informere om andre boliger til salgs, utlevere informasjon til banker for tilbud om finansiering eller å tilby foretakets tjenester må det innhentes spesifikke samtykker for dette.
Det er eiendomsmeglingsforetaket som er behandlingsansvarlig for visningslistene. Dette betyr blant annet at dersom andre, herunder selger, ønsker visningslistene utlevert, må foretaket forsikre seg om at det foreligger et rettslig grunnlag for dette. I utgangspunktet vil det kun være samtykke som vil være aktuelt som et rettslig grunnlag i dette tilfellet. Dette betyr at

UTKAST

dersom visningslistene skal bli utlevert må foretaket forsikre seg om at det foreligger samtykke fra hver enkelt av de personene som er registrert på visningslistene.

Visningslister inneholder informasjon som kan være svært verdifull, og som kan ha potensielt sett store økonomiske konsekvenser for de registrerte og også selger dersom de kommer på avveie, eller dersom informasjonen er ukorrekt. Det er viktig at det etableres sikkerhetstiltak som gjør at uvedkommende ikke har anledning til å fjerne eller endre visningslistene, og at ikke andre får innsyn i hvem som har skrevet seg på visningslistene. Av den grunn skal visningslister ikke ligge åpent tilgjengelig under visninger. Som hovedregel skal det kun brukes elektroniske visningslister, og ikke visningslister i papirformat. De elektroniske visningslistene skal ha tilfredsstillende sikkerhetstiltak for å sørge for opplysningenes konfidensialitet, integritet og tilgjengelighet. Det skal etableres tilgangsstyring for megleres bruk av visningslistene slik at informasjonen ikke blir tilgjengelig for uvedkommende.

5.1.8 Budgivning/Budjournal

Alle bud skal gis skriftlig og føres inn i en budjournal i henhold til eiendomsmeglingsforskriften § 3-5. Normalt sett vil det første budet sendes inn pr- epost eller annen elektronisk løsning, før eventuelle videre bud formidles pr. SMS. Megler har videre en plikt til å innhente gyldig legitimasjon og signatur fra budgiver før bud formidles til kunden/selger. Kravet til legitimasjon og signatur er oppfylt for budgivere som benytter e-signatur, eksempelvis BankID eller MinID. Dersom det ikke benyttes BankID eller Min ID anbefales det at legitimering skjer ved personlig oppmøte og fremvisning av gyldig identifikasjonsbevis. Dersom dette ikke er mulig kan kopi av legitimasjonsbevis, samt signert bud sendes inn til foretaket pr e-post. Foretaket må i den forbindelse gjøre den registrerte oppmerksom på at kopi av ID-kort bør beskyttes med passord. Dersom megleren tar kopi av pass/ID skal dette kun gjøres ved bruk av foretakets scanner/kopimaskin eller dedikerte scanningsapper, jf. punkt 11.3.8 nedenfor. Det skal ikke brukes privat utstyr herunder kamera på mobiltelefon, eller kommersielle scanneapper til å
ta kopi av disse dokumentene. Dersom disse kopiene oversendes pr. e-post skal de passordbeskyttes.

Kopi av budjournalen skal gis til kjøper og selger uten ugrunnet opphold etter at handel er kommet i stand. Eventuelle rettelser i budjournalen skal fremgå tydelig av slik kopi.

Etter at handel er kommet i stand, eller dersom en budrunde avsluttes uten at handel er kommet i stand, kan den som har lagt inn bud på eiendommen kreve kopi av budjournalen i anonymisert form.

5.1.9 Inngåelse av kontrakt

Med mindre begge parter ønsker noe annet etter at handel har kommet i stand, skal megler opprette skriftlig kjøpekontrakt mellom partene i minst tre eksemplarer, ett til hver av partene og ett for meglers arkiv. Kontrakten kan opprettes elektronisk dersom begge parter

UTKAST

samtykker til dette.

5.1.10 Gjennomføring av oppgjør

Med mindre kjøper og selger ønsker noe annet skal megler gjennomføre det økonomiske oppgjøret mellom partene, jf. eiendomsmeglingsloven § 6-8. I så tilfelle vil foretaket være å anse som behandlingsansvarlig for alle personopplysninger som behandles som ledd i gjennomføring av oppgjøret.

I den forbindelse vil det bli behandlet personopplysninger som fremgår av saksdokumentene, herunder tinglyst pantedokument, transporterklæring, inneståendeseserklæring, styregodkjennelse/avklaring av forkjøpsrett, hjemmelsdokument og eventuelle pantedokument, oppgjørsinstruks, bekreftelse på sletting av selgers pant i eiendommen, ny grunnbokutskrift, og registrering av kjøper hos forretningsfører.

Opplysningene vil bli innhentet fra blant annet kjøper, selger, kjøpers långiver (lånebeløp), selgers panthaver (pantedokument), grunnboken, forretningsførere/kommunen (restanse på felleskostnader/kommunale avgifter), og finansinstitusjoner (restgjeld på selgers lån).

I forbindelse med gjennomføring av oppgjøret vil utlevering av personopplysninger være påkrevd i følgende tilfeller:

Oppgjørsansvarlig skal avgi en bekreftelse til selgers bank om overføring av netto salgssum etter innfrielse av tinglyst pant i eiendommen (transporterklæring), samt en inneståendeseserklæring til kjøpers bank etter en totalvurdering av kjøpers finansiering.

Videre vil oppgjørsansvarlig sende hjemmelsdokument og eventuelle pantedokument for tinglysing til Kartverket for så å motta disse dokumentene i retur fra Kartverket i tinglyst stand.

UTKAST

5.2 BEHANDLING AV PERSONOPPLYSNINGER FOR Å MARKEDSFØRE BOLIGER

Markedsføring av boliger er en naturlig del av et eiendomsmeglingsoppdrag. Tradisjonelt sett består markedsføringen av blant annet annonsering på foretakenes hjemmesider, på foretakenes ulike kontorer, fysiske aviser, samt på www.finn.no. I den senere tid har det også blitt vanlig med annonsering på sosiale medier.

Såfremt det ikke er mulig å identifisere hvem som har mottatt eller sett annonsen vil dette ikke by på særlige personvernmessige problemstillinger. Det samme vil være tilfellet der hvor annonsen ikke er sendt ut til spesifikke personer som potensielle kjøpere. Dersom det er mulig å identifisere hvem som har mottatt eller sett annonsen, eller annonsen sendes ut til spesifikke personer (mulige kjøpere) må foretakene påse at det foreligger rettslig grunnlag for den aktuelle behandlingen av personopplysninger.

Som hovedregel skal behandlingen av personopplysninger om potensielle kjøpere/interessenter som ledd i markedsføring av boliger være basert på samtykke. Det vil imidlertid også være tilfeller hvor foretakets berettigete interesse i å markedsføre boliger vil veie tyngre enn personvernet til den registrerte. Et eksempel på dette kan være markedsføring til eksisterende kunder, eksempelvis der hvor megler tidligere har solgt boligen til en person, og ønsker å tipse denne personen om en ny bolig på markedet. Markedsføringsloven § 15 forbyr, som hovedregel, utsendelse av elektroniske markedsføringshenvendelser til fysiske personer som ikke har samtykket til å motta slik markedsføring, men gir unntak for markedsføring ved e-post[3] i eksisterende kundeforhold. Eventuelle markedsføringshenvendelser i eksisterende kundeforhold som baseres på foretakenes berettigede interesse må skje innen rimelig tid etter den opprinnelige saken er arkivert og oppdraget er avsluttet, ellers må kundeforholdet anses som avsluttet. Det må videre informeres i oppdragsavtalen at megler kan kontakte kunden for markedsføringsformål, og kunden må gis anledning til å reservere seg mot dette.

All bruk av personprofiler til bruk i markedsføringsformål skal baseres på samtykke. Et eksempel på en personprofil er at foretakene antar at den registrerte, som potensiell kjøper, vil være interessert i en spesiell type bolig fordi vedkommende har en bestemt inntekt, en bestemt familiesituasjon osv. Dette kan særlig være aktuelt for markedsføring av boliger på sosiale medier. Dersom annonsene kun vises til spesifikke personer basert på en personprofil, og ikke til en videre angitt gruppe, eksempelvis alle Facebookbrukere i Oslo, må dette baseres på samtykke.

Dersom annonsering foretas ved hjelp av automatisering eller profilering skal foretakene ha kunnskap om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte. Dette gjelder selv om det ikke er foretakene som står for selve profileringen.

Det er ikke adgang til å utarbeide lister over «følgere» eller personer som «liker» en post på sosiale medier til markedsføringsformål med mindre vedkommende har samtykket til dette. Et slikt samtykke kan ikke være en forutsetning for å «følge» et foretak eller «like» en post på sosiale medier.

[3] Ordlyden i mfl. § 15 er «bruk av elektroniske kommunikasjonsmetoder". Både e-post og SMS regnes som elektroniske kommunikasjonsmetoder.

UTKAST

Med unntak av de personopplysninger som fremgår av salgsoppgaven/annonsen, kan foretakene ikke utlevere personopplysninger til eksterne aktører, herunder finn.no, og sosiale medier, uten at det foreligger samtykke eller annet behandlingsgrunnlag for dette. Dette betyr at det i utgangspunktet ikke er anledning til å oversende adresselister/kundelister eller oversikt over mulige interessenter uten at det er innhentet samtykke til dette.

Dersom en person ønsker å laste ned en salgsoppgave digitalt, kan det settes som vilkår at vedkommende må oppgi fullt navn, postnummer, telefonnummer og e-post og at foretaket kan kontakte vedkommende for informasjon om boligen, som for eksempel endringer i salgsoppgaven. Formålet med denne behandlingen av personopplysninger er å oppfylle meglerens opplysningsplikt etter eiendomsmeglingsloven § 6-7. Foretakene vil videre ha en berettiget interesse i å kunne dokumentere hvem som har vært i kontakt med de (megleren) dersom megleren har krav på vederlag etter eiendomsmeglingsloven § 7-3-nr. 2. Denne informasjonen kan imidlertid ikke brukes til markedsføringsformål med mindre den registrerte samtykker til dette.

5.3 BEHANDLING AV PERSONOPPLYSNINGER FOR Å MARKEDSFØRE FORETAKETS TJENESTER

Som ledd i markedsføring av sine tjenester vil det være nødvendig for eiendomsmeglingsforetakene å behandle en rekke personopplysninger. Dette kan blant annet være navn, adresse, boligforhold, osv.

Som hovedregel skal behandlingen av personopplysninger som ledd i markedsføring av foretakenes tjenester være basert på samtykke. Det vil imidlertid også være tilfeller hvor foretakets berettigete interesse i å markedsføre sine tjenester vil veie tyngre en personvernet til den registrerte. Et eksempel på dette kan være markedsføring til eksisterende kunder. Markedsføringsloven § 15 forbyr, som hovedregel, utsendelse av elektroniske markedsføringshenvendelser til fysiske personer som ikke har samtykket til å motta slik markedsføring, men gir unntak for markedsføring ved e-post i eksisterende kundeforhold. Eventuelle markedsføringshenvendelser i eksisterende kundeforhold som baseres på foretakenes berettigede interesse må skje innen rimelig tid etter salget, ellers må kundeforholdet anses som avsluttet. Det bør videre informeres i oppdragsavtalen at megler kan kontakte kunden for markedsføringsformål, og kunden må gis anledning til å reservere seg mot dette. Det vil ikke være anledning til å benytte foretakenes berettigede interesse som rettslig grunnlag for markedsføringsformål overfor personer som ikke har et kundeforhold til foretaket, eksempelvis kjøpere av en bolig.

Dersom markedsføringen baserer seg på profilering eller automatiserte avgjørelser må behandlingen baseres på samtykke. All markedsføring skal følge markedsføringslovens regler, samt bransjenorm for direkte markedsføring.

Foretakene kan opprette lister over potensielle kunder, men alle som er oppført på slike lister skal få informasjon om dette, samt hvor opplysningene er hentet fra. Det skal også opplyses om hvor lenge opplysningene vil bli lagret og at vedkommende kan be om å bli slettet fra denne listen og reservere seg mot fremtidige oppføringer. Denne informasjonen kan gis som en del av den første henvendelsen til den potensielle kunden. Det oppfordres til

UTKAST

at foretakene oppretter kundeportaler/min side, hvor potensielle kunder selv kan logge seg inn og styre hva de ønsker at foretakene skal bistå de med.

Kundelister skal kun lagres i foretakenes fagsystem og skal slettes senest ett år etter henvendelse til kunden, med mindre det etableres et kundeforhold.

5.4 BEHANDLING AV PERSONOPPLYSNINGER SOM LEDD I EIENDOMSMEGLINGSFORETAKETS KONTROLLTILTAK.

Eiendomsmeglingsforetak er underlagt hvitvaskingsloven og er derfor pålagt å gjennomføre kundekontroll, samt rapportere om mistenkelige transaksjoner. Som ledd i dette vil det bli behandlet personopplysninger som blant annet, navn, kopi av pass/ID-kort, opplysninger om mulige straffbare handlinger. Dette er personopplysninger som vil ha høy grad av beskyttelsesbehov og det er derfor viktig at foretakene etablerer gode sikkerhetstiltak.

Kopi av pass/ID skal kun gjøres ved bruk av foretakets scanner/kopimaskin eller dedikerte scanningsapper, jf. punkt 11.3.8 nedenfor. Det skal ikke brukes privat utstyr herunder kamera på mobiltelefon, eller kommersielle scanneapper til å ta kopi av disse dokumentene. Dersom disse kopiene oversendes pr. e-post skal de passordbeskyttes.

MT-meldinger skal sendes via Altinn.

6 SAMTYKKE

Det er et grunnleggende personvernprinsipp at enhver person har råderett over sine egne personopplysninger. Dersom den aktuelle behandlingen av personopplysninger ikke kan baseres på at det er nødvendig for å inngå eller oppfylle en avtale som den registrerte er del i, bør behandling av personopplysninger, så langt det lar seg gjøre, baseres på samtykke. Dersom behandlingen av personopplysninger omfatter automatiserte avgjørelser, herunder profilering, eller spesialtilpasset markedsføring skal behandlingen alltid baseres på samtykke fra den registrerte.

Samtykke defineres som *«enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende».*

At samtykket er frivillig betyr at det ikke må være knyttet til tvang eller negative konsekvenser med å ikke samtykke. Formålet med et samtykke er å gi den registrerte et valg, og kontroll over sine egne personopplysninger. Et samtykke vil derfor ikke anses å være frivillig dersom den registrerte ikke har et reelt eller fritt valg. Det vil være tillatt å gi små incentiver for å innhente samtykker, men foretakene må være oppmerksom på at det ikke må være forbundet med uforholdsmessige negative konsekvenser dersom vedkommende ikke samtykker. Eventuelle incentiver bør derfor holdes til et minimum.

UTKAST

Ved vurdering av om et samtykke er gitt frivillig skal det tas størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale.

At samtykket skal være spesifikt betyr at det ikke kan være generelt utformet og at det må inneholde en presis angivelse av formålet med behandlingen av personopplysninger. Et samtykke skal derfor være så konkret at det klart og tydelig fremgår hva som vedkommende samtykker til. En angivelse av formål som «forbedre våre tjenester» vil ikke oppfylle kravet om å være spesifikt.

Hvis en behandling av personopplysninger tjener flere formål, skal det innhentes særskilte samtykker for hvert enkelt formål. Eksempelvis vil et samtykke som ved hjelp av ett kryss gir foretakene tillatelse til å bruke personopplysningene til å motta boligrelatert informasjon, til å markedsføre verdivurdering fra megleren, til å motta tilbud fra en samarbeidsbank på finansiering, samt til å motta tips om eiendommer til salgs, ikke anses som gyldig. Det må i slike tilfeller innhentes spesifikt samtykke for alle de ovennevnte formål.

At samtykket skal være informert, betyr at den registrerte skal vite hva han/hun samtykker til. Det skal gis tilstrekkelig informasjon slik at den registrerte kan treffe sin beslutning på et informert grunnlag.

Som et minimum må det opplyses om følgende:

- Navn og kontaktinformasjon til behandlingsansvarlige
- Formålet med den aktuelle behandlingen av personopplysninger
- Hvilke kategorier av personopplysninger som behandles
- Hvilken type behandling av personopplysninger som finner sted
- At den registrerte når som helst kan trekke samtykket.

Ofte vil samtykket bli innhentet samtidig med at det samles inn personopplysninger fra den registrerte. Kravet om informasjon ved avgivelse av samtykke vil derfor også måtte ses i sammenheng med kravet om informasjonsplikt, jf. punkt 10 ovenfor.

At samtykket må være en utvetydig viljesytring innebærer at det ikke kan foreligge noe tvil om at det er avgitt et samtykke. Samtykker skal derfor innhentes ved bruk av «opt-in», og ikke «opt-out», og det er ikke tillatt med utfylte samtykkebokser. En utvetydig viljesytring kan eksempelvis meddeles ved å signere på et dokument, krysse av i et felt eller ved valg av tekniske innstillinger.

Samtykket skal være innhentet før foretakene begynner den aktuelle behandlingen av personopplysninger. Foretakene skal kunne dokumentere at det det er gitt samtykke, herunder også tidspunkt for samtykket.

Dersom den registrertes samtykke gis i forbindelse med en skriftlig erklæring som også gjelder andre forhold, skal anmodningen om samtykke framlegges på en måte som gjør at den tydelig kan skilles fra nevnte andre forhold, i en forståelig og lett tilgjengelig form og på et klart og enkelt språk. Deler av en slik erklæring som er i strid med denne forordning, skal ikke være bindende.

UTKAST

Den registrerte har rett til å trekke tilbake sitt samtykke til enhver tid. Dersom samtykket trekkes tilbake, skal det ikke påvirke lovligheten av behandlingen som bygger på samtykket før det trekkes tilbake. Det skal være like enkelt å trekke tilbake som å gi samtykke.

7 LAGRING OG SLETTING AV PERSONOPPLYSNINGER

Etter eiendomsmeglingsforskriften § 3-7 nr. (3) skal kontrakter, dokumenter og journaler oppbevares i papirform eller på annen betryggende måte i minst 10 år etter at saken er arkivert. Senest innen ett år etter at den lovpålagte lagringsfristen er gått ut skal alle personopplysningene som er behandlet i forbindelse med det aktuelle oppdraget slettes, med mindre det foreligger konkrete holdepunkter for at det er/vil bli nødvendig å lagre personopplysningene videre for å gjøre gjeldende eller forsvare et rettskrav.

Personopplysninger som behandles som ledd i markedsføringsformål skal slettes når den registrerte ber om det, eller når formålet med den aktuelle behandlingen er oppfylt, senest ett år etter at siste henvendelse er sendt ut.

Personopplysninger som behandles som ledd i etterlevelse av hvitvaskingsregelverket skal lagres i fem år etter opprettelse og slettes senest ett år etter at lagringsfristen har utløpt, med mindre oppbevaringsplikten på 10 år etter eiendomsmeglingsforskriften også gjelder.

8 AVVIK

Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerhet, skal dette behandles som et avvik.

Alle ansatte er ansvarlig for å rapportere avvik fra gjeldende rutiner og andre hendelser til den som er ansvarlig for det aktuelle området eller sikkerhetsansvarlig. Feil i programvare og maskinvare rapporteres til IKT-ansvarlig.

9 INTERNKONTROLL

Eiendomsmeglingsforetakene skal gjennom tydelig definerte roller og ansvarsområder sørge for at virksomheten når de definerte sikkerhetsmål, og at personvernregelverket etterleves.

Hver enkelt behandlingsansvarlig skal utpeke en rolle/person som skal være foretakets personvernkoordinator. Denne personen skal ha fått delegert det daglige oppfølgingsansvaret for at virksomheten etterlever personvernregelverket. Personvernkoordinatoren skal videre være ansvarlig for at foretakene har etablert skriftlige rutiner for oppfyllelse av sine plikter og de registrertes rettigheter til enhver tid. Det skal blant annet utarbeides rutiner som sikrer følgende:

- vurdering av formål med og rettslig grunnlag for behandling av personopplysninger
- innhenting og kontroll av de registrertes samtykke
- inngåelse av databehandleravtale

UTKAST

- gjennomføring av risiko- og konsekvensvurdering
- sletting av personopplysninger
- håndtering av anmodninger om innsyn, retting, sletting, reservasjon, og dataportabilitet

Maler til disse rutinene presenteres i vedlegg 3.

10 INFORMASJON OG INNSYN I PERSONOPPLYSNINGER

10.1 INFORMASJONSPLIKT

Den registrerte, altså personen som foretaket behandler personopplysninger om, skal få informasjon om følgende forhold:

- Identiteten og kontaktopplysningene til det ansvarlige eiendomsmeglingsforetaket (behandlingsansvarlige).
- Kontaktopplysningene til personvernombudet (hvis aktuelt).
- Formålene med den tiltenkte behandlingen av personopplysningene, samt det rettslige grunnlaget for behandlingen. Dersom behandlingen baseres på at foretaket har en berettiget interesse, skal denne interessen beskrives.
- Hvilke kategorier personopplysninger som behandles.
- Dersom personopplysningene vil bli utlevert til andre behandlingsansvarlige skal det opplyses om dette, herunder hvilke selskap som vil få informasjonen. Det er ikke nødvendig å opplyse om at opplysninger eventuelt vil bli overlevert til offentlige myndigheter.
- Dersom foretaket akter å overføre personopplysninger til land utenfor EU/EØS (tredjeland) skal det opplyses om dette. Dette vil særlig være aktuelt dersom det benyttes en databehandler eller supportpersonnell er basert i tredjeland. Det skal også opplyses om hvilke sikkerhetstiltak som er gjennomført.
- Hvor lenge personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet.
- Retten til å be om innsyn i og korrigering eller sletting av personopplysninger eller begrensning av behandlingen som gjelder den registrerte, eller til å protestere mot behandlingen samt retten til dataportabilitet.
- Dersom behandlingen er basert på samtykke, retten til når som helst å trekke tilbake et samtykke uten at det påvirker lovligheten av en behandling basert på et samtykke før samtykket trekkes tilbake.
- Retten til å klage til en tilsynsmyndighet (Datatilsynet).
- Om det foreligger et lovfestet eller avtalefestet krav om å gi personopplysninger eller et krav som er nødvendig for å inngå en avtale, samt om den registrerte har plikt til å gi personopplysningene og om mulige konsekvenser dersom vedkommende ikke gjør det.
- Dersom det brukes automatiserte avgjørelser, herunder profilering, skal det opplyses om dette og i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

UTKAST

10.1.1 Når skal informasjonen gis?

Dersom personopplysningene samles inn fra den registrerte selv skal informasjonen gis på tidspunktet for innsamlingen av personopplysningene.

Dersom personopplysningene samles inn fra andre enn den registrerte, eksempelvis fra offentlige registre, andre behandlingsansvarlige mv., skal informasjonen gis innen rimelig tid etter at personopplysningene er samlet inn, men senest innen 30 dager. For behandling av personopplysninger om kunder (selgere av boliger) kan dette løses ved å innta informasjonen i oppdragsavtalen.

, elDersom personopplysningene skal brukes til å kommunisere med den registrerte, eksempelvis gjennom markedsføring av tjenester, skal informasjonen senest gis på tidspunktet for den første kommunikasjonen med vedkommende.

Dersom det er planlagt at personopplysningene skal utleveres til en annen mottaker, skal informasjonen gis senest når personopplysningene første gang utleveres.

10.1.2 Hvordan skal informasjonen gis?

Alle eiendomsmeglingsforetak skal utarbeide en personvernerklæring som inneholder generell informasjon om behandlingen av personopplysninger. Personvernerklæringen skal publiseres på foretakets nettsider. Mal til denne personvernerklæringen presenteres i vedlegg 4.

10.1.3 Unntak fra informasjonsplikten

Informasjonsplikten gjelder ikke dersom og i den grad den registrerte allerede har informasjonen, dersom det foreligger lovfestet taushetsplikt, eller dersom det viser seg umulig å gi nevnte informasjon eller det vil innebære en uforholdsmessig stor innsats. I sistnevnte tilfeller skal foretakene treffe egnede tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser, herunder gjøre informasjonen offentlig tilgjengelig.

Informasjonsplikten gjelder videre ikke i de tilfeller der innsamling eller utlevering av personopplysningene er uttrykkelig fastsatt i norsk rett. Dette innebærer blant annet at foretakene ikke har informasjonsplikt om behandlingen av personopplysninger knyttet til innsendelse av MT-meldinger til det offentlige, eller meglers plikt til å innhente personopplysninger etter eiendomsmeglingsloven.

10.2 RETT TIL INNSYN

Den som er registrert i foretakenes systemer har rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om vedkommende behandles, og, dersom dette er tilfellet, innsyn i personopplysningene og følgende informasjon:

- formålene med behandlingen
- de berørte kategoriene av personopplysninger
- mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til
- dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,
- retten til å anmode om korrigering eller sletting av personopplysninger eller begrensning av

UTKAST

behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling

- retten til å klage til en tilsynsmyndighet (Datatilsynet)
- dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra
- forekomsten av automatiserte avgjørelser, herunder profilering. Dersom det foretas automatiserte avgjørelser skal den registrerte også få relevant informasjon om den underliggende logikken, samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte. Dette vil være særlig aktuelt i de tilfeller hvor den registrerte mottar tilpasset markedsføring basert på profilering.
- Dersom personopplysningene overføres til en tredjestat skal den registrerte ha rett til å bli underrettet om de nødvendige garantiene i forbindelse med overføringen.

10.2.1 Når skal innsyn gis?

Anmodninger om innsyn skal besvares så snart som mulig etter at anmodningen er mottatt og senest innen 30 dager.

10.2.2 Hvordan skal innsyn gis?

For å få innsyn i personopplysningene som behandles må den som anmoder om innsyn legitimere seg. Det anbefales at legitimering skjer ved personlig oppmøte og fremvisning av gyldig identifikasjonsbevis. Dersom dette ikke er mulig kan kopi av legitimasjonsbevis, samt signert innsynsbegjæring sendes inn til foretaket pr e-post. Foretaket må i den forbindelse gjøre den registrerte oppmerksom på at kopi av ID-kort bør beskyttes med passord.

Den behandlingsansvarlige skal gjøre tilgjengelig en kopi av personopplysningene som behandles. Dersom den registrerte anmoder om flere kopier, kan den behandlingsansvarlige kreve et rimelig gebyr basert på administrasjonskostnadene. Dersom den registrerte inngir anmodningen elektronisk, og med mindre den registrerte anmoder om noe annet, skal informasjonen gis i en vanlig elektronisk form. Dersom foretaket har etablert en kundeportal kan innsyn gis via denne.

10.2.3 Unntak fra retten til innsyn

Retten til å motta en kopi av personopplysninger som behandles skal ikke krenke andres rettigheter og friheter.

Megleres kommentarer i kommentarfelt og interne notater vil i utgangspunktet anses som tekst utarbeidet for den interne saksforberedelse og således unntatt fra retten til innsyn.

Registrerte har ikke rett til innsyn i MT-meldinger som er sendt til offentlige myndigheter.

UTKAST

10.3 ØVRIGE RETTIGHETER FOR DEN REGISTRERTE

10.3.1 Innsigelsesrett

Dersom behandlingen av personopplysninger er basert på allmennhetens interesse eller foretakets berettigede interesse, har den registrerte til enhver tid, av grunner knyttet til vedkommendes særlige situasjon, rett til å protestere mot behandlingen.

Dersom den registrerte protesterer mot behandlingen skal foretaket ikke lenger behandle personopplysningene, med mindre foretaket kan påvise at det foreligger tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav.

Dersom personopplysninger behandles med henblikk på direkte markedsføring, skal den registrerte til enhver tid ha rett til å protestere mot behandling av personopplysninger som angår vedkommende, til slik markedsføring, herunder profilering i den grad dette er knyttet til direkte markedsføring.

Dersom den registrerte gjør innsigelse mot behandling med henblikk på direkte markedsføring, skal personopplysningene ikke lenger behandles for slike formål.

Dersom personopplysninger behandles for statistiske formål har den registrerte, av grunner knyttet til vedkommendes særlige situasjon, rett til å protestere mot behandling av personopplysninger om vedkommende, med mindre behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse.

10.3.2 Automatiserte avgjørelser

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende.

Retten til å protestere mot automatiserte avgjørelser gjelder ikke dersom avgjørelsen er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og foretakene, eller er basert på samtykke. Videre gjelder ikke denne retten dersom avgjørelsen er tillatt i henhold til norsk rett og det er fastsatt egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser.

Dersom den registrerte ikke har rett til å protestere mot den automatiserte avgjørelsen etter reglene ovenfor, skal foretakene allikevel, ved menneskelig inngripen, gi den registrerte mulighet til å uttrykke sine synspunkter og til å bestride avgjørelsen.

Det er ikke tillatt å behandle særlige kategorier av personopplysninger som ledd i automatiserte avgjørelser.

11 INFORMASJONSSIKKERHET

Foretakene skal påse at det er etablert tiltak for tilfredsstillende informasjonssikkerhet. Dette innebærer at det må utarbeides dokumenterte rutiner for informasjonssikkerhet. Alt

UTKAST

arbeid knyttet til informasjonssikkerhet skal være risikobasert. Risikovurdering skal være et kontinuerlig arbeid, og skal gjennomføres i tråd med foretakenes rutiner for risikovurderinger og konsekvensanalyser.

11.1 OVERORDNET RISIKOVURDERING:

Kjernevirksomheten til eiendomsmeglingsforetak består i å selge boliger for kunder. Som ledd i dette vil det bli behandlet personopplysninger knyttet til boligens tilstand, økonomiske forhold, personnummer, samt om kjøper, selger og potensielle interessenter. Det vil som hovedregel ikke bli behandlet særlige kategorier av personopplysninger (sensitive personopplysninger).

Opplysningene som behandles er personopplysninger som kan ha konsekvenser for de registrerte dersom de kommer på avveie, eller ikke er korrekte. Av den grunn skal personopplysningenes konfidensialitet og integritet tillegges særlig vekt i valg og prioriteringer i sikkerhetsarbeidet.

Potensielle konsekvenser for de registrerte ved sikkerhetsbrudd kan være identitetstyveri, tap av budrunder, økonomisk tap ved kjøp/salg av bolig mm.

11.2 INNEBYGD PERSONVERN

Eiendomsmeglerforetakenes informasjonssikkerhetsarbeid skal være basert på prinsippet om innebygd personvern. Dette betyr blant annet at foretakene ved utvikling og implementering av nye informasjonssystem må tenke personvern på lik linje med brukervennlighet, effektivitet og lønnsomhet. Det må tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Videre skal alle standardinnstillinger i IT-systemene skal være stilt inn på det mest personvernvennlige nivået, såfremt det er rimelig. I rimelighetsvurderingen skal det tas hensyn til hva som er teknisk mulig, kostnadene ved den tekniske løsningen, samt hvilken risiko for personvernet til den registrerte IT-systemet representerer.

Ved utvikling av ny programvare eller nye informasjonssystemer skal det sees hen til Datatilsynets veileder om «Programvareutvikling med innebygd personvern» (https://www.datatilsynet.no/globalassets/global/skjema-maler/sjekkliste-for-innebygd-personvern.pdf). Dersom programvareutviklingen utføres av databehandlere skal foretakene påse at dette kravet er en del av databehandleravtalen.

11.3 GENERELLE INFORMASJONSSIKKERHETSTILTAK

11.3.1 Tilgangsstyring

Tilgang til systemer og informasjon skal kun gis til medarbeidere med tjenstlig behov. Tilgang til systemer og informasjon for uvedkommende skal forhindres. Tilgangsstyringen bør være rollebasert. Det bør etableres en rollemal som beskriver hvilke tilganger de som opptrer i rollen skal ha og hvilke kategorier personopplysninger de som innehar rollen, normalt skal gis tilgang til. Det vil som hovedregel være det enkelte foretaks ansvarlige leder som tildeler autorisasjon for tilgang. I dette ligger at ansvarlig leder, innen eget ansvarsområde, skal vurdere og godkjenne det enkelte personells behov for å få tilgang til personopplysninger.

UTKAST

11.3.2 Særlig om tilgang til personopplysninger på tvers av foretakene.

Meglere ved de ulike avdelinger/foretak vil ofte ha behov for å ha tilgang til hele saksporteføljen i fagsystemene på tvers av de lokale kontor for å kunne yte kundene best mulig service. Dette for å fullt ut kunne utnytte stordriftsfordelene som ligger i å være en større enhet. Dersom kontorene er organisert som en enkelt juridisk enhet vil alle meglere som er ansatt der kunne ha tilgang til alle saksporteføljer på tvers av de ulike avdelingene/kontorene.

Dersom foretakene er organisert som konsern med mor- og datterselskap eller som franchise, med franchisegiver- og taker, må det tas aktivt stilling til hvem som er behandlingsansvarlig, jf. punkt 3.1 ovenfor.

I de tilfeller hvor morselskapet eller franchisegiver vurderes å være behandlingsansvarlig vil normalt alle ansatte i de ulike datterselskapene eller franchisetakerne ha tilgang til personopplysninger på tvers av de juridiske enhetene.

Dersom behandlingsansvaret vurderes å ligge hos hver enkel juridisk enhet vil det å gi tilgang til saksporteføljene på tvers av enhetene være å anse som en utlevering av personopplysninger. Dette krever da at det foreligger et rettslig grunnlag for dette, og at den/de registrerte informeres om dette.

Aktuelle rettslige grunnlag for dette vil enten være dersom den registrerte samtykker til slik utlevering eller dersom foretakene (både mottaker og sender) vurderer det slik at deres berettigede interesse i å foreta denne behandlingen overstiger personvernulempen til den/de registrerte. Foretakene må her være oppmerksom på at dersom sistnevnte rettslige grunnlag påberopes, kan den registrerte reservere seg mot slik behandling. Det skal derfor etableres sperrer i systemet som hindrer at meglere fra andre juridiske enheter innenfor samme konsern/franchise har tilgang til personopplysninger dersom den registrerte reserverer seg mot dette.

11.3.3 Hjemmekontor

Meglere har utstrakt behov for å arbeide utenfor kontoret. Behandlingen av personopplysninger utenfor kontoret vil derfor forekomme i stor grad ved hjelp av mobiltelefon, nettbrett, eller PC eller andre mobile enheter. Det skal derfor legges til rette for tilfredsstillende sikkerhetstiltak for bruk av disse. Det anbefales blant annet at det installeres «Mobile Device Management» (MDM) på alle foretakenes mobile enheter for å kunne gjøre nødvendige tiltak for å unngå at uvedkommende får tilgang på foretakenes personopplysninger som ligger lagret der. Dersom det installeres MDM, må foretakene være oppmerksom på at de ansatte har krav på informasjon om dette tiltaket, jf. punkt 10.1.

Videre skal alle ansatte til enhver tid ha kodelås og siste programvareoppdatering på sine mobile enheter.

PC på hjemmekontor skal ikke ha kundeopplysninger lagret lokalt. Disse opplysningene skal kun nåes ved oppkobling til foretakenes fagsystemer eller andre sentralt lagrede data.

Dersom det brukes nettbrett skal dette som hovedregel ikke benyttes til privat bruk.

UTKAST

Terminalserverløsning er anbefalt og skal fortrinnsvis benyttes (bl.a. fordi kravet til at data ikke skal lagres lokalt på PC kan ivaretas, løsningen kan forhindre klipp og lim, løsningen kan forhindre utskrift lokalt, osv.). Det skal kun benyttes foretakenes PC, mobiltelefoner, nettbrett eller annet elektronisk utstyr til virksomhetsrelatert arbeid.

Det skal utpekes en IT-ansvarlig som skal ha ansvaret for å ivareta kravene til oppsett av hjemmekontor, herunder mobile enheter.

11.3.4 Kommunikasjon

Det anbefales at all intern kommunikasjon pr. e-post krypteres. For ekstern kommunikasjon bør e-post som inneholder særlige kategorier personopplysninger eller fødselsnummer krypteres. Dersom det ikke er mulig å kryptere slik e-post skal den beskyttelsesverdige informasjonen vedlegges i et passordbeskyttet vedlegg. Passordet må ikke oversendes pr. e-post, men kan formidles via SMS eller pr telefon. Det kan også brukes et forhåndsdefinert passord. Dersom det sendes e-post utenfor foretakenes nettverk skal det benyttes VPN.

11.3.5 Konfigurasjon

Foretakene skal selv ha oversikt over og ha kontroll med konfigurasjon av alt utstyr og programvare som benyttes i behandlingen av personopplysninger.

11.3.6 Kopimaskiner

Det skal etableres rutiner som sikrer at harddisken på foretakets kopi- skanning- og/eller printere slettes. Det anbefales at det innstilles på automatisk, fortløpende sletting. Som et minimum skal maskinenes harddisk slettes eller på annen måte destrueres før den blir avhendet.

11.3.7 Passord

Det skal etableres tilfredsstillende rutiner for passord, herunder oppdatering av passord. Rutinene skal følge allment aksepterte anbefalinger.

For systemer som inneholder kundeinformasjon bør det benyttes to-faktor autentisering.

11.3.8 Legitimering av kunder/budgivere

Det anbefales at BankID benyttes til legitimering av budgivere og til kundekontroll. Det anbefales også at foretakene etablere egne, dedikert scanningsapper, til å foreta legitimering/kundekontroll. En slik scanningsapp bør kunne overføre bildet som blir tatt direkte på relevant mappe i fagsystemet og deretter slettes fra telefonen, slik at det ikke vil ligge kopier av bildene på meglerens telefon etter gjennomført legitimasjon/kontroll. Det kan benyttes leverandører for å utvikle og drifte slike apper, men det må da inngås databehandleravtale med denne leverandøren.

UTKAST

Det skal ikke brukes privat utstyr, herunder kamera på mobiltelefon, eller kommersielle scanneapper til å ta kopi av disse dokumentene. Dersom kopier av pass/ID-kort oversendes pr. e-post skal de passordbeskyttes. Dersom det er kunden som eventuelt vil sende over slike kopier pr. e-post til foretaket, skal foretaket gjøre han/henne oppmerksom på at kopi av pass/ ID-kort bør beskyttes med passord.

11.4 DATABEHANDLERE

Dersom foretaket bruker en underleverandør som skal behandle personopplysninger på vegne av foretaket, eller dersom foretaket skal behandle personopplysninger på vegne av et annet selskap, skal det inngås en databehandleravtale som regulerer den aktuelle behandlingen av personopplysninger.

Databehandleravtalen skal fortrinnsvis være en selvstendig og uttømmende avtale som benevnes «databehandleravtale». Databehandleravtalen kan også være et vedlegg til en tjenesteavtale inngått mellom de samme parter.

For leverandørene av de tre fagsystemene er det utarbeidet egne databehandleravtaler som tilfredsstiller kravene i personopplysningsloven. For andre databehandlerrelasjoner vises det til mal for databehandleravtaler som fremgår av vedlegg 5.

UTKAST