



# Personverndokument

Tittel	Personverndokument	Avdeling	Alle
Opprettet	21.05.2018	Type	Instruks
Dokumentnummer		Sist revidert	30.05.2018
Revisjonsnummer	2	Sist revidert av	Thorsrud Richard Skaar
Godkjent av	Thorsrud Richard Skaar	Kategori	Administrasjon

## 1. Om personverndokumentet

Dette dokumentet skal bidra til at vi etterlever lov om personopplysninger fra 2018. Dokumentet skal også bidra til å påvise at vår behandling av personopplysninger er i samsvar med loven.

## 2. Ansvar for behandling av personopplysninger hos oss

Bedriften er ansvarlig for personopplysninger vi behandler, for eksempel om egne ansatte, kontaktpersoner hos kunder og leverandører, privatkunder og andre forretningsforbindelser. Bedriften har ansvaret for å overholde de pliktene som følger av reglene om personopplysninger.

Det daglige behandlingsansvaret har Richard Skaar Thorsrud tilsammen med John R. Uppard

## 3. Kunnskap over reglene om personopplysninger

Vi skal sørge for at de relevante ansatte har kjennskap til reglene om personopplysninger, herunder dette dokumentet om personvern. Kunnskapsnivået skal være tilpasset den enkelte ansattes behandling av personopplysninger. Vi skal vurdere om noen grupper av ansatte har behov for særlig kunnskap, for eksempel personalfunksjoner og IT-ansvarlige. Ledelsen hos oss skal alltid ha kjennskap til regelverket.

## 4. Kartlegging av behandling av personopplysninger

Vi skal kartlegge all behandling av personopplysninger. Dette skal gjøre vi i et eget skjema der vi angir blant annet kategorier av registrerte, formål med behandlingen, hvordan vi behandler opplysningene og hvilke grunnlag den har for behandlingen. Skjemaene skal bidra til at vi etterlever reglene om behandling av personopplysninger.

## 5. Grunnkrav for behandling av personopplysninger

Loven stiller opp seks grunnlag som gjelder for all behandling av alle personopplysninger. Vi skal sørge for at personopplysninger skal:

1. behandles på en lovlig, rettferdig og gjennomiktig måte med hensyn til den registrerte («lovlighet, rettferdighet og gjennomiktighet»)
2. samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene («formålsbegrensning»)



3. være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»)
4. 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 («riktighet»)
5. 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 («lagringsbegrensning»)
6. 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 («integritet og fortrolighet»)

Hvis personopplysninger brukes til andre formål enn de er samlet inn for, se punkt 2 ovenfor, skal vi alltid vurdere om det nye eller endrede formålet er forenlig med det opprinnelige. Vi skal da ta hensyn til de faktorene som fremgår av personvernforordningen artikkel 6 nr. 4.

## 6. Grunnlag for å behandle personopplysninger

### 6.1. Behandlingsgrunnlag

Vi skal ha minst ett av følgende grunnlag for all behandling av personopplysninger: den registrerte har gitt samtykke til behandling av sine personopplysninger for ett eller flere spesifikke formål

1. behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse
2. behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige
3. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn (interesseavveining)

Det skal gå frem av kartleggingseskjemaet hvilke(t) grunnlag vi har for å behandle opplysninger. Hvis grunnlaget for behandling er samtykke fra den registrerte (se nr. 1), skal vi sette oss inn i de særlige reglene som gjelder for slike samtykker, blant annet kravet om dokumentasjon.

Hvis grunnlaget for behandling er vår berettigede interesse (interesseavveining) (se nr. 4), skal vi konkret og skriftlig dokumentere avveiningen, se nærmere nedenfor.

### 6.2. Ansatte

Behandling av opplysninger er i hovedsak rettslige forpliktelser. Noe av behandlingen er basert også på interesseavveining. Vi har behov for å dokumentere at vi har oppfylt forpliktelser etter lov og avtale etter at de er oppfylt. Vi har også behov for dokumentasjon for personaladministrasjon til bruk for fremtidig personaladministrasjon. Dette er berettigede interesser. Det er ikke mulig å ha tilgang til opplysningene på annen måte enn å lagre opplysningene. Behandling er derfor nødvendig.

Ansatte hos oss har et løpende avtaleforhold med oss. Personopplysningene vi behandler er knyttet til dette avtaleforholdet. Det er i stor grad snakk om opplysninger ansatte har gitt oss. Opplysningene gjelder forhold det er nærliggende at en arbeidsgiver behandler.



Vi mener at den berettigede interessen går foran den ansattes interesser.

### **6.3. Tidligere ansatte**

Behandlingen av de fleste av personopplysningene er basert på interesseavveining. Det kan oppstå behov for oss for å dokumentere personalforhold også etter at arbeidsforholdet er avsluttet, for eksempel en tvist med den tidligere ansatte. Dette kan gjelde for eksempel dokumentasjon for at vi som arbeidsgiver har oppfylt våre forpliktelser etter lovgivning eller arbeidsavtalen. Dette er en berettiget interesse. Det er ikke mulig å ha tilgang til opplysningene på annen måte. Behandling er derfor nødvendig.

Behandlingen går ut på å lagre opplysningene i inntil tolv måneder. Opplysninger om at den ansatte har vært ansatt, varighet av arbeidsforholdet og arbeidsoppgaver kan vi lagre lenger. Opplysningene vil ikke bli utlevert til andre uten at den tidligere ansatte ber om det, for eksempel i forbindelse med vurdering av ansettelse hos ny arbeidsgiver.

Vi mener at den berettigede interessen går foran den tidligere ansattes interesser.

### **6.4. Jobbsøkere**

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å bruke opplysninger for å vurdere søknader jobbsøkere sender oss. Dette er en berettiget interesse. Det er ikke mulig å vurdere en søknad uten å behandle personopplysninger. Behandling er derfor nødvendig.

Vi ber de som vil søke jobb hos oss om å sende oss minst opplysninger om navn, utdanning, arbeidserfaring, referansepersoner mv (CV). Jobbsøkere vil ofte gi ytterligere personopplysninger de regner som relevante for vurderingen av søknaden, for eksempel om kontaktinformasjon, familieforhold og interesser, i tillegg. I intervjuer stiller vi spørsmål for å avgjøre om jobbsøkeren passer til stillingen. I noen tilfeller kan vi bruke tester eller spørsmålsskjemaer for dette formålet. Hvis det blir aktuelt å ansette jobbsøkeren vil vi kunne be om ytterligere informasjon samt om dokumentasjon for opplysninger vi allerede har fått. Det er frivillig å gi oss opplysninger.

Vi bruker ikke opplysningene til noe annet enn å vurdere søknaden. Vi gir ikke opplysningene til noen andre. Vi kan beholde opplysninger fra jobbsøkere i seks måneder, i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt.

Vi mener at den berettigede interessen går foran jobbsøkerens interesser.

### **6.5. Kontaktpersoner hos leverandører**

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med våre leverandører for å følge opp blant annet tilbud, bestillinger og leveranser. Dette er en berettiget interesse. Den kontakten blir effektiv bare ved å kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som ønsker å være leverandør hos oss. I tillegg til navn behandler vi kontaktopplysninger, som telefonnummer, epostadresse og arbeidsgiver, som alle er knyttet først og fremst til kontaktpersonens arbeidsforhold og ikke til kontaktpersonens privatliv. Omfanget av opplysningene er svært begrenset. Behandlingen av opplysningene er knyttet til leverandørens næringsvirksomhet og ikke til kontaktpersonens privatliv. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.



## 6.6. Kontaktpersoner hos bedriftskunder

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med våre bedriftskunder for å følge opp tilbud, bestillinger og leveranser. Dette er en berettiget interesse. Den kontakten blir effektiv bare ved å kontakte enkeltpersoner direkte. Behandling er derfor nødvendig. Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som er kunde hos oss. I tillegg til navn behandler vi alminnelige opplysninger, som telefonnummer, epostadresse og arbeidsgiver, som alle er knyttet først og fremst til kontaktpersonens arbeidsforhold. Omfanget av opplysningene er derfor begrenset. Behandlingen av opplysningene er knyttet til leverandørens næringsvirksomhet og ikke til kontaktpersonens privatliv. Når det er påkrevet med samtykke etter markedsføringsloven, vil kontaktpersonen dessuten ha gitt samtykke før vi sender eposter med markedsføring. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

## 6.7. Andre kontaktpersoner

Behandling av personopplysninger er basert på interesseavveining. Vi har behov for å ha kontakt med offentlige myndigheter, for eksempel NAV og tilsynsmyndigheter i forbindelse med offentligrettslige forhold der vi kan ha forpliktelser og rettigheter. Dette er en berettiget interesse. I en del tilfeller vil den kommunikasjonen kunne være effektiv bare hvis vi kan kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Vi lagrer navn og kontaktdetaljer og vi bruker opplysningene til å kontakte personens arbeidsgiver. Opplysningene er knyttet til kontaktpersonens arbeidsgivers virksomhet og ikke til kontaktpersonens privatliv. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

## 6.8 Beboere og pårørende

Det registreres ulike typer personopplysninger i arkiv- og saksbehandlingssystemet. Dette er opplysninger som navn, adresse, telefonnummer og annen relevant informasjon som fremgår av oppdrag og henvendelser.

Saksdokumentene knyttet til våre oppdrag inneholder sensitive personopplysninger. Som en del av den pålagte saksbehandlingen innhenter vi opplysninger fra andre etater på eget initiativ etter lovhjemmel (forvaltningsloven §17).

Behandling av personopplysningene skjer innenfor rammen av gjeldende lov og forskrift, samt i henhold til eventuell konsesjon fastsatt av Datatilsynet. Vi benytter følgende elektronisk pasientjournalssystem (EPJ): Extensor.

Personopplysninger hentes inn for at virksomheten skal kunne utføre de oppgaver og tjenester vi er pålagt å utføre i henhold til lov og/eller avtale (Personopplysningloven med forskrift, Pasientrettighetsloven, Forskrift om IKT- standarder i helse – og omsorgstjenester, Helse og omsorgsloven, Forskrift om pasientjournal, Helsepersonell loven, Spesialisthelsetjenesteloven, Forvaltningslov, offentlighetslov og arkivlov).

Det hender at vi blir kontaktet av andre helseforetak eller instanser som også gir, har gitt eller skal gi medisinsk behandling, og som ber om å få utlevert pasientopplysninger. Helsepersonell har anledning til å utlevere taushetsbelagte opplysninger til samarbeidende helsepersonell som er underlagt samme taushetsplikt som våre ansatte. Dette gjøres kun i den grad det anses som nødvendig for å gi forsvarlig helsehjelp og reglene følger av helsepersonelloven § 25. Som pasient har man rett til å motsette seg slik



utlevering. Opplysningene som eventuelt deles er begrenset til det som er nødvendig. Vi deler kun slik informasjon dersom det etterspørres av det samarbeidende personell.

Likeledes utleverer vi kun personsensitiv informasjon til den som beboer eller verge har oppgitt som hovedpårørende/verge for beboer. Andre familiemedlemmer har ikke anledning til å motta slik informasjon om våre beboere.

## 7. Grunnlag for behandling av sensitive personopplysninger

Behandling av sensitive personopplysninger krever behandlingsgrunnlag i tillegg til de som er nevnt i punkt 6.

Sensitive personopplysninger er: opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Skal vi behandle slike opplysninger, skal vi sørge for å ha behandlingsgrunnlag. For ansatte hos oss vil opplysninger om helse og fagforeningsmedlemskap være særlig aktuelle. Helse omfatter for eksempel sykdom og skader og fravær begrunnet i dette. Særlig aktuelt behandlingsgrunnlag vil være at behandling er nødvendig i egenskap av arbeidsgiver, for eksempel ved oppfølging og rapportering til offentlige myndigheter eller ved tilrettelegging av arbeidsforholdet.

Behandling av opplysninger om straffbare forhold og lovovertridelser o.l. er underlagt særlige regler som vi skal sette oss inn i hvis vi skal behandle slike opplysninger.

For beboere er det spesielt opplysninger om helse som omfattes som sensitive personopplysninger. Behandling her følger av punkt 6.8 samt gjeldende lover og forskrifter som regulerer utøvelsen av pleie og omsorgstjenester.

## 8. Informasjon til de registrerte (personvernerklæring)

Vi skal gi lovbestemt informasjon til de registrerte. Vi skal gi slik informasjon i en personvernerklæring. Alle registrerte skal ha tilgang til den informasjonen som gjelder dem. Informasjon til ansatte gir vi i personalhåndbok eller lignende. Beboere og pårørende informeres i vårt velkomsthfte og via vår nettside.

Informasjonen skal inneholde blant annet navnet på bedriften og kontaktinformasjon, formålet med behandlingen, kategoriene av personopplysninger, mottakere av personopplysninger (dersom de utleveres), informasjon om eventuell utlevering av personopplysninger til andre land, hvor lenge personopplysningene vil bli lagret, de registrertes rett til å kreve innsyn, rette eller kreve slettet personopplysningene, hvordan virksomheten fikk tilgang til personopplysningene og muligheten til å klage virksomheten inn til Datatilsynet.

## 9. Registrertes rettigheter

Vi skal besvare henvendelser fra registrerte uten ugrunnet opphold. Mottar vi slike henvendelser, skal de sendes til adm.dir og personvernombud, Richard Skaar Thorsrud. Vi skal sørge for at registrerte får gjennomført rettighetene sine hos oss.



## **Rett til innsyn og informasjon om behandling av personopplysninger.**

Tjenestemottager avgir helse- og personopplysningene til virksomheten under et informert samtykke (jmf. Norm for informasjonssikkerhet 5.3.3 ).

Enhver kan henvende seg til våre enheter og be om innsyn i egen journal, få begrunne formålet med innhentet opplysninger, og hvor de er innhentet fra. Dette gjelder så vel elektroniske som manuelle journaler/arkiv dokumenter. Det gis informasjon om de nødvendige sikkerhetstiltak som benyttes i behandlingen av personopplysninger ifølge personopplysningsloven (pol) § 18.

Ved mangelfulle eller feilaktige opplysninger kan den registrerte kreve at opplysningene korrigeres eller slettes (Forskrift om pasientjournal, Personopplysningsforskriften).

Det innhentes samtykke i fra tjenestemottager om utlevering /overføring av helse- og personopplysninger til spesialisthelsetjenesten og kommunehelsetjenesten (jmf. Norm for informasjonssikkerhet 5.2.4).

## **10. Sletting av personopplysninger**

Vi skal slette personopplysninger uten ugrunnet opphold når de ikke lenger er "nødvendig" for formålet som de ble samlet inn eller behandlet for. Minst én gang i året skal vi gjennomgå dette. Våre retningslinjer for sletting følger nedenfor eller av kartleggingseskjemaet.

### **Ansatte**

Vi beholder som hovedregel alle opplysninger i hele ansettelsestiden. Ansatte kan be om at opplysninger blir slettet. Dette vil bli vurdert konkret. Lovgivningen kan stille krav til lengre oppbevaringstid.

### **Tidligere ansatte og jobbsøkere**

Se ovenfor om behandlingsgrunnlaget for disse kategoriene. Lovgivningen kan stille krav til lengre oppbevaringstid enn det som fremgår der.

Kontaktpersoner hos leverandører og kunder

Vi skal slette opplysningene når vi blir kjent med at kontaktpersonen har sluttet hos leverandøren eller kunden eller at leverandøren eller kunden har utpekt en ny kontaktperson. Det samme gjelder når leverandør- eller kundeforholdet er opphørt.

Vi kan likevel lagre opplysningene for en lengre periode hvis vi mener det kan bli nødvendig med dokumentasjon av den kontakten vi har hatt med leverandøren eller kunden. Det kan gjelde for eksempel spørsmål om rettigheter eller forpliktelser i avtaleforholdet med leverandøren eller kunden. Også lovgivningen kan stille krav til lengre oppbevaringstid.

### **Andre kontaktpersoner**

Vi skal slette opplysningene når vi blir kjent med at personen ikke lenger er relevant for våre behov, herunder hvis personen slutter hos den bedriften, offentlig etaten osv.

Vi kan likevel lagre opplysningene for en lengre periode hvis vi mener det kan bli nødvendig med dokumentasjon kontakt med personen eller personens arbeidsgiver. Det kan gjelde for eksempel spørsmål om rettigheter eller forpliktelser i avtale-, offentligrettslige eller andre forhold.



## Beboere

Informasjon fra vår elektroniske pasientjournal behandles, lagres og slettes i henhold til gjeldende lov og forskrift. Når det gjelder opplysninger i pasientjournaler så er adgangen til å få opplysninger slettet svært begrenset på grunn av regler i helsepersonelloven. Vi sikrer at opplysninger ikke kan endres eller slettes av andre enn de som er autorisert til å gjøre dette.

Vi vil i utgangspunktet ikke lagre personopplysninger lenger enn det som er nødvendig for å oppfylle formålet med behandlingen og de lovpålagte pliktene vi har. Når det kommer til personopplysninger lagret i pasientjournal så gjelder andre regler. Hovedregelen er at journalene skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem. Vi er etter helsearkivforskriften forpliktet til å avlevere journalmateriale til norsk helsearkiv etter dette.

## 11. Personvernombud

Vi har vurdert om personvernforordningen krever at vår bedrift skal ha personvernombud.

Vi har konkludert med at vår bedrift er underlagt krav om å ha personvernombud. Personvernombud er Richard Skaar Thorsrud, tlf. 91855603, e-post: richard@villaskaar.no

## 12. Alminnelig risikovurdering

Vi skal risikovurdere behandlingen av personopplysninger. Denne vurderingen skal gjøre at vi er i stand til å identifisere og definere hvilke sikkerhetstiltak vi skal gjennomføre.

Vurderingene skal gjelde sannsynlighet og alvorlighetsgrad (risiko) for personers "rettigheter og friheter", som fysisk skade, skade på ting eller formue og medisinsk skade. Eksempler på skader er diskriminering, identitetstyveri, omdømmeskade, tap av sosial aktelse, at konfidensielle opplysninger blir kjent for uvedkommende og uakseptable inngrep i privatlivets fred.

Kartleggingsskjemaet viser at vi:

- behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser
- har få eller ingen privatkunder
- ikke behandler opplysninger om barn
- behandler opplysninger som er en del av det å drive alminnelig næringsvirksomhet
- behandler personsensitiv informasjon som helseopplysninger knyttet til våre beboere

Vi har aldri vært utsatt for datainnbrudd. Vi er heller ikke kjent med at utenforstående har vist interesse for de personopplysningene vi behandler.

Basert på arten og omfanget av de opplysningene vi behandler, mener vi at konsekvensene ved regelbrudd kan være alvorlige.

Vi har derfor egne rutiner for behandling av opplysninger, herunder begrensnig av tilgang til dem.

Vi skal risikovurdere endringer som kan påvirke informasjonssikkerheten, for eksempel når vi kjøper nye IT-tjenester.



Resultatene av risikovurderinger skal godkjennes av den som har det daglige behandlingsansvaret i bedriften.

### 13. Informasjonssikkerhet

Vi skal etter loven treffe passende tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som svarer til risikoen knyttet til vår behandling av personopplysninger. Vi skal da ta hensyn til teknikkens stand, gjennomføringskostnadene og behandlingens karakter, omfang og formål, samt sammenhengen den utføres i.

Risikoene våre er vurdert overordnet i punktet ovenfor.

På denne bakgrunn har vi gjennomført disse tiltakene:

- Det er utpekt en person hos oss med særlig oppgave å påse sikkerheten: Richard Skaar Thorsrud
- Uvedkommende skal hindres tilgang til personopplysningene eller utstyr disse er lagret på,
- Det skal sikres at virksomhetens nettverk er beskyttet mot inntrengning fra eksterne nettverk med brannmur som kun slipper gjennom nødvendig datatrafikk,
- Det skal sikres at virksomhetenes nettverk er beskyttet mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.
- Ekstra tiltak skal iverksettes for spesielt beskyttelsesverdige opplysninger som for eksempel sykemeldinger, opplysninger rundt tilrettelegging av arbeidsplassen, vurderinger av den ansatte, merknader og advarsler.
- Ekstra tiltak skal iverksettes for spesielt beskyttelsesverdige opplysninger som er lagret i elektronisk pasientjournal, samt informasjon som sendes mellom vårt journalsystem og øvrige helseinstanser (spesialisthelsetjeneste, sykehus o.l.).
- Ansatte skal gis opplæring i bruk av virksomhetens IT-system.
- Vi sikrer at kun de som har et tjenstlig formål får tilgang til opplysningene.
- Helse og person opplysningene behandles i tråd med reglene om taushetsplikt og er beskyttet for innsyn fra uvedkommende. Uvedkommende omfatter også personell som ikke har tjenstlig behov (mål for konfidensialitet).
- Videre sikrer vi at opplysninger ikke kan endres eller slettes av andre enn de som er autorisert til å gjøre dette.
- Vi sikrer at personopplysningene er tilgjengelige når det er nødvendig for å utføre våre arbeidsoppgaver, for å gi best mulig tjeneste.
- Det er etablert særlige sikkerhetstiltak og rutiner for svært beskyttelsesverdig informasjon i arkivet og i journalsystemet.
- Det sendes ikke sensitive personopplysninger med e-post. Mottatte e-post som inneholder sensitive opplysninger skal ikke distribueres videre, og tas ut av e-postsystemet.
- Vår policy er at vi ikke skal videreformidle informasjon av noen art, om tjenestemottager, kunde eller medarbeider, til tredjepart uten at de har samtykket til dette.

### 14. Avvik, analyse av avvik og tiltak for å rette opp i dem

Vi må finne ut om behandlingen av personopplysninger følger reglene i personopplysningsloven og rutinene i dette dokumentet. Er det ikke tilfellet, må vi finne ut hvordan vi kan øke etterlevelsen. Vi skal dokumentere skriftlig både hvilke avvik vi har funnet og hva vi har gjort for å rette dem opp.

I kartleggingsskjemaet vil svar på spørsmål 15 kunne oppsummere avvik for hver kategori av registrerte. Den som fyller ut skjemaet skal gi beskjed til bestyrer om slike avvik. Den som oppdager avviket skal sette i gang umiddelbare tiltak hvis det er nødvendig for å begrense eller hindre vesentlige ulemper eller





følgeskader. Den som mottar meldingen skal først vurdere om det er nødvendig med umiddelbare tiltak. Deretter skal vedkommende sørge for at det blir gjennomført tiltak som skal gjøre at avvik ikke skjer igjen.

Viser det seg at rutinene ikke er godt nok tilpasset vår bedrift, bør vi vurdere å endre rutinene, se punkt 18.

## 15. Kjøp av IT-tjenester – databehandleravtaler

Vanligvis vil vi opptre som behandlingsansvarlig når virksomheten kjøper IT-tjenester fra en tjenesteleverandør. Vi har da fortsatt ansvaret for at personvernlovgivningen blir etterlevd ved kjøp av IT-tjenester, for eksempel elektronisk pasientjournal, HR-løsninger, avviksystemer eller kundedatabaser/CRM.

Før vi kjøper IT-tjenester skal vi derfor blant annet vurdere om leverandøren tilfredsstillende de kravene til sikkerhet som personopplysningsloven krever (artikkel 32) og forskrift om pasientjournal. Seriøse leverandører vil ofte kunne dokumentere at de oppfyller kravene. Vi må også sørge for å inngå en databehandleravtale som regulerer hvordan databehandleren skal håndtere personopplysningene den mottar fra og behandler på vegne av oss. Leverandører vil ofte ha egne avtaler som oppfyller kravene i regelverket.

Dersom tjenesteleverandøren skal overføre personopplysninger til land utenfor EU/EØS, må det foreligge et lovlig grunnlag for dette.

## 16. Innhenting av informasjon i andre sammenhenger

### 16.1 Bruk av pasientundersøkelser

For å måle våre beboere og/eller pårørendes tilfredshet så benytter vi spørreundersøkelser. Undersøkelsene er anonyme og all informasjon som hentes inn behandles konfidensielt. Informasjon offentliggjøres ikke dersom det er mulighet for at svar kan spores tilbake til den enkelte beboer.

All behandling av personopplysninger krever rettslig behandlingsgrunnlag. Relevant behandlingsgrunnlag for denne behandlingen er interesseavveining. Interesseavveining kan brukes som behandlingsgrunnlag der hvor behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger.

### 16.2 Markedsføring og nyhetsbrev

#### Sosiale media

Vi ønsker å være tilgjengelig for våre kunder og potensielle kunder i sosiale medier og har derfor profil på Facebook. Formålet med disse sidene er å gjøre våre tjenester, vår kontaktinformasjon og åpningstider tilgjengelige for våre kunder og potensielle beboere. Dersom man ønsker å ta kontakt med oss ved hjelp av disse kanalene så oppfordrer vi til å ikke dele personopplysninger. Dersom det kommer spørsmål som



innebærer deling av sensitive personopplysninger (eks opplysninger om helse) så anbefaler vi at kontakt opprettes per telefon.

## Nyhetsbrev

Vi sender nyhetsbrev til pårørende og kommuner. Vårt nyhetsbrev sendes per e-post. I nyhetsbrevet fir vi informasjon om aktiviteter, meny og andre aktuelle saker fra våre hjem.

Nye pårørende forespørres om de ønsker å motta nyhetsbrevet. Når man registrerer seg for å motta nyhetsbrevet samtykker man til at vi kan sende deg nyhetsbrev med informasjon om våre helsetjenester, samt at vi måler åpningsgrad og klikk på linker i nyhetsbrevet etter hver utsendelse. Dette gjøres ved hjelp av «e-marketeer», som har kvalitetssikret sine tjenester i tråd med ny GDPR-policy.

Man kan når som helst melde seg av nyhetsbrevet. Dette gjør du ved å gå inn på vårt siste nyhetsbrev, og trykke på avmeldingslinken.

Vi vil ikke bruke dine opplysninger til annen markedsføring eller andre tjenester enn til å sende ut dette nyhetsbrevet.

## Chat

På våre hjemmesider har vi en chat-tjeneste hvor du enkelt kan komme i kontakt med oss. I chatten kan vi behandle enkle forespørslers som for eksempel åpningstider, adresser og svare på generelle spørsmål. Vi behandler ikke sensitiv informasjon eller personlige opplysninger i denne kanalen.

## 16.3 Cookies (informasjonskapsler)

Informasjonskapsler (cookies) er små tekstfiler som plasseres på din datamaskin eller enhet når du laster ned en nettside. Bruk av informasjonskapsler er svært vanlig og kan for eksempel brukes til å lagre innloggingsdetaljer eller registrere hvordan en nettside blir brukt. Informasjonskapsler kan således være nyttig både for nettstedseier og brukeren. For å verne brukerens personvern og kommunikasjonsutstyr er det gitt krav om informasjon og samtykke når en virksomhet ønsker å benytte informasjonskapsler.

Ved å gå inn og hente informasjon og/eller benytte tjenester på våre nettsider, samtykker brukeren i at det settes informasjonskapsler. Forhåndsinnstilling i en nettleser om at brukeren aksepterer informasjonskapsler/cookies anses som samtykke i henhold til norsk rett. Dersom du ikke vil akseptere vår bruk av informasjonskapsler, kan du gå inn og trekke tilbake ditt samtykke ved å endre innstillingene i nettleseren. Vi gjør imidlertid oppmerksom på at dette kan medføre at tjenestene på våre nettsider ikke fungerer optimalt. For nærmere informasjon om dette, se vår cookiepolicy her.

## 17. Brudd på personopplysningssikkerheten

Ved brudd på personopplysningssikkerheten (for eksempel hackerangrep eller tap av personopplysninger) skal vi straks kontakte Datatilsynet for å finne ut hva vi bør gjøre.

"Brudd på personopplysningssikkerheten" betyr brudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som vi behandler.



Ved visse brudd på personopplysningssikkerheten skal vi varsle Datatilsynet og av og til også den registrerte. Varsling til Datatilsynet skal skje med én gang, og senest 72 timer etter at vi ble kjent med bruddet. Det er ikke nødvendig å varsle Datatilsynet hvis det er lite trolig at bruddet på personopplysningssikkerheten vil føre med seg risiko for enkeltpersoners rettigheter. Et eksempel er der et sikkerhetsbrudd har ført til at uvedkommende har fått tilgang til personopplysninger som allerede er offentlig tilgjengelige.

Vi har plikt til å varsle den registrerte dersom det er trolig at bruddet på personopplysningssikkerheten vil medføre høy risiko for enkeltpersonenes rettigheter og friheter. Vi mener at vår behandling av personopplysninger bare helt unntaksvis kan føre til slik risiko.

Vi skal dokumentere eventuelle brudd på personopplysningssikkerheten. Dette gjør vi ved å beskrive de faktiske forholdene rundt bruddet ("Hva har skjedd?"). I tillegg skal vi beskrive virkningene av bruddet og hvilke tiltak som er truffet for å avhjelpe bruddet. Denne dokumentasjonen skal gjøre det mulig for Datatilsynet å kontrollere at virksomheten har etterlevd kravene i loven.

## 18. Vurdering av personvernkonsekvenser og forhåndskonsultering med Datatilsynet

Vi skal utrede personvernkonsekvensene når den planlegger en behandling av personopplysninger som sannsynligvis vil utgjøre høy risiko for personers rettigheter, som retten til personvern. I vurderingen av om det er nødvendig med en slik utredning skal vi ta hensyn til arten, omfanget, sammenhengen og formålet med behandlingen. Den skal også ta hensyn til om den benytter ny teknologi.

Det er flere typetilfeller der det er nødvendig å utrede personvernkonsekvenser: Systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser, behandling av sensitive personopplysninger i stort omfang eller systematisk overvåking av offentlig område i stort omfang. I tilfellene ovenfor skal vi sette oss inn i de særlige reglene som gjelder, blant annet om at Datatilsynet av og til skal involveres i forhåndsdrøftelser.

## 19. Kontroll, oppdatering og revisjon av dokumentet

Vi skal oppdatere og revidere dette dokumentet jevnlig. Bakgrunnen er blant annet at reglene i lov og forskrift kan bli endret, vår behandling av personopplysninger kan bli endret eller erfaringer kan tilsi at vi bør endre rutineene våre. Av de samme grunnene skal vi også jevnlig gjennomgå og oppdatere skjemaene med kartlegging av behandling av personopplysninger.

Det er Bestyrer som har ansvar for at behov for endringer og revisjoner blir identifisert og innarbeidet i dokumentet og i skjemaet. Dette skal gjøres årlig.

Evalueringen bør omfatte for eksempel på følgende spørsmål:

Har vi siden forrige revisjon endret (nye, endrede eller avsluttede) behandlinger av personopplysninger som ikke er behandlet i dokumentet eller i skjemaene?

Tilsier de seks grunnkravene til behandling av personopplysninger at vi bør endre rutiner eller praksis?

- Har det siden forrige revisjon trådt i kraft nye regler i lov eller forskrift som tilsier endringer?
- Har virksomheten siden forrige revisjon oppdaget andre områder for forbedring av dokumentet eller skjemaene?
- Har det kommet ny teknologi som gjør at personopplysninger kan sikres på en bedre måte