Når det må fungere.

Gjelder GDPR for borettslag

Vennligst merk at dette informasjonsskrivet inneholder kun generell informasjon og utgjør ikke juridisk rådgivning. Hvis dere har spesifikke spørsmål eller bekymringer knyttet til GDPR, er det tilrådelig å konsultere en juridisk ekspert som er kjent med personvernreguleringer.

Hva er GDPR?

Personvernforordningen (General Data Protection Regulation) er et sett med regler som er implementert for å beskytte enkeltpersoners grunnleggende rettigheter og personvern innenfor den europeiske unionen (EU). Den gir retningslinjer for behandlingen av personopplysninger og har til hensikt å sørge for gjennomsiktighet, rettferdighet og sikkerhet for den registrerte.

Hvem er den registrerte?

Den registrerte er den enkeltpersonen som kan identifiseres - enten direkte eller indirekte - gjennom personopplysningene som samles inn. Den registrerte har visse rettigheter og beskyttelser når det gjelder behandlingen av deres personopplysninger.

Disse rettighetene inkluderer blant annet:

- **Rett til informasjon:** Den registrerte har rett til å få informasjon om hvordan og hvorfor deres personopplysninger blir behandlet, for eksempel hvilke typer opplysninger som samles inn, formålet med behandlingen og hvem som er involvert.
- **Rett til innsyn:** Den registrerte har rett til å be om innsyn i hvilke personopplysninger som behandles om dem, og å få tilgang til denne informasjonen.
- **Rett til rettelse:** Hvis personopplysningene som behandles er unøyaktige eller ufullstendige, har den registrerte rett til å be om at opplysningene blir rettet eller oppdatert.
- **Rett til sletting:** Under visse omstendigheter har den registrerte rett til å be om sletting av deres personopplysninger, for eksempel når opplysningene ikke lenger er nødvendige for det formålet de ble samlet inn for.
- **Rett til begrensning av behandling:** Den registrerte kan be om begrensning av behandlingen av deres personopplysninger i visse situasjoner, for eksempel hvis nøyaktigheten av opplysningene bestrides.
- **Rett til dataportabilitet:** I noen tilfeller har den registrerte rett til å motta deres personopplysninger i et strukturert, vanlig brukbart format og har rett til å overføre disse opplysningene til en annen behandlingsansvarlig.
- **Rett til å protestere:** Den registrerte har rett til å protestere mot behandlingen av deres person-opplysninger basert på sin spesifikke situasjon, med mindre det er tvingende berettigede grunner for behandlingen som veier tyngre.

Hva er en personopplysning?

En personopplysning er enhver opplysning som direkte eller indirekte kan identifisere en fysisk person. Dette kan omfatte navn, adresse, e-postadresse, telefonnummer, fødselsdato, IP-adresse, biometriske data eller andre identifikatorer knyttet til en spesifikk person.

StepLock Access, Øvre Storgate 86, 3018 Drammen, Norway
+47 23 00 30 00 | post@steplock.no | www.steplockaccess.no

Når det må fungere.

Hvem må følge GDPR?

Enhver person, organisasjon eller virksomhet som behandler personopplysninger om EU-borgere, uavhengig av deres geografiske beliggenhet, må følge GDPR. Dette gjelder også for Norge, selv om vi ikke er medlemstat i EU.

Hva er en behandlingsansvarlig?

En behandlingsansvarlig er en person eller en organisasjon som bestemmer formålet med og midlene for behandlingen av personopplysninger. Behandlingsansvarlige har ansvaret for å sikre at behandlingen av personopplysninger skjer i samsvar med personvernlovgivningen, spesielt personvernforordningen (GDPR). Dersom borettslagstyre går til anskaffelse av en IT-tjeneste på vegne leietakere og leietakeres navn, telefon-nummer og epost-adresse samles inn til bruk i tjenesten, vil borettslagstyre være behandlingsansvarlig.

Den behandlingsansvarlige har følgende hovedansvar i henhold til GDPR:

- **Formålet med behandlingen:** Den behandlingsansvarlige må klart definere formålet med innsamling og behandling av personopplysninger. Formålet må være lovlig, spesifikt og legitimt.
- **Lovlig grunnlag:** Den behandlingsansvarlige må sikre at det finnes et gyldig lovlig grunnlag for behandlingen av personopplysninger. Dette kan være samtykke fra den registrerte, oppfyllelse av en avtale, juridiske forpliktelser, beskyttelse av vitale interesser, oppgaver av allmenn interesse eller utøvelse av offentlig myndighet, eller legitime interesser som veier tyngre enn personvernhensynet.
- **Informasjon og gjennomsiktighet:** Den behandlingsansvarlige har plikt til å informere de registrerte om hvilke personopplysninger som samles inn, formålet med behandlingen, rettighetene til de registrerte og annen relevant informasjon som er nødvendig for å sikre en rettferdig og gjennomsiktig behandling.
- **Sikkerhet og personvern:** Den behandlingsansvarlige må implementere egnede tekniske og organisatoriske tiltak for å sikre at personopplysningene behandles på en sikker måte og beskyttes mot uautorisert tilgang, tap, ødeleggelse eller skade.
- **Rettigheter til de registrerte:** Den behandlingsansvarlige må respektere og legge til rette for de registrertes rettigheter, inkludert retten til tilgang, retting, sletting, begrensning av behandling, dataportabilitet og retten til å protestere mot behandlingen.
- **Databehandleravtale:** Hvis den behandlingsansvarlige engasjerer en tredjepart (databehandler) til å behandle personopplysninger på deres vegne, må det etableres en databehandleravtale som regulerer forholdet og sikrer at databehandleren også handler i samsvar med GDPR.

Hva er en databehandler?

En databehandler er en tredjepart eller organisasjon som behandler personopplysninger på vegne av den behandlingsansvarlige i henhold til GDPR. Databehandleren kan være en ekstern tjenesteleverandør eller et selskap som er engasjert av den behandlingsansvarlige for å utføre spesifikke oppgaver knyttet til behandlingen av personopplysninger. For eksempel leveranse av skybasert porttelefontjenester. Det er viktig å merke seg at databehandleren har klare ansvarsområder i henhold til GDPR. De må behandle personopplysninger i samsvar med instruksjoner fra den behandlingsansvarlige og har et ansvar for å

implementere passende sikkerhetstiltak for å beskytte personopplysningene. Databehandleren har også plikt til å melde fra til den behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten.

Hva er en Databehandleravtale?

En databehandleravtale er en juridisk avtale mellom behandlingsansvarlige og databehandleren som regulerer behandlingen av personopplysninger på vegne av den behandlingsansvarlige. Databehandleravtalen er et viktig verktøy for å sikre at personopplysninger behandles i samsvar med GDPR (General Data Protection Regulation) og at begge parter oppfyller sine juridiske forpliktelser.

En databehandleravtale inneholder vanligvis følgende elementer:

- **Formål og omfang:** Avtalen beskriver formålet med behandlingen av personopplysninger og angir hvilke typer personopplysninger som skal behandles av databehandleren.
- **Instruksjoner fra behandlingsansvarlig:** Avtalen fastsetter at databehandleren kun kan behandle personopplysninger i samsvar med instruksjoner gitt av behandlingsansvarlig. Dette sikrer at databehandleren handler på vegne av den behandlingsansvarlige og i samsvar med deres ønsker.
- **Konfidensialitet:** Databehandleravtalen fastsetter at databehandleren må opprettholde konfidensialitet når det gjelder personopplysningene som behandles. Dette innebærer å implementere passende sikkerhetstiltak og begrense tilgangen til personopplysningene til autoriserte personer.
- **Underleverandører:** Hvis databehandleren benytter seg av underleverandører for å utføre behandlingen av personopplysninger, skal avtalen regulere hvordan slik underleverandørbehandling skal håndteres, inkludert krav til konfidensialitet og sikkerhet.
- **Rettigheter og forpliktelser:** Databehandleravtalen fastsetter de spesifikke rettighetene og forpliktelsene til både behandlingsansvarlig og databehandleren i henhold til GDPR. Dette inkluderer forpliktelser til å håndtere personopplysninger sikkert, varsle om brudd på personopplysningssikkerheten og samarbeide med tilsynsmyndigheter.
- **Varighet og oppsigelse:** Avtalen fastsetter varigheten av samarbeidet mellom behandlingsansvarlig og databehandleren, samt vilkårene for oppsigelse av avtalen.

Hva menes med lovlig grunnlag for innsamling av personopplysninger?

Lovlig grunnlag for innsamling av personopplysninger refererer til det rettslige grunnlaget eller den lovbestemte grunnen som en behandlingsansvarlig må ha for å samle inn og behandle personopplysninger i henhold til GDPR. Det lovlige grunnlaget danner det rettslige fundamentet for å kunne behandle personopplysninger på en rettferdig og transparent måte.

GDPR fastsetter flere alternative juridiske grunnlag som kan brukes for innsamling og behandling av personopplysninger. De viktigste lovlige grunnlagene inkluderer:

- **Samtykke:** Behandlingsansvarlig kan innhente samtykke fra de registrerte som gir dem tillatelse til å behandle deres personopplysninger for spesifikke formål. Samtykket må være frivillig, informert, uttrykkelig og kan trekkes tilbake når som helst.
- **Avtaleutførelse:** Hvis behandlingen av personopplysninger er nødvendig for å oppfylle en avtale med den registrerte, for eksempel levering av varer eller tjenester, utgjør avtaleutførelse et juridisk grunnlag for innsamling og behandling av personopplysninger.
- **Rettslige forpliktelser:** Hvis behandlingsansvarlig er pålagt å behandle personopplysninger for å overholde en juridisk forpliktelse, for eksempel skattelovgivning eller arbeidsrett, kan dette utgjøre et juridisk grunnlag for behandlingen.
- **Beskyttelse av vitale interesser:** Hvis behandlingen av personopplysninger er nødvendig for å beskytte liv eller fysiske interesser til den registrerte eller en annen person, kan dette utgjøre et juridisk grunnlag.
- **Legitime interesser:** Dersom behandlingsansvarlig har legitime interesser som veier tyngre enn personvernhensynet til de registrerte, kan behandling av personopplysninger være tillatt som et juridisk grunnlag. Det må foretas en balansevurdering mellom behandlingsansvarliges interesser og personvernet til de registrerte.

Hva er sensitive personopplysninger?

Sensitive personopplysninger inkluderer informasjon om rase eller etnisk opprinnelse, politiske meninger, religiøse eller filosofiske overbevisninger, medlemskap i fagforeninger, genetiske data, biometriske data, helsedata eller data om en persons seksualliv eller seksuell orientering. Behandlingen av sensitive data er underlagt ytterligere sikkerhetskrav og betingelser i henhold til GDPR. Normalt sett er det ikke lov å samle inn og behandle slike opplysninger.

Hva bør virksomheten gjøre?

Trinn 1: Bli kjent med GDPR:
Ta deg tid til å forstå de viktigste prinsippene, forpliktelsene og rettighetene som er beskrevet i GDPR. Dette inkluderer prinsipper som lovlighet, rettferdighet og gjennomsiktighet i databehandlingen, samt enkeltpersoners rettigheter til å få tilgang til, korrigere og slette sine personopplysninger.
Identifiser de viktigste definisjonene, inkludert begreper som "personopplysninger", "behandlings-ansvarlig" og "databehandler", for å sikre en klar forståelse av deres roller og ansvar.

Trinn 2: Kartlegging og oversikt over data:
Gjennomfør en grundig kartlegging av all personopplysningene som vil bli samlet inn, lagret eller behandlet. Bestem det lovlige grunnlaget for behandling av denne informasjonen.

Dokumenter flyten av data, inkludert hvor dataene kommer fra, hvordan de samles inn, hvem som har tilgang til dem, og hvor de lagres eller overføres. Dette vil hjelpe deg med å identifisere potensielle risikoer og implementere passende sikkerhetstiltak.

Trinn 3: Personvernerklæring:
Lag en personvernerklæring som tydelig kommuniserer til de registrerte formålet og det rettslige grunnlaget for behandling av deres personopplysninger. Inkluder informasjon om den registrertes rettigheter, som for eksempel retten til å få tilgang til og korrigere sine personopplysninger, samt hvor lenge personopplysningene vil bli lagret.

Trinn 4: Data-sikkerhet og beskyttelse:
Implementer passende tekniske og organisatoriske tiltak for å beskytte de personopplysningene som samles inn. Dette kan inkludere to-stegs-autentisering og regler for lenden på passord, tilgangskontroller og opplæring av ansatte rundt nettsikkerhet og databeskyttelse.

Vurder sikkerhetstiltakene som tilbys av tjenesteleverandøren som benyttes. Sjekk at de overholder standarder for databeskyttelse og har riktige databehandleravtaler på plass.

Trinn 5: Rettigheter for registrerte:
Etabler prosedyrer for å håndtere forespørsler fra de registrerte på en effektiv måte. Dette inkluderer å svare på forespørsler om tilgang, korrigering, sletting og begrensning av behandling innenfor rimelighetens tid. Utpeke en ansvarlig person eller et team i organisasjonen for å håndtere slike forespørsler og sørge for at de er opplært til å håndtere dem på riktig måte.

Trinn 6: Konsekvensvurdering for databeskyttelse (DPIA):
Gjennomfør en DPIA for å vurdere og redusere potensielle risikoer for enkeltpersoners personvernrettigheter. Dette er spesielt viktig når man implementerer et nytt system som innebærer behandling av person-opplysninger.

Vurder faktorer som arten, omfanget, konteksten og formålene med behandlingen, samt potensielle risikoer for enkeltpersoners rettigheter og friheter.

Trinn 7: Kontinuerlig etterlevelse:
Gjennomgå og oppdater personvernpraksis og prosedyrer jevnlig for å sikre kontinuerlig etterlevelse av GDPR-kravene. Hold deg oppdatert om eventuelle endringer i personvernlovgivningen og juster prosessene deretter. Gjennomfør jevnlige revisjoner og vurderinger for å verifisere effektiviteten av dine tiltak for data-beskyttelse.