GDPR vedlegg til internkontrollrutiner for FeFor Høifjellshotell

Dato: 9.4.2018

1.0 Lagring av data

Data som kan identifisere individer finnes i vårt CRM system, i vår epost klient, i vårt salgssystem, i vårt regnskapssystem og i noen excel filer som befinner seg på datamaskinen til daglig leder. I tillegg har vi ulike leverandører som besitter personopplysninger slik som markedsføringsselskapet og regnskapsføring selskapet.

1.1 Formål med lagring av data

Vi lagrer data for å kunne utvikle våre tjenester. Vi lagrer data der det er lovpålagt. Vi lagrer data for å bedre kundereisen og ha en god kundeservice basert på kundens historikk. Vi lagrer data for å kunne utvikle våre ansatte. Vi lagrer data på eksterne/innkommende forespørsler der det er formålstjenlig å kartlegge hvem som har kommet med henvendelsen. Vi selger ikke ikke data som kan identifisere individer videre til noen tredjepart.

1.1.1 Ansatte

Vi vil lagre personopplysninger om våre ansatte slik at vi sammen med den ansatte i best mulig grad kan utvikle dennes arbeidssituasjon i en positiv retning for begge parter. Vi lagrer kontrakter, evalueringssamtaler, advarsler, forespørsler og etterutdanning. I tillegg til med søknader, CV, vår økonomiske relasjon samt digital kommunikasjon og digitale klienter. Vi lagrer også all digital kommunikasjon slik som epost, tekstmeldinger, samtaler på sosiale medier og eventuelle kommentarer på sosiale medier

1.1.2 Kunder

Vi lagrer personopplysninger om våre klienter for å i størst mulig grad legge til rette for en så god kunderelasjon som mulig. Informasjon vi lagrer er transaksjoner vi har gjort, navn, telefonnummer, adresse og epost der det finnes, profiler fra sosiale medier med tilhørende kommunikasjonsmuligheter samt tekstmeldinger og epost.

1.1.3 Andre

Vi lagrer personopplysninger på innkommende henvendelser, der den som henvender seg velger å dele slikt med vår virksomhet. Informasjon lagres fordi det er formålstjenlig å ha en klar og tydelig motpart med hensyn på konstruktive dialoger med eksterne parter.
Vi lagrer den informasjon som den som henvender seg deler med oss. Vi lagrer ytterligere informasjon om den som henvender seg der denne har/bruker den innkommende adressen i ulike sosiale medier. Vi lager all digital kommunikasjon som forekommer med den som henvender seg.

1.2 Hvilke data lagres

Det er ulik informasjon som lagres om de ulike interessegruppene. Informasjon er avhengig av formålet med informasjon samt hvilke ulike samtykker som ligger til grunn. Det viktigste for oss er at informasjonen er lett oversiktlig, tilgjengelig og at alle parter forstår hvorfor vi lagrer informasjonen. Noe som i sin tur også sørger for at informasjonen er enkel å slette enten automatisk eller på forespørsel

1.2.1 Ansatte

Vi lagrer CV, vi lagrer personopplysninger inkludert skattekort, vi lagrer etterutdanning, vi lagrer advarsler, vi lagrer lønn og trekksoppgaver, vi lagrer digital kommunikasjon samt løpende evalueringer og advarsler.

1.2.2 Kunder

Vi lagrer navn, telefonnummer, adresse, epost der vi har, betalingshistorikk samt endringer på nevnte. I tillegg lagrer vi profiler fra sosiale medier og digital kommunikasjon.

1.2.3 Andre

Vi lagrer innkommende henvendelser og fyller ut med tilgjengelig informasjon slik at henvendelsen kan identifiseres. Vi lagrer profiler fra sosiale medier samt tilhørende og ytterligere digital kommunikasjon

1.3 Hvor lagres dataene

1.3.1 Ansatte

Regnskapssystem
HMS system
Epost klient
Digitale profiler

1.3.2 Kunder

CRM system
Regnskapssystem
Epost klient
Tekstmeldinger
Digitale profiler

1.3.3 Andre

CRM system

Epost klient
Digitale profiler

2.0 Sletting av dataene

Vårt premiss for all lagring av data som kan identifisere et individ. Er at dataene har en naturlig livssyklus og derav begrenset levetid. Levetiden kontrolleres for oss av to faktorer 1) hvor lenge det er hensiktsmessig og formålstjenlig for vår virksomhet å oppbevare dataene. 2) hva vi er pålagt ved lov å oppbevare

2.1 Automatisk sletting

2.1.1 Ansatte

For ansatte avhenger det av hvilken data det er snakk om. Vi oppbevarer personopplysninger som er relevante for arbeidsforholdet så lenge arbeidsforholdet eksisterer. Deretter slettes alle personopplysninger fra våre HMS systemer, sletting av den ansatte sin epostklient og andre digitale brukerprofiler den har har i forbindelse med arbeidsforholdet samt annen kommunikasjon den ansatte har gjort slik som tekstmeldinger eller kommentarer på våre brukerprofiler i sosiale medier. De økonomiske dataene relatert til arbeidsforholdet, slettes når gjeldene regnskapslover tilater det.

2.1.2 Kunder

Vi lagrer personopplysninger så lenge det forekommer aktive transaksjoner i relasjonen. Vi anser aktive transaksjoner med et minimum hver 24 måned. Deretter slettes alle opplysninger som kan identifisere et individ. Med det menes; vi beholder transaksjonshistorikken samt husstanden, men sletter alle opplysninger som kan henvise til og eller identifisere et individ.

2.1.3 Andre

Vi lagrer de personopplysningene vi besitter fra innkommende henvendelser avhengig av hvilken type forespørsel det er og hvilken risiko/gevinst henvendelsen kan være for virksomheten. Henvendelser fra offentlige etater og institusjoner som har innvirkning for vår virksomhets daglige drift, lagres så lenge det anses formålstjenlig. Her er formålstjenlig så lenge personen som tok kontakt, innehar samme posisjon som ved kontakt og det er en part vi som virksomhet må forholde oss til. Når vi mottar eller identifiserer informasjon som tilsier at informasjonen vi besitter ikke lengre er formålstjenlig eller har relevans. Slettes den fra vårt CRM system samt epost klient. Informasjon som kan identifisere andre individer, slettes fra vårt CRM system og epost klient, når henvendelsen kan anses først som løst og deretter som utenfor fare for gjentakelse.

2.1.4 Rutine for automatisk sletting

Rutinene for automatisk sletting er basert på de overnevnte tidsintervallene for ansatte, klienter og andre. Det som prosessteknisk da gjøres er at behandlingsansvarlig (en som arbeider i vår virksomhet og som har nødvendig systemopplæring - se forøvrig opplæring i pkt 4.1) søker opp individet i de underliggende systemene og sletter personopplysninger, tar vare på opplysningene vi er lovpålagt og erstatter individ med husstand der det er formålstjenlig.

- CRM system
- HMS system
- Interne dokumenter
    - Excelark
    - Personalmapper
- Epost klient
- Tekstmeldinger o.l.
- Kommunikasjon på sosiale medier
- Regnskapssystem

2.2 Sletting på forespørsel

Rutinene for sletting på forespørsel har liten eller ingen teknisk forskjell til den automatiske slettingen, med unntak av eventuelle uoverensstemmelser om hvilken informasjon som skal slettes. Spesielt i tilfeller hvor de som ber om slettingen avviker fra de som eier informasjon og således ikke er en juridisk part i transaksjonen. Samt forespørsler om sletting hvor vi ser at det er sannsynlig at interessenten kan dukke opp i våre systemer igjen fra andre kanaler og begge parter er enige om at det ikke er formålstjenlig for noen av partene. Slike forespørsler behandles individuelt.

2.2.1 Rutine for sletting

Det som prosessteknisk da gjøres er at behandlingsansvarlig (en som arbeider i vår virksomhet og som har nødvendig systemopplæring - se forøvrig opplæring i pkt 4.1) søker opp individet i de underliggende systemene og sletter personopplysninger, tar vare på opplysningene vi er lovpålagt og ta vare på og erstatter individ med husstand der det er formålstjenlig.

- CRM system
- HMS system
- Interne dokumenter
    - Excelark
    - Personalmapper
- Epost klient
- Tekstmeldinger o.l.

- Kommunikasjon på sosiale medier
- Regnskapssystem, i samråd med databehandler

3.0 Samtykke til lagring av data

Primært forholder vi oss til lagring av personopplysninger der det er i tråd med vårt formål og det skjer i aktive relasjoner. Men i forbindelse med initierende kontakt med våre interessegrupper, der en felles forståelse av vår virksomhets formål ikke faller seg naturlig, benytter vi ulike former for samtykkeerklæringer slik at individ forstår hvilken informasjon de overlater til vår virksomhet, hva/hvordan vi benytter denne informasjon og hvor informasjon lagres. Se forøvrig standard samtykke i appendix. Situasjoner hvor vi ber om samtykke er fek,s, men ikke begrenset til, vil selge/tilby andre tjenester (et annet nyhetsbrev enn det de har signert seg opp for) eller lignende.

3.1 Samtykke erklæring

Vår virksomhet lagrer primært data og tilhørende personopplysninger basert på formål og gjensidig forståelse mellom vår virksomhet og våre interessegrupper om formålene. Det vil likevel forekomme situasjoner hvor det er naturlig å mer eksplisitt bekrefte forståelsen. I den forbindelse benytter vi egne samtykkeerklæringer. Slike situasjoner er som regel i forbindelse med innkommende henvendelser fra interessenter og eller innkommende henvendelser fra tidligere ansatte, men selvfølgelig ikke begrenset til.

3.1.1 Ansatte

Om ansatte tar kontakt og etterspør informasjon slik som, men ikke begrenset til; referanser og annen info. Må den ansatte bekrefte i egen epost at den godtar at vi oppbevarer informasjon virksomheten produserer i den perioden informasjonen skal benyttes av den ansatte slik at vi har kontroll/kan bekrefte at virksomheten står inne for budskapet. Deretter foretas en automatisk sletting av informasjonen.

3.1.2 Kunder

I situasjoner hvor klienter etterspør sletting av personopplysninger, innhenter vi en samtykkeerklæring hvor klienten tillater at vi oppbevarer deler av personopplysningene for å påse at klienten ikke dukker opp i våre systemet fra andre kanaler på et senere tidspunkt.

3.1.3 Andre

I forbindelse med enkelte innkommende henvendelser til virksomheten, besvares de med en general epost hvor det bes om eksplisitt samtykke til at vi lagrer personopplysninger i den tid

interessenten har en relasjon til virksomheten og det er naturlig og formålstjenlig for begge parter å lagre denne informasjonen.

3.1.4 Ytterligere bekreftelser

Vi opplyser i våre digitale flater om hvilken informasjon som lagres, med hvilket formål informasjon lagres på innkommende henvendelser og hvordan interessenten kan gå frem for å få slettet informasjonen.

4.0 Behandlingsansvarlig og rutiner

Virksomheten er behandlingsansvarlig. Med det menes; de er den ansvarlige part som har samlet inn, besitter og “eier” personopplysningene. Virksomheten kan inkludere 3- parts virksomheter i forbindelse med utførelse av tjenester i.h.t avtale og sånn gjøre en 3 part ansvarlig for samme data. Men det betyr ikke at virksomheten kan overføre ansvaret. Det gir bare flere enheter med samme ansvar. For å sikre at at virksomheten er compliant med GDPR hele veien, gir vi samme opplæringen av hva det innebærer til alle som arbeider/er tilknyttet organisasjonen.

4.1 Opplæringsrutiner

Alle ansatte i vår virksomhet skal gjennom et foredrag med opplæring i personvern, foredraget ligger i appendix. Men grunnprinsippene er som følger;

- Behandlingen må være tillatt. Med det menes; vi må ha et behandlingsgrunnlag
- Personopplysningene kan bare brukes til uttrykkelig angitte formål som må være saklig begrunnet i virksomheten
- Bruk til nye, uforenlige formål er forbudt uten samtykke
- Personopplysningene må være nødvendige for formålet (samt korrekte og oppdaterte)
- Personopplysningene må slettes når formålet ikke lenger begrunner lagring/behandling

5.0 Databehandler

Databehandlere er organisasjoner vår virksomhet samarbeider med og som i den forbindelse, i gitte tilfeller, må håndtere personopplysninger vi har samlet inn. For å påse at de opptrer i tråd med gjeldende lovverk, har vi utviklet en avtale hvor vår samarbeidspartner bekrefter sin compliance med GDPR.

5.1 Instruksjon

Formålet med denne Databehandleravtalen er å regulere Partenes rettigheter samt plikter, for å sikre at Personopplysninger behandles i overensstemmelse med de vilkår som følger

av personopplysningsloven (lov av 14 april 2000 nr. 31) og personopplysningsforskriften (forskrift av 15 desember 2000 nr. 1265,) og senere lovgivning som erstatter disse, heretter benevnt i felleskap som Personopplysningsloven

5.2 Avtaler

Databehandleravtale mellom orgnummer_____ heretter benevnt som databehandler og leverandør og orgnummer_____ heretter benevnt som behandlingsansvarlig og kunde. I fellesskap benevnt som partene

1. Avtalens formål og virkeområde

Partene har (dato) inngått en avtale hvor leverandøren skal bistå kunden med (beskrivelse.) Leveransen medfører at leverandør behandler personopplysninger på vegne av kunden

“Formålet med denne Databehandleravtalen er å regulere Partenes rettigheter samt plikter, for å sikre at Personopplysninger behandles i overensstemmelse med de vilkår som følger av personopplysningsloven (lov av 14 april 2000 nr. 31) og personopplysningsforskriften (forskrift av 15 desember 2000 nr. 1265,) og senere lovgivning som erstatter disse, heretter benevnt i felleskap som Personopplysningsloven.”

Definisjonene i personopplysningsloven §2 gjelder tilsvarende for begreper som er angitt med stor forbokstav i denne Databehandleravtale.

2. Behandlingens formål, art og omfang

Formålet med behandlingen av Personopplysningene er (beskrivelse.) Databehandler skal bare behandle personopplysninger for det formål å oppfylle tjenesteavtalen

Behandlingen vil omfatte følgende kategorier av personopplysninger:

- (Navn, adresser, epost)

Personopplysningene vil knytte seg til

- (Medlemmer, ansatte, abonnenter, kunder)

3. Behandlingsansvarlig sine plikter

Behandlingsansvarlig skal etablere rutiner i egen virksomhet for bl.a.;

- Påse at det foreligger et behandlingsgrunnlag etter personopplysningsloven for at Personopplysningene behandles for de formål som er oppgitt ovenfor
- Ivareta den registrertes rett til informasjon og innsyn, og til å få Personopplysningene slettet/korrigert
- Melde fra om eventuelle sikkerhetsbrudd til tilsynsmyndigheter samt de registrerte, i.h.t. Personvernlovgivningen

4. Databehandlers plikter

4.1 Internkontroll

Databehandler skal etablere tekniske og organisatoriske tiltak for å sikre at Personopplysningene blir behandlet i tråd med dennes plikter, Personopplysningsloven og vilkårene i denne databehandleravtale. Tiltakene skal kunne dokumenteres på forespørsel

4.2 Rådighetsbegrensning og instruksjonsmyndighet

Databehandler skal bare behandle Personopplysninger i tråd med denne avtalen og behandlingsansvarliges dokumenterte instruksjoner. Med mindre noe annet pålegges databehandler i medhold av nasjonal/EØS rett.

Dersom databehandler mener at behandlingsansvarlig sine instruksjoner er i strid med relevant personvernlovgivning, skal databehandler straks melde fra til behandlingsansvarlig

Dersom databehandler behandler Personopplysningene på en annen måte en det som følger av denne databehandleravtalen eller andre dokumenterte instruksjoner fra behandlingsansvarlig, blir databehandleren å anse som ny behandlingsansvarlig for denne aktuelle handlingen.

Dersom databehandler behandler personopplysninger på en annen måte enn det som følger av denne databehandleravtalen, andre dokumenterte instruksjoner fra behandlingsansvarlig eller i strid med bestemmelser i Personopplysningsloven. Kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av Personopplysninger med øyeblikkelig virkning.

4.3 Utlevering og taushetsplikt

Databehandleren skal ikke levere ut personopplysninger uten behandlingsansvarliges uttrykkelig forhåndstillatelse eller at det foreligger en lovpålagt plikt til en slik utlevering. Som utlevering regnes ikke autorisert personell hos databehandleren eller denne underleverandører der det er nødvendig med hensyn på tjenesteavtalen

Databehandleren skal påse at at personer som gis tilgang til personopplysninger har taushetsplikt. Dersom det ikke foreligger lovpålagt taushetsplikt, skal disse personene istedenfor avgi en taushetserklæring

Denne bestemmelsen gjelder også etter at behandlingen og samarbeidet er avsluttet

4.4 Bruk av underleverandører

Databehandler kan ikke sette ut hele eller deler av behandlingen til en annen virksomhet, underleverandør, uten at behandlingsansvarlig har gitt skriftlig samtykke

Partene er enig om at databehandler kan sette ut hele eller deler av behandlingen til

- (Underleverandør)
- Databehandler skal inngå en skriftlig avtale med underleverandørene som pålegger underleverandørene de samme forpliktelsene som databehandleren har selv i.h.t denne avtalen.
- Databehandleren er fullt ut ansvarlig for den databehandlingen som underleverandøren gjør.

4.5 Overføring til tredjeland

Dersom databehandleren skal overføre personopplysningene til et land som ikke sikrer en forsvarlig behandling av personopplysningene skal databehandler og mottaker inngå EU-kommisjonens standard avtale for overføring til tredjeland (SCC)

Personopplysningene kan også overføres til virksomheter i USA som er sertifiserte i.h.t Privacy shileld avtalen mellom EU og USA

4.6 Informasjonssikkerhet

Databehandlere skal etablere tekniske og organisatoriske informasjonssikkerhetstiltak som står i et rimelig forhold til den risikoen databehandlingen representerer. Det omfatter også tiltak som sikrer at personer med autorisert tilgang til personopplysninger bare behandler disse i tråd med denne databehandleravtale og behandlingsansvarlige sine instrukser. Tiltakene må kunne dokumenteres

Tiltakene skal minimum omfatte følgende;

- (Fysiske tiltak)
- (Tekniske tiltak)

4.7 Avviksmelding ved sikkerhetsbrudd

Databehandler skal umiddelbart melde fra til behandlingsansvarlig om sikkerhetsbrudd som har medført en; tilintetgjørelse, tap, endring, uautorisert utlevering av eller tilgang til personopplysningene.

4.8 Tilgang til informasjon og sikkerhetsrevisjoner

Databehandler skal på forespørsel gi behandlingsansvarlig tilgang til informasjon som er nødvendig for;

- Å påvise at behandlingen skjer i samsvar med denne databehandleravtale og behandlingsansvarlige sine instruksjoner
- At behandlingsansvarlige skal kunne oppfylle sine lovpålagte forpliktelser

5. Databehandleravtalens varighet

Denne avtalen gjelder så lenge databehandler behandler og eller oppbevarer personopplysninger på vegne av databehandleransvarlig

6. Ved opphør

Ved opphør av denne databehandleravtalen plikter databehandler å tilbakelevere alle dokumenter som det har mottatt som inneholder personopplysninger som omfattes av denne avtalen.

Databehandler skal gi behandlingsansvarlige kopi av alt innhold i databaser og andre lagringer som inneholder personopplysninger

Databehandler skal deretter slette og eller makulere alle personopplysninger, i sin besittelse, som omfattes av denne avtalen.

Databehandler skal sende bekreftelse på at dette er gjort senest 30 dager etter avtalens opphør.

7. Kontaktpersoner i avtalen
Følgende kontaktpersoner er oppnevnt i forbindelse med avtalen

For behandlingsansvarlig _____
For databehandler _____

8. Lovvalg og verneting
Partenes rettigheter og plikter etter denne avtalen bestemmes i helhet av norsk rett.

Eventuelle tvister som springer ut av denne avtalen skal behandles av de ordinære domstoler

Avtalen undertegnes i to eksemplarer, ett til hver av partene. Og er vedlegg til samarbeidsavtalen i sin helhet

Appendix

Foredrag

Slide 1 - Hva menes med personvern

- Individets rett til beskyttelse av privatliv, familieliv og korrespondanse
- Individets rett til egne personopplysninger
- Behov for regulering
- Digitalisering, ny teknologi, globale aktører, big data
- Tilrettelegge for lovlig utnyttelse (lik regulering)
- Rettslige rammer
- EMK art. 8, EU Charter artikkel 7 og 8
- Grunnloven § 102
- EUs personverndirektiv – avløses av GDPR
- Personopplysningsloven
- Vern av opplysninger om enkeltindivider, ikke juridiske personer

Slide 2 - Grunnleggende begreper
Personopplysning

- Opplysninger og vurderinger som kan knyttes til en enkeltperson (navn, e-post, bilde, fødselsnummer, IP-adresse, fingeravtrykk mv.)

Sensitive personopplysninger

- Opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, helseforhold, seksuelle forhold, medlemskap i fagforeninger

Registrert
- Den enkeltpersonen som personopplysningen kan knyttes til

Behandlingsansvarlig
- Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes bedriften

Databehandler
- Den som behandler personopplysninger på vegne av den behandlingsansvarlige

Slide 3 - Når er GDPR aktuelt

Personvernregelverket kommer til anvendelse ved bruk av personopplysninger om; partnere, ansatte, kunder, leverandører og bedriften

Slide 4 - Bruk av personopplysninger for ulike formål

HR
- Rekruttering
- Personalarkiv/-mappe
- Sykefraværsoppfølging
- Varsling
- Arbeidsmiljøundersøkelser
- Disiplinærsaker

Sikkerhet
- Adgangskontroll
- Kameraovervåkning
- Rustesting
- Tracking av personell/kjøretøy

Drift
- Regnskap, skatt, pensjon, forsikring
- Oppfølging av samarbeidspartnere
- Oppfølging av kunder
- Salg/markedsføring

IT
- E-postsystem
- Logger
- Informasjonssikring
- Outsourcing, skytjenester

Slide 5 - Grunnkrav
- Behandlingen må være tillatt - ha et behandlingsgrunnlag
- Personopplysningene kan bare brukes til uttrykkelig angitte formål som må være saklig begrunnet i virksomheten
- Bruk til nye, uforenlige formål er forbudt uten samtykke

- Personopplysningene må være nødvendige for formålet (samt korrekte og oppdaterte)
- Personopplysningene må slettes når formålet ikke lenger begrunner lagring/behandling

Slide 6 - Behandlingsgrunnlag

- Ikke sensitive personopplysninger
    - Lovhjemmel
    - «Nødvendighetsgrunner»
    - For å oppfylle en avtale med den registrerte
    - For å oppfylle en rettslig forpliktelse
    - For å ivareta en legitim interesse og hensynet til de registrerte ikke overstiger denne interessen

- Sensitive personopplysninger
    - Lovhjemmel
    - «Nødvendighetsgrunner»
    - For å fastsette, gjøre gjeldende eller forsvare et rettskrav
    - For å oppfylle/ivareta arbeidsrettslige plikter/rettigheter
    - Samtykke (i hovedsak for kommersiell bruk av data)

Slide 7 - Krav til samtykke

Samtykke er ett av flere mulige rettslig grunnlag

- Krav til gyldig samtykke
- Klar angivelse av hvert formål
- Lettfattelig språk
- Atskilt fra annen tekst
- Bør ikke være en betingelse for adgang til tjeneste
- Skal kunne trekkes tilbake når som helst
- Må dokumenteres (av den behandlingsansvarlige)
- Konsekvenser for virksomhetene
- Nødvendig med bevisst forhold til bruk av personopplysninger og samtykke som rettslig grunnlag
- System for å informere samt innhente og dokumentere gyldig samtykke

Slide 8 - Utvalgte hovedpunkter GDPR

Dokumentasjon for overholdelse

- Kartlegging – oversikt og kontroll (art. 30)

Meldeplikt ved sikkerhetsbrudd

- Rutiner for hvordan brudd skal oppdages og håndteres (art. 33 og 34)

Risikovurdering (DPIA)

- Rutiner for vurdering av personvernkonsekvenser av nye tiltak (art. 35) Rutiner for vurdering av personvernkonsekvenser av nye tiltak (art. 35)

Innebygget personvern (design and default)

- Rutiner for å bygge personvern inn i systemer og prosesser, krav til leverandører mv. (art. 25)

Databehandleravtale

- Revisjon av kontraktsmal, oppdatering av avtaler, styrkede rutiner for revisjoner (art. 28)

Sletting (the right to beforgotten)

- Fastsette lagringstid på bakgrunn av formål og innføre sletterutiner (art. 17)

Registrertes rettigheter

- Forbedre innhold i samtykker samt informasjons og innsynsrutiner (art. 7, 13,14,15 mv.)

Slide 9 - GDPR artikkel 30 første ledd

Each controller [...] shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- the name and contact details of the controller [...]
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients [...];
- where applicable, transfers of personal data to a third country or an international organization [...];
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures [...]

Slide 10 - Sjekkliste lovlig bruk av personopplysninger

Hva er formålet og det rettslige grunnlaget?

- Hvilke personopplysninger vil bli behandlet?
- Hvordan skal personopplysningene brukes?
- Er bruken nødvendig og forholdsmessig?
- Hvem skal ha tilgang til personopplysningene?
- Er registrertes rett til informasjon ivaretatt?
- Hvor/hvordan vil personopplysningene bli sikret? (Krav om risikovurdering)
- Er bruk av databehandler og/eller overføring av personopplysninger ut av EU/EØS aktuelt?
- Innebærer behandlingen et kontrolltiltak?

Slide 11 - 10 punkter for praktisk etterlevelse av GDPR

Forankring hos ledelsen/de ansvarlige ("tone of the top")

- Kartlegging - oversikt over systemer og aktiviteter (inkludert kunnskap om hvor data befinner seg og eventuelt overføres)

- Retningslinjer og rutiner for bruk av data, herunder klargjøre rettslig grunnlag for behandling (for eksempel samtykke)
- Risikovurdering og informasjonssikkerhet
- Opplæring
- Databehandleravtaler (og evt. overføring grunnlag ut av EU/EØS)
- Retten til informasjon mv. for de ansatte og andre registrerte
- Sletterutiner (og sletting i praksis)
- Rutiner for håndtering av sikringshendelser
- Den mest personvern vennlige innstillingen skal være standard

Slide 12 - veien til etterlevelse

1. FORANKRING
    a. Personvern på agendaen
    b. Støtte hos ledelsen
    c. Allokering av ressurser
    d. Ansvar

2. KARTLEGGING
    a. Kartlegge prosesser og risiko
    b. Velge strategi og “design”
    c. Risikobasert og skalert

3. IMPLEMENTERING
    a. Eierskap
    b. Rutiner og retningslinjer
    c. Opplæring og bevisstgjøring
    d. Risikovurdering
    e. Informasjonssikkerhet

4. ETTERLEVELSE
    a. Kompetanse
    b. Internkontroll
    c. Verifikasjon
    d. Teknologi
    e. Repeat

Samtykkeerklæring

For at et samtykke skal være gyldig, må det være informert. Det innebærer at informanten har fått informasjon som gjør at de kan forstå hva de samtykker til, og hvilke for konsekvenser det vil få for seg. Informasjonen må omfatte:

1. Navn og adresse virksomheten som er ansvarleg (behandlingsansvarlig)
2. Hva opplysningene skal brukast til
3. Om opplysningene skal deles med andre, og i tilfelle til hvem
4. Om det er frivillig å gi fra seg opplysningene
5. Hvordan informanten skal gå frem for å kreve rettighetene sine, innsyn og sletting
6. Hvor lenge personopplysningene skal lagres
7. Bekreftelse på at informanten når som helst kan ta tilbake samtykket
8. Samtykket skal være frivillig