



Bli klar for GDPR

En håndbok for ISPer om overgangen til EUs nye personvernforordning

Denne håndboka er utarbeidet av Eye Networks AS i samråd med senioradvokat Simen Breen i SANDS.

Publisert september 2017

Redaktør: Jorunn D. Newth

Denne eboka er lisensiert med [Creative Commons Navngivelse-IkkeKommersiell 4.0 Internasjonal](#)



Innhold del 1: Oversikt

Hvorfor denne håndboka?	5
Tre dyptgripende endringer	6
Del 1: Oversikt	7
Hva er en personopplysning?	8
Tre sentrale roller	9
Hva er nytt fra mai 2018?	10
Den registrertes rettigheter: Informasjon og innsyn	11
Den registrertes rettigheter: Dataportabilitet og sletting	12
Den behandlingsansvarliges plikter	13
Databehandlers plikter	14
Databehandling i utlandet	16
Eksempler på databehandlere	17
Lover, forskrifter og direktiver om personvern	18

Innhold del 2: Slagplan

Del 2: Slagplan	18
Advokatens tommelfingerregler	19
Fase 0: Rollefordeling	20
Fase 1: Kartlegging	21
Fase 2: Prioritert prosjektplan	22
Fase 3: Implementering	23
A og B: Lovlighet og rammeverk	23
C: Internkontroll	24
D: Informasjonssikkerhet og IT	25
E: Særlige tema	26
Etterlevelse og kvalitetssikring	27
EyeSaaS: Velg en plattform designet for personvern	28

Hvorfor denne håndboka?

Når denne håndboka kommer ut, har Eye Networks mast på bedriftskundene våre om EUs personvernforordning i over et år. Hvorfor er dette egentlig noe vi bryr oss om, og hvorfor skal norske ISPer bry seg?

Linda Firveld

Leder for forretningsutvikling i Eye Networks



Vi er midt i en digital revolusjon

Ingen vet så godt som ISPer hvor mye data som faktisk er tilgjengelig til enhver tid. Norske ISPer har hatt en godt utarbeidet praksis og håndtering for behandling av personopplysninger – men nå kommer det mer.

Økt innsikt betyr økt ansvar

Med nye tjenester og nye verktøy som gir bedre innsikt ned på pakkenivå, kan vi også se og vite mer om kundene våre på personnivå. Vi i Eye Networks og EyeSaaS både utvikler og forhandler flere av disse tjenestene.

Derfor inviterte vi i 2016 våre juridiske rådgivere i SANDS, gode samarbeidspartnere for oss gjennom flere år, til et samarbeid om å forberede våre kundebedrifter på de nye personvernreglene fra EU som trer i kraft fra 2018.

Samarbeidet har gitt seg utslag i et webinar, en presentasjon på Eye Networks fagdager, og nå denne håndboka. Tre punkter fra juristenes gjennomgang har gjort særlig inntrykk på oss.

Tre dyptgripende endringer

6

1. Bedriftene får større ansvar for å vise at regelverket overholdes

Det er bedriften som holdes ansvarlig for:

- avgjørelsene som tas av den behandlingsansvarlige på bedriftens vegne om hvorfor og hvordan personopplysninger skal behandles.
- at kunden er informert om hva dataene benyttes til og hvordan de håndteres.
- at databehandlingen er i tråd med regelverket selv når den utføres eksternt.

2. Alle tjenester levert til EU/EØS-borgere vil omfattes

Uansett hvor tjenester leveres fra og hvor du lagrer data – lokalt eller i en enterprise-sky eller hos globale aktører som Azure, Amazon eller Google: Hvis du retter deg mot personer i EU/EØS, er du omfattet av reglene.

3. Sanksjonene blir sterkere, bøtene blir større

Ved brudd på personvernlovgivningen vil selskaper nå bøtelegges med inntil 4% av selskapets globale, årlige omsetning. Overtredelser vil virkelig svi. Mediebildet viser også at *omdømmerisikoen* ved å ta for lett på personvern og datasikring, er betydelig.

Vi har stor glede og utbytte av vårt samarbeid med SANDS, og vi håper denne håndboka vil hjelpe din bedrift på veien mot tilpasning til ny personvernforordning.

Del 1: Oversikt

I denne første delen ser vi nærmere på noen grunnleggende roller og begreper innenfor behandling av personopplysninger, og på hvilke forpliktelser hver bedrift har.

Vi tar også for oss hva som egentlig er endringene i EUs nye personvernforordning, slik den vil tre i kraft mai 2018.

Mye omtalt forordning har mange navn

Mange, også her i Norge, foretrekker å bruke den offisielle engelske forkortelsen GDPR. Det står for General Data Protection Regulation.

I denne boka brukes også den formelle betegnelsen *personvernforordningen*, eller bare “forordningen”, om det nye regelverket.



Hva er en personopplysning?

Loven sier at personopplysninger er

*“opplysninger og vurderinger som
kan knyttes til en enkeltperson”*

I realiteten betyr dette alle former for informasjon som kan knyttes til en *identifisert eller identifiserbar* enkeltperson.

For ISPer kan det være spesielt viktig å merke seg følgende:

- Statiske IP-adresser er alltid å betrakte som persondata.
- For ISPer gjelder normalt det samme for dynamiske IP-adresser.
- “Big data” blir persondata når enkeltpersoner er identifiserbare, for eksempel gjennom kartlagte mønstre.

Personopplysninger er altså all tenkelig informasjon – *uavhengig av art, omfang eller format* – som kan knyttes til en fysisk person, et enkeltindivid, direkte *eller* indirekte.

Genuint anonyme/anonymiserte data er ikke persondata.

Definisjonen av personopplysninger i personvernforordningen er i realiteten den samme som i dag.

Tre sentrale roller

9

Den registrerte

Er den enkelte som personopplysningene kan knyttes til. I IS Pens tilfelle er den registrerte som oftest kunde eller ansatt.



Den behandlingsansvarlige

Den som bestemmer hvorfor (formålene med behandlingen) og hvordan personopplysninger skal behandles. I en bedrift er det virksomhetens øverste ledelse som er behandlingsansvarlig.



Databehandlere

Alle som behandler personopplysninger på vegne av bedriften som er behandlingsansvarlig, er databehandlere. En ekstern databehandler er normalt et selskap. Merk at *lagring* er å anse som databehandling.



Hva er nytt fra mai 2018?

10

- Virksomhetsområdet utvides.
Reglene gjelder nå behandlingsansvarlige og databehandlere også utenfor EU/EØS, så lenge de retter seg mot personer i området. Dette vil ikke minst ramme en rekke amerikanske tjenestetilbydere, som nå må konkurrere mer på like fot med europeiske.
- Melde- og konsesjonsplikt erstattes med krav til forsterkede interne systemer.
- Databehandlere får direkte forpliktelser og kan stilles direkte til ansvar.
- Større ansvar for både behandlingsansvarlig og databehandler:
 - Plikt til konsekvensutredning og systemplikter. Personvern blir et virksomhetsansvar.
 - Personvern må bygges inn i utvikling og prosesser: Det er dette som omtales som "data protection by design and default".
 - Skjerpede krav til avviksbehandling og varsling til Datatilsynet og de berørte personene.
- Krav om å ha et personvernombud som både myndigheter og kunder kan rette seg til om de har spørsmål. Dette kravet gjelder blant annet ISPer.
- Innskjerping av når den registrertes samtykke er gyldig som behandlingsgrunnlag.
- Strengere sanksjonsregime. Maks grense for bøter ved overtredelse blir nå 20 millioner euro eller inntil 4% av en virksomhets årlige, *globale* omsetning.

Den registrertes rettigheter: Informasjon og innsyn

11

Informasjon

Registrerte har rett til informasjon om blant annet:

- Hvem som behandler opplysningene deres, hvordan og hvorfor, det vil si hva de kan bli brukt til.
- Hvor lenge persondata lagres.
- Om data behandles utenfor EU/EØS.
- Hvorvidt opplysningene vil eller kan bli utlevert til andre.

Det siste punktet vil mange være spesielt opptatt av som kunde hos en ISP. Pass på at dette er entydig dekket i selskapets personvernerklæring.

Innsyn og tilgang

Registrerte har også rett til å kreve å få tilgang til de personopplysningene som en bedrift har lagret om dem.

Merk at dette er en rettighet som allerede ligger i personopplysningsloven og ikke endrer seg i 2018.



Den registrertes rettigheter: Dataportabilitet og sletting

12

Dataportabilitet

Nytt i reglene fra 2018 er derimot retten til *dataportabilitet*, som vil si at man som registrert kan kreve å få dataene utlevert *i et format som gjør det mulig å gjenbruke dem*.

Et eksempel for en ISP som tilbyr eposttjenester, kan være at kunden vil ha alle meldingene sine med seg i et format som kan importeres hos ny leverandør.

Kravet til dataportabilitet er et eksempel på at de nye juridiske kravene også fører med seg nye krav til hva selskapets tekniske løsninger må kunne håndtere.



Sletting, retting og andre rettigheter

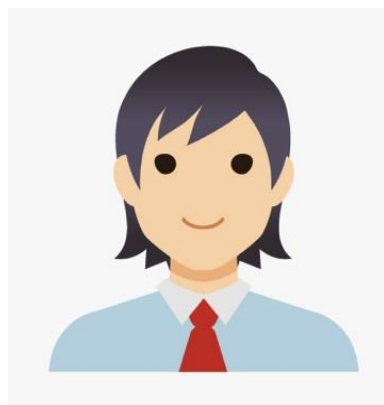
Den registrerte har også rett til å:

- Be om at lagrede personopplysninger slettes eller rettes opp i.
- Bli “glemt” på nettet.
- Protestere på behandling gjort etter interesseavveining.
- Nekte å være gjenstand for automatiserte beslutninger.
- Avgrense behandling hos gitte databehandlere midlertidig eller permanent.

Den behandlingsansvarliges plikter

13

- ❑ Loven stiller krav til at bedriftens behandlingsansvarlige har tilstrekkelige rutiner (internkontroll) og informasjonssikkerhet.
- ❑ Datatilsynet fører tilsyn etter dagens lov, og også den framtidige loven som implementerer personvernforordningen.
- ❑ Alle som behandler personopplysninger, må kunne vise til et *behandlingsgrunnlag*, som kan være:
 - ❑ Samtykke (må være informert, frivillig og uttrykkelig)
 - ❑ Lov, for eksempel krav fra sikkerhetsmyndigheter
 - ❑ Avtale



Databehandlers plikter

14

Alle som håndterer personopplysninger på vegne av en bedrift, er å regne som databehandlere. Dette omfatter ren lagring av data og tilgang til data, for eksempel for å kunne utføre support på IT-tjenester.



Databehandleravtale

Når bedriften tar i bruk en ekstern tjeneste som berører personopplysninger for kunder, ansatte, leverandører eller andre, må behandlingsansvarlig inngå en *databehandleravtale* med den nye leverandøren.



Det er viktig å undersøke på forhånd om eksterne databehandlere som man vurderer å inngå avtale med, oppfyller lovens krav, og behandlingsansvarlig må vurdere om databehandlers informasjonssikkerhet er tilfredsstillende.

Nyttig peker:

[Datatilsynets
maler for
databehandler-
avtale](#)

Databehandling i utlandet

15

Innenfor EU/EØS

Med databehandleravtale kan norske personopplysninger lagres på servere i et hvilket som helst land *innenfor* EU/EØS.



I USA

Databehandling i USA kan bare gjøres av selskaper som er tilknyttet Privacy Shield-avtalen.



Utenfor EU/EØS og USA

Skal data behandles av en aktør utenfor EU/EØS, er et alternativ å bruke et sett standardavtaler godkjent av EU-kommisjonen, som er tilgjengelig her: [Model Contracts for the transfer of personal data to third countries](#).

Inntil videre må overføring av data med grunnlag i denne typen avtale meldes Datatilsynet.

Eksempler på databehandlere

16

A//bruk av eksterne datasentre og skylagring av persondata er bruk av databehandler.

Med utbredelsen av skytjenester og Software as a Service-produkter, har antall eksterne databehandlere som brukes av den gjennomsnittlige bedriften, altså gått rett til vær.

Det er viktig å huske på at personvernforordningen omfatter *alle deler av bedriftens virksomhet* — fra teknisk drift og kundestøtte til salg, markedsføring, regnskap og personal.

Typiske eksempler er:

- ❑ Skybaserte CRM-systemer og andre verktøy for kundeoppfølging, for eksempel Salesforce, Hubspot, Marketo, Zoho, Pipedrive ...
- ❑ Microsoft Azure, Amazon Web Services, Office 365
- ❑ Skybaserte nettbutikker som Shopify og Mystore
- ❑ Kommunikasjonsplattformer som Gmail, Google Hangouts, Slack, Workplace by Facebook,
- ❑ Kundestøtteverktøy som Zendesk, Desk.com, Help Scout ...
- ❑ Mailinglisteverktøy som Mailchimp, GetResponse, Aweber ...
- ❑ Undersøkellesverktøy som Questback og Surveymonkey.
- ❑ Eksterne tjenester for opplæring/elæring og webinarer.
- ❑ Eksterne tjenester for lønn og regnskap.

Lovene, forskriftene og direktivene om personvern

17

Norge

- [Personopplysningsloven](#)
- [Personopplysningsforskriften](#)
- [Ekomloven](#)
- [Ekomforskriften](#)
- [E-handelsloven](#)
- [E-handelsforskriften](#)



EØS/EU

- [Personopplysningsdirektivet \(dir. 95/46\)](#)
- [Datapersonverndirektivet \(dir. 2002/58\)](#)
- [E-handelsdirektivet \(dir. 2000/31\)](#)



Del 2: Slagplan

18

Er du klar for å komme i gang?

Her gir vi deg opplegget for å lage din egen slagplan for å bli klar til mai 2018.

Proessen er delt i tre hovedfaser:

1. Kartlegging
2. Prioritert plan
3. Implementering

Vi vil også understreke at dette *ikke* er en sjekkliste, men et rammeverk for å legge din egen plan.

På neste side forklarer vi litt mer om hvorfor vi ikke gir deg en enkel, punktvis sjekkliste.



Advokatens tommelfingerregler

19

Ikke la deg overvelde! Ta én ting av gangen og gjør prioriteringer underveis. Her er noen av de viktigste tingene å ha bakhodet når du skal i gang.

Senioradvokat Simen Evensen Breen

1. Du ligger allerede godt an hvis du følger norske regler.

I Norge har vi allerede ganske strenge krav til dokumentasjon og internkontroll for behandling av personopplysninger. Følger du allerede det norske regelverket, er du godt rustet til å møte de nye kravene, og arbeidet trenger ikke være all verden.

2. Ikke stol på enkle sjekklister.

Det finnes ingen one-size-fits-all, og mange "sjekklister" som distribueres, inviterer til falsk trygghet. GDPR har mange skjønnsmessige regler, og mange krav innebærer at du selv må vurdere hvordan kravene kan oppfylles. Alle krav er heller ikke relevante for alle. Grundig kartlegging av hvordan virksomheten din behandler personopplysninger, er avgjørende.

3. Ansatte er også registrerte.

Mange fokuserer mest på kundedata i denne prosessen. Ikke glem behandlingen av de ansattes opplysninger, som også kan være sensitive.

4. Tenk på omdømmet ditt.

Det er mye snakk om det nye bøtenivået under GDPR, men vern av virksomhetens omdømme bør være like motiverende for å tenke på personvern som trusselen om bøter.

5. Den viktigste fasen er evigvarende.

Det er etter implementering av nye rutiner og systemendringer at bedriften begynner på det aller viktigste: Etterlevelse og kontinuerlig kvalitetssikring og forbedring av de nye rutinene.

Fase 0: Rollefordeling

20

Er bedriften liten, kan det være i overkant å si at du trenger å danne en prosjektgruppe, men det er fint å starte med å finne ut hvem som skal og må være involvert.

- Hvem skal drive implementasjonsprosjektet?
- Hvem må godkjenne planer og prioriteringer underveis?
- Hvem må orienteres om prosjektet fra første dag, selv om de ikke har noen aktiv rolle?

Kartleggingsfasen kan selvfølgelig komme til å avdekke flere som bør være involvert underveis, eller endre på ansvarsforholdene.

Fase 1:

Kartlegging

21

1. Kartlegging av behandling av personopplysninger

Har du ikke en oversikt over hvilke behandlinger av personopplysninger din virksomhet gjør, bør du begynne med dette. Grunnlaget for hele implementasjonsprosjektet ditt legges i denne fasen. En grundig kartlegging er forutsetningen for alt som kommer etterpå, og gjør det også langt enklere og rimeligere å involvere jurister eller andre rådgivere for kortere perioder senere i prosessen.

Husk å ta for deg alle deler av bedriftens virksomhet, og se på behandlingen av både kunde- og ansattdata.

Relevante spørsmål i kartleggingsfasen er for eksempel disse:

- ❑ Hvilke typer personopplysninger behandler vi?
- ❑ For hvilke formål behandler vi personopplysninger?
- ❑ Hva er behandlingsgrunnlaget for behandlingen?
- ❑ Hvor kommer opplysningene fra?
- ❑ I hvilke datasystem eller arkiv behandles opplysningene?
- ❑ Hvem er ansvarlig for systemene internt?
- ❑ Hva er omfanget av personopplysninger under behandling?
- ❑ Overføres/behandles opplysningene av eksterne? Eksempelvis regnskap, skytjenester, bemanningsbyråer, tilsyn, myndigheter ...
- ❑ Behandles personopplysninger utenfor EU/EØS?

2. Kartlegging av dagens rutiner, systemer og dokumentasjon

Få en oversikt også her: Hvilke rutiner for internkontroll rundt behandling av personopplysninger eksisterer per i dag?

Fase 2:

Prioritert prosjektplan

22

Når du nå forhåpentlig har skaffet bedriften full oversikt over eksisterende databehandling og rutiner, er det på tide å lage en plan for arbeidet.

Målet må være full etterlevelse av personvernforordningen, men prioriter om nødvendig.

Har du mye å gjøre og er i tvil om hva som bør gjøres først? Advokatens anbefalinger er å prioritere:

- ❑ Behandling av personopplysninger med stort omfang.
- ❑ Behandlinger av spesielt sensitive data.
- ❑ Behandlinger med høy risiko.

Fase 3:

Implementering

23

Implementeringsfasen vil se forskjellig ut avhengig av resultatet av kartleggingen. For større prosjekter kan implementeringen med fordel deles opp, for eksempel slik:

- A. Vurdere lovmessighet her i dag
- B. Legge strategi og rammeverk
- C. Internkontroll
- D. Informasjonssikkerhet og IT
- E. Særlige regler

A. Vurdere lovmessighet per i dag

Før bedriften begynner å gjøre endringer, anbefaler vi å få gjort en *lovmessighetsvurdering* av dagens databehandling i lys av den nye personvernforordningen.

Her bør man ha hjelp av en jurist, internt eller eksternt. Dette er ikke nødvendigvis en stor jobb, det avhenger helt og holdent av om kartleggingen er grundig gjort og hva den avdekker.

B. Legge strategi og rammeverk

Få på plass den styrende delen av internkontrollen først. Her må du dokumentere:

- Organisering og ansvarsfordeling
- Ledelsens strategi for internkontroll og informasjonssikkerhet

3 C:

Internkontroll

24

Internkontrollen er bedriftens dokumenterte kvalitetssikringssystem med rutiner for etterlevelse.

Igjen, hvis du allerede etterlever norske regler for internkontroll, kan du bygge på den eksisterende internkontrollen når du skal tilpasse deg det nye regelverket. Du må selv vurdere hvilke krav i forordningen som treffer virksomheten din.

Systemet må omfatte regler og rutiner for blant annet:

- ❑ Registrertes rettigheter og bedriftens informasjonsplikter.
- ❑ Inngåelse av nye databehandleravtaler og rutiner ved nye behandlinger. Her er det viktig å huske på at ny anvendelse av gamle data også teller som en ny databehandling.
- ❑ Kvalitetssikring av personopplysninger, retting og sletting.
- ❑ Eventuell databehandling utenfor EU/EØS.
- ❑ Utlevering av opplysninger til andre.
- ❑ Kontrolltiltak for ansatte og taushetserklæringer
- ❑ Avvikshåndtering
- ❑ Vedlikehold og kvalitetssikring av internkontrollen over tid.

Det som i forordningen heter "[Records of processing activities](#)", er i utgangspunktet primært påkrevd for organisasjoner med mer enn 250 ansatte, men vi anbefaler alle bedrifter å ha en slik oversikt.

3 D:

Informasjonssikkerhet og IT

25

Informasjonssikkerhet er en viktig del av GDPR. Det kan også være nødvendig med tilpasning av IT-systemene for å kunne etterkomme enkelte krav, for eksempel retten til dataportabilitet.

Rutiner og kvalitetssikring

Fra et IT- og informasjonssikkerhetsperspektiv må bedriften vurdere og sette rutiner for:

- ❑ Risikovurderinger
- ❑ Konsekvensutredning (hvis påkrevd): DPIA – Data Protection Impact Assessment.
- ❑ Oppfyllelse av forordningens krav om “data protection by design and default”.
- ❑ Awikshåndtering.

Tekniske tilpasninger

Bedriften må også teknisk legge til rette for oppfyllelse av registrertes rett til for eksempel:

- ❑ Innsyn
- ❑ Dataportabilitet
- ❑ Retting og sletting av opplysninger
- ❑ Reservasjon mot automatiserte beslutninger

3 E:

Særlige tema

26

Det siste sporet er hensynet til bransjespesifikke og særlige regler som ikke nødvendigvis passer inn i de andre sporene.

- Opprettelse av et personvernombud i henhold til artikkel 37. Dette er påkrevd i organisasjoner der kjerneaktivitetene involverer regelmessig og systematisk databehandlinger, som vil si at ISPer flest trenger et personvernombud. Ombudet kan være internt eller leies inn eksternt (advokat eller konsulent).
- Koder, sertifiseringer, eller andre bransjenormer som forenkler etterlevelsen av forordningen. Her er det foreløpig ikke mye å ta utgangspunkt i for en norsk ISP, men det er viktig å holde seg oppdatert på hva som kommer og er hensiktsmessig innenfor egen bransje.
- Sektorlovgivning. Den nye kommunikasjonsvernforordningen ePrivacy er på vei, og er egentlig ment å tre i kraft samtidig med personvernforordningen i mai 2018. Denne forordningen skal samkjøre regelverket på dette området med den nye personvernforordningen.
- Myndighetsforhold. Har bedriften virksomhet i flere land? Da må dere vurdere hvilket lands datatilsyn som blir "lead authority". Vanligvis er dette en enkel avgjørelse basert på hvor virksomhetens hovedkontor befinner seg.

Etterlevelse og kvalitetssikring

27

Har du nå alle rutiner og systemendringer på stell og i henhold til regelverket? Ikke legg rutinene i en skuff!

Kvalitetssikringssystemet du nå har fått på plass, skal også inneholde oppskriften på å holde det oppdatert og i takt med bedriftens skiftende behov og systemer, nye bransjenormer og endrede markedsforhold.

Sørg for at alle ansatte, også nyansatte, kjenner til dette systemet, og at de vet hvem de skal henvende seg til hvis de er i tvil om noe som har med behandling av personopplysninger å gjøre. Lykke til!

Velg en tjenesteplattform designet for personvern

28

Eye Networks utvikler tjenesteplattformen EyeSaaS spesielt for ISPer og deres behov, og vi setter personvern i høysetet.

De første tjenestene våre gir deg effektive verktøy for administrasjon og kundestøtte på gatewayer og smarte aksesspunkter.

EyeSaaS Pearl – administrasjon og innsikt for smart wifi

Har du allerede AirTies smart wifi på plass hos kundene dine, eller planlegger å levere det? Med Pearl får du både administrasjonsmuligheter og innsikt i hjemmenettverket som i dag er en svart boks for ISPer flest – på den andre siden av gatewayen.

EyeSaaS Amber – ACS uten stress

Din egen, fullverdige autokonfigurasjonsserver i privat sky, uten spesifikasjonene, konfigurasjonene og vedlikeholdet som følger med å sette opp og drifte selv.

Personvern og sikkerhet

- Støtte for EUs nye personvernregler rett ut av boksen.
- Privat sky i sikkert datasenter i Sverige.
- Kunden er bare identifiserbar for deg som ISP, ikke for oss som plattformleverandør.

Finn ut mer på <https://eyesaaS.com>, eller ta kontakt med oss i Eye Networks for en samtale om hvilke tjenester som passer for din bedrift.

