GDPR etterlevelse i finansbransjen – Internrevisors rolle

Signhild Blekastad og Ove Skåra - Datatilsynet

Datatilsynet

Dette skal vi si noen ord om:

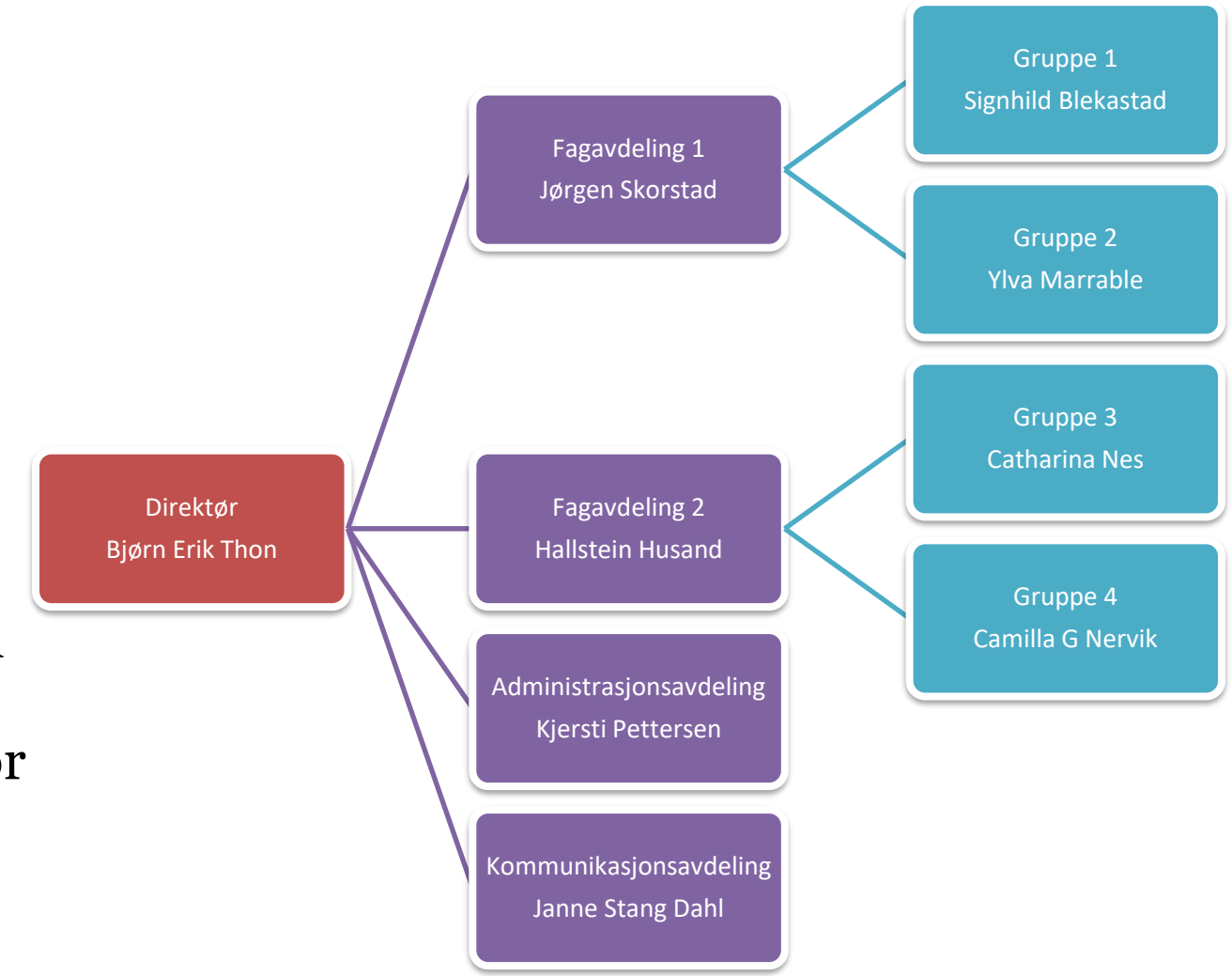
Del 1. Datatilsynet

Hva er det Datatilsynet særlig vil se etter når de skal kontrollere finansbransjens etterlevelse av personvernlovgivningen, og hvordan gjennomføres slike kontroller? Hvilke forventninger har Datatilsynet til internrevisorenes rolle i dette – og hva med personvernombudene? I tillegg også litt om status pr i dag når det gjelder atferdsnormer og meldinger om brudd på personopplysningssikkerheten.

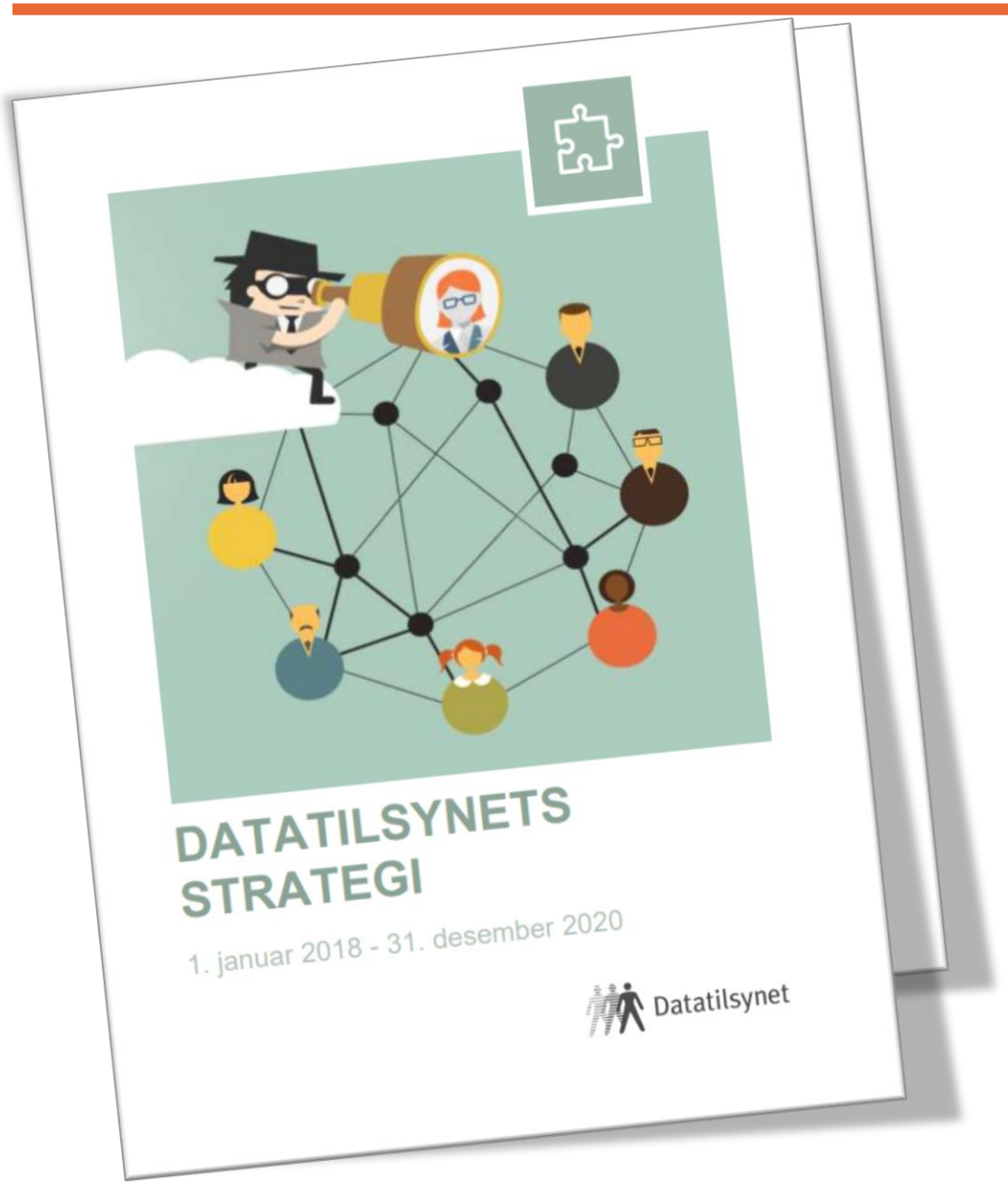
Juridisk seniorrådgiver og faggruppeleder Signhild Blekastad og fagdirektør Ove Skåra.

Datatilsynet

- Opprettet 1980, lokalisert i Oslo
- 48 medarbeidere
- Uavhengig forvaltningsorgan under KMD
- To roller – tilsynsorgan og ombud
- Regelverk:
  - Personopplysningsloven
  - Helseregisterloven
  - Helseforskningsloven
  - Politiregisterloven
  - Lov om Schengen informasjonssystem
  - mv.
- Personvernnemnda er klageorgan for våre vedtak



Strategi 2018 – 2020: Omverdensanalyse



- Digitalisering, personalisering og automatisering
  - Stordata
  - Tingenes internett
  - Lagrings- og analysekapasitet
  - Kunstig intelligens
  - Infrastruktur og deling
  - Forventninger til bruk av data
- Data er makt – maktubalanse
- Personvern versus kriminalitet
- Internettrelatert kriminalitet

Strategi 2018 – 2020: Overordnede mål

1. Datatilsynet skal arbeide for en mer rettferdig maktbalanse mellom individet på den ene siden, og kommersielle aktører og det offentlige på den andre.
2. Datatilsynet skal arbeide for å fremme personvernvennlig digitalisering, innovasjon og utvikling.
3. Datatilsynet skal arbeide for at virksomheter blir kompetente, forstår viktigheten av godt personvern og etterlever regelverket.
4. Datatilsynet skal bidra til at individet i større grad kan ivareta sitt eget personvern.

5. Datatilsynet skal påvirke og ta lederrollen i noen utvalgte internasjonale prosesser for å fremme bedre personvern.
6. Datatilsynet skal være et kompetent og fremtidsrettet tilsyn.

Kort om vårt arbeid rettet mot finansbransjen

- Fagområdet er gjennomregulert og det er høy grad av egenkorreksjon
- Samtidig, bransje i raskt endring og behandling av store mengder data
- Tidligere standardkonsesjoner,
- Lite klager fra enkeltpersoner
- Mange avvik
- Fremover mer tilsyn
- Arbeid med atferdsnormer

Artikkel 57. *Oppgaver*

1. Uten at det berører andre oppgaver fastsatt i denne forordning, skal hver tilsynsmyndighet på sitt territorium
   a) føre tilsyn med og håndheve anvendelsen av denne forordning,
   b) fremme allmennhetens kjennskap til og forståelse for risikoer, regler, garantier og rettigheter i forbindelse med behandling. Aktiviteter rettet spesielt mot barn skal vies særlig oppmerksomhet,
   c) rådgi, i samsvar med medlemsstatenes nasjonale rett, det nasjonale parlament, regjeringen og andre institusjoner og organer om lovgivning og administrative tiltak knyttet til vern av fysiske personers rettigheter og friheter ved behandling,
   d) fremme de behandlingsansvarliges og databehandlernes kjennskap til de forpliktelsene de har i henhold til denne forordning,
   e) på anmodning informere registrerte om utøvelse av de rettighetene de har i henhold til denne forordning og, dersom det er relevant, samarbeide med tilsynsmyndighetene i andre medlemsstater om dette,
   f) behandle klager som er inngitt av en registrert eller et organ, en organisasjon eller en sammenslutning i samsvar med artikkel 80, og undersøke, i den grad det er hensiktsmessig, klagens gjenstand og underrette klageren om forløpet og utfallet av undersøkelsen innen en rimelig frist, særlig dersom det er behov for videre undersøkelse eller samordning med en annen tilsynsmyndighet,
   g) samarbeide med andre tilsynsmyndigheter, herunder ved å utveksle informasjon og yte gjensidig bistand, for å sikre ensartet anvendelse og håndheving av denne forordning,
   h) gjennomføre undersøkelser om anvendelsen av denne forordning, herunder på grunnlag av informasjon mottatt fra en annen tilsynsmyndighet eller en annen offentlig myndighet,
   i) følge relevant utvikling, i den grad den har innvirkning på personvern, særlig utviklingen innen informasjons- og kommunikasjonsteknologi og handelspraksis,
   j) vedta standardavtalevilkår som nevnt i artikkel 28 nr. 8 og artikkel 46 nr. 2 bokstav d),
   k) opprette og vedlikeholde en liste i forbindelse med kravene til vurderingen av personvernkonsekvenser i henhold til artikkel 35 nr. 4,
   l) gi råd om behandlingsaktivitetene nevnt i artikkel 36 nr. 2,
   m) oppmuntre til utarbeiding av atferdsnormer i henhold til artikkel 40 nr. 1 og avgi uttalelse om og godkjenne slike atferdsnormer som gir tilstrekkelige garantier, i henhold til artikkel 40 nr. 5,
   n) oppmuntre til innføring av mekanismer for personvernsertifisering samt personvernsegl og -merker i henhold til artikkel 42 nr. 1, og å godkjenne kriteriene for sertifisering i henhold til artikkel 42 nr. 5,
   o) dersom det er relevant, foreta en regelmessig gjennomgåelse av sertifiseringene utstedt i samsvar med artikkel 42 nr. 7,
   p) utarbeide et utkast til og offentliggjøre kravene for akkreditering av et organ med ansvar for tilsyn med atferdsnormer i henhold til artikkel 41 og et sertifiseringsorgan i henhold til artikkel 43,
   q) foreta akkreditering av et organ med ansvar for overvåking av atferdsnormer i henhold til artikkel 41 og et sertifiseringsorgan i henhold til artikkel 43,
   r) godkjenne avtalevilkår og bestemmelser som nevnt i artikkel 46 nr. 3,
   s) godkjenne bindende virksomhetsregler i henhold til artikkel 47,
   t) bidra i Personvernrådets arbeid,
   u) føre interne registre over overtredelser av denne forordning og over tiltak som er truffet i samsvar med artikkel 58 nr. 2, og
   v) utføre enhver annen oppgave knyttet til vern av personopplysninger.

2. Hver tilsynsmyndighet skal legge til rette for inngivelse av klager som nevnt i nr. 1 bokstav f) ved hjelp av tiltak som f.eks. et klageskjema som også kan fylles ut elektronisk, uten å utelukke andre kommunikasjonsmidler.

3. Oppgavene som hver tilsynsmyndighet utfører, skal være gratis for den registrerte og, dersom det er relevant, for personvernombudet.

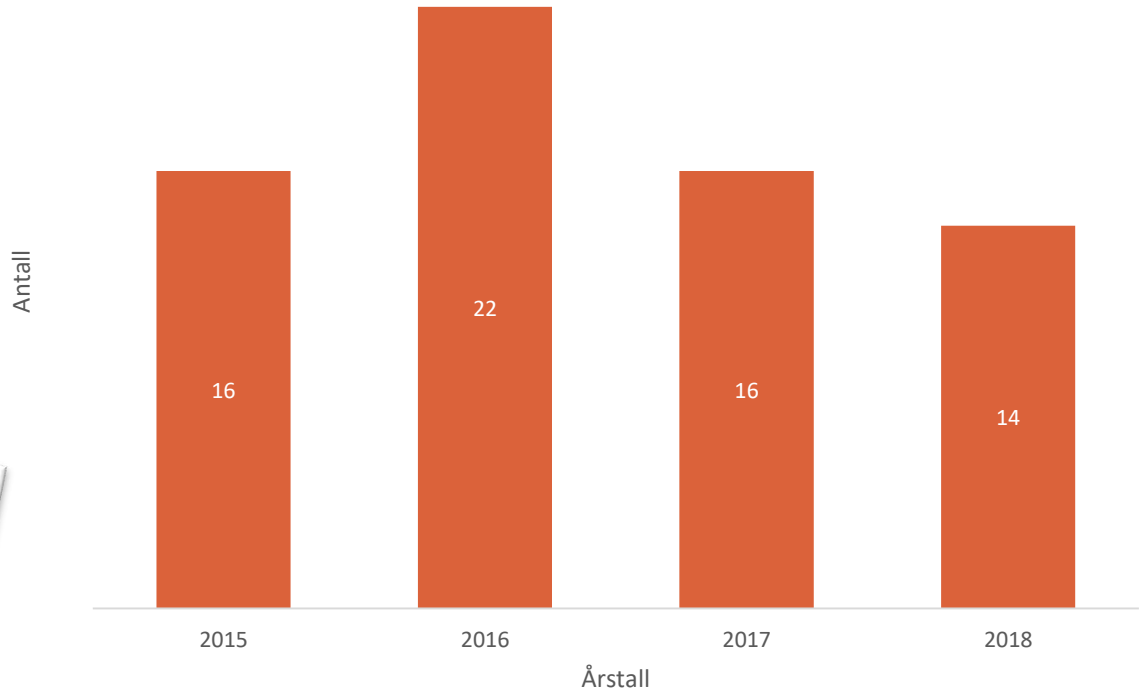
4. Dersom anmodninger er åpenbart grunnløse eller overdrevne, især fordi de gjentas, kan tilsynsmyndigheten kreve et rimelig gebyr basert på administrasjonskostnadene, eller nekte å etterkomme anmodningen. Tilsynsmyndigheten skal bære bevisbyrden for at en anmodning er åpenbart grunnløs eller overdreven.

a)føre tilsyn med og håndheve anvendelsen av denne forordning,

h)gjennomføre undersøkelser om anvendelsen av denne forordning, herunder på grunnlag av informasjon mottatt fra en annen tilsynsmyndighet eller en annen offentlig myndighet,

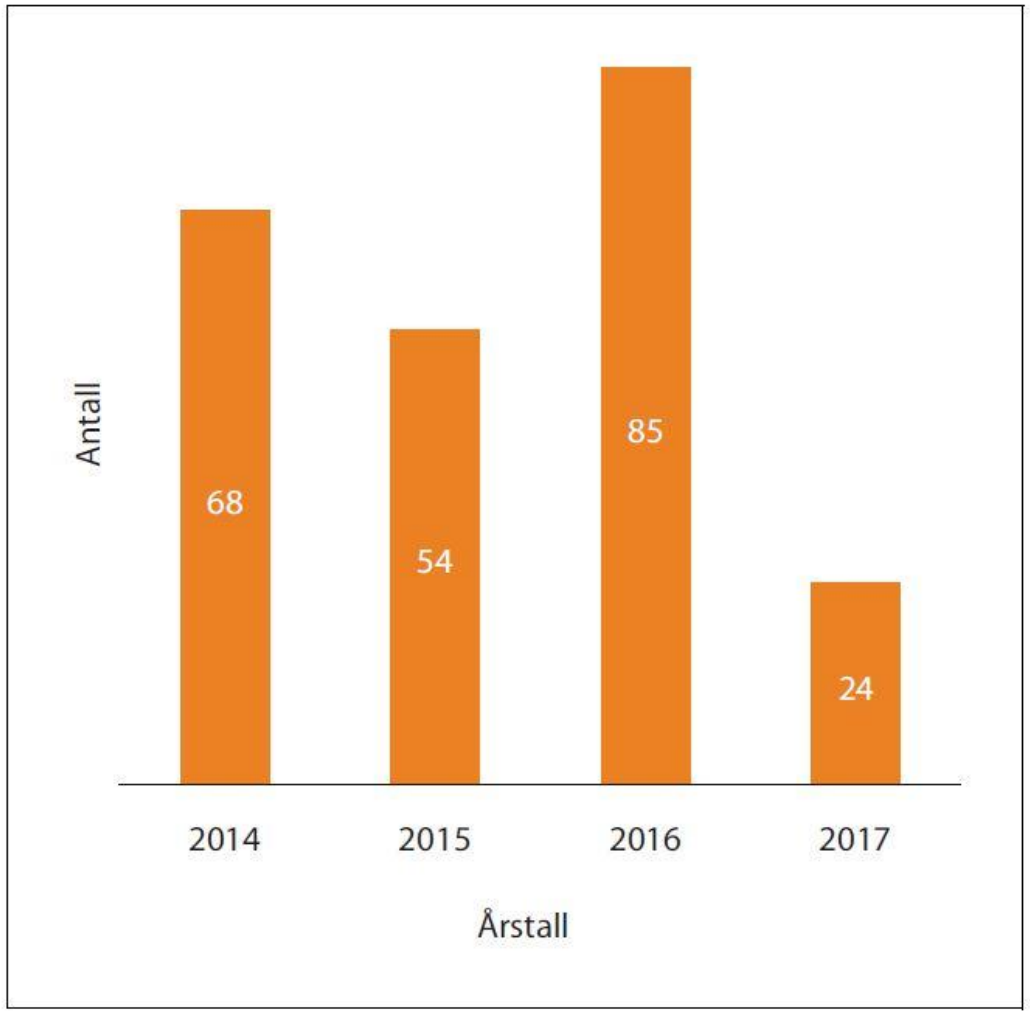
Datatilsynets virkemidler

Vedtak om overtredelsesgebyr de siste årene



Våre kontroller – hvordan og hva?

Tilsynsvirksomheten



Figur 1.2 Antall gjennomførte tilsyn de siste årene

2018

Bransje/sektor/område	Stedlig	Brevlig
Helsesektoren	0	19
PVO hos offentlige virksomheter	0	177
Sum	**0**	**196**

Hva nå?

- Vi har hatt en «hvilefase» når det gjelder tilsynsvirksomhet.
  Den går over….
- Vi utvikler ny metodikk for vår kontrollvirksomhet
  - Herunder også hvordan kontrollere systemer som baserer seg på algoritmer og kunstig intelligens
- Vi er nå i en VP-prosess for perioden mars og ut året

- Det vil bli gjennomført tilsyn i 2019

Artikkel 58. *Myndighet*

1. Hver tilsynsmyndighet skal ha følgende undersøkelsesmyndighet:
   a) pålegge den behandlingsansvarlige og databehandleren og, dersom det er relevant, disses representant, å framlegge all informasjon den trenger for å kunne utføre sine oppgaver,
   b) utføre undersøkelser i form av personvernrevisjoner,
   c) foreta en gjennomgåelse av sertifiseringer utstedt i henhold til artikkel 42 nr. 7,
   d) underrette den behandlingsansvarlige eller databehandleren om en påstått overtredelse av denne forordning,
   e) få tilgang, fra den behandlingsansvarlige og databehandleren, til alle personopplysninger og all informasjon som er nødvendig for å kunne utføre oppgavene den er gitt,
   f) få adgang til alle lokaler hos den behandlingsansvarlige eller databehandleren, herunder til alt databehandlingsutstyr og -midler, i samsvar med unionsretten eller medlemsstatenes prosessrett.

2. Hver tilsynsmyndighet skal ha myndighet til å beslutte følgende korrigerende tiltak:
   a) utstede advarsler til en behandlingsansvarlig eller databehandler om at de planlagte behandlingsaktivitetene sannsynligvis er i strid med bestemmelsene i denne forordning,
   b) utstede irettesettelser til en be… behandler dersom behandlingsaktivitetene er i strid med bestemmelsene i denne foror…
   c) pålegge den behandlingsans… rettigheter i henhold til denne…
   d) pålegge den behandlingsans… bestemmelsene i denne foro…
   e) pålegge den behandlingsan…
   f) innføre en midlertidig eller v…
   g) pålegge retting eller sletting… underretning av mottakere…
   h) trekke tilbake en sertifiseri… og 43, eller pålegge sertifi…
   i) ilegge overtredelsesgebyr… av omstendighetene i hve…
   j) gi påbud om et midlertidig…

3. Hver tilsynsmyndighet skal h…
   a) rådgi den behandlingsan…
   b) avgi uttalelse, på eget i… medlemsstatenes nasjo… av personopplysninger,
   c) godkjenne behandlinge…
   d) avgi uttalelse om og g…
   e) akkreditere sertifiserin…
   f) utstede sertifiseringer…
   g) vedta standard perso…
   h) godkjenne avtalevilkå…
   i) godkjenne administra…
   j) godkjenne bindende…

4. Utøvelse av den myndighet som tilsynsmyndigheten gis i henhold til… herunder effektive rettsmidler og rettferdig rettergang, fastsatt i unionsretten og medlemsstatenes nasjo… pakten.

5. Hver medlemsstat skal ved lov fastsette at dens tilsynsmyndighet skal ha myndighet til å opplyse rettshåndhevende myndigheter om overtredelser av denne forordning og, der det er relevant, til å innlede eller på annen måte opptre i rettssaker med det som mål å håndheve bestemmelsene i denne forordning.

6. Hver medlemsstat kan ved lov fastsette at dens tilsynsmyndighet skal ha mer omfattende myndighet enn det som angis i nr. 1, 2 og 3. Utøvelsen av nevnte myndighet skal ikke hindre en effektiv anvendelse av kapittel VII.

Artikkel 58. *Myndighet*

1. Hver tilsynsmyndighet skal ha følgende undersøkelsesmyndighet:
   a) pålegge den behandlingsansvarlige og databehandleren og, dersom det er relevant, disses representant, å framlegge all informasjon den trenger for å kunne utføre sine oppgaver,
   b) utføre undersøkelser i form av personvernrevisjoner,
   c) foreta en gjennomgåelse av sertifiseringer utstedt i henhold til artikkel 42 nr. 7,
   d) underrette den behandlingsansvarlige eller databehandleren om en påstått overtredelse av denne forordning,
   e) få tilgang, fra den behandlingsansvarlige og databehandleren, til alle personopplysninger og all informasjon som er nødvendig for å kunne utføre oppgavene den er gitt,
   f) få adgang til alle lokaler hos den behandlingsansvarlige eller databehandleren, herunder til alt databehandlingsutstyr og -midler, i samsvar med unionsretten eller medlemsstatenes prosessrett.

Valg av tilsyn som virkemiddel

Tilsyn som virkemiddel kan være aktuelt når vi:

- Har mistanke om ”systematisk” lovbrudd i en bransje
- Trenger nærmere kunnskap om en spesifikk bransje, eller tematikk
- Ønsker å studere virkningene av regelverket
- Har mangelfull forvaltningspraksis
- Ønsker å sette fokus på vårt regelverk i en bransje og skape arena for samhandling med bransje

➢ Får tips eller på andre måter blir oppmerksom på konkrete hendelser

Standard faser i de tilsyn vi har gjennomført

- Det sendes varsel om kontroll
- Kontroll gjennomføres
- Det utarbeides foreløpig rapport og tilhørende oversendelsesbrev ”varsel om vedtak”
- Virksomheten gis anledning til tilsvar
- Tilsvaret vurderes og det utformes en endelig rapport hvor det er tatt hensyn til virksomhetens tilsvar. Endelig rapport sendes over i følge med oversendelsesbrev ”vedtak om pålegg” – med opplysning om klageadgang.
- Virksomheten bekrefter skriftlig at avvik er brakt til opphør
- Sak avsluttes med brev til virksomhet – ”Avslutning av sak”

NB! Offentleglova gjelder

Overordnet sett er det artikkel 5 alt handler om:

Lovlighet, rettferdighet og åpenhet
Opplysningene skal behandles lovlig, rettferdig og på en åpen måte. Respekter de registrertes interesser og rimelige forventninger. Informasjon skal være tilgjengelig og forståelig, ikke manipulerende.

Formålsbegrensning
Opplysningene skal brukes for spesifikke, uttrykkelig angitte og berettigede formål. Opplysningene skal ikke brukes til andre uforenlige formål.

Dataminimering
Personopplysningene skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

Korrekte og oppdaterte
Opplysningene skal være korrekte og om nødvendig oppdaterte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Lagringsbegrensning
Det skal være rutiner som sikrer at det ikke er mulig å identifisere de registrerte lenger enn hva som er nødvendig for de formål de er samlet inn for.

Integritet, konfidensialitet og tilgjengelighet
Personopplysninger skal sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, utilgjengelighet, ødeleggelse eller skade. Det skal brukes egnede tekniske og organisatoriske tiltak.

Ansvarlighet
Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, at personvernprinsippene blir etterlevd.

(Artikkel 5)

Artikkel 24 – den behandlingsansvarliges ansvar

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller godkjente sertifiseringsmekanismer som nevnt i artikkel 42 kan brukes som en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes.

Artikkel 32 – sikkerhet ved behandlingen

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a) pseudonymisering og kryptering av personopplysninger,

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,

c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Dokumentasjon av internkontroll – dokumentstruktur

Styringsdokument internkontroll

Styrende

Sikkerhetsmål og -strategi

Sikkerhetsorganisasjon

Ledelsens gjennomgang (rutine)

Risikovurdering

Beskrivelse av informasjonssystem

Gjennomførende

Sikkerhetstiltak, f.eks.:
- Tilgangskontroll
- Logging
- Informasjonshåndteringsrutine
- Sjekkliste nyansatt / slutter
- Taushetserklæring

Fysisk sikring

Driftsrutiner

Beredskapsplan

Sikkerhetsinstrukser

Opplæring

Rutiner for:
- Innhenting av samtykke
- Informasjon
- Innsyn
- Korrigering
- Sletting/retten til å bli glemt
- Begrenset behandling
- Innsigelse
- Dataportabilitet
- Automatiserte avgjørelser
- Særskilte rettigheter for beskyttelse av barns personvern

Kontrollerende

Ledelsens gjennomgang

Egenkontroll

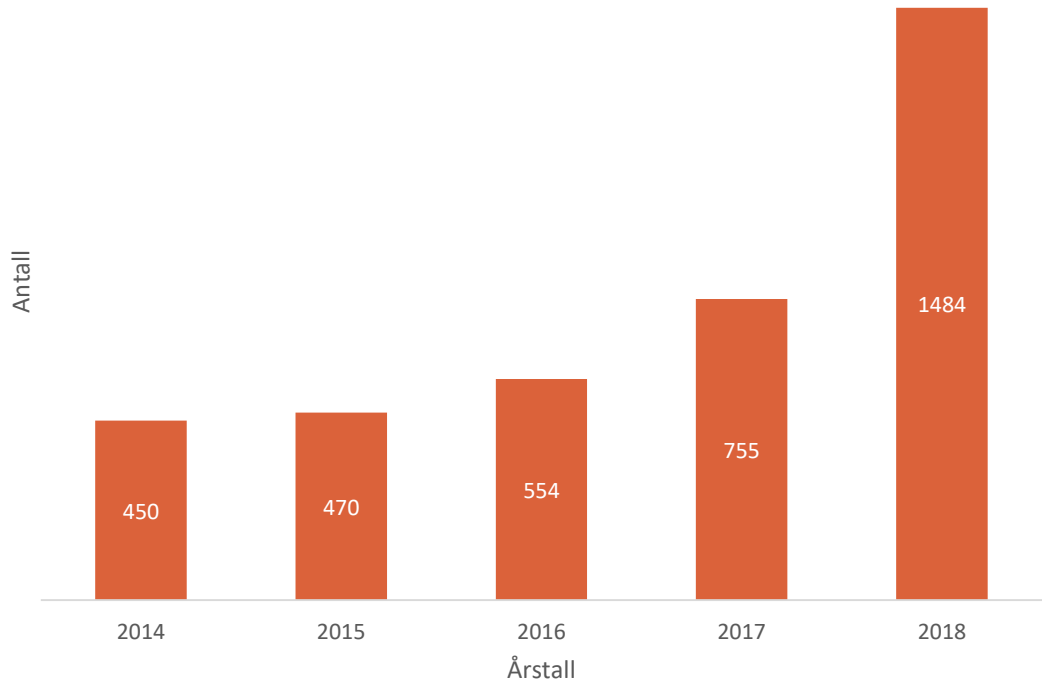
Avvikshåndtering

Sikkerhetsrevisjon

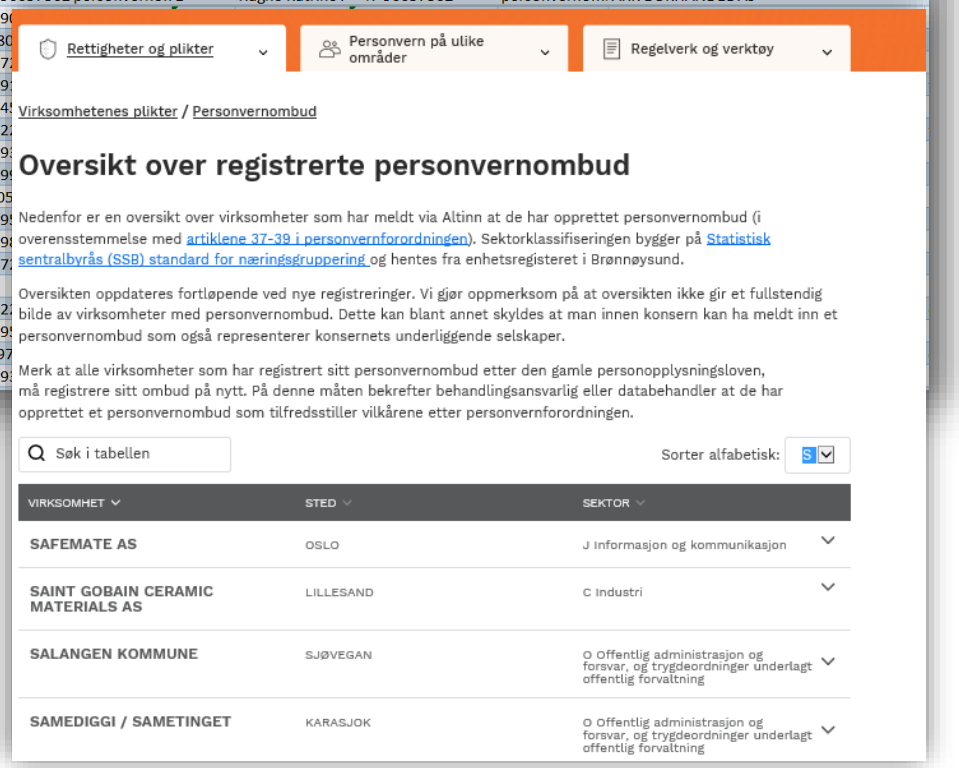
Personvernombudsordningen

Pr 2. januar 2019: 1 017 ombud for 1 484 virksomheter

Antall virksomheter med personvernombud de siste årene



Name	Telephone	Email	CanS	PublicName	PublicTelephone	PublicEmail	Company
Britt Brekke	48100116	britt.brekke@	1				ANALYSETJENESTER AS
Hilde Furdal Wold	+47 99648523	hilde.wold@b	1	Hilde Furdal Wo	+47 99648523	hilde.wold@bu	ANBUDSTORGET.NO AS
Alf Leinan	+47 90100080	aleinan@onlir	1	Alf Leinan	+47 90100080	aleinan@onlin	ANDØY KOMMUNE STAB
Anette Schei	+47 92207578	anette@retth	1	Anette Schei	+47 92207578	anette@retthr.	ANETTE SCHEI
Grete Beck-Heede	+45 52150205	grete.beck-he	0				AON NORWAY AS
Katrine Olsen	40639733	personvern@.	1				APRILA BANK ASA
Hege Huus-Hansen	+47 41122786	hhu@arba.no	1	Hege Huus-Han	+47 41122786	hhu@arba.no	ARBA AS
Maria Gammersvik	22248287	personvernon	1				ARBEIDS- OG SOSIALDEPARTEMENTET
Anders Holt	+47 41249267	personvernon	1	Anders Holt	+47 21070000	personvernoml	ARBEIDS- OG VELFERDSETATEN
Fredrik Bergsmark Grimstad	+47 98459372	fbg@governa	0	Fredrik Bergsma	+47 98459372	fbg@governan	ARDOQ AS
Mary Anne Gløboden	+47 98212182	Mary.Anne.Gl	1	Mary Anne Gløl	+47 98212182	Mary.Anne.Glo	AREMARK KOMMUNE
Ragne Katrine Ågnes Hansmoen	+47 90057362	personvernon	1	Ragne Katrine Å	+47 90057362	personvernoml	ARK BOKHANDEL AS
Rolf Haavik	+47 90						
Bettina Aarmo	40880						
Anna Forsebäck	+46 72						
Anne Grete Nesset	+47 91						
Nils Foss	+47 45						
Kari Rustad	+47 22						
Astrid Trostheim	+47 93						
Hilde Furdal Wold	+47 99						
Therese Andersen Myrvang	95105						
Carl-Richard Nyborg-Christensen	+47 95						
Gøran Breivik	+47 98						
Anna Forsebäck	+46 72						
Anders Bäckström							
Mette Knutsen	+47 22						
Jonas Dahl Spiris	+47 95						
Sandra Run Johannesdottir	41397						
Hans Birger Buer Abrahamsen	+47 93						



Hva sier forordningen om PVO's relasjon til Datatilsynet?

Art. 37 (utpeking av PVO): *Den behandlingsansvarlige eller databehandleren skal offentliggjøre kontaktopplysningene til personvernombudet og meddele disse til tilsynsmyndigheten*

Art 39 (PVOs oppgaver): *…fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftinger nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål*

Art 36 (forhåndsdrøftelser): *…Dersom det er relevant, fremlegge kontaktopplysninger til personvernombudet*

Art. 33 (melding om brudd skal minst inneholde): *....navnet på, og kontaktopplysningene til personvernombudet, eller annet kontaktpunkt der mer informasjon kan innhentes*

Atferdsnormer – kort status

Atferdsnormer – artikkel 40

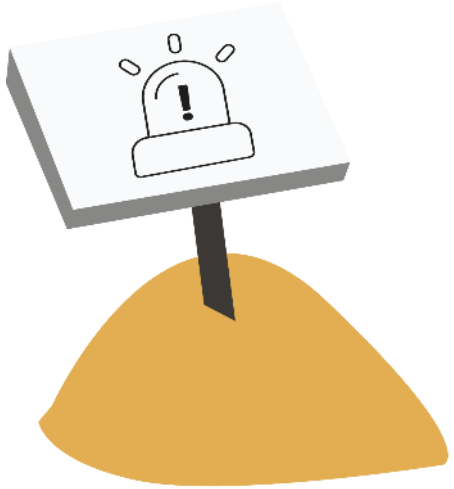
- Atferdsnormer skal være et viktig virkemiddel for å oppnå et godt og harmonisert personvern i Europa. Personvernmyndighetene skal derfor oppmuntre til utarbeidelse av atferdsnormer.
- Utvikles av bransjen selv, men må godkjennes av Datatilsynet.
- Konkrete regler og retningslinjer for hvordan virksomhetene skal innrette seg for å etterleve GDPRs krav.
- Fleksible rammer for hva normen regulerer
- Flere fordeler, f.eks for å påvise regeletterlevelse.
- Retningslinjer fra EDPB på høring

Noen relevante initiativ til atferdsnormer

- Finans Norge - Bransjenorm for bank- og forsikringsbransjen
- Eiendom Norge - Bransjenorm for eiendomsmegling
- Energi Norge - Bransjenorm for energibransjen
- Den norske Revisorforening - Bransjenorm for revisjonsbransjen
- Virke Inkasso - Ny bransjenorm for behandling av personopplysninger i inkassobransjen - Behandlingsgrunnlag
- Regnskap Norge / Revisorforeningen / Økonomiforbundet - Atferdsnorm for behandling av personopplysninger i regnskapsbransjen
- HR Norge / Advokatfirmaet Føyen Torkildsen AS - Bransjenorm for HR og personalarbeid

Brudd på personopplysningssikkerheten - avvikshåndtering

Avviksmeldinger – art. 33



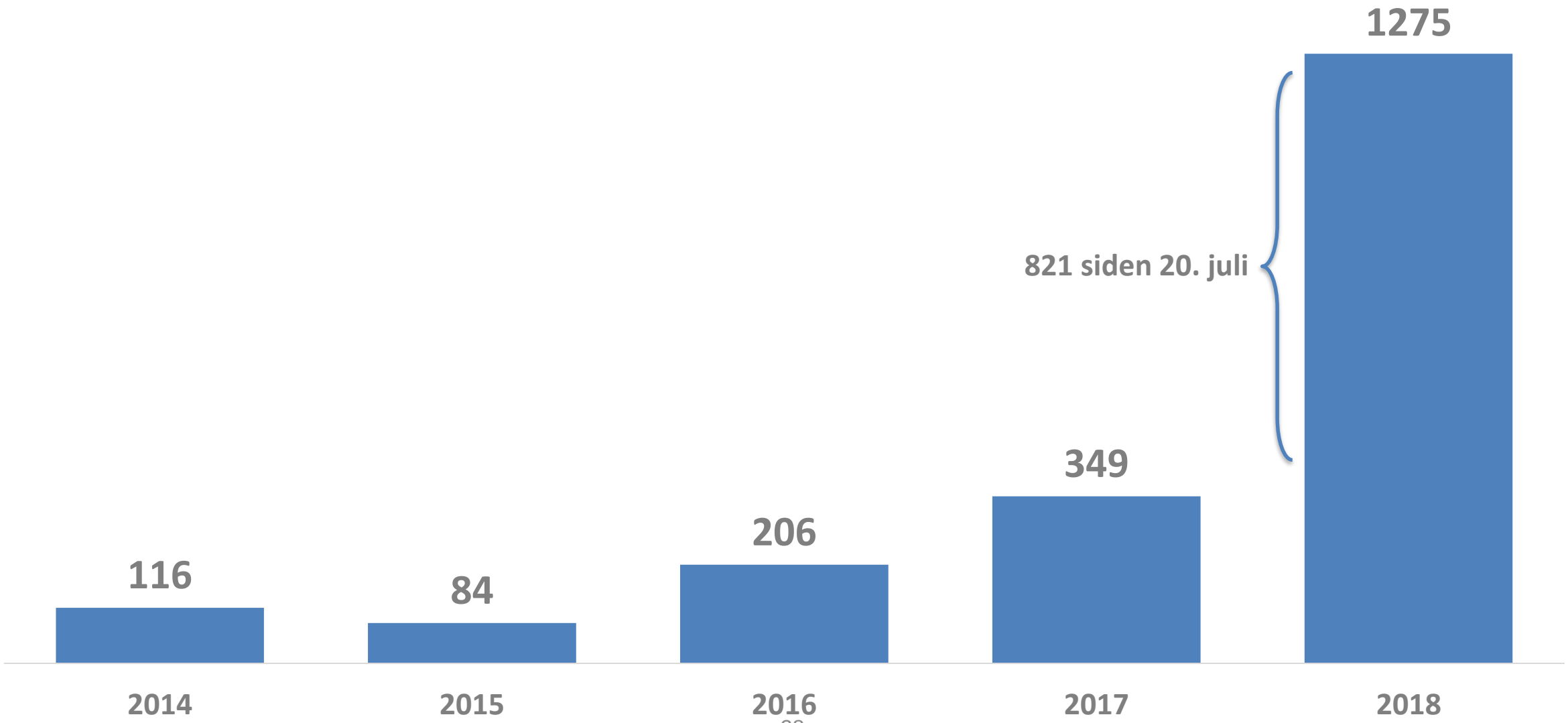
Når må virksomheten sende melding om avvik til Datatilsynet?

«Ved brudd på personopplysningssikkerheten …, med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter.»

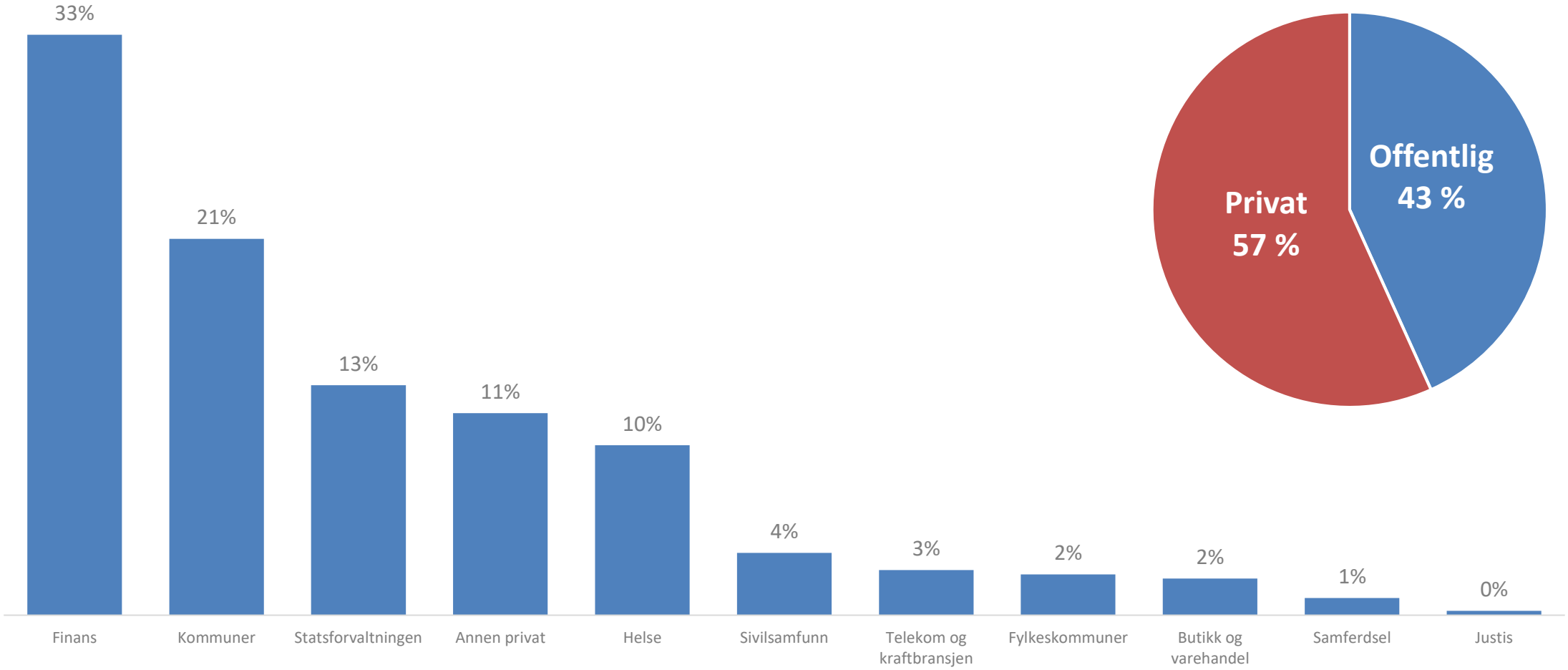
Ikke bare konfidensialitet, men også tilgjengelighet og integritet

Definisjon: *«brudd på personopplysningssikkerheten» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet* (art. 4 (12))

Kraftig vekst i antall avviksmeldinger etter 20. juli 2018



Hvem melder avvik?



Prosess for å håndtere avvik

- Utarbeid interne rutiner:
  - Rutine for å oppdage og raskt håndtere brudd
    - Er det brudd på personopplysningssikkerheten?
  - Vurdere risikoen for de registrerte (konsekvens og sannsynlighet)
  - Avgjøre:
    - Er det nødvendig å melde til Datatilsynet? (risiko: middels og høy)
    - Er det nødvendig å informere de berørte? (risiko: høy)
  - Avvik skal alltid håndteres internt. Dersom det ikke meldes til Datatilsynet, begrunn internt hvorfor i intern rapport.
- Meld avvik til Datatilsynet innen 72 timer etter at dere er klar over bruddet (der det er mulig)
  - Meldingsskjema i Altinn (lenke fra vår nettside). I Altinn: rolle eller kun tilgang til skjema.
  - Kan rapporteres trinnvis.
  - Dersom 72 timers fristen ikke nås, forklar hvorfor.
- Databehandlere melder uten ugrunnet opphold til behandlingsansvarlig
  - Det kan spesifiseres i en databehandleravtale at databehandler melder til Datatilsynet på vegne av behandlingsansvarlig.

Informasjon til de berørte

Dersom det er sannsynlig at bruddet vil medføre en høy risiko…

- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.
- Bruk den kanal som det er størst sjanse for å nå ut til den berørte (f.eks. telefon, SMS, e-post, brev..)

Unntak i kravet om varsling:

- Eksisterende tiltak som gjør informasjonen uleselig, f.eks. kryptering
- Tiltak i ettertid som sikrer at den høye risikoen ikke lengre vil oppstå
- Uforholdsmessig innsats. Må i stedet informere offentlig eller tilsvarende.
- Personopplysningsloven § 16 4. ledd, jf. bokstav a, b og d

Art. 34

Ta gjerne kontakt!

- Signhild Blekastad
- Tlf 22 39 69 51
- Mobil 909 83 258
- Epost sbl@datatilsynet.no

- Ove Skåra, fagdirektør
- Tlf 22 39 69 30
- Mobil 917 91 797
- Epost osk@datatilsynet.no