Del 1 Fagdag GDPR - Arkiv Troms

Fokus på ny personopplysningslov og personvern

Ole Mikalsen, GDPR-konsulent, IT Partner Tromsø AS

Agenda og tidsplan

Tid	Emne
09.00 – 09.45	GDPR og ny personvernlovgivning
10.00 – 10.45	Databehandleravtaler, ansvar og utforming, Rollefordeling i GDPR-arbeidet, kommunene og Arkiv Troms
11.00 – 11.45	Risiko og sårbarhetsanalyser og GAP-analyser for GDPR
12.45 – 13.45	Workshop om analyser, bevisstgjøring og opplæring i forhold til nytt regelverk

INNHOLD, FØRSTE SESJON

- Om loven
- Oppgaver å fylle
- Viktige definisjoner
- GDPR-info for ledere
- GDPR-prosesser består av
- Sanksjoner ved brudd på GDPR
- Grunnprinsipper i GDPR
- Dokumentasjon av behandlinger

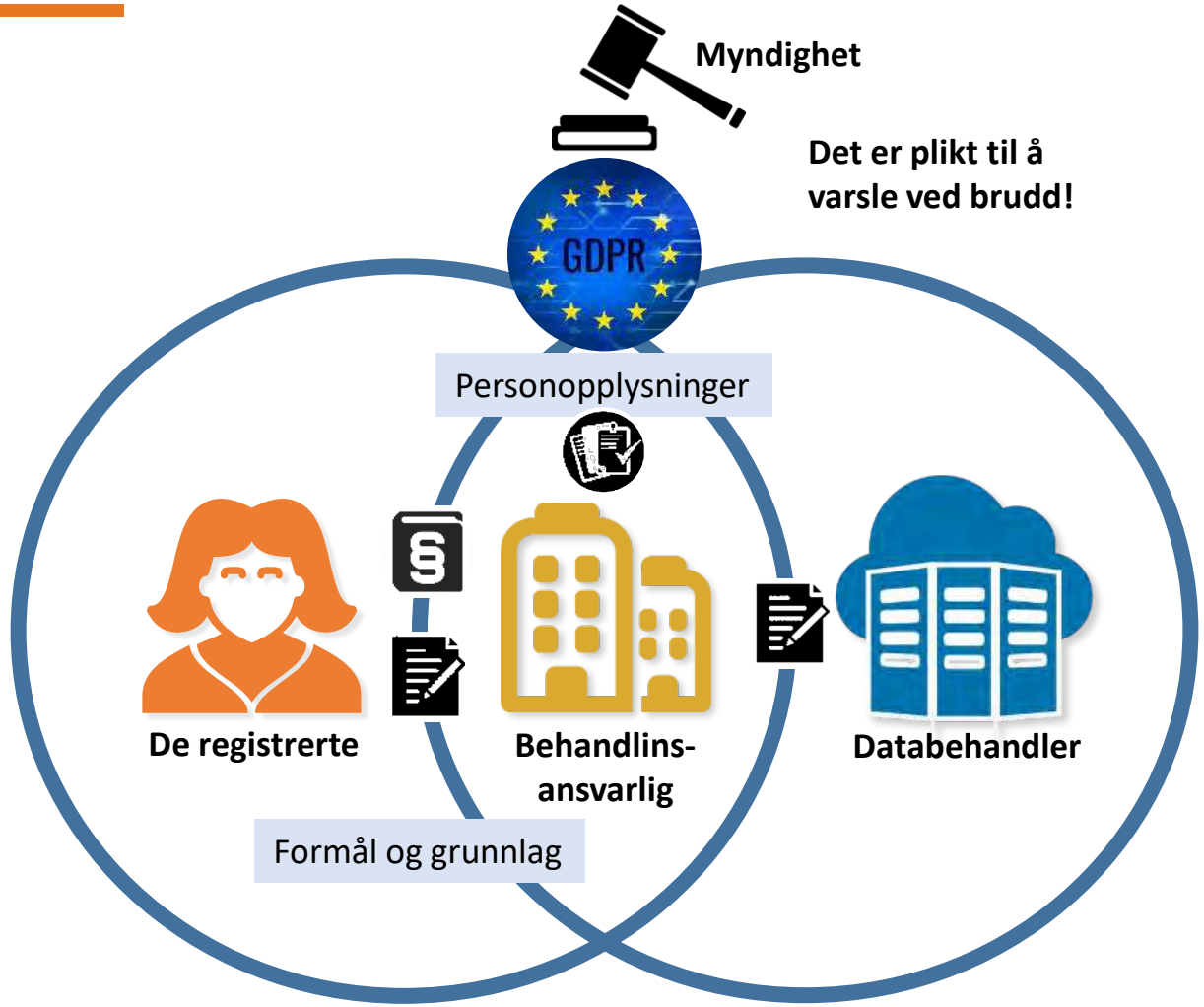
NB: Innholdet i denne presentajonen er nedjustert og forenklet fra vår vanlige presentasjon i forbindelse med opplæring innen GDPR. Noen unøyaktigheter vil derfor forekomme.

General Data Protection Regulation (GDPR)

Den europeiske personvernforordningen fra 2016, som trer i kraft i 2018
Lov om behandling av personopplysninger (personopplysningsloven)

serit
IT Partner Tromsø

GDPR på få minutter



GDPR handler om personvern

Den nye personvernforordningen har som mål å:

- Styrke enkeltindividets personvern med nye rettigheter og kontrollmuligheter
- Gi individet større kontroll over sine egne personopplysninger og bruk av disse.
- Ansvaret for gjennomføring og dokumentering legges på de som har og behandler persondata

Se også:
https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/

serit
IT Partner Tromsø

Hvilke personer og selskaper berøres av GDPR?

Ny europeiske personvernforordning:

- gjelder for alle personer i EU og EØS.
- implementeres i alle lokale personvernlover i hele EU og EØS-området
- gir harmonisert behandling av persondata i hele EU/EØS, og forenkler og standardiserer dataflyt mellom medlemslandene
- vil gjelde for alle selskaper som lagrer persondata om europeiske statsborgere, - inkludert selskaper på andre kontinenter som selger til Europa

GDPR – gir et styrket personvern

Det nye regelverket gir enkeltpersoner nye rettigheter:

- rett til å bli informert via en lettforståelig personvernerklæring om at det foretas innsamling av persondata, og til hvilken bruk
- personer må aktivt gi sitt samtykke
- rett til enkel tilgang til lagret informasjon
- rett til korrigering av informasjon
- rett til å bli glemt - sletting
- rett til å begrense behandling
- rett til å bli varslet ved databrudd
- rett til dataportabilitet
- rett til å motsette seg profilering og automatisk beslutningstaking

Opplysninger skal ikke brukes til nye uforenlige formål, uten at det innhentes nytt samtykke

GDPR – gir nye plikter til virksomheter

Det nye regelverket gir virksomheter plikt til å ha rutiner og verktøy som støtter målsettingene.

- Alle skal ha en forståelig personvernerklæring
- Alle skal vurdere risiko og personvern-konsekvenser
- Alle skal bygge personvern inn i nye løsninger
- Alle får nye krav til avvikshåndtering
- Alle databehandlere får nye plikter
- Alle må kunne oppfylle borgernes nye rettigheter

Det kan gis bøter på opptil 4 % av årlig omsetning for hele konsernet dersom man ikke oppfyller lovkravene

Se også:
https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/

Passivitet = Ansvar!

Personlig ansvar for styret/daglig leder ved uaktsomhet

Uaktsomhet er at noen har gjort noe de ikke burde ha gjort, eller unnlatt å gjøre noe de burde ha gjort

Må vi … hva med … kan vi ikke … hva hvis …

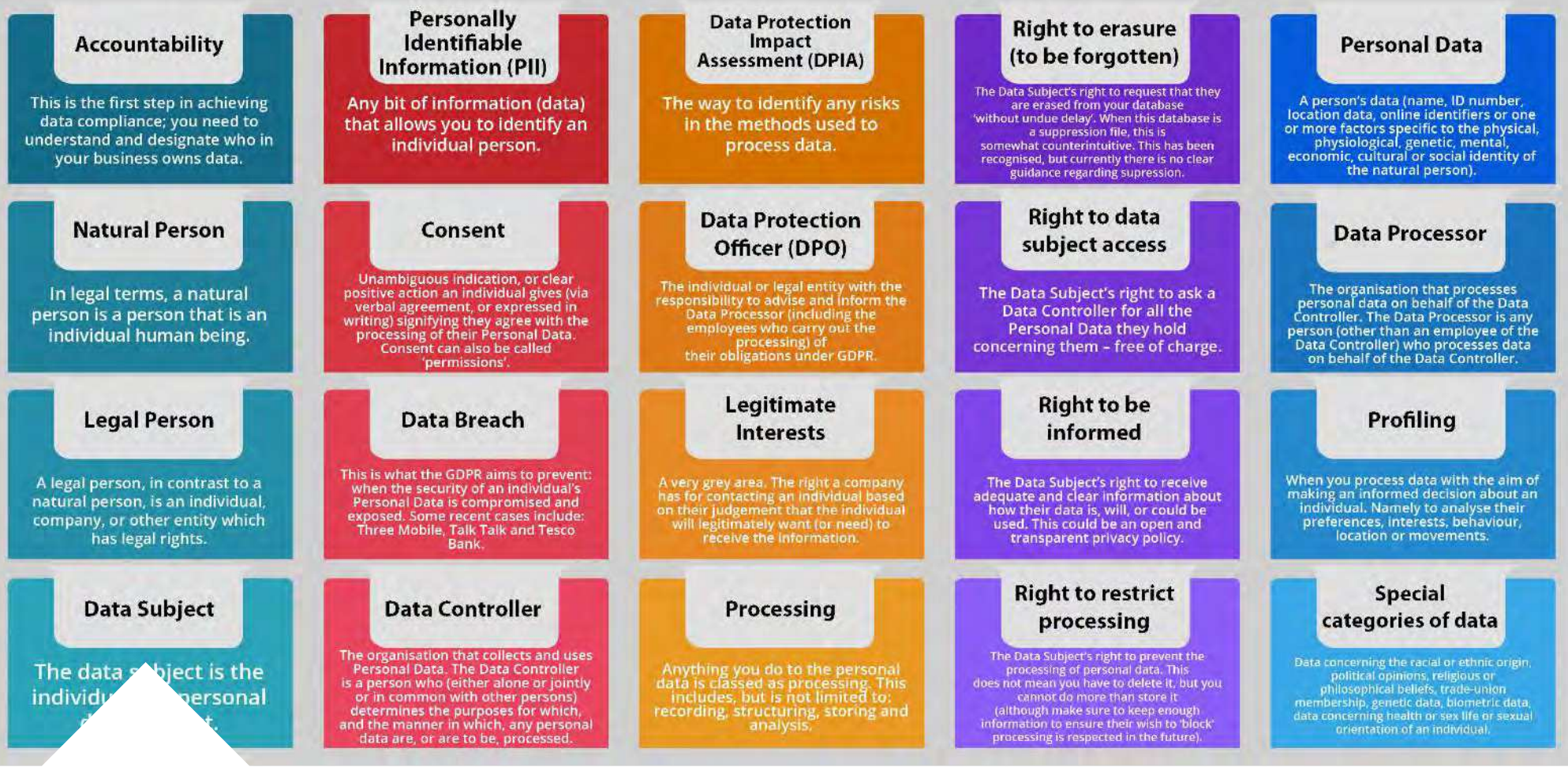
Er det nødvendig å bli GDPR compliant?

Hva må dere gjøre for å bli GDPR-compliant?

- lære dere det nødvendige om GDPR – slik at dere kan følge loven
- kartlegge all persondata dere har i virksomheten
- vurdere grunnlag og formål med dataene, og sikre at behandlingen er deretter
- vurdere om sikkerhetstiltakene dere har satt inn for å sikre behandlingen av persondataene gir tilstrekkelig sikkerhet
- gjennomgå, vurdere og evt endre ulike policyer, rutiner og prosedyrer i selskapet
- Innføre en form for sikkerhetssystem for håndtering av systemer, dokumentasjon, policy og rutiner
- Dokumentere behandlinger i protokoll (for evt presentasjon til Datatilsynet)

Hva må dere gjøre for å bli GDPR-compliant?

- Vurdere opprettelse av personvernombud
- Lage nye databehandleravtaler med deres databehandlere
- Lage nye personvernerklæringer (og samtykke-skjema)
- Lage rutiner for å håndtere de registrertes rettigheter for innsyn og korrigeringer
- Lage rutiner for avvikshåndtering
- Lage rutiner for å vurdere risiko og personvern-konsekvenser
- øke kunnskapen og bevissthet rundt personvern for alle i selskapet (selv om ledelsen har ansvaret for å gjøre endringer, må alle i organisasjonen kjenne til og følge de nye kravene)



Artikkel 4

GDPR – Viktige definisjoner

Noen definisjoner i GDPR, kjennskap til disse gjør det enklere å forstå forordningen.

Definisjon:

De registrerte

De personer som personopplysningene relaterer seg til (ansatte, brukere, kunder, kontakter osv.)

Definisjon:

Personopplysninger

I forordningen defineres personopplysninger som alle opplysninger eller vurderinger som kan knyttes til en bestemt person (Eksempelvis ansatt, kunde, kontakt, leverandør, gjest).

Slike vurderinger eller opplysninger regnes som personopplysninger uavhengig av om de foreligger som tekst, bilder, lyd- eller videoopptak.

Eksempler på personopplysninger kan være:

- navn, adresse, alder, telefonnummer, e-postadresse, bankkontonummer og fødselsnummer
- innholdet i undersøkelser, jobbsøknader, CV'er o.l.
- innhold i saksdokumenter, utredninger eller vurderinger som omhandler ansatte, kunder og kontakter.
- video- og lydopptak som gjøres ved bruk av overvåkningskamera og hvor enkeltpersoner kan gjenkjennes
- logging av aktivitet i datasystemer hvor loggene kan knyttes til bestemte ansatte eller brukere.

Definisjon:
Sensitive personopplysninger

I forordningen defineres «særlige kategorier av personinformasjon» som alle typer opplysninger eller vurderinger som kan knyttes til en bestemt person og som omhandler:

- Helseopplysninger
- Genetiske og biometriske opplysninger for identifikasjon
- Rasemessig eller etnisk opprinnelse
- Politiske oppfatninger, religion og filosofisk overbevisning
- Seksuelle forhold eller seksuell orientering
- Fagforeningsmedlemskap

Eksempler på sensitive personopplysninger kan være:

- ansattes sykdom, diagnoser, grunn for sykefravær, alkohol- eller rusmisbruk
- holdninger til ulike typer religiøse eller politiske spørsmål i spørreundersøkelser

EU definerer disse opplysninger å ha stor misbrukspotensiale

Definisjon:

Behandling

I forordningen beskrives «Behandling» som enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke.

For eksempel: innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Innsamling → Bruk → Overføring → Arkivering og sletting

Definisjon:

Behandlingsansvarlig

I forordningen defineres behandlingsansvarlig som vedkommende virksomhet eller enkeltperson som bestemmer hva personopplysningene skal brukes til (formål) og hvilke elektroniske hjelpemidler (IT-systemer, -tjenester, -utstyr eller -infrastruktur) som skal anvendes til å behandle opplysningene.

Behandlingsansvarlig er ansvarlig for at personopplysninger håndteres i tråd med reglene i forordningen og i den nye personopplysningsloven.

Dersom dette ikke er tilfelle, kan den behandlingsansvarlige bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt.

Definisjon:

Databehandler

I forordningen defineres databehandler som en virksomhet eller enkeltperson som behandler personopplysninger på vegne av den behandlingsansvarlige.

Databehandleren skal bare behandle personopplysninger i henhold til avtale med den behandlingsansvarlige.

Databehandleren har et selvstendig ansvar for at person-opplysninger som tilhører den behandlingsansvarlige håndteres i tråd med reglene i forordningen og i den nye person-opplysningsloven.

Dersom dette ikke er tilfelle, kan databehandleren bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt.

Kort GDPR-info for ledelsen

Et utdrag av informasjon relevant for ledelsen i selskapet
(som presenteres i detalj senere i prosjektet for prosjektdeltakerne)

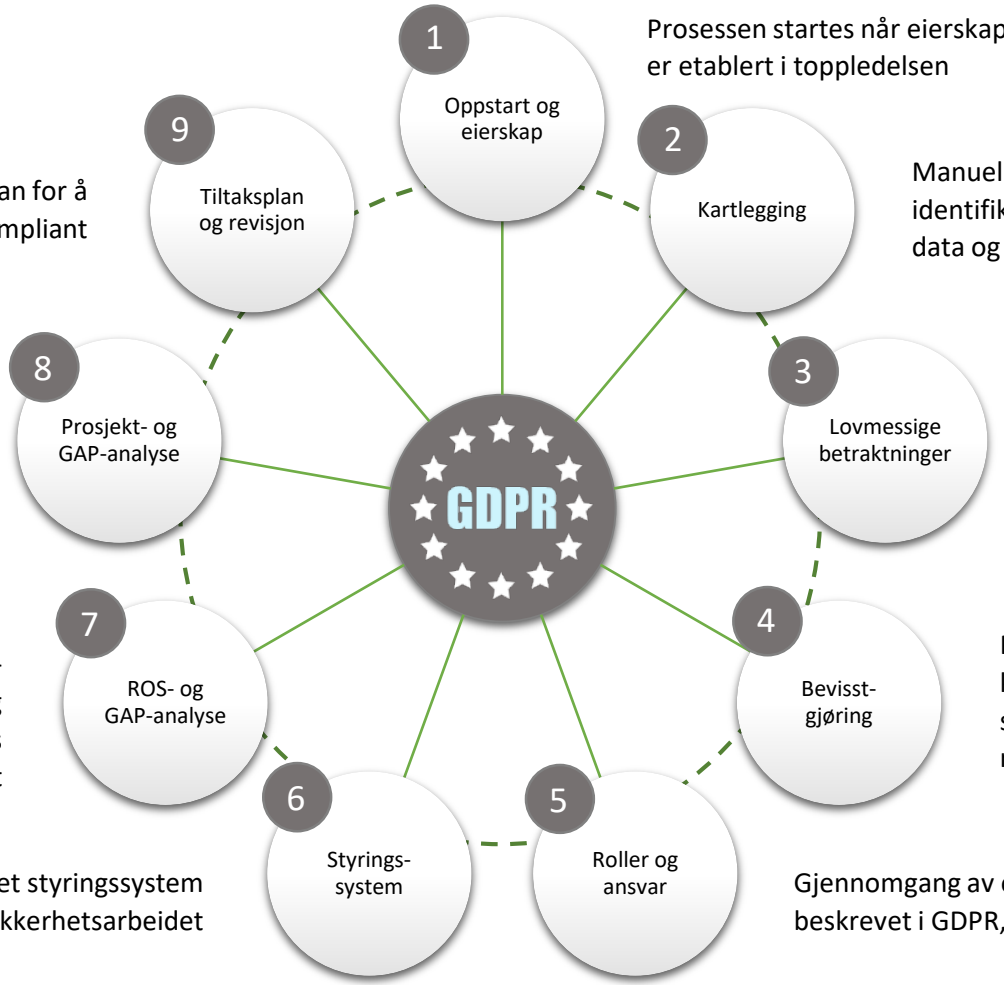
Noen beslutningspunkter for ledelsen

- Utpeking av prosjektgruppe for å gjennomføre GDPR-analyse/prosjekt
- Allokere ressurser til f.eks kartlegging
- Definere/godkjenne GDPR-prosjektets risikomodell og grenseverdier for f.eks igangsetting av tiltak og restrisiko
- Beslutte hastetiltak ved høyrisikofunn
- Vedta tiltak ut fra prosjektets forslag, prioritere og iverksette forbedrings-tiltak
- Akseptere restrisko for systemer
- Evaluere GDPR-prosjektets informasjons og opplæringsplan, godkjenne og iverksette denne

GDPR-prosesser

Hva går GDPR-prosjekter ut på?

PROSESS FOR Å BLI KLAR FOR GDPR



Prosessen startes når eierskapet er etablert i toppledelsen

Manuell og automatisert identifikasjon og klassifikasjon av data og kildesystemer

Vi ser nærmere på lovmessige GDPR-krav opp mot organisasjonen

Planlegging av informasjons-kampanjer i organisasjonen som løfter bevisstheten rundt GDPR

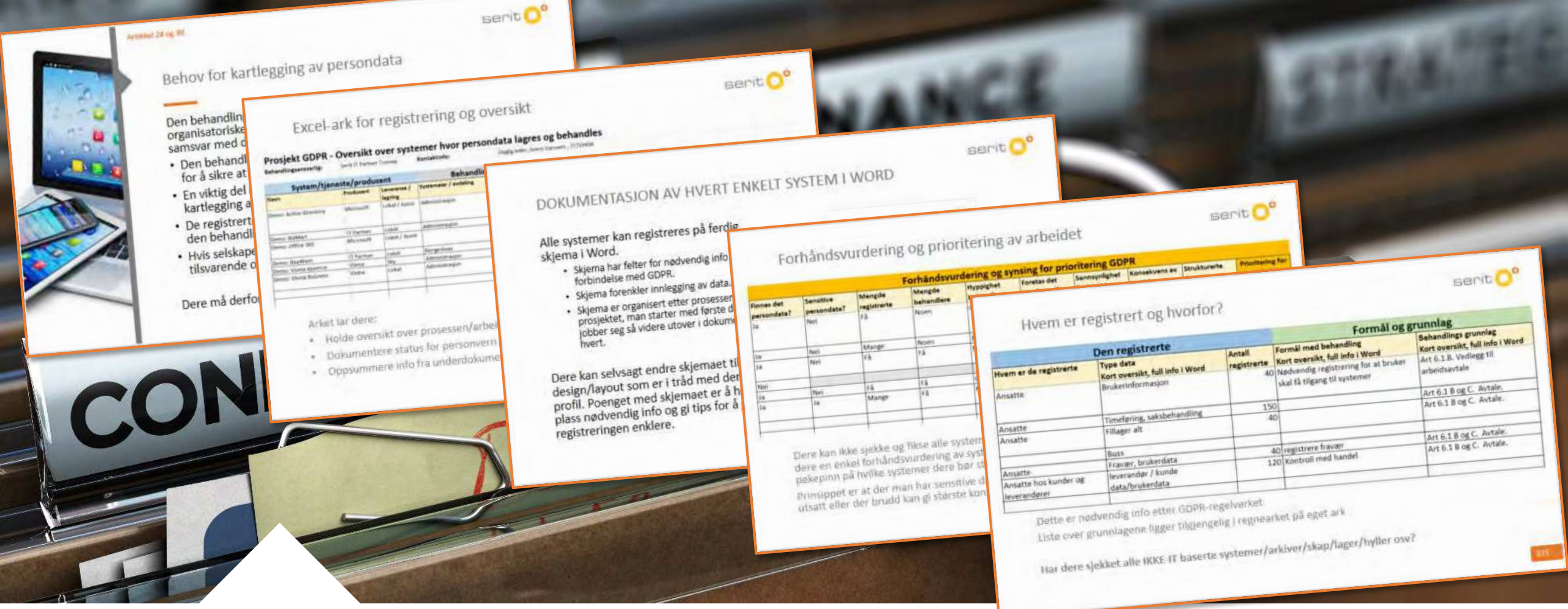
Gjennomgang av og evt etablering av roller beskrevet i GDPR, f.eks Personvernombud

Etablering av et styringssystem for sikkerhetsarbeidet

Risiko og sårbarhets-analyser for IT og forretningen med fokus på personvernsikkerhet

Analyse av oppfyllelsesgrad ihht. kravene i GDPR

Etablere tiltaksplan for å bli GDPR compliant



Kartlegging av persondata, hvor og hva?

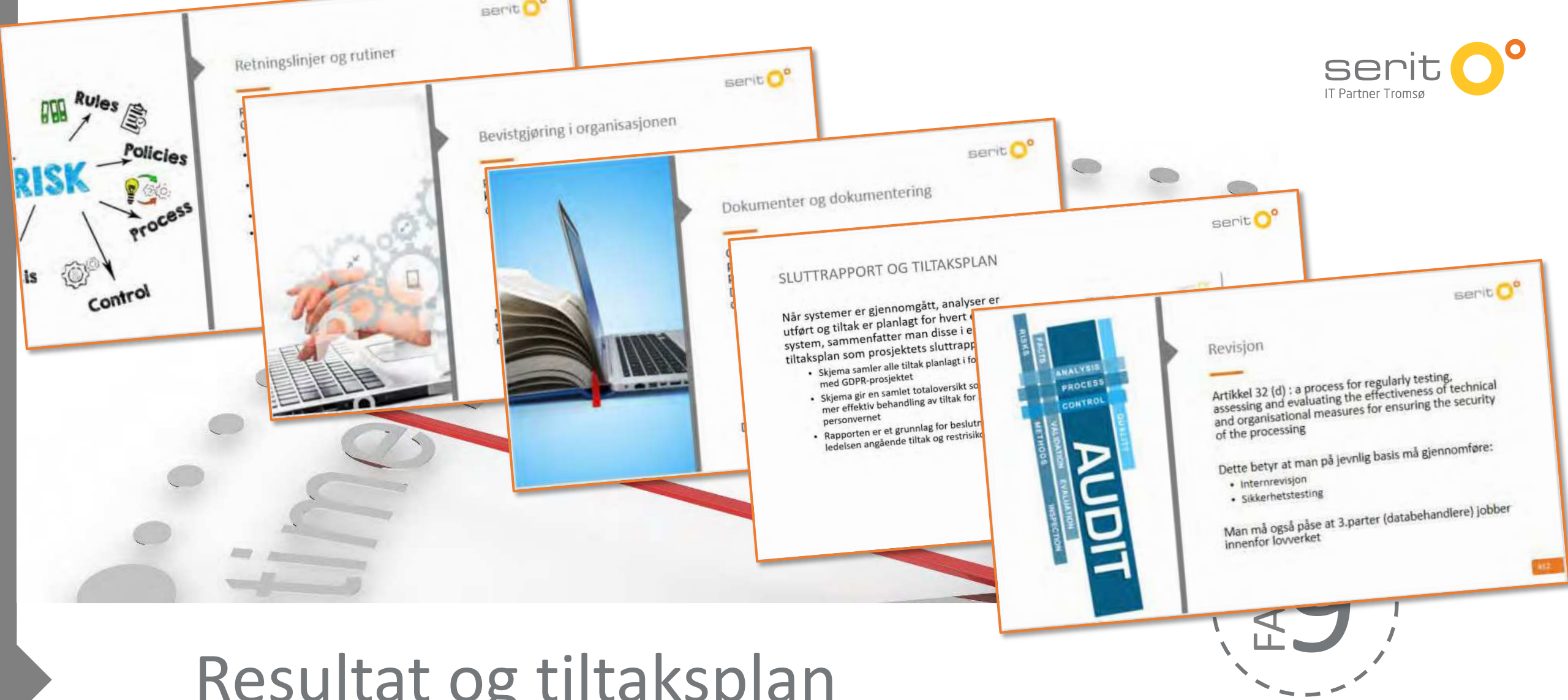
Hvor er alle persondata registrert (data og manuelle register), kategorisering og prioritering av disse for detaljkartlegging, Detaljkartlegging: data, hensikt og formål.

Lovverk og informasjonssikkerhet

Lovverk (GDPR og annet), sikkerhet, roller

ROS og GAP

Risiko, risikoanalyse, tilstandsanalyse og tiltak



Resultat og tiltaksplan

Serit GDPR-prosjekt

9

Tiltaksplan for å være i samsvar med GDPR

Forslag til tiltak legges frem for ledelsen for igangsetting. Persondata og behandling av disse sikres i organisasjonen. Startede prosesser ferdigstilles.

Sanksjoner ved brudd på GDPR

Tilsynsmyndigheten (Datatilsynet) har et sett med sanksjoner overfor Behandlingansvarlige (og Databehandler) hvis brudd avdekkes

Sanksjoner kan ilegges ved brudd på GDPR-forordningen

- en skriftlig advarsel i tilfeller av førstegangs og ikke-tilsiktede brudd
- krav om dokumentering og jevnlig tilsyn
- Begrensninger i behandling og eller krav om korrigerende tiltak
- en bot på opptil 10 000 000 EUR eller opptil 2% av total årlig omsetning
- en bot på opptil 20 000 000 EUR eller opptil 4% av total årlig omsetning

Håndtering av administrative bøter

Hver tilsynsmyndighet skal sikre at ilegging av administrative bøter i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i forhold til overtredelsen og virker avskrekkende.

Avhengig av omstendighetene i hvert enkelt tilfelle skal administrative bøter ilegges i tillegg til eller istedenfor tiltakene nevnt i artikkel 58 nr. 2 bokstav a)–h) og j).

Hvor dyrt kunne dette blitt etter nye regler ??

Ledelsen i Helse Sør-Øst får sterk kritikk for mangelfull sikkerhetsledelse og manglende etterle
rapporten fra Datatilsynet.

Datatilsynet kaller det en unik sak, og se
Sør-Øst RHF ikke har forankret beslutnin

Tilsammen ni sykehus må punge ut med 800.000 kroner hver i overtredelsesgebyr. Til sammen må foretakene ut med 7, 2 millioner kroner for lovbrud

Etter NRKs avsløring
arbeidere i India, Bul
hadde tilgang til pasie
millioner nordmenn, b
helseforetakene i Hels
om å redegjøre for hvi
risiko som ble gjort i fo
beslutningen om å flagg

Kreftregisteret må betale 400 000 kroner etter at blodprøver til kreftforskning ble samlet inn med mangelfullt samtykke. – Dette er en svært trist sak som ikke har noen vinnere, bare tapere, sier Hilde Langseth, leder av Janus serumbank.

Publisert 21.12.2017

- Vi har bare hatt gode hensikter, og har forsøkt å legge forholdene til rette for viktig og tryg
kreft

Rekordbot for slurv med personvern

Av Julie Brundtland Løvseth - 7. oktober 2017

NKI Nettstudier brøt personopplysningsloven da sensitiv informasjon om studenter ble tilgjengelig på nettet. – Et svært alvorlig brudd, som krever en konsekvens, sier Datatilsynet.

I begynnelsen av mai ble det meldt om at omtrent 9000 filer med personopplysninger lå åpent tilgjengelig på internett via NKI Nettstudiers hjemmeside. Det var dokumenter som vitnemål, CVer, selvangivelser og informasjon om arbeidsforhold som hadde blitt lastet opp på NKIs nettside ved opptak av nye studenter.

Filene antas å være fordelt på rundt 3-4000 studenter. Tall fra Google analytics viser, ifølge NKI, at rundt 120-125 filer ble åpnet minst en gang.

Datatilsynet påla NKI å betale et overtredelsesgebyr til staten på 150.000 kroner, da tilfellet var et brudd på personopplysningsloven. Gebyret er det høyeste noen gang gitt til et studiested.

Nasjonal kommunikasjons-myndighet

SIST OPPDATERT 06.02.2018

Skriv ut

Nkom varsler overtredelsesgebyr etter tilsyn med Broadnet

06.02.2018

Nasjonal kommunikasjonsmyndighet (Nkom) gjennomførte i 2017 tilsyn hos Broadnet som en del av saken omtalt i media som «Nødnettsaken». Flere alvorlige avvik ble funnet, og Nkom varsler nå et gebyr til Broadnet på 14 millioner kroner.

I januar i fjor mottok Nkom varsel fra Broadnet om at det var oppdaget avvik fra selskapets sikkerhetsrutiner, der ansatte hos en underleverandør i India skal ha hatt mer omfattende tilganger til IKT-systemer enn forutsatt.

På denne bakgrunn startet Nkom tilsynssak med Broadnet. Tilsynet avdekket flere mangler ved Broadnets sikkerhetsstyring. Som et resultat av tilsynet, påla Nkom Broadnet å rette avvikene.

I pålegget om retting, forhåndsvarslet Nkom at myndigheten ville vurdere overtredelsesgebyr.

I vurderingen av overtredelsesgebyret, har Nkom lagt vekt på at Broadnet har utvist grov uaktsomhet i flere av de undersøkte tilfellene som har avdekket avvik.

Blant forholdene som ligger til grunn for overtredelsesgebyret, er at Broadnet ikke har gjennomført tilstrekkelige og relevante risiko- og sårbarhetsanalyser av egne systemer og av tjenesteutsettingen til India. Videre at selskapet ikke har hatt tilstrekkelig tilgangsstyring for å forhindre uautorisert tilgang til sine systemer, og at det ble gitt uautorisert tilgang fra India til kritisk infrastruktur i Norge.

Nkom har varslet Broadnet at myndigheten vil ilegge et gebyr på 14 millioner kroner. Beløpet utgjør om lag én prosent av Broadnets omsetning i siste regnskapsår.

Nkom kan ifølge ekomforskriften ilegge gebyr på maksimum fem prosent av omsetningen.

Kontakt

Direktør
Elisabeth Sørbøe Aarsæther
Tlf: 95700624
E-post: elisabeth.aarsaether@nkom.no

Seksjonssjef
Rune Kanck
Tlf: 92025250
E-post: rune.kanck@nkom.no

Grov uaktsomhet, ikke gjennomført risiko- og sårbarhetsanalyser, ikke tilstrekkelig tilgangsstyring

Høyt bøtenivå på 1%, sammenlignbart med regelverket for GDPR (maks 4-5%)

Administrative bøter - Hensyn

Når det avgjøres om det skal ilegges en bot samt botens størrelse, skal det tas behørig hensyn til følgende (utdrag og forkortet):

- alvorlighetsgraden og varigheten av overtredelsen, kategoriene av personopplysninger som er berørt og den skade de registrerte har lidd,
- tiltak truffet for å begrense skaden som de registrerte har lidd,
- grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak som er gjennomført
- om overtredelsen er begått forsettlig eller uaktsomt, og om tidligere overtredelser er begått
- Hvordan tilsynsmyndigheten fikk kjennskap til overtredelsen, om hendelsen var varslet, og graden av samarbeid med tilsynsmyndigheten
- enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen.

Bot på opptil 4% av samlet global årsomsetning

Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges administrative bøter på opptil 20 000 000 euro eller, dersom det dreier seg om et foretak, på opptil 4 % av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes:

a) de grunnleggende prinsippene for behandling, herunder vilkår for samtykke, i henhold til artikkel 5, 6, 7 og 9, 83

b) de registrertes rettigheter i henhold til artikkel 12–22,

c) overføring av personopplysninger til en mottaker i en tredjestat eller en internasjonal organisasjon i henhold til artikkel 44–49,

d) ……..

Andre kostnader ved databrudd

Driftstap

- Varslingskostnader
- Gjenoppretting og avhjelpstiltak
- Tap av renommé og kunder
- Skade på driftsmiljø med redusert leveranseevne

Erstatningskrav

- Personer som lider tap kan kreve erstatning
- Solidarisk ansvar med omvendt bevisbyrde
- Personlig ansvar for styret/daglig leder ved uaktsomhet

  Uaktsomhet er at noen har:

  - *gjort noe de ikke burde har gjort, eller*
  - *unnlatt å gjøre noe de burde ha gjort.*

  Det sentrale er at ansvarlige har fraveket en handlingsnorm.

Grunnprinsipper i GDPR

Styrket vern av personopplysninger

GRUNNPRINSIPPER I GDPR
PERSONOPPLYSNINGER SKAL:

- behandles lovlig, rettferdig og på en transparent måte

Lawfullnes, fairnes and transparency

- være tilstrekkelige, relevante og begrenset til det som er nødvendig i forhold til formålene de behandles for

Data minimization

- være nøyaktige og, når det er nød-vendig, holdes oppdatert

Accuracy

- Den behandlings-ansvarlige skal være ansvarlig for, og kunne demonstrere samsvar med GDPR

Accountability

GRUNNPRINSIPPER I GDPR
PERSONOPPLYSNINGER SKAL:

- samles inn for spesifiserte, eksplisitte og legitime formål, og ikke behandles til andre formål som er uforenlig med disse

Purpose limitation

- ikke oppbevares i en form som tillater identifisering av de registrerte lenger enn det er nødvendig for de formålene som personopplysningene behandles med

Storage limitation

- behandles på en hensikts-messig sikret måte, herunder beskyttelse mot uautorisert eller ulovlig behandling, utilsiktet tap, ødeleggelse eller skade, ved hjelp av passende tekniske eller organisatoriske tiltak

Integrity and confidentiality

Artikkel 30

Dokumentasjon av behandlingsaktiviteter

Behandlingsansvarlig og databehandler skal dokumentere sine behandlings-aktiviteter. Oversikten vil være en del av institusjonenes internkontroll.

Dokumentasjon av behandlingsaktiviteter

Hver behandlingsansvarlig skal føre en protokoll over behandlings-aktiviteter som utføres under deres ansvar (skriftlig og elektronisk).

Nevnte protokoll skal inneholde følgende informasjon:

a) navn og kontaktopplysningene til den behandlingsansvarlige
b) formålene med behandlingen
c) kategoriene av registrerte og kategoriene av personopplysninger
d) kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til samt eventuell dokumentasjon på nødvendige garantier ved utlevering til tredjestat
e) planlagte tidsfrister for sletting av kategoriene av opplysninger
f) en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene

Oversikten skal gjøres tilgjengelig for datatilsynet på forespørsel