Personvern og internrevisjon

Lillian Engebø – Konsernrevisjonen DNB

IIA Norge – GDPR etterlevelse i Finansbransjen – Hvordan ka
internrevisjonen bidra.
6.Mars 2019

Personvern og internrevisjon

Personvern – forordningen og Personopplysningsloven

- GDPR - General Data Protection Regulation – Personvernforordningen ble innlemmet i norsk rett gjennom personopplysningsloven §1
- Personopplysningsloven ikrafttredelse 20.7 2018

Personvern-prinsippene og registrertes rettigheter

- Syv grunnleggende personnvernprinsipper
- Den registrertes rettigheter
- Prinsipper og rettigheter = Grunnlaget for revisjonsprogram med tilhørende revisjonshandlinger

Personvern og internrevisjon

- Revisjon utføres med hjemmel i lov (Finansforetaksloven) for å *«kontrollere at finanskonsernet er organisert og drives på forsvarlig måte og i samsvar med gjeldende krav til virksomheten*
- *Når internrevisjonen innhenter personopplysningen som revisjonsbevis - for å dekke revisjonsformålet (som er saklig begrunnet i virksomheten jr. Finansforetaksloven m.m.) - så hentes det fra IT system eller annen dokumentasjon m .m. i virksomheten.*

Begrep og definisjoner

Person Opplysninger Art. 4 .1	**«Personopplysninger»** enhver opplysning om en identifisert eller identifiserbar fysisk person **(«den registrerte»);** en identifiserbar fysisk person er en person som **direkte eller indirekte kan identifiseres**, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.
Behandling Art. 4.2	**«Behandling»** enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. 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.
Særlige kategorier person-Opplysninger Art.9 nr.1	Rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Roller og ansvar

Behandlings Ansvarlig Art.4.7

Den **«behandlingsansvarlige»** en fysisk eller juridisk person (representert ved øverste ledelse dvs. styret og daglig leder), en offentlig myndighet, en institusjon eller ethvert annet …

Den behandlingsansvarlige bestemmer formålet med behandlingen av personopplysninger, samt hvilke midler som skal benyttes i behandlingen, det vil si hvordan personopplysninger skal behandles

Databehandler Art.4.8

«Databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger**på vegne av** den behandlingsansvarlige.

Personvernprinsippene og rettigheter

PERSONVERNPRINSIPPENE

1. Lovlig, rettferdig og gjennomsiktig
2. Formålsbegrensning
3. Dataminimering
4. Riktighet
5. Lagringsbegrensning
6. Personopplysningssikkerhet
7. Ansvarlighet

REGISTRERTES RETTIGHETER

1. Informasjon
2. Innsyn
3. Korrigering
4. Sletting – «retten til å bli glemt»
5. Begrenset behandling
6. Dataportabilitet
7. Innsigelser

Personvernprinsippene (1/4)

1. Lovlig Gjennomsiktig Rettferdig

- Krav om behandlingsgrunnlag
  - Behandlingen av personopplysninger er **nødvendig** for å oppfylle en avtale som den registrerte er part i, et samtykke, følge av lovgivning (for eksempel. hvitvaskingsloven)
  - Respekt for den registrertes, rettigheter og interesser
  - Åpenhet, informasjon, klart og tydelig språk (forventing og forståelse for bruken) .

2. Formåls-begrensning

- Krav om bestemt, legitimt behandlingsformål
  - Saklig begrunnet i virksomheten
  - Forståelse og kontroll - hos den registrerte
- Ikke gjenbrukes til nye/andre formål som ikke er forenlig med det opprinnelige formålet
  - Uforenlige formål – krav om lovlig behandlingsgrunnlag for eksempel. samtykke
  - Dersom ikke lovlig grunnlag – må opplysningene innhentes på nytt med korrekt angitt formål

Personvernprinsippene (2/4)

3. Data-minimering

- Begrenset til det som er nødvendig for formålet/formålene (sml. formålsbegrensningsprinsippet)
- Adekvate (forholdsmessig/tilstrekkelig)
- Relevante
- Digitale løsninger skal ha funksjonalitet som kun samler inn nødvendige personopplysninger

4. Riktighet

- Kvalitetskrav
- Korrekte, oppdaterte (se opp mot rettferdig behandling)
- Digitale løsninger kan ha funksjonalitet for regelmessig å varsle brukere om å kontrollere sine personopplysninger

Personvernprinsippene (3/4)

5. Lagrings-begrensning

- Personopplysninger lagres så lenge det er **nødvendig** for behandlingsformålet, dvs. personopplysningene slettes når formålet med den enkelte behandling er oppfylt * (vurdering)
- Å slette betyr å anonymisere eller tilintetgjøre opplysningene
- Etablere rutiner og prosesser for sletting og slettefrister – strukturert lagring / utstrukturert

6. Person-opplysnings-sikkerhet

- Personopplysninger behandles på en måte som sikrer tilstrekkelig vern for den **registrerte**
  - verne mot uautorisert eller ulovlig behandling, utilsiktet tap, ødeleggelser eller skader
- Krav om risikobasert tilnærming for å fastsette hvor sannsynlig og hvor alvorlig risikoen er. Gjennomføre risikovurderinger. Sikkerhetsnivå settes i forhold til risiko.
- Sikre vedvarende konfidensialitet (fortrolighet), integritet, tilgjengelighet og robusthet i behandlingssystemene og tjenester
- Sikkerhet og sikkerhetskrav for personvern må sees i sammenheng med generelle og spesielle informasjonssikkerhetskrav /bestemmelser standarder for informasjonssikkerhet (jf. også IKT forskriften)

Personvernprinsippene (4/4)

7. Ansvarlighet

- Prinsippet retter seg mot den «behandlingsansvarlige» og dennes **ansvar**
  - Sikre risikostyring og internkontroll (art. 24)
  - Etablere prosesser og rutiner som sikrer implementering av alle prinsippene (førstelinje)
  - Etablere prosesser og rutiner som sikrer at den registrerte kan utøve sine rettigheter
  - Sikre at etterlevelse kan dokumenteres
  - Privacy by design og by default (art. 25)
  - Protokoll over behandlingsaktiviteter (art. 30)
  - Risikobasert tilnærming og krav om Data Proteciton Impact Assessment (DPIA) (art. 35 og 36)
  - Krav om varsling ved brudd på personopplysningssikkerheten (art.33)
  - Krav til databehandlere – tredjeparts risikostyring (art.28)

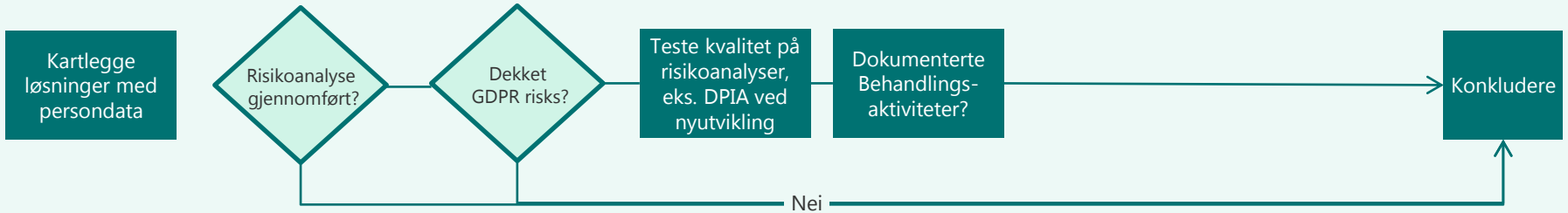
Registrertes rettigheter

REGISTRERTES RETTIGHETER

1. Informasjon
2. Innsyn
3. Korrigering
4. Sletting – retten til å bli glemt
5. Begrenset behandling
6. Dataportabilitet
7. Innsigelser

Eks: på revisjonsprogram GDPR –

GDPR risk assesment & DPIA – art. 5 f) art. 24, 25, 30, 32 og 35 jf. nr. 5 nr. 2



Sletterutiner – GDPR art. 5 e) jf. 17, jf. 30 jf. 5 nr. 2

- Dokumenterte sletterutiner?
- Er slettefrister satt for alle systemer / tjenester? Dokumentert i protokoll
- Kvalitet på sletting (maunelt vs automatisk)
- Prosess for «Slett meg» etablert?
- Teste etterlevelse av rutiner

Avviksrutiner – art. 5 f) GDPR art. 33 jf. 5 nr. 2

- Dokumenterte avviksrutiner?
- Kvalitet på avviksrutiner (Walk through)
- Teste etterlevelse av rutiner

Tredjeparts leverandører – art. 28 jf. art. 30 jf. art. 5 nr. 2

- Kartlegge 3.parter
- Er 3.part databehandler?
- Er avtalene oppdatert med databehandleravtale?
- Er databehandleravtale standardisert iht GDPR-mal DNB?
- Teste utvalgte databehandleravtaler
- Brukes underleverandører . Foreligger godkjent/tillatelser

Dataanalyser

Dataanalyser i internrevisjon

1. Hva er nødvendig for å dekke revisjonsformålet
2. Hvilke type personopplysninger skal innhentes
3. Dataminimering
4. Personopplysningssikkerhet
5. Er det personopplysninger som kan slettes (overskudds info.)
6. Dataanalysen lagres sammen med endelig revisjonsrapport
7. Sletting av revisjonsrapport med tilhørende dokumentasjon

Behandlingsprotokoll art. 30

C	D	E	F	G	H	I	J	K
Hva gjelder behandlingen Virksomhetsområde, overordnet behandlingsaktivitet	**Formål med behandlingen**	**Kategorier av registrerte**	**Kategorier av personopplysninger**	**Hvor kommer personopplysningene fra? (Kilde)**	**Kategorier av mottakere** Dersom aktuelt også i tredjestater, eller internasjonale organisasjoner	**Behandlingsgrunnlag artikkel 6**	**Rettslig forpliktelse, berettighet interesse mv** Henvise til dersom beh.grunnlag er 6.1.c.e eller f Dersom relevant	**Behandlingsgrunnlag artikkel 9 eller 10** Med ev henvisning også til annen lovgivning Dersom relevant
Revisjonsoppdrag	Revisjonsformålet	Kunder og ansatte.	Saklig begrunnet i revisjonsformålet	KR henter alle data fra DNB systemer	Mottakere av revisjonsrapporter er den reviderte enhet. Revisjonsrapporter inneholder som hovedregel ikke personopplysninger, for uten om navn på de aktuelle mottakere i den revisderte enhet. Revisjonsrapporter sendes ikke til internasjonale organisasjoner. Dersom revisjonsrapporter sendes over landegrenser mellom DNB internasjonale virksomheter, vil slike rapporter sendes på DNB interne elektroniske kommunikasjonskanal	Nødvendig for å oppfylle en rettslig forpliktelse GDPR art. 6C jf. Finansforetaksloven §§ 8-16 og 13-5.. 2 ledd CRR/CRD IV-forskriften § 31 (3) Virkeområde for forskriften er §1	Nødvendig for å oppfylle en rettslig forpliktelse GDPR art. 6C jf. Finansforetaksloven §§ 8-16 og 13-5.. 2 ledd CRR/CRD IV-forskriften § 31 (3) Virkeområde for forskriften er §1 jf. art. 35 nr. 10hvor det forutsetningsvis fremgår at det rettslige grunnlaget for behandling av personopplysninger etter art. 6 nr. 1 bokstac c ikke behøver å spesifikt regulere behandlingsaktivitetene se. Prop 56LS s. 32 pkt. 6.3.2	
Dataanalyser	Revisjonsformålet	kunder og ansatte.	Når dataanalyser skal utarbeides, skal personopplysningene minimeres til det som er relevant og nødvendig for formålet med revisjonen.	strukturerte data fra DNB systemer		GDPR art 6 c jfr. Finansforetaksloven og CRR/CRD IV-forskriften	(se prop 56 LS s. 32,33	
Prosjekthuset		kunder og ansatte.	saklig begrunnet i revisjonsformålet	strukturerte data , lagret ustrukturert		GDPR art 6 c jfr. Finansforetaksloven og CRR/CRD IV-forskriften		
Ekstern revisjon	Formål å sikre kvalitet i det finansielle regnskapet, er oppnadd og tilstrekkelig dokumentert	kunder og ansatte.	saklig begrunnet i revisjonsformålet	strukturerte data fra DNB system, lagret i internrevisjonens system Teammate	EY (lovpålagt revisjon)	GDPR art 6 c Finansforetaksloven §8-17		
Ekstern kvalitetssikring	Formålet er å sikre etterlevelse av IIA standarder , gjennom uavhengig kontroll	kunder og ansatte.	saklig begrunnet i revisjonsformålet	strukturerte data fra DNB system, lagret i internrevisjonens system Teammate	IIA for 2018 (lovpålat kontroll)			
Administrere arbeidsforhold	Personaladministrasjon innad i KR, herunder kompetanse kartlegging og utvikling, ressursplanlegging m.m.	ansatte	Navn, og andre identifikasjonsfaktorer, lønn,	Teammate, og HR systemer, samt innhenting fra ansatte		Personopplysningsloven §6 jf. GDPR art.9 nr. 1 jf 9 nr.2 b (sml ot.prp nr. 92 (1998-1999) s. 110 og 111 - bestemmelsen viderefører	6c og 6f	