SpareBank 1 ØSTLANDET

SIKKERHETS FESTIVALEN

Konsekvenser for fysiske personer

TONE HODDØ BAKÅS
SPAREBANK 1 ØSTLANDET

30.8.2023, SIKKERHETSFESTIVALEN

Litt om meg

- Fagsjef personvern, SpareBank 1 Østlandet (CPO)
- Høgskolen i Innlandet, emneansvarlig for et grunnkurs innen personvern og digital sikkerhetskultur
- Personvernombud, Innlandet fylkeskommune (DPO) (Oppland og Hedmark fylkeskommune)
- Oslo kommune, fagsjef informasjonssikkerhet
- EY, senior manager, informasjonssikkerhet og personvern
- NorSIS
- Norges Bank, datasikkerhetssjef

- Master i informasjonssikkerhet, NTNU
- Sertifiseringer: CISA, CRSIC, CDPSE

Inspirasjon for foredraget

- Jeg er ansvarlig for å ivareta at banken har verktøy, metoder, maler og veiledere innen personvern

- Medarrangør for en workshop sammen med Eva Jarbekk, Schjødt og Simen Sommerfeldt, Bouvet våren 2023

  - DPIA/ personvernkonsekvensvurdering-workshop
  - Inviterte et utvalg kompetente diskusjonspartnere
  - Formål å samle erfaringer med personvernkonsekvensvurderinger

  - Arrangert som en verdenscafe

SpareBank 1 ØSTLANDET

Personvern-forordningen

SpareBank 1 ØSTLANDET

Art 32 – Sikkerhet ved behandlingen – skal alltid gjøres

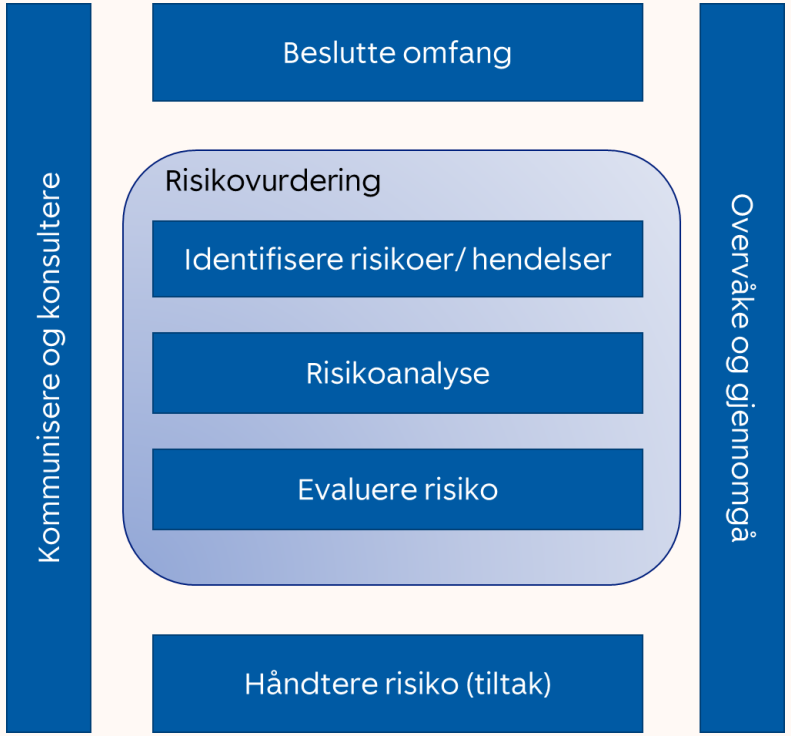
Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren 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,

SpareBank 1 ØSTLANDET

Risikovurdering – art 32 nr 2

Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av **utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang** til personopplysninger som er overført, lagret eller på annen måte behandlet.

Tilgjengelighet, integritet og konfidensialitet

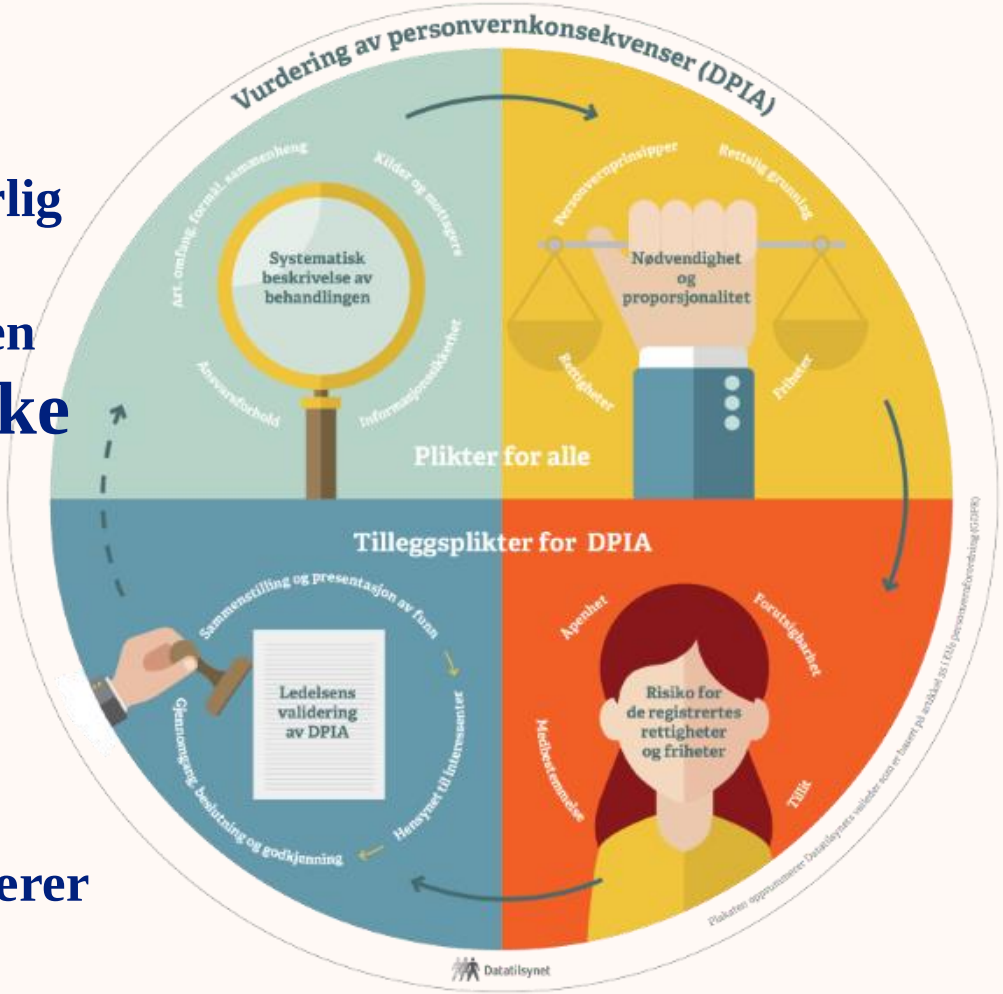


ISO 27005 Information Security Risk Management

SpareBank 1 ØSTLANDET

Personvernforordningen art 35

Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.



Se Sjekkliste fra Datatilsynet

Litt mer hjelp...

§

Fortalen punkt 76

Hvor sannsynlig og alvorlig risikoen for den registrertes rettigheter og friheter er, bør fastslås ut fra behandlingens art, omfang, formål og sammenhengen den utføres i. Risikoen bør vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko.

SpareBank 1 ØSTLANDET

Konsekvens for personopplysningsvernet

1. Dersom det er **sannsynlig**…
   - Dette avklarer vi ved å vurdere behovet for PVK (behovsvurdering, forundersøkelse / pre-DPIA mv)
2. Dersom det er HØY risiko (svarer JA)
3. Da skal vi vurdere **konsekvensene**

Er det unødvendig å vurdere sannsynlighet??

SpareBank 1 ØSTLANDET

Hva skal vi vurdere KONSEKVENS av?

Hvilke konsekvenser kan de fysiske **personene** oppleve?

- Konsekvenser for personopplysningsvernet
- Risiko for «rettigheter og friheter»

Har vi ivaretatt prinsippene, rettighetene og frihetene?

SpareBank 1 ØSTLANDET

Eksempel 1

Intern risikovurdering: skal Datatilsynet ha egen side på Facebook?

Sluttrapport 2021

Vedlegg 2 – vurdering av personopplysningssikkerhet

Datatilsynet opererer med følgende fire risikonivåer: LAV, MODERAT, HØY og SVÆRT HØY.

Vurdering av risiko for de registrertes rettigheter og friheter

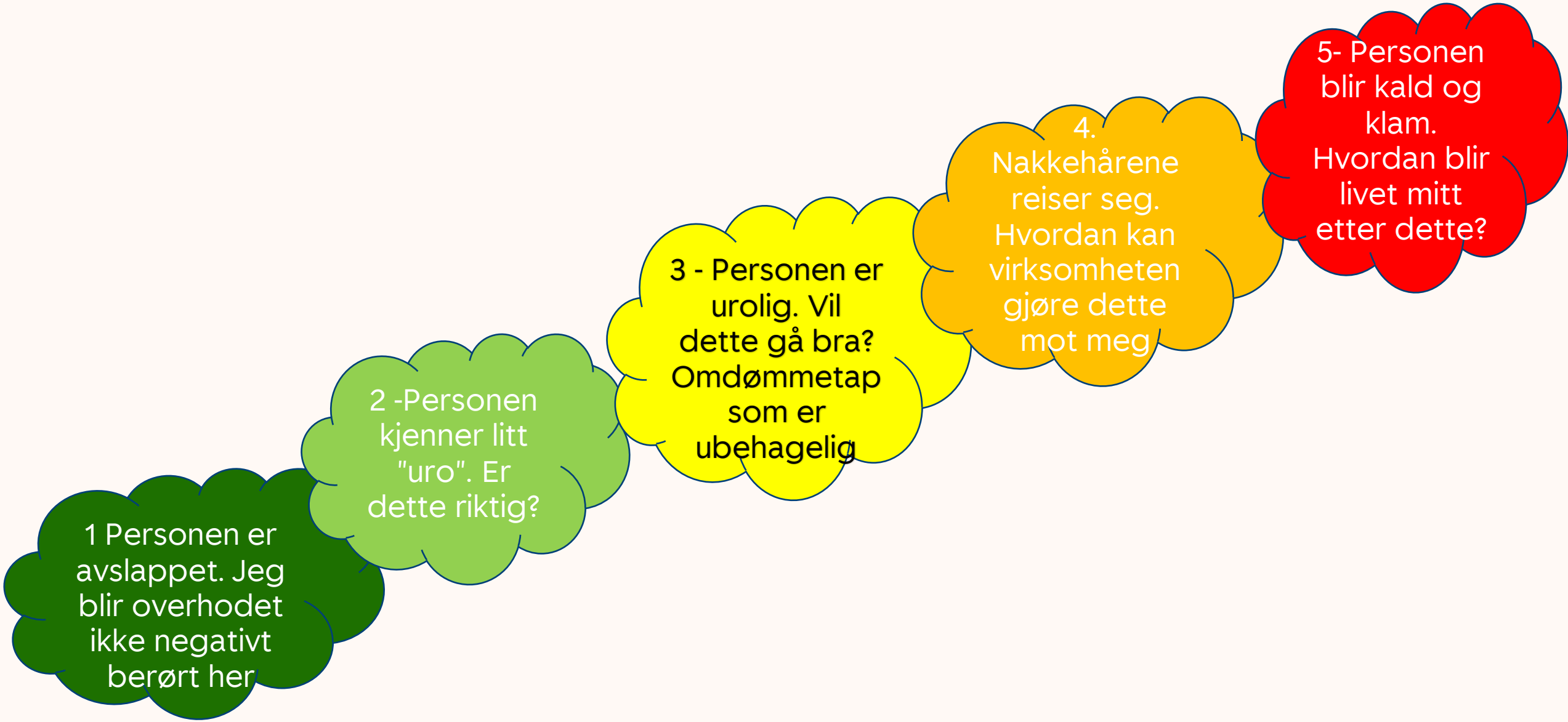
Trusselen ved eventuell manglende reell åpenhet er at Facebook potensielt kan skjule illegitim behandling bak uklar, uforståelig og mangelfull informasjon. Det kan medføre at den registrerte ikke får godt nok informasjonsgrunnlag til å ta gode valg i sin tilstedeværelse på plattformen, eller de kan være uvitende om hvorfor gitte beslutninger blir tatt om dem. Lite tilgjengelig informasjon kan potensielt medføre at den registrerte heller ikke får utøvd sine rettigheter etter personvernforordningen. I en situasjon der den ene parten vet mye mer om den andre vil det også være snakk om et skjevt maktforhold.

Eksempler

Konsekvensnivå personvern	Observerbare prosesser	*Rutiner i et ledelsessystem som skal ivareta personvernet, behandlingsprotokoll, personvernerklæring...
	Etterlevelsesdokumentasjon*	Kontroller / implementerte tiltak
Svært alvorlig	Det eksisterer ingen formelle styrende dokumenter eller etterlevelsesdokumentasjon som kan bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes. *F.eks: Det finnes ingen interne rutiner som skal sikre at personvernprinsippet etterleves.*	Det finnes ingen definerte kontroller som kan bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes. Tiltak innføres som en reaksjon på «eksterne overraskelser», f.eks. at en registrert ber om innsyn.
Alvorlig	Det er etablert noen styrende dokumenter og etterlevelsesdokumentasjon som kan bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes, men de er lite kjent. Prinsippet eller rettigheten ivaretas av nøkkelpersonell på en tilfeldig måte.	Det er etablert risikoreduserende tiltak for å sikre at den aktuelle rettigheten eller personvernprinsippet , men de er i all hovedsak kontrollerende, og i liten grad forebyggende. Tiltakene har ikke tydelige tiltakseiere, og de blir ikke fulgt opp systematisk over tid. Tiltakene avhenger av at ansatte følger manuelle prosesser.
Moderat	De aller fleste styrende dokumenter og etterlevelsesdokumentasjon som kan bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes, er på plass. De er imidlertid godt kjent i virksomheten og kan være utdatert, da de ikke oppdateres regelmessig. Prinsippet eller rettigheten ivaretas i hovedsak av nøkkelpersonell.	Det er etablert kontrollerende og forebyggende personverntiltak for å sikre den aktuelle rettigheten eller personvernprinsippet. De fleste av tiltakene har
Lavt	Alle styrende dokumenter og etterlevelsesdokumentasjon som bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes, er på plass. De er oppdaterte og kjent i virksomhe Det vil være lett for alle ansatte i virksomheten å ivareta personvernprinsipper og rettigheter, ikke bare nøkkelpersonel	
Ubetydelig	Alle styrende dokumenter og etterlevelsesdokumentasjon som bidra til at den aktuelle rettigheten eller personvernprinsippet overholdes, er på plass og integrert i virksomhetens ISMS. De oppdaterte og godt kjent i virksomheten. Det er lett for ansatt virksomheten å ivareta personvernprinsipper og rettigheter.	

Konsekvenskategorier og -nivåer	For virksomheten					For den registrerte
	Liv og helse	Økonomi	Tillit	Etterlevelse av lover og regler	Måloppnåelse	Konsekvenser for den registrerte
Svært alvorlig	Dødsfall eller flere personer rammes av alvorlig varig funksjons-nedsettelse eller skade.	Tap/skade på over 5 mill kroner for virksomheten	Langvarige og svært negative oppslag i riksdekkende media. Vesentlig tap av tillit hos innbyggere og samfunnet.	Kan medføre eller bidra til alvorlig brudd på lov, forskrift eller annet regelverk.	Manglende oppnåelse av kritiske mål i tildelingsbrevet.	-Tap av liv. -Varige og alvorlige helsemessige konsekvenser. -Varig og betydelig økonomisk Tap for den registrerte. -Varig og alvorlig Tap av den registrertes omdømme. -Hendelsen kan føre til at den registrertes rett til personvern krenkes på en svært alvorlig måte. -den registrerte og samfunnet taper tilliten til Oslo kommune.
Alvorlig	Alvorlig personskade eller varig funksjons-nedsettelse.	Tap/skade mellom kr 1 og 5 mill for virksomheten	Negative oppslag i riksdekkende media over flere dager. Tap av tillit hos innbyggere og samfunnet.	Kan medføre eller bidra til brudd på lov, forskrift eller annet regelverk.	Manglende oppnåelse av mindre kritiske mål i tildelingsbrevet.	-Varige eller alvorlige helsemessige konsekvenser. - Økonomisk tap av betydelig varighet for den registrerte. - Varig eller alvorlig tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes alvorlig. - Den registrerte taper tilliten til Oslo kommune.
Moderat	Mindre alvorlig personskade	Tap/skade mellom kr 250.000 til 1 mill for virksomheten	Mindre eller kortvarige oppslag i media.	Kan medføre eller bidra til mindre alvorlige brudd på lov, forskrift eller annet regelverk. Kan medføre brudd på intern instruks eller reglement.	Moderat innvirkning på oppnåelse av virksomhetens mål.	- Midlertidige eller noe mer alvorlige helsemessige konsekvenser. - Økonomisk tap av noe varighet for den registrerte. - Midlertidige eller noe mer alvorlige tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes noe mer alvorlig. - Den registrertes tillit til Oslo kommune utfordres.
Lav	Småskader	Tap/skade mellom kr 50.000 og 250.000 for virksomheten	Henvendelse fra media uten negative oppslag.	Kan medføre brudd på intern instruks eller reglement, uten at dette medfører brudd på lov, forskrift eller annet regelverk.	Liten innvirkning på oppnåelses av virksomhetens mål.	- Midlertidige eller mindre alvorlige helsemessige konsekvenser. - Forbigående økonomisk tap for den registrerte. - Midlertidig eller begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode eller uten å involvere særlige kategorier/sårbare grupper. - Den registrertes tillit til Oslo kommune utfordres midlertidig.
Ubetydelig	Ingen skade	Tap/skade på mindre enn 50.000 kroner for virksomheten	Ubetydelig påvirkning fra media.	Påvirker ikke etterlevelse	Ubetydelig innvirkning på oppnåelse av virksomhetens mål.	- Forbigående, mindre økonomisk tap for den registrerte. - Midlertidig og begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode og uten å involvere særlige kategorier/sårbare grupper.

Hva er konsekvensene for den **registrerte**...?



Men dette må operasjonaliseres!

Lukk | Personvernkonsekvensvurdering for TEST-formål | PDF

Uønsket hendelse	Årsak	Beskrivelse av mulig konsekvens	Risikonivå	Tiltak			Risikonivå etter tiltak	Fremdrift	
				Beskrivelse	Ansvarlig	Frist			
Det er manglede åpenhet (informasjon) til den registrerte. F. eks. at informasjonen om behandling ikke er tilstrekkelig tilpasset målgruppen, ikke er tilstrekkelig beskrevet slik at den registrerte forstår hva som behandles)								●	⚙
Det er manglede informasjon i personvernerklæringen slik at den ikke inneholder alle rettigheter til den registrerte.								●	⚙
Behandlingen er ikke forståelig for de registrerte og/eller foregår på skjulte eller manipulerende måter (gjennomsiktig).								●	⚙
Formålet er ikke tilstrekkelig spesifikt, uttrykkelig og lovlig.								●	⚙
Personopplysningene blir behandlet til et annet og uforenelig formål enn det de opprinnelig ble samlet inn for «formålsutglidning», og det er ikke foretatt en «forenelighetsvurdering» for å legitimere dette (For eksempel ved at logger som skal benyttes til feilsøk blir brukt til markedsføring)								●	⚙
Mengden innsamlede personopplysninger er ikke begrenset til det som er nødvendig for formålet med innsamlingen. Det samles inn for mye personopplysninger fordi det er enklest, «kjekt å ha» eller ubetenksomt.								●	⚙
Personopplysninger er ikke korrekte eller oppdaterte								●	⚙
Personopplysninger blir ikke anonymisert eller slettet når de ikke lenger er nødvendige for formålet de ble innhentet for.								●	⚙
Behandlingen av personopplysninger ivaretar ikke tilfredsstillende konfidensialitet (det er sårbarheter eller feil i teknologi, rutiner eller måten vi håndterer data på slik at uvedkommende får tilgang til personopplysningene. F. esk brudd på intern taushetsplikt, dårlig tilgangsstyring (tilgang til flere personopplysninger enn nødvendig («tjenstlig behov») og/eller flere ansatte enn nødvendig								●	⚙

Velg personvernkonsekvens

Personvernkonsekvens	Ubetydelig (1)	Mindre viktig (2)	Middels viktig (3)	Viktig (4)	Forretningskritisk (5)
Krenkelse av privatlivet for den registrerte	Personen opplever at egne personopplysninger er trygge og at privatlivet er ivaretatt	Brudd på taushetsplikten som kan medføre krenkelse av privatlivet. «Kan personer uten tjenstlig behov ha tilgang til mine personopplysninger?»	Personen får opplysninger på avveier som medfører moderat krenkelse av privatlivet. Brudd på taushetsplikten. «Kan dette påvirke livet mitt?»	Fysisk eller psykisk påkjenning eller belastning som påvirker hverdagen noe	Fysisk eller psykisk skade som preger hverdagen, som sykefravær, behov for helsehjelp, alvorlig skade, tap av liv. Spesielt om det gjelder sårbare grupper
Tap av tillit og anseelse for den registrerte	Ingen tap av anseelse	Lite tap av anseelse. Tilliten til banken er ikke, eller i mindre grad, svekket.	Anseelse er moderat. Tilliten til banken er svekket. «Jeg vurderer å bytte bank»	Tapet av anseelse opplevest høyt. Tilliten til banken er sterkt svekket. «Jeg vil ikke bruke alle tjenestene i banken»	Tapet av anseelse oppleves som uoverkommelig. Tilliten til finansnæringen er tapt for alltid. «Hvor skal jeg ha pengene mine?»
Økonomisk konsekvens for den registrerte	Ingen økonomiske tap	Økonomiske tap på «timelønn» eller mindre	Økonomisk tap på en dagslønn	Økonomisk tap på ukelønn	Økonomisk tap på en månedslønn eller mer
Helsen til den registrerte	Ingen påvirkning på fysisk eller psykisk helse	Minimal fysisk eller psykisk påkjenning	Fysisk eller psykisk påkjenning eller belastning som påvirker hverdagen noe	Fysisk eller psykisk påkjenning eller belastning som påvirker hverdagen, uten behov for helsehjelp	Fysisk eller psykisk skade som preger hverdagen, som sykefravær, behov for helsehjelp, alvorlig skade, tap av liv. Spesielt om det gjelder sårbare grupper

Spørsmål til diskusjon

1. Hvem er den registrerte og hvor «normal» eller «spesiell» er de?
   - Skal vi tenke på *konsekvensen for* den utrygge (f.eks. en flyktning fra krigsområde) eller gjennomsnitts-Ola (voksen eller barn?)
2. Kan vi bruke skalaen vi har for risikovurderinger og gjøre personvernkonsekvensvurdering sammen med risikovurderingen?
3. Skal konsekvens være så konkret som mulig eller mer abstrakt?
4. Samme skala for hele virksomheten, bransjen, Norge, EU?
5. Gir sannsynlighet mening per risiko for konsekvens av dårlig etterlevelse av hver rettighet?

Tones oppsummering

- Det er stor grad av usikkerhet hvordan konsekvenser for de registrerte vurderes fra «personvernekseperter»
- Skalaen som brukes er ofte «utydelig» – og det er vanskelig å velge
- Det er lite litteratur på området
- Det er lite deling og samordning i bransjer/ sektorer

SpareBank 1 ØSTLANDET

Takk for gode diskusjoner