Sjekklistebasert revisjon for behandling av elektroniske samtykker

Svein Olaf Bennæs
14. juni 2018
Aalborg Universitet / MIR
Masteravhandling
Veileder: Tine Weirsøe

Innholdsfortegnelse

Innledning

De fleste av oss har i den senere tiden mottatt en rekke henvendelser fra ulike virksomheter som ønsker vårt samtykke til å fortsatt kunne behandle personopplysninger etter at den nye personvernforordningen ble innført i EU den 25. mai 2018.

Vera Jourová, EUs justiskommisjonær, understreker at selskaper som tjener penger på bruk av personopplysninger, får et spesielt ansvar[1].

> *«Personopplysninger er vår tids gull. Og vi gir fra oss opplysninger ved så godt som hvert eneste skritt vi tar, spesielt i det digitale rommet. Det er som om folk står nakne i en gullfiskbolle.»*

Dette gjelder naturligvis ikke bare selskaper som tjener penger på bruken. Overordnet i målsettingen for personvernforordningen, er gi borgerne bedre kontroll over hvilke personopplysninger ulike virksomheter samler inn om dem, og hva de bruker opplysningene til.

Krav om samtykker ligger i kjernen av dette.

Virksomhetene som behandler personopplysninger, har etter den nye forordningen bevisbyrden, følgelig også dokumentasjonsbehovet[2], for samtykker som er inngått etter forordningens ikrafttredelse.

Saken mot Facebook og deres deling av personopplysninger til blant andre Cambridge Analytica[3] har bidratt til at oppmerksomheten rundt behandling basert på samtykke fra den registrerte har nådd uante høyder, og har medført at mange virksomheter tar temaet mer på alvor enn tidligere.

I perioden hvor jeg har befattet meg med problemstillingen for denne oppgaven, har temaet ofte kommet opp i samtaler med kolleger, medstudenter og andre i min omgangskrets. I retrospekt er jeg overrasket over hvor ofte jeg har funnet meg selv langt nede i detaljene, av ren nødvendighet, for å gjøre rede for hva dette handler om. Oppgaven vil av mange oppfattes som relativt teoritung, men grunnen vil forhåpentligvis være tydelig når teorien settes sammen til praktiske verktøy. Samtykker spiller en svært viktig rolle i personvernsammenheng, og – som erfaringene fra bl.a. Cambridge Analytica-saken indikerer – så vil denne rollen bli enda mer sentral i fremtiden.

En av utfordringene for de behandlingsansvarlige er, og blir, å holde orden i den etter hvert omfattende mengden av samtykker som de til daglig behandler personopplysninger på grunnlag av, og sørge for at virksomheten er godt rigget for å dokumentere sin praksis, enten det er i forbindelse med rettssaker eller annet. Dette treffer et skjæringspunkt mellom teori og praksis som jeg til nå ikke har funnet noe godt verktøy å benytte for å sikre. Oppgaven er et forsøk på å bidra til at behandlingsansvarlige virksomheter lettere kan sikre at sin samtykkebaserte behandling av personopplysninger skjer på en strukturert, systematisk, hensiktsmessig og dokumentert måte.

---

[1] https://www.digi.no/artikler/eu-lover-a-bite-fra-seg-i-handhevingen-av-gdpr/438250 (lest 25.5.2018)

[2] Personvernforordningen art. 7 jf. art. 24

[3] https://www.ft.com/content/c1f326a4-2b24-11e8-9b4b-bc4b9f08f381 (lest 30.5.2018)

Problemformulering

Hvilke kontroller kan etableres for å sikre at behandlingsansvarlige virksomheter kan følge opp samtykkene på en forsvarlig måte i prosesser der hvor behandlingen av personopplysninger er basert på samtykke som eneste rettslige grunnlag?

Kan man benytte elementer fra eksisterende standarder og rammeverk for å etablere et praktisk og anvendelig verktøy, en sjekkliste, for å sikre forsvarlig håndtering av samtykker hos en behandlingsansvarlig?

Relevans

Personopplysningene tilhører den registrerte – som behandlingsansvarlig har man opplysningene kun på lån. Reguleringen av forutsetningene for dette lånet manifesteres i samtykket, og samtykket kan ses på som en kontrakt mellom den registrerte og den behandlingsansvarlige.

Problemstillingen er relevant for behandlingsansvarlige som gjennomfører behandling av personopplysninger basert på samtykke fra den registrerte, siden personvernforordningen legger dokumentasjonsansvaret på den behandlingsansvarlige.

Den er spesielt relevant der hvor det benyttes teknologiske løsninger som gjør oppslag/systemkall for å kontrollere samtykkets gyldighet, som altså er fullstendig baserte på at samtykket til en hver tid har korrekt status (gyldig eller ugyldig), hvilke eventuelle tredjeparter personopplysningene deles med, at formålet er det samme som det opprinnelig var, at det dreier seg om de samme personopplysningene og at behandlingsprosessen ikke har endret materiell karakter siden samtykket opprinnelig ble gitt.

For den registrerte er problemstillingen interessant fordi samtykket representerer retten den registrerte gir den behandlingsansvarlige til å behandle personopplysningene, og den registrerte kan trekke tilbake samtykket, dvs. frata den behandlingsansvarlige retten til videre behandling. Dette er en faktor som tidligere ikke har hatt ønsket effekt; det har langt på vei vært opp til den behandlingsansvarlige om en tilbaketrekking har medført stans i videre behandling, langt mindre om ens personopplysninger har blitt slettet som følger av at samtykket har blitt trukket tilbake.

Til nå har vi ikke sett mange eksempler på at integriteten og autentisiteten til samtykkeobjektet, dokumentasjonen som sådan, har blitt utfordret i særlig grad i rettslige anliggender, men det er ingen grunn til å anta at så ikke kommer til å skje i fremtiden.

I en verden hvor de teknologiske løsningene i stadig større grad benytter automatisering og/eller kunstig intelligens for hele eller deler av behandlingsprosessen, vil det være kritisk at samtykkets gyldighet er ubestridelig, og at dette er ubestridelig dokumentert. Den behandlingsansvarlige må derfor være trygg på, og til en hver tid kunne kontrollere, at denne behandlingen foregår basert på samtykke som er gyldig, ivaretatt og dokumenterbart på korrekt måte.

Teori

Personvern

Jeg har gått til personvernforordningen fra EU (General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) for å knytte oppgaven til reglene som gjelder behandling av personopplysninger.

Vedtaket som ble gjort i EU-parlamentet[4] betyr at alle EU-land fikk en ny og enhetlig personvernlovgivning fra 25. mai 2018. Norge vil som EØS-medlem også implementere forordningen, men det gjenstår ennå noe arbeid før den vil vedtas i EØS-komitéen. Det legges opp til at regelverket skal innføres i Norge i løpet av sommeren 2018. Innføringen vil medføre endringer[5] sammenlignet med dagens lovverk, som reguleres gjennom personopplysningsloven[6].

Samtykker

Personvernforordningens artikkel 6 stiller opp seks ulike rettslige grunnlag for behandling av personopplysninger, hvorav ett er eksplisitt samtykke.

Samtykket, slik jeg behandler det videre i denne oppgaven, må forstås som *et objekt*, altså noe hvorpå man kan utføre en handling eller operasjon, og som for revisjonsformål må kunne følges gjennom hele objektets livssyklus.

Jeg har redegjort for kravene med forordningens originalutgave som grunnlag. I tillegg til dette har jeg, for noen begrepsdefinisjoner, benyttet den uoffisielle, norske oversettelsen som finnes på nettstedet til Datatilsynet i Norge[7] samt Stortingsproposisjon 56 LS (2018-2019) som ble behandlet i Stortinget 22. mai 2018[8].

Ny norsk personopplysningslov vil gjennomføre forordningen i norsk rett. Hovedprinsippene i gjeldende lov blir langt på vei videreført, og det er i regjeringens uttalelser om arbeidet med høringsuttalelsene[9] ingen vesentlige, materielle endringer hva angår de grunnleggende definisjonene som er benyttet i oppgaven.

Her vil jeg gjerne påpeke muligheten for å tolke begrepet som en referanse til selve handlingen *å gi sitt samtykke* (til noe), versus samtykket som *et objekt*. Å skille disse to tolkningene er vesentlig for oppgavens innhold og konklusjon, og samtykke må i det følgende forstås som et objekt.

---

[4] http://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era

[5] https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/hva-blir-nytt-med-forordningen/

[6] https://lovdata.no/lov/2000-04-14-31

[7] https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/forordningens-lovtekst/

[8] https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=71720

[9] https://www.regjeringen.no/no/aktuelt/ny-lov-om-behandling-av-personopplysninger-pa-horing/id2564315/

Om samtykker som records

Med samtykke som eneste behandlingsgrunnlag stilles det spesielle krav til dokumentasjon i forordningen, som fremgår av artikkel 7(1):

> *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

Sammen med forordningens fortale 82 fremstår kravet om dokumentasjon av behandlingsaktivitetene tydelig:

> *In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.*

Arkivering av samtykker

Lov om arkiv[10] gjelder alle offentlige organer i Norge, jf. § 5:

> *Føresegnene i dette kapitlet gjeld for alle offentlege organ med unnatak for Stortinget, Riksrevisjonen, Stortingets ombodsmann for forvaltninga og andre organ for Stortinget.*

Jeg har i en tidligere oppgave fastslått at samtykker er arkivverdige for offentlig sektor, og knyttet selve samtykket opp mot krav til behandling av arkivverdig dokumentasjon[11].

Livssykklusperspektivet

Livssykklusperspektivet er beskrevet av mange, og i oppgaven har jeg undersøkt Bawden og Robertson (2012), JISC (2007), Tayfun & Gibson (1996), Hoke (2011) og Weirsøe (2016) for å finne en hensiktsmessig og anvendelig modell for livssyklusen til elektroniske samtykker. Jeg kommer tilbake til denne modellen i Figur 1, s. 13.

Standarder

Records og records management

Standarder er normative dokumenter, utgitt av et medlemsbasert og faglig forankret standardiseringsorgan. En standard uttrykker faglig konsensus; oftest gjennom en bredt sammensatt gruppe av kompetanse innen et område som beslutter innholdet. Hva gjelder *records management* er det i all hovedsak International Organization for Standardization (ISO) som står bak standardiseringen.

---

[10] https://lovdata.no/lov/1992-12-04-126

[11] Bennæs (2018)

ISO 15489 var den første internasjonale Records Management-standarden, og har en funksjon som overordnet referansestandard for en voksende portefølje av senere standarder på tilgrensende områder[12].

ISO 15489 tar for seg en rekke fundamentale konsepter, prinsipper, begreper og definisjoner knyttet til records og håndteringen av records (records management). Den siste versjonen av ISO 15489 refererer til ISO 23081-1:2006 og ISO 23081-2:2007 for noen av begrepsdefinisjonene.

ISO 16175 har som formål å etablere harmoniserte prinsipper og funksjonelle krav for systemløsninger som produserer og vedlikeholder elektronisk dokumentasjon (records), dog ikke for langtidsbevaring.

I det videre vil jeg bruke begrepene *dokument* eller *dokumentasjon* for å representere *records*.

Kommunikasjon
ISO 30302:15 Information and documentation – Management systems for records – Guidelines for implementation, kapittel 7.4, finnes det en rekke anbefalte kommunikasjonstiltak for å øke bevisstheten rundt behandlingen av records, samt for målsetting, gevinster, organisering, roller, ansvar og dokumentasjon knyttet til behandlingen. Disse kan med fordel inngå som en del av forberedelser for, gjennomgang av og etterarbeid etter en revisjon. I kapittel 10 finnes gode eksempler på hvordan å drive korrigerende tiltak og kontinuerlig forbedring – som også i denne sammenhengen – kan være nyttige å vurdere under og i etterkant av revisjoner.

Klassifikasjon og metadata
ISO 15489 definerer klassifikasjon slik:

> *«...systematic identification and/or arrangement of business activities and/or records into categories»*

Oversatt til norsk innebærer dette systematisk identifikasjon og/eller kategorisering av forretningsaktiviteter og/eller dokumentasjon.

En gjennomtenkt klassifisering av samtykker er vesentlig for å kunne finne korrekte samtykker om man blir nødt til å lete etter dem, og absolutt avgjørende i tilfeller hvor det fullt ut benyttes automatiserte prosesser i behandlingen.

ISO 23081-serien, standardene om metadata for records, kom i 2006. Disse omhandler typer av metadata til dokumentasjon for ulike formål; identifisere, tidfeste, angi kontekst for, definere rettigheter til og gjenfinne dokumentasjon som virksomheten mottar og produserer. Standarden tar også for seg forvaltningsmessige forhold rundt metadatatypene. Standarden stiller opp prinsipper og et rammeverk for etablering, forvaltning og bruk av metadata innen dokumentasjonshåndtering. Standarden krever ingen obligatoriske metadata, men refererer til andre sett av metadata som eksempelvis følger av ISO 15489.

[12] Andresen (2016)

Krav om klassifikasjon av arkiver i offentlige organer følger av bestemmelsene i Forskrift om offentlege arkiv, § 5[13]:

> *Organet skal ha ei ordning for klassifikasjon som omfattar alle dei saksområda organet har ansvar for. I staten skal klassifikasjonen skilje mellom eigenforvaltning og fagsaker.*

Revisjon

Dette begrepet brukes i mange sammenhenger, på tvers av fagfelt og organisatoriske grenser, og har vært til dels vanskelig å finne entydighet rundt. Utsagnet fra COSO[14], som har laget rammeverk for kontroll, tyder på at mange har kommet til samme konklusjon som meg:

> *«internal control means different things to different people»*

Jeg har først og fremst sett til ISO 9001:2015, ISO 19011:2012, COSO (2012, 2015) samt Pickett (2011) for å finne perspektiver og metoder for revisjoner, og har av dette forsøkt å trekke ut noen generelle prinsipper og praktiske holdepunkter som kan gjøres relevante uavhengig av virksomhetenes bransje, størrelse og struktur.

[13] https://lovdata.no/SF/forskrift/2017-12-15-2105/§5

[14] http://www.coso.org

Metode

Jeg har i hovedsak hentet ulike perspektiver fra pensumlitteraturen for å forsøke å gi noen konkrete, anvendelige svar til min problemformulering.

Jeg har i tillegg innhentet annen litteratur slik det fremgår av fotnoter og referanseliste for å kunne innrette sluttresultatet mot noe praktisk anvendelig.

Omfang, forutsetninger og begrensninger

Oppgaven omhandler revisjonspunkter og kontroller som angår livssyklusen til samtykker i forbindelse med behandling av personopplysninger som gjøres med samtykke som eneste rettslige grunnlag.

Oppgaven er ikke en uttømmende gjennomgang av personvernforordningens bestemmelser om samtykker, men omhandler de bestemmelser som har særlig relevans for å kunne føre kontroll med hvordan samtykker behandles.

Jeg har forutsatt at samtykket og dets innhold er utformet på en slik måte at det ikke anses for å utgjøre personopplysninger i seg selv, og at samtykket som sådan ikke omfattes av rettsreglene for behandling av personopplysninger.

Videre har jeg forutsatt at personell- og formkrav til samtykker, spørsmål om tilstrekkelig samtykkekompetanse samt krav til formålsbeskrivelser er ivaretatt. Disse kravene er redegjort for i Schartum og Sætre (2016), og tas ikke opp til diskusjon i denne oppgaven.

I noen tilfeller brukes samtykkebasert behandling av personopplysninger selv om virksomheten har annet juridisk grunnlag, eksempelvis for oppfyllelse av en kontrakt mellom behandlingsansvarlig virksomhet og den registrerte. Dette er således en overoppfyllelse av kravene i personvernforordningen. Innholdet i denne oppgaven vil være relevant for disse også, selv om det rent juridiske kravet til dokumentasjon ikke er overlappende.

Analyse og diskusjon

For å komme frem til et hensiktsmessig sett med kontroller for revisjonsøyemed, er det nødvendig å foreta noen avklaringer og valg i det teorigrunnlaget som danner utgangspunktet, samt identifisere noen faste holdepunkter som gir mening når revisjoner skal gjennomføres.

I personvernforordningen ligger kravene til behandling av selve samtykkene mer implisitt i forordningens tekst og dens forarbeider, heller enn som konkrete krav og føringer. Dette gjør at man som behandlingsansvarlig, i tillegg til å sørge for at samtykkene i seg selv er i tråd med reglene og dokumentert deretter, også må sikre at *behandlingen av samtykkene* også gjøres på en måte som sikrer både personvernet til den registrerte, men også og den behandlingsansvarliges rettsstilling.

Begrepene og deres innhold står så vidt sentralt i forståelsen av hvilken rolle samtykker spiller i behandlingsprosessen, så i det følgende vil jeg redegjøre for de viktigste.

Sentrale begreper

De begrepene i personvernforordningen som er vesentligst for oppgaven er *behandling, personopplysninger*, *samtykke*, *behandlingsansvarlig* og *databehandler*. Begrepene er i hovedsak en videreføring av dagens regelverk, men med enkelte presiseringer. Definisjonene fremgår av forordningens artikkel 4.

Med *behandling* mener forordningen 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, konsultasjon, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Dette vil i praksis være det samme som i dagens lovverk. Typiske eksempler fra interaksjonen mellom borgere og virksomheter kan være elektroniske søknader, registrering av demografiske opplysninger, GPS-posisjonering, borgermapper, biometriske data og kommunikasjonsopplysninger.

Personopplysninger er, i den uoffisielle norske oversettelsen av personvernforordningen[15], definert som

> *«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 online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet».*

Forordningen inneholder en deling av personopplysninger i kategorier. Noen typer personlige data er ansett som mer følsomme enn andre og underlagt strengere regler for behandling. Dette er redegjort for i forordningens artikkel 9 og 10.

---

[15] https://www.datatilsynet.no/globalassets/global/regelverk-skjema/forordningen/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf

Begrepet «sensitive personopplysninger», slik vi kjenner det fra personopplysningslovens § 9 i dag, er ikke videreført i forordningen. Begrepet er erstattet av «*særlige kategorier av personopplysninger*», jf. forordningens artikkel 9. Behandling av personopplysninger som omfattes av slike *særlige kategorier* er som utgangspunkt ikke tillatt, men artikkel 9.2 flg. gir unntak fra hovedregelen, og i bokstav a) finner vi at *eksplisitt samtykke* kan gis av den registrerte.

I denne sammenhengen gjøres samtykket til et vippepunkt for den behandlingsansvarlige; personopplysninger som faller inn under denne betegnelsen kan altså ikke overhodet ikke behandles uten særskilt grunnlag.

Samtykke fra den registrerte er i personvernforordningens oversettelse (ibid.) definert som

> *«enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende».*

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig eller privat virksomhet, institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Den behandlingsansvarlige har en rekke forpliktelser og har ansvar for å oppfylle regelverket overfor både de registrerte og myndighetene. I et arbeidsforhold er det normalt arbeidsgiveren (det juridiske selskapet) som vil er behandlingsansvarlig, i et kunde-leverandør-forhold er det normalt leverandøren som er behandlingsansvarlig.

Databehandler er en fysisk eller juridisk person, en offentlig eller privat virksomhet, institusjon eller ethvert annet organ som behandler personopplysninger på vegner av den behandlingsansvarlige. Dette kan for eksempel være leverandøren av et fagsystem, et bemanningsbyrå, en skyløsning for personal- og lønnstjenester eller en IT-driftsleverandør.

I denne oppgaven er det som angår behandlingsansvarlig like relevant for databehandler, men jeg har for bedre lesbarhet kun benyttet begrepet *behandlingsansvarlig*.

Nye regler gir endring i perspektiver

En vesentlig endring er at personvernforordningen, i motsetning til 95-direktivet[16], gir direkte forpliktelser for databehandlerne. I tillegg kommer muligheten for at de registrerte kan utøve sine rettigheter direkte mot databehandlerne, og et regime for håndhevelse som stiller databehandlere som ikke følger regelverket åpne for sanksjoner. Selv om databehandlere har ulike forretningsmodeller – fra lokale leverandører til skytjenester, fra den lokale IT-virksomheten til internasjonale aktører – vil de bestemmelsene i forordningen som gjelder for behandling av personopplysninger i stor grad være de samme, eksempelvis krav til informasjonssikkerhet og krav til dokumentasjon.

Personvernforordningen åpner for sanksjoner inntil 20 millioner euro, eventuelt inntil 4 % av en virksomhets samlede omsetning, noe som vil påvirke de fleste virksomheter i betydelig grad. For

[16] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Facebook medførte omtalen av Cambridge Analytica-saken et umiddelbart verditap på rundt 60 millioner US dollar i løpet av kun to døgn[17] etter at saken ble kjent i media.

Allerede på datoen for den nye personvernforordningens ikrafttredelse gikk den østerrikske juristen Max Schrems til sak mot gigantene WhatsApp, Instagram, Google og Facebook. I sistnevnte sak er det nettopp brudd på reglene knyttet til samtykke som danner hovedanklagen, og på side 8 i anklagen peker den juridiske analysen blant annet på at bevisbyrden, «burden of proof», ligger hos Facebook[18]. For denne saken mot Facebook alene representerer maksimumskravet ca. 1,3 milliarder euro.

Datatilsynet i Danmark viser til dom i sak C-2010/16 hos EU-domstolen av 5. juni[19] hvor domstolen blant annet fastslår at Facebook og administratoren av en fanside har et felles dataansvar for behandlingen av personopplysninger som er samlet inn i forbindelse med besøk på den aktuelle fansiden[20]. I tolkningen fra Datatilsynet fremgår det at databehandleren skal være oppmerksom på hvilke opplysninger cookies leverer til tredjepart. Hvis en behandlingsansvarlig virksomhet for eksempel bruker cookies fra Google eller Facebook, kan virksomheten få et delt databehandleransvar med disse selskapene. Prinsipielt er dette interessant, da bruken av cookies krever samtykker fra brukeren[21], og krever en logisk referanse mellom samtykket og cookie-objektet. Det være svært krevende, om i det hele tatt mulig, å gjennomføre slike referanser i praksis, men saken

Når man vurderer samtykkenes sentrale betydning i bevisførsel, når de åpenbart bærer en økonomisk og/eller omdømmemessig verdi, gjøres de naturlig også til gjenstand for tettere oppfølging og kontroll.

Behandlingsansvarlige skal dokumentere

Veiledningen for samtykker[22] fra Datatilsynet i Danmark, som igjen viser til Article 29-gruppens retningslinjer for samtykker (2017), er også anbefalt benyttet av Datatilsynet i Norge. Sammen med retningslinjene gir veiledningen ikke et tydelig svar på om hvordan samtykker må behandles, men gir imidlertid noen tydelige idéer om hvilke kontroller som må etableres for å sikre god forvaltning av samtykkene.

Samtykket er, etter definisjonene i ISO 30300 og ISO 15489, å anse som dokumentasjon (angitt i standardene som *record)*.

---

[17] https://www.bloomberg.com/news/articles/2018-03-20/facebook-sees-tesla-sized-chunk-vanish-from-market-cap-in-2-days

[18] https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf (lest 28.5.2018)

[19] https://www.datatilsynet.dk/media/6872/eu-domstolens-afgoerelse-om-dataansvar-for-fansider-paa-facebook.pdf

[20] http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=421635

[21] https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/uttalelser-fra-artikkel-29-gruppen/cookies_internasjonalt/

[22] https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledning_om_samtykke__formateret_.pdf

Den praktiske delen av behandlingen av samtykkene, som dokumentasjon, må imidlertid implementeres hos de behandlingsansvarlige virksomhetene, noe som realiseres gjennom systemløsninger, arbeidsprosesser og informasjonsstrukturer.

Det er altså den behandlingsansvarlige virksomheten som er gjort ansvarlig for at prinsippene som er gitt i personvernforordningen overholdes. De skal kunne dokumentere at de behandler personopplysninger i tråd med personvernprinsippene, og i denne konteksten skal de altså kunne *dokumentere at behandlingen av personopplysningene er i tråd med samtykket* som er gitt av den registrerte.

Cambridge Analytica-saken, som ble nevnt innledningsvis, gir åpenbare argumenter til at man som behandlingsansvarlig må ta sitt ansvar på alvor, og aktivt følge med på behandlingen og dens gyldighet til en hver tid. Det vil derfor, naturlig nok, være i enhver virksomhets interesse – i tillegg til ansvaret som følger direkte av kravene i personvernforordningen – å kunne føre solide bevis for at den samtykkebaserte behandlingen av personopplysninger som er gjennomført, er gjort på gyldig, rettslig grunnlag, og for øvrig i tråd med de gjeldende krav i regelverket.

Samtykker sett i ulike perspektiver

Kahn (2009) argumenterer for at verdien av dokumentasjon kan vurderes ut fra sin forretningsmessige, operasjonelle og/eller regulatoriske verdi. Etableringen av kontroller og kontrollmekanismer for revisjon vil naturlig få sitt preg ut fra hvilket verdiperspektiv som anses som viktigst for virksomheten, noe som kan være med på å påvirke hvilken tilnærming en virksomhet bruker for å etablere kontroll med forvaltningen av samtykker.

Et naturlig ledd i kontrollen vil være revisjoner og risikoanalyse; det vil være av interesse for virksomhetene å etablere kontroller for å kunne følge opp på den faktiske behandlingen hvis det truer økonomiske eller omdømmemessige forhold.

United Nations (2014)[23] peker på risikovurdering som verktøy for å forsterke en virksomhets ytelse (performance), redusere forretningsmessig risiko og til strategisk hjelp for informasjonsforvaltere. De har satt opp to risikomomenter som primære; inadekvat styringsrammeverk for dokumentasjonforvaltning («inadequate record-keeping governace framework») og manglende bevissthet om viktigheten av dokumentasjon som bevismateriale («lack of awareness of the importance of records as evidence»). Videre peker de på en rekke operasjonelle konsekvenser, samt gir en utlisting av sekundære risikomomenter, før de til slutt stiller opp to tiltak som danner kjernen i risikohåndteringen av de to primære momentene.

Det som gjør USs tilnærming interessant, og dertil relevant, er identifikasjonen av «indiscriminate application of information technology end tools without effective record-keeping». På norsk blir det noe i retning av «lite gjennomtenkt bruk av teknologiske sluttbrukerløsninger uten ordentlig dokumentasjonshåndtering». Dette er noe som de aller fleste informasjonsforvaltere kan kjenne seg igjen i; løsninger for sluttbrukere blir satt i produksjon uten at man har helt tenkt igjennom

[23] United Nations (2014)

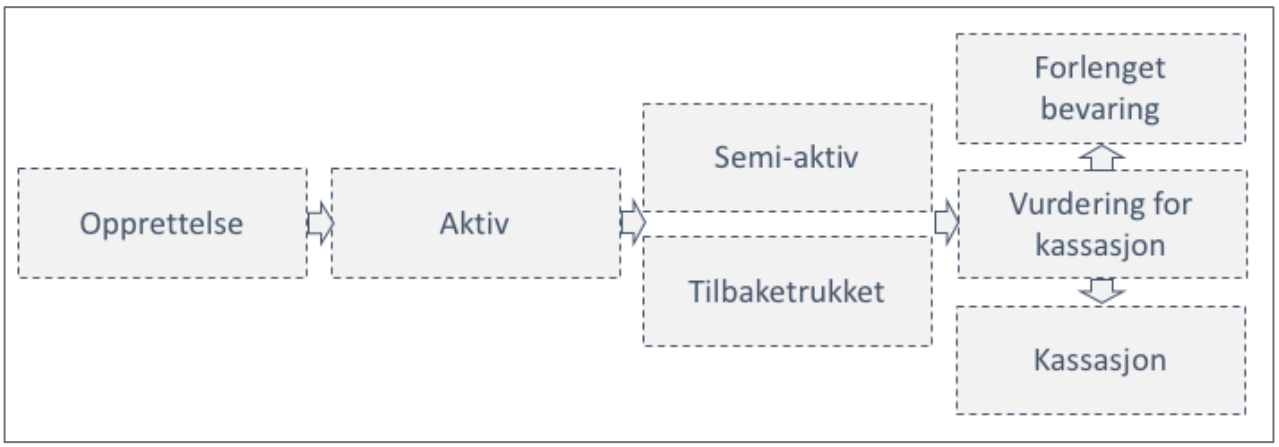
verdien av og livssyklusen til de ulike elementene av dokumentasjon som produseres og/eller behandles.

Et samtykkes livssyklus

Bawden og Robertson (2012) stiller opp et prinsipp om at informasjon, herunder dokumentasjonen den bæres av, foregår i en syklus av tydelig definerte steg; dokumentasjonens livssyklus. Dokumentasjonen bærer verdi så lenge den eksisterer, og «levetiden» avgjøres av dens livssyklus; fra den oppstår til den er slettet eller lagres for evigheten. Dette prinsippet legges til grunn for at forvaltning av dokumentasjon kan skje på hensiktsmessig måte.

Prosessene for forvaltning av dokumentasjonen bygger på helhetlig forståelse og operasjonalisering av livssyklusen, og sikrer effektivitet i arbeidet knyttet til hvert steg.

Bawden og Robertson (2012), s. 257, refererer til en livssyklusmodell fra Joint Information Systems Committee (JISC, 2007) som fungerer som et godt utgangspunkt for å dele inn samtykkers livssyklus i relevante faser:



Figur 1 Livssyklus for samtykker

I modellen fra JISC er det i denne sammenhengen hensiktsmessig å legge til et ekstra element som representerer tilbaketrekking av samtykket, slik som vist i Figur 2. Det er nærliggende å tenke at dette bare er en status for samtykket, men all den tid tilbaketrekking skal utløse et stopp-signal for videre behandling, eventuelt også sletting av personopplysningene det gjelder, bør det også representeres som et eget steg/element i syklusen.

Metadata og klassifisering

For å kunne behandle samtykkene etter god forvaltningspraksis, må de tilføres metadata.

Berikelse av samtykkene med metadata bør gjøres på en standardisert måte, for eksempel slik som jeg har foreslått i Bennæs (2018); basert på ISO 23081 og Dublin Core. Dette gir muligheter for automatisering og deling av dokumentasjon mellom ulike systemløsninger og/eller virksomheter, og legger til rette for automatisering av behandlingsprosesser. Metadata er i tillegg helt vesentlige for å kunne gjennomføre en troverdig revisjon; i de fleste av kontrollene vil det være nettopp metadataelementer som er gjenstand for undersøkelse.

Opprettelsen av samtykket fremstår som resultat av den behandlingsansvarliges virksomhet, og skal man søke idealet hva gjelder klassifisering av dokumentasjon, så må samtykket klassifiseres på en måte som både gjør det gjenfinnbart i hele livssyklusen, og det må også kunne håndteres korrekt i tilfeller hvor forretningsprosessen endres.

For å få en sammenheng helt fra samtykket opp til kvalitetsstyringen av forretningsprosessen, vil en hensiktsmessig klassifisering være avgjørende.

Bawden (2012) peker på at klassifisering i færre, mer overordnede nivåer vil gagne informasjonsforvaltningen i fremtiden, rett og slett fordi informasjonsmengden i seg selv vokser så voldsomt at detaljert klassifisering vil kreve for mye ressurser. I tillegg er dagens teknologi for søk og gjenfinning så godt utviklet at den demmer opp for ulempen med mye dokumentasjon innenfor hver klasse.

Færre og grovere kategorier kan være med på å redusere sannsynligheten knyttet til at dokumentasjon blir knyttet til feil klasse, eller at den blir vanskeligere å gjenfinne fordi det simpelthen blir for mange klasser å søke mellom.

I forbindelse med spørsmål om klassifiseringsstruktur kommer gjerne spørsmålet om proveniens til overflaten; en diskusjon om hvor samtykket har sin opprinnelse. Begrepet proveniens kommer av latinsk *pro-venire* som betyr å *komme fra* eller *stamme fra*, og er det som knytter arkivdokumenter, arkiver og deler eller serier av arkiver til arkivskaperen. Verdien til proveniensen er at den gir brukeren muligheten til å forstå et arkivdokument og dets innhold relatert til hvem som skapte det, hvordan, med hjelp av hvilke teknologier og systemer, hvor, når og hvorfor, og hvilke endringer som har funnet sted med dokumentene over tid og hvorfor dette har skjedd.

Å sette dokument i kontekst er et identifiserende mantra for arkivarer og andre som driver dokumentasjonsforvaltning. Provenienssprinsippet har blitt beskrevet som «hjørnesteinen» i arkivvitenskapen, som «det viktigste av alle prinsipper» som styrer arkivfaglig praksis, som det avgjørende symbolet på arkivarenes faglige identitet, i motsetning til bibliotekarer på den ene siden og forskere eller dokumentalister på den andre[24].

Samtykkets iboende relasjon til formålet og behandlingsprosessen hvor det opprettes, gjør det naturlig å spørre frem til i hvilken prosess, eller til hvilket formål, samtykket ble gitt. En prosess uten et formål synes meningsløst, og et formål uten en eller flere tilhørende prosess(er) er tilnærmet utenkelig i et digitalt produksjonsperspektiv. Samtykket er således naturlig knyttet til prosessen, og det naturlige vil da være å klassifisere basert på prosess. ISO 15489 peker på behovet for å utvikle metadata-skjemaer i kapittel 8.2, hvor foreslåtte klassifiseringsprinsipp faller under bokstav c) *Business (or Function) – business functions, activities and transactions or work processes*.

I norsk offentlig sektor vil det være en ganske kontroversiell øvelse, da det er lange tradisjoner med å benytte emnebaserte arkivnøkler for klassifisering. Torres (2006) peker på noen av

[24] Cook (2010)

fordelene med prosessbaserte kassasjonsplaner, og selv Riksarkivaren i Norge anbefaler i sin *Veileder for bevaring og kassasjon i kommunale og fylkeskommunale arkiver skapt etter 1950*[25] anbefaler prosessorientering av arkiver som dannes i fagsystemer (s. 35):

> *Ingen fylkeskommunale eller kommunale arkivskapere har i dag et rent funksjons- og prosessbasert klassifikasjonssystem. Dette må på plass før en automatisert registrering av bevarings- og kassasjonsvedtak er mulig. Inntil det er på plass, er en manuell registrering på den enkelte sak (eventuelt journalpost eller dokument) eneste alternativ.*

For offentlige virksomheter er klassifikasjon pålagt gjennom Arkivforskriften § 2-3; et organ normalt skal ha et klassifikasjonssystem (arkivnøkkel) som omfatter alle saksområdene organet steller med.

Riksarkivaren har dog tidligere, blant annet i brev til Helse- og omsorgsdepartementet av 31. oktober 2014[26], advart mot at prosesskartlegging kan være en krevende øvelse, hvor det må foretas en grundig og detaljert prosessanalyse i virksomheten.

Dette må tolkes som om at det skal gode grunner til for å få dispensasjon fra kravet. Dessuten er arkivkoden (etter arkivnøkkelen) et obligatorisk informasjonselement i virksomhetens journal, jf. Arkivforskriften § 2-7. I Noark 5[27] er klassifikasjon obligatorisk for sakarkiver (arkiver med saksdokumenter).

Når jeg foreslår å utføre kontrollene i en revisjon med samtykkene i sentrum, må de følgelig kunne finnes der hvor samtykkene håndteres. Når krav om håndtering av samtykkene krever lagring i Noark-løsninger, noe som gjelder alle norske offentlige organer, så bør kontrollene kunne gjennomføres også der.

Endringer i forretningsprosesser kan skje av ulike årsaker, og i velorganiserte virksomheter vil det typisk kunne følge av en *Plan-Do-Check-Act*-syklus (ISO 9001:2015) med formål om å forbedre prosessen. Da må man som behandlingsansvarlig virksomhet også være trygg på at dokumentasjonen som behandles i den aktuelle forretningsprosessen også kan gjenfinnes og følge med over den forbedrede forretningsprosessen.

ISO 16175 anfører identifisering av et sett informasjonselementer som utgjør dokumentasjonen, inkludert en relasjon til behandlingsprosessen og -konteksten. Den bygger på et prinsipp om å la behandlingsprosess og underliggende systemer generere så mye metadata til

---

[25] https://www.arkivverket.no/for-arkiveiere/bevaring-og-kassasjon/bevaring-og-kassasjon-hos-kommuner-og-fylkeskommuner/_/attachment/download/090f5a39-d4d1-4b3c-a14c-4a9f617ff364:42d89081f777f2a4433e1525785b3bd6178fb912/Veiledning%20BK-bestemmelser%20for%20kommunale%20arkiv%20skapt%20etter%201950%20(2015).pdf (lest 16.5.2018)

[26] http://www.arkivrad.no/sites/arkivrad/files/user/Dokumenter/bruk_av_arkivnokkel_i_hod_brev_fra_ra_31.10.14.pdf (lest 26.5.2018)

[27] https://www.arkivverket.no/forvaltning-og-utvikling/noark-standarden/noark-5/noark5-standarden

dokumentasjonselementet som mulig. Dette støtter også en grunntanke om at (forretnings)prosessen legges til grunn for klassifiseringen.

Forutsatt at samtykket er blitt tilført tilstrekkelige metadata, vil behandlingsansvarlig kunne gjøre endringer i prosessen uten å risikere at behandlingen av personopplysninger trues ved at relasjonen mellom samtykket, formålet, personopplysningene, prosessen og den registrerte brytes. En revisjon av livssyklusen for samtykkene vil kunne avdekke mangler i metadatatilgangen, og forhåpentligvis kunne bidra til at dette blir bragt i orden uten uheldige konsekvenser.

Valg av angrepsvinkel og nivåer for kontroll

Det er mange måter å tilnærme seg revisjon av samtykker knyttet til behandling av personopplysninger, og risikoinngangen er det som vanligvis rangerer høyt – i særdeleshet hvis det potensielt kan påvirke økonomiske eller omdømmemessige sider av virksomheten i negativ retning. Igjen er Cambridge Analytica-saken et godt eksempel på at begge disse sidene fort blir påvirket når omfattende behandling av personopplysninger uten gyldig samtykke er i søkelyset.

Effektiviseringseffekten er ikke like lett å få øye på; det ser man dog kanskje bedre når man vurderer det hele ut fra store volumer og med automatisering for øye. Her åpenbarer det seg store gevinstpotensialer når volumet blir stort; se for eksempel til Udbetaling Danmark, SU, Pension Danmark, de store bankene, Skat, Lånekassen og Skatteetaten i Norge m.fl., hvor automatisering og selvbetjening står for mye av produksjonen. I den grad deres forretningsprosesser hadde vært basert på samtykker alene, måtte operasjonaliseringen av samtykkenes livssyklus automatiseres tilsvarende.

Revisjon med tanke på forbedring er således også høyst relevant, og for øvrig helt i tråd med det grunnleggende prinsippet om «kontinuerlig forbedring» fra blant annet ISO 9001 og ISO 30302. Revisjon av livssyklusen for samtykker er også et delsvar på ISO 30301 punkt 9.2 *Internal system audit* hva gjelder compliance til personvernforordningens dokumentasjonskrav på området.

Et godt utgangspunkt, uavhengig av virksomhet og perspektiv, er å følge brukerreisene, altså hvordan den registrerte kan holde kontroll med bruken av sine personopplysninger gjennom en eller flere virksomheters digitale tjenester. Med denne tilnærmingen vil man se behandlingen mer «utenfra og inn», med individet i fokus.

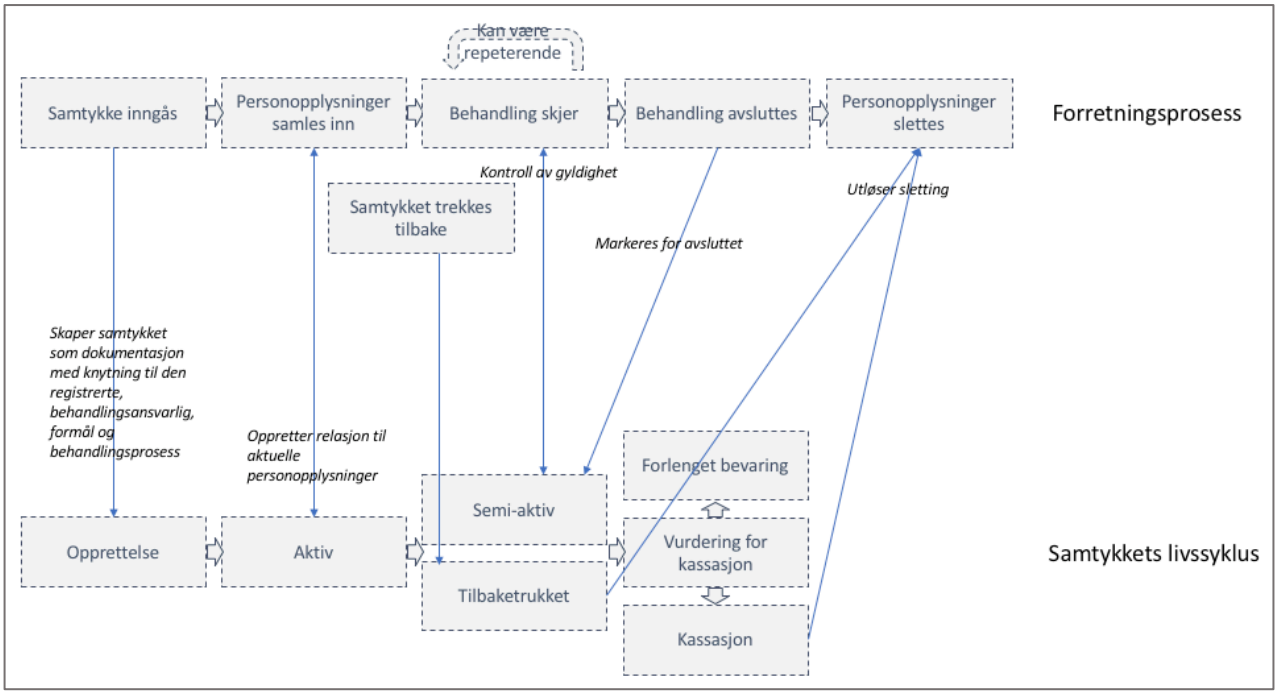
I tilfeller hvor man har flere behandlingsforløp, gjerne med flere ulike formål og/eller flere ulike aktører, vil denne tilnærmingen kunne gi et godt bilde av den totale påvirkningen på individet når det gjelder behandling av vedkommendes personopplysninger. Også i tilfeller hvor de registrerte etterspør informasjon, eller når det vurderes gjennomført en DPIA[28], vil denne tilnærmingen være relevant.

En annen tilnærming kan være å ta utgangspunkt i behandlingsprosessen/tjenesteprosessen slik den er beskrevet av virksomheten – den behandlingsansvarlige. Til sammenligning blir dette en

[28] Digital Privacy Impact Assessment (vurdering av personvernkonsekvenser), jf. personvernforordningens art. 35

tilnærming «innenfra og ut», som setter systemets, ansattes og virksomhetens aktiviteter i fokus. Tilnærmingen kan være relevant for eksempelvis gjennomføring av internkontroll knyttet til ulike tjenesteområder.

Denne siste tilnærmingen er benyttet for å modellere sammenhengen mellom forretningsprosessen og samtykkets livssyklus:



Figur 2 Sammenhengen mellom en forretningsprosess og samtykkets livssyklus

Figur 2 viser en modell av en generisk forretningsprosess øverst, med en tilhørende modell av livssyklus for et tilhørende samtykke under. Modellen er noe forenklet, eksempelvis ville man ideelt sett ta med et steg hvor en borgers død ville medføre at virksomhetens personvernombud / Data Protection Officer (DPO) ville ugyldiggjøre samtykket på vegner av den registrerte eller dens pårørende.

Typiske prosessmodellelementer som svømmebaner er ikke tatt inn i modellen for å unngå organisatoriske bindinger som i prinsippet ikke er relevant i denne sammenhengen.

I figuren har jeg valgt å ta utgangspunkt i den prosessen som omhandler opprettelsen og behandlingen av samtykker, og satt samtykket i sentrum for revisjon. Denne prosessen er sånn sett underordnet forretningsprosessen, men har i seg selv en viktig betydning, jf. de tidligere nevnte verdiperspektivene. Denne tilnærmingen er nyttig når kontrollen skal ned på detaljnivå, eksempelvis i eller som forberedelser til en rettslig gjennomgang.

Tilnærmingen har dog en iboende risiko ved at den ser på livssyklusen for samtykket separat fra den overordnede forretningsprosessen av personopplysningene – derfor må en slik revisjon skje i lys av forretningsprosessen hvor samtykket inngår, slik at helheten i behandlingen gjøres til gjenstand for en totalvurdering.

Typiske revisjonsaktiviteter fremgår av ISO 19011, punkt 6.1, og hovedaktivitetene er som følger: igangsettelse, forberedelse, gjennomføring, utarbeidelse og distribusjon av revisjonsrapporten, samt avslutning av revisjonen. I etterkant vil det også kunne være en gjennomføring av oppfølgende tiltak etter revisjonen.

Nivåbestemt revisjon

En revisjon av samtykkebehandlingen vil kunne foregå på ett eller flere ulike nivåer, og det følgende eksempelet viser en nivåmessig inndeling i fire nivåer:

Kontrollnivå 1 – grunnleggende policy for dokumentasjonsforvaltning
Er det, som en del av tjenesteleveransen, etablert behandling av samtykker på en systematisk og dokumentert måte som er i tråd med personvernforordningen?

Kontrollnivå 2 - styringsrammeverk
Er det, som en del av tjenesteleveransen, etablert strukturer og prosedyrer for å støtte behandlingen av samtykker og for å sikre at den overordnede strategien er forstått, implementert og følges opp?

Kontrollnivå 3 - forretningsprosessene
Er det gjennomført risikovurdering knyttet til den enkelte behandlingsprosess som helhet?

Kontrollnivå 4 – operasjonaliseringen av samtykkers livssyklus
Er alle stegene i livssyklusen for samtykker i den enkelte behandlingsprosess ivaretatt i tråd med kravene i personvernforordningen, og vurdert med tanke på operasjonell verdi og/eller bevisverdi?

En gjennomgående revisjon vil omfatte kunne omfatte nivåer, enten de er inndelt på denne eller annen måte, noe som vil innebære vesentlig flere krav enn det jeg går inn på i denne oppgaven. For å finne dekkende svar på min problemformulering er revisjon på kontrollnivå 4 som kreves for å sikre samtykkene som sådan, og som omtales herfra og ut.

Valg av teknikker for kontrollnivå 4

Som nevnt tidligere, er risikoperspektivet det mest nærliggende å ta til, og ISO 31010 tabell A.2 gir en oversikt over en rekke alternative teknikker for risikovurdering som kan gjennomføres for å få et overblikk over risikofaktorene i de ulike behandlingene. Oversikten er rangert etter hvor ressurskrevende teknikken er, hvor stor usikkerhet som tillegges utfallet og hvor kompleks teknikken regnes for å være.

I skrivende stund, mens mange virksomheter har det travelt nok med å komme á jour med de mest grunnleggende kravene i personvernforordningen, har jeg sett etter teknikker som både er lett tilgjengelige, som også kan bidra til at ansvaret for gjennomføring kan distribueres på en hensiktsmessig måte, ikke er for komplekse og som har lav terskel for gjennomføring.

I en virksomhet med mange enheter, avdelinger eller sektorer vil det typisk også finnes mange behandlingsprosesser for personopplysninger, flere systemløsninger og tilhørende systemansvarlige, hvor den daglige oppfølgingen naturlig vil plasseres.

Det er to av disse teknikkene som tilfredsstiller utvalgskriteriene; *sjekklister* og *strukturerte intervjuer og brainstorming*. Av disse to har jeg valgt sjekklister, da denne teknikken er kjent for de fleste, intuitiv, kan bære holdnings- og kunnskapsbærende elementer, og er mindre avhengig av at den gjennomføres synkront med annet personell.

Sjekklister er også en av anbefalingene til arbeidsdokumenter i ISO 19011, punkt. 6.3.4. Denne standarden inneholder for øvrig en rekke gode anbefalinger, og er svært relevant å kikke til under forberedelser og gjennomføring av revisjoner. Tilsvarende anbefaling om sjekkliste som metode finnes i ISO 30302, punkt 9.1.1.

I praksis ville det være naturlig å velge en samling av flere teknikker når man beveger seg ut i virksomheten for å gjennomføre en revisjon. Egen erfaring tilsier dog at sjekklister fungerer godt for den typen revisjon som det her er snakk om; de kommuniserer på en forståelig måte og etterlater seg strukturerte og dokumenterte resultater som igjen kan brukes for å utarbeide effektive rapporterer og initiere passende tiltak.

Sjekkliste for revisjon av livssyklus for samtykker

Den følgende sjekklisten er utarbeidet som et utgangspunkt for å kunne gjennomføre revisjoner av hvordan elektronisk avgitte samtykker konkret behandles i elektroniske systemløsninger, med formål om å kontrollere at personvernforordningen etterleves og for å sikre konsistens i dokumentasjonen av samtykker – også over tid.

ISO 15489 er lagt til grunn for krav til dokumentasjon, men her kunne kravene i ISO 16175 vært et naturlig alternativ. ISO 15489 ivaretar som nevnt langtidsperspektivet, noe ISO 16175 ikke gjør i tilstrekkelig grad.

Kontrollspørsmål og oppfølgende spørsmål er ment som hjelp til den eller de som skal gjennomføre revisjonen, og bidrar forhåpentligvis også noe til forståelsen av hvorfor spørsmålene må stilles.

Kolonnen *Samtykkets livssyklus* henviser til livssyklusen for samtykker i Figur 1 og 2, med korresponderende statuser for samtykket og den tilhørende brukeraktiviteten i de to påfølgende kolonnene *Status* og *Årsak*.

Innholdet i kolonnen *GDPR* henviser til relevant(e) artikler i den nye personvernforordningen, og de to siste kolonnene henviser til relevante klausuler som representerer records-relaterte prosesser i ISO 15489.

Samtykkets livssyklus	Status	Årsak	Kontrollspørsmål	Oppfølgende spørsmål	Jq / Nei / Kommentarer	GDPR ref.	ISO 15489 prosess	ISO 15489 ref.
Opprettelse	Gyldig	Samtykket er inngått	Er samtykket frivillig, informert, uttrykkelig og spesifikt?	Hvis nei – hvilke tiltak må settes i verk for å sikre dette?		Art. 4, 7	Creating records Capturing records	Clauses 9.2, 9.3
			Er samtykket gitt en unik identifikator?	Hvis nei – hvilke tiltak må settes i verk for å sikre dette?				Clause 9.3 a
			Er samtykket tilført metadata ved opprettelsen?	Hvis nei – hvilke tiltak må settes i verk for å sikre dette?				Clause 9.3 b
			Er det opprettet referanser mellom samtykket og behandlingsprosessen?	Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som tilfredsstiller kravene hvis behandlingsprosessenendres?				Clause 9.3 c
			Er samtykket en del av en samtykkeerklæring som inneholder andre elementer, f.eks. "terms and conditions"?	Hvis ja - fremgår det tydelig at samtykke etterspørres?		Art. 4		N/A
			Omhandler samtykket personopplysninger i særlige kategorier? Opplysninger om: • rasemessig eller etnisk opprinnelse • politisk oppfatning, religion, overbevisning • Fagforeningsmedlemskap • genetiske og biometriske oppl. med det formål å entydig identifisere en fysisk person • helseopplysninger • persons seksuelle forhold eller seksuelle orientering Straffedommer og lovovertredelser kan kun behandles under offentlig myndighets kontroll.	Hvis ja - fremgår dette eksplisitt?		Art. 9.1, 9.2,10, ft. 10, 32, 34, 35, 42 og 51.		Clause 9.3
Aktiv	Gyldig	Samtykket er inngått	Skjer det automatisk behandling eller profilering?	Er det tilrettelagt mekanismer for at brukeren kan motsette seg automatisert behandling eller profilering?		Art. 18, 21, 22		Clauses 9.3, 9.7

			Har samtykket referanser til de personopplysninger det gjelder?	Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som tilfredsstiller kravene hvis samtykket trekkes tilbake?		Art. 7.1, 7.3		Clause 9.3 c
			Har samtykket referanser til det formålet behandlingen gjelder?	Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som tilfredsstiller kravene hvis formålet endres?		Art. 5,6		Clause 9.3 c
			Er samtykket lagret på en måte som gjør det mulig å bevise at den registrerte har inngått samtykket i ettertid?	Hvis nei – hvilke tiltak må settes i verk for å sikre dette?		Art. 7		N/A
			Er det like lett for den registrerte å trekke tilbake sitt samtykke som å gi det?	Hvis nei – hvilke tiltak må settes i verk for å sikre dette?		Art. 7.3		N/A
			Inneholder samtykket metadata om hvor det er lagret?	Hvis nei - finnes det en egnet, tilgjengelig oversikt som gir tilstrekkelig svar innen rimelig tid?				Clause 9.6 a
			Følger samtykket, eller referanser til dette, som en del av behandlingen av personopplysningene?	Hvis nei - finnes det andre rutiner, prosedyrer eller funksjoner som knytter samtykket mot de aktuelle personopplysningene? - Samtykkets materielle innhold må være knyttet til de faktiske opplysningene det gjelder - Muliggjør dataportering		Art. 20	Storing records Use and reuse	Clauses 9.6,9.7
			Valideres samtykkets gyldighet før behandlingen av personopplysninger iverksettes?	Hvis nei - finnes det andre rutiner, prosedyrer eller funksjoner som sikrer at behandlingsgrunnlaget er gyldig?		Art. 5, 6, 7	Use and reuse	Clause 9.7
			Tillegges samtykket eller personopplysningene metadata om at den aktuelle behandlingen er gjennomført basert på et gyldig samtykke?	Hvis nei - finnes det andre rutiner, prosedyrer eller funksjoner som sikrer at samtykket var gyldig på behandlingstidspunktet og at dette kan dokumenteres i ettertid?		Art. 6, 7		
Semi-aktiv	Gyldig	Samtykket er inngått	Er samtykket tidsbegrenset, dvs. har den registrerte samtykket for behandling av sine personopplysninger i en avgrenset tidsperiode?	Hvis ja - finnes det rutiner, prosedyrer eller funksjoner som sikrer at samtykket merkes som ugyldig etter at perioden er over?			Storing records Use and reuse	Clauses 9.6, 9.7
				Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som sikrer at den registrerte bekjentgjøres med dette innen rimelig tid?				
			Tilføres samtykket nødvendige metadata hvis behandlingsprosessen endres etter opprettelse?	Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som sikrer samtykket blir			Use and reuse	Clause 9.7

				kontrollert riktig hvis behandlingsprosessen endres?				
			Utløser semi-aktivitet dataminimering?	Hvis ja – finnes det rutiner, prosedyrer eller funksjoner for å oppdatere relasjonen mellom samtykket og de aktuelle personopplysningene etter dataminimeringen?				
				Hvis nei - finnes det rutiner, prosedyrer eller funksjoner som sikrer at den registrerte bekjentgjøres med dette innen rimelig tid?			Use and reuse	Clause 9.7
Tilbaketrukket	Tilbake-trukket	Samtykket er trukket tilbake	Er samtykket markert ugyldig hvis det er trukket tilbake fra den registrerte?	Hvis ja - finnes det rutiner, prosedyrer eller funksjoner som sikrer at (mengden) personopplysninger minimeres, hvis relevant?		Art. 35		
			Utløser tilbaketrekking sletting av personopplysningene det gjelder?	Hvis nei – finnes det rutiner, prosedyrer eller funksjoner som sikrer sletting av de aktuelle personopplysningene?		Art. 17	Use and reuse	Clause 9.7
			Er samtykket markert ugyldig hvis det er trukket tilbake fra andre enn den registrerte?	Hvis ja - er det sikret spor etter hvem som har trukket det tilbake på vegner av den registrerte, og på hvilket grunnlag?		Art. 7	Storing records	Clause 9.6
Vurdering for kassasjon	Gyldig	Samtykket er inngått	Er verdien av samtykket vurdert dithen at det kan kasseres?	Hvis ja – finnes det rutiner, prosedyrer eller funksjoner som sikrer kassasjon av samtykket? Hvis nei – finnes det rutiner, prosedyrer eller funksjoner som ivaretar samtykket gjennom en forutbestemt, forlenget bevaringstid for samtykket?		Art. 7	Use and reuse Storing records Disposition	Clauses 9.6,9.7,9.9
	Tilbake-trukket	Samtykket er trukket tilbake	Er personopplysningene samtykket gjelder sperret for videre behandling, eller slettet, når samtykket er trukket tilbake?	Hvis nei – finnes det rutiner, prosedyrer eller funksjoner som besørger sperring for behandling og sletting?		Art. 6, 17	Disposition	Clause 9.9
Forlenget bevaring	Gyldig	Samtykket er inngått	Er det grunn til å bevare samtykket videre?	Hvis ja - finnes der rutiner, prosedyrer eller funksjoner som sikrer at samtykket beholder sine relasjoner til personopplysningene det gjelder, formålet, behandlingsprosessen og den registrerte?		Art. 7	Storing records	Clause 9.6
Kassasjon		N/A	Finnes det logg over kassasjonen som inngår i virksomhetens plan for dokumentasjonshåndtering?			Art. 21, 22	Disposition	Clause 9.9

Konklusjon og videre perspektivering

Formålet med denne oppgaven har vært å besvare følgende problemformuleringer:

> *Hvilke kontroller kan etableres for å sikre at behandlingsansvarlige virksomheter kan følge opp samtykkene på en forsvarlig måte i prosesser der hvor behandlingen av personopplysninger er basert på samtykke som eneste rettslige grunnlag?*
>
> *Kan man benytte elementer fra eksisterende standarder og rammeverk for å etablere et praktisk og anvendelig verktøy, en sjekkliste, for å sikre forsvarlig håndtering av samtykker hos en behandlingsansvarlig?*

I arbeidet med å besvare disse punktene har det vært viktig å kunne isolere livssyklusprinsippet for samtykkeobjektet fra den overordnede forretningsprosessen, og forsøke å hvordan samtykker, som bevismateriale, må behandles spesielt i lys av den nye personvernforordningen.

Kontrollmekanismer som fremgår av sjekklisten adresserer de konkrete kravene i personvernforordningen, og er knyttet til prosesser som er beskrevet i anerkjente standarder og rammeverk. Kontrollene gjøres ved å besvare spørsmålene i sjekklisten, med eventuelle henvisninger der hvor det ikke umiddelbart finnes svar i behandlingsprosessen.

Når det en gang i fremtiden kommer en rettsak, av en viss størrelsesorden, hvor ubestrideligheten omkring hvor vidt samtykket kan aksepteres som autentisk dokumentasjon, vil kanskje flere virksomheter få det travelt med å undersøke hvor vidt deres egne systemer, rutiner og prosedyrer faktisk understøtter kravene om dokumentasjon.

Inntil da kan denne sjekklisten benyttes som utgangspunkt for å revidere både egne og andres samtykkebaserte behandlinger av personopplysninger. Den er sammensatt av elementer fra anerkjente prinsipper og standarder, og vil kunne bidra til å sikre at samtykket i seg selv blir ivaretatt på en forsvarlig måte. Den kan implementeres som en del av et større revisjonsarbeid, som en del av en risiko- og sårbarhetsanalyse, eller simpelthen benyttes som frittstående verktøy.

Figurliste

Referanseliste

- Andresen, Herbjørn (2016), Ny versjon av standarden ISO 15489, Tidsskriftet Arkiv, vol. 7/2016 DOI: http://dx.doi.org/10.7577/ta.1799
- Article 29 Data Protection Working Party (2017), 17/EN WP259, Guidelines on Consent under Regulation 2016/679
- Bawden, David & Robinson, Lyn (2008) The dark side of information: overload, anxiety and other paradoxes and pathologies
- Bawden, David & Robinson, Lyn (2012) Introduction to information Science, kap. 12 Information management and policy, 251-285
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), Internal Control– Integrated Framework, COSO, CA.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), Internal Control– Integrated Framework, COSO, CA.
- Cook, T. (1997) What is past is prologue. A history of archival ideas since 1898, and the future paradigm shift. Archivaria 43 (https://archivaria.ca/index.php/archivaria/article/view/12175/13184)
- Cook, T. (2014). Proveniens i den digitale tida: Gammel bør eller framtidshåp for arkivarprofesjonen?. Tidsskriftet Arkiv, 2. https://doi.org/10.7577/ta.910
- Datatilsynet, Samtykke (2017), (https://www.datatilsynet.dk/media/6562/samtykke.pdf)
- IEEE Standards Department (2002), Draft standard for learning object metadata, 1484.12.1-2002 (https://biblio.educa.ch/sites/default/files/20130328/lom_1484_12_1_v1_final_draft_0.pdf)
- Hoke, Gordon E. J. (2011) Information management: Records life cycle: A Cradle-to-grave metaphor, Arma International, RIM Fundamentals, vol. September/October 2011
- Houten, Gerry van (2010), Drafting a Function-based File Classification Plan, ARMA International
- ISO (2015) Dansk Standard, DS/EN ISO 9001:2015 Kvalitetsledelsessystemer – Krav
- ISO (2010) Dansk Standard DS/ISO 16175-1:2010 Information og dokumentation – Principper og funktionelle krav til registreringer i elektroniske kontormiljøer – Del 1: Oversigt over og redegørelse for principper
- ISO (2012) Dansk Standard, DS/EN ISO 19011:2012 Auditering af ledelsessystemer – Vejledning
- ISO (2016) Standard Norge, NS-ISO 15489-1:2016 Informasjon og dokumentasjon – Dokumentasjonsforvaltning Del 1: Begreper og prinsipper
- ISO (2017) Dansk Standard DS/ISO 23081:2017-1 Information and documentation – Records management processes – Metadata for records – Part 1: Principles

- ISO (2013) Dansk Standard DS/ISO/IEC 27001:2013-1 Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Krav
- ISO (2011) Standard Norge, NS-ISO 30300:2011 Informasjon og dokumentasjon – Ledelsessystemer for dokumentasjon – Grunntrekk og terminologi
- ISO (2011) Standard Norge, NS-ISO 30301:2011 Informasjon og dokumentasjon - Ledelsessystemer for dokumentasjon – Krav
- ISO (2010) Dansk Standard DS/ISO 31010 Risikoledelse – Teknikker til risikovurdering
- Kahn, Randolph (2009) Information Nation - Seven Keys to Information Management Compliance, Wiley Publishing, kap 3. An overview of records management, 23-33
- Lykke, Marianne (2017), Enterprise search – informationssøgning og videndeling i virksomheder, Institut for Kommunikation, Aalborg Universitet, forelesning MIR november 2017
- Det kongelige Justis og Beredskapsdepartement (2018), Proposisjon 56 LS (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen (https://www.regjeringen.no/contentassets/1a36e88f124d4a1ea92a9c790be2d69a/no/pdfs/prp201720180056000dddpdfs.pdf)
- Pickett, K H Spencer (2011), The Essential Guide to Internal Auditing, Wiley
- Schartum, Dag Wiese & Sætre, Kjetil Wick (2016) Samtykke til å behandle personopplysninger i offentlig forvaltning, CompLex 2/2016, Senter for rettsinformatikk, Universitetet i Oslo
- The European Parliament and the Council of the European Union (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL)
- Torres, Tina (2006), Creating a Process-Focused Retention Schedule, The Information Management Journal, September/October 2006, s. 62-69
- Riksarkivet (2016) Noark 5 Standard for elektronisk arkiv v. 4.0 (https://www.arkivverket.no/forvaltning-og-utvikling/noark-standarden/noark-5/noark5-standarden)
- Tayfun, Angela C. & Gibson, Sherrill (1996) A model for life cycle records management, DOE/RW/00134--M96-013; CONF-9610182--1
- United Nations (2014), Department of Management, Archives and Records Management Section; Managing Records To Manage Information Risks (https://archives.un.org/sites/archives.un.org/files/uploads/Manage%20records%20to%20manage%20info%20risks%2Bgraphs_0.pdf)
- Weirsøe, Tine (2016) Livscyklus fra en records management vinkel, Aalborg Universitet, MIR, forelesning 3.11.2016