UiO : Det juridiske fakultet

Behandlingssikkerhet for personopplysninger etter GDPR

Kandidatnummer: 674
Leveringsfrist: 25.11.2018
Antall ord: 17617

Innholdsfortegnelse

1 Innledning

1.1 Tema

Oppgavens tema er behandlingssikkerhet for personopplysninger etter GDPR – EUs nye personvernforordning. Det blir gitt en fremstilling av kravene til behandlingssikkerhet for personopplysninger etter forordningen. Dette inkluderer hvordan risikovurderinger for behandlingssikkerhet skal utføres, og hvordan disse er veiledende for hvilke sikkerhetstiltak som bør tas i bruk i det enkelte tilfelle.

Som mennesker i det moderne samfunnet har vi en oppfatning av hva som er vår private sfære. Denne inkluderer som regel de personopplysningene vi gir fra oss. Behandlingssikkerhet er essensielt for å sikre at disse opplysningene beskyttes.

Rettslig grunnlag for behandlingssikkerheten i GDPR er artikkel 32 til 34. Disse, med utdypende avsnitt i fortalen, danner hovedrammen for min drøftelse.

Behandlingssikkerhet for personopplysninger er tolket inn i EMK artikkel 8 i saken I v. Finland[1]. Prinsippet er dermed inkludert i en av våre mest sentrale menneskerettigheter. Behandlingssikkerhet er også et aktuelt tema. I dagens samfunn står sikkerheten for personopplysninger overfor mange trusler, som kan få fatale følger. De siste årene har det inntruffet flere slike truende hendelser for personvernet. Wannacry var en slik trussel.[2]

Det denne oppgaven vil forsøke å besvare er hvordan EUs nye personvernforordning skal forhindre at slike brudd skjer, og hvordan de som behandler personopplysninger etter forordningen bør tilnærme seg forordningen for å oppnå etterlevelse.

1.2 Rettskildebildet og aktualitet

«EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR]»[3], heretter kalt GDPR eller personvernforordningen, danner rettslig utgangspunkt for problemstillingen i oppgaven. Forordningen ble tatt i bruk i EU den 25. mai 2018.[4] I Norge trådte forordningen i kraft 20. juli 2018 gjennom Lov om behandling av personopplysninger (personopplysningsloven) av 15.06.2018 nr. 38.[5]

[1] I v. Finland avsn. 47-48

[2] Hotvedt (2017)

[3] For 2016/679/EU

[4] For 2016/679/EU art. 99 nr. 2

[5] Personopplysningsloven §§ 1 og 32

GDPR er et nytt regelverk med stor aktualitet. Forordningen og endringene som følger med den har skapt mye medieomtale, og har medført endringer for hvordan personopplysninger skal behandles for alle forordningen omfatter.

1.2.1 Rettskildebildet og EU-rettslig metode

Rettskilder fra EU skal tolkes etter den metoden EU-domstolen anvender, også når de er inntatt i norsk lov.[6] Ved tolkning av GDPR skal en derfor anvende EU-rettslig metode. For å fastlegge innholdet i GDPR i denne oppgaven blir derfor denne metoden anvendt.

Etter Fredriksen og Mathisen innebærer denne metoden at rettsaktene tolkes med utgangspunkt i en «selvstendig og ensartet fortolkning av EU-rettslige bestemmelser – uavhengig av nasjonal begrepsbruk, nasjonal juridisk metode og nasjonal rettskultur i de enkelte medlemsstater».[7] På samme måte som i den alminnelige rettskildelæren her i Norge og i folkeretten, begynner en EU-rettslig tolkning, dersom det ikke er holdepunkter for noe annet, med en naturlig forståelse av ordlyden.[8]

EU-retten inneholder mange ulike språkversjoner av de samme rettsaktene. Alle disse språkversjonene er likeverdige, og dersom de ulike språkversjonene åpner for ulike tolkningsresultater av rettsakten, må de ulike språkversjonene sammenholdes for å finne en harmoniserende betydning.[9]

Forordningen er gjort til norsk lov gjennom personopplysningsloven. I denne loven er hele forordningen tatt inn på norsk. Denne oversettelsen er ikke en offisiell EU-versjon, og slike versjoner vil i følge Fredriksen og Mathisen neppe få rettskildemessig vekt når rettsakter fra EU skal tolkes.[10] Fordi denne oppgaven er vinklet etter hvordan forordningen skal forstås i Norge, forholder den seg til den versjonen som er gjort til norsk lov. Det er derfor den norske språkversjonen som anvendes.

Etter at ordlyden er fastlagt, skal det etter EU-rettslig metode foretas en formålsrettet og kontekstuell tolkning.[11] At tolkningen skal være formålsrettet innebærer at den aktuelle bestemmelsen tolkes «slik at formålet med dem fremmes i størst mulig utstrekning, eller i det minste

[6] Arnesen (2009) s. 53
[7] Fredriksen (2014) s. 218
[8] Fredriksen (2014) s. 219
[9] Fredriksen (2014) s. 219-220 og Stemsrud (2015) s. 107
[10] Fredriksen (2014) s. 249
[11] Fredriksen (2014) s. 221

slik at måloppnåelsen ikke hindres»[12]. At tolkningen skal være kontekstuell tilsier at «man trekker den sammenheng som en EU-rettslig tekst inngår i, inn i tolkningen av den»[13]. I denne fremstillingen forsøkes det å gjøre en formålsrettet og kontekstuell tolkning av forordningen, men der dette ikke har vært tilstrekkelig til å fastlegge innholdet, blir det sett hen til andre kilder.

EU-avgjørelser anses etter Fredriksen og Mathisen som «tungtveiende rettskilder som det kreves gode grunner for å fravike.»[14] Det er derfor blitt brukt avgjørelser fra EU-domstolen som får betydning for tolkning av forordningen flere steder i denne oppgaven.

Fortalen til en rettsakt kan få betydning for tolkning av rettsakten ved at den er med på å gi uttrykk for formålet og konteksten til rettsakten, fordi den inneholder en begrunnelse av den aktuelle bestemmelsen eller rettsakten. EU-domstolen anvender ofte fortalen som et støttemoment under tolkningen, men fortalen er ikke i seg selv bindende. [15]

Fortalen til forordningen er anvendt i denne oppgaven for å utdype og begrunne det som er inntatt i den aktuelle artikkelen.

Etterfølgende retningslinjer, fra etter at rettsakten er vedtatt, vil vanligvis ha en begrenset rettskildemessig vekt i EU-domstolen.[16] Enkelte slike dokumenter er likevel blitt gitt vekt i denne fremstillingen for å utdype tolkningen av forordningen. Slike retningslinjer er laget for at de som praktiserer forordningen i det virkelige liv skal ha noe å støtte seg på, og disse er derfor blitt ansett som nyttige illustrasjoner for hvordan personvernforordningen skal anvendes i det praktiske liv. Disse retningslinjene ble også gitt stor vekt i den norske kommentarutgaven til GDPR[17].

Article 29 Data Protection Working Party har kommet med slike retningslinjer og veiledende dokumentasjoner av betydning for behandlingssikkerhet i GDPR, som vil bli brukt i denne oppgaven. Artikkel 29 gruppen var et uavhengig EU organ som ga rådgivende retningslinjer innen personvern.[18] Artikkel 29 gruppen eksisterer imidlertid ikke lenger, og denne rollen er tatt over av European Data Protection Board fra samme tid som forordningen trådte i kraft i EU.[19]

[12] Fredriksen (2014) s. 231
[13] Fredriksen (2014) s. 222
[14] Fredriksen (2014) s. 238
[15] Fredriksen (2014) s. 228
[16] Fredriksen (2014) s. 230
[17] Skullerud (2018) s. 39
[18] WP29 (2017) s. 1
[19] The European Commission (2018)

ENISA – The European Union Agency for Network and Information Security har også kommet med veiledende retningslinjer og andre publikasjoner der kravene til behandlingssikkerhet i GDPR illustreres.[20] Disse publikasjonene har blitt brukt for å utdype kravene i forordningen og knytte dem til det praktiske liv.

Annen juridisk litteratur er brukt fordi det gir bakgrunnsinformasjon om rettstilstanden, og hvordan jurister med kompetanse på området tolker forordningens bestemmelser. Jeg har derfor brukt dette som støtte, selv om slik juridisk litteratur ikke normalt er en kilde EU-domstolen anvender.[21]

Den norske kommentarutgaven er en form for juridisk litteratur fra flinke personvernjurister som har tolket forordningen. Jeg har derfor funnet den nyttig for å få utfyllende informasjon om hvordan forordningen skal tolkes.

Convention 108 fra 1981 er en traktat om behandling av personopplysninger fra The Council of Europe. Denne er den eneste i sin art og det første internasjonale rettslige dokumentet som tok stilling til de problemstillingene som oppstår når personopplysninger skal behandles i data-systemer.[22]

Convention 108 er derfor brukt for å illustrere kravet om behandlingssikkerhet.

For å belyse problematikken med behandlingssikkerhet for personopplysninger har jeg også tatt med en avgjørelse fra EMD, som ikke har direkte rettskildemessig relevans for innholdet i GDPR, men som kan illustrere hvordan spørsmål rundt behandlingssikkerhet for personopplysninger stiller seg i det virkelige liv. Det er imidlertid blitt hevdet at EU-retten skal tolkes i lys av enkelte prinsipper, og at de grunnleggende rettighetene som fremgår av EMK er noen av disse.[23] Slik kan dommen fra EMD også få indirekte betydning for innholdet i behandlingssikkerhet etter forordningen.

Datatilsynet gir noe forvaltningspraksis, og dette er tatt med i oppgaven for å belyse hvordan krav tilsvarende de i forordningen er blitt håndhevet i tidligere praksis. Dette blir ansett som nyttig for å illustrere forordningens krav opp mot virkeligheten. Datatilsynet har også utarbeidet veiledere for etterlevelse av forordningen. De som skal anvende forordningen i Norge kan støtte seg på disse, og disse er derfor ansett som nyttige rettskilder.

[20] ENISA (2016), ENISA (2017)
[21] Stemsrud (2015) s. 105
[22] Bygrave (2014) s. 31-32
[23] Fredriksen (2018) s. 301

Videre har jeg anvendt en avgjørelse fra Personvernnemda for å underbygge drøftelsene mine. Denne saken illustrerer hvordan spørsmål rundt behandlingssikkerhet oppstår i praksis, men ettersom dette er forvaltningspraksis basert på den tidligere norske personopplysningsloven og -forskriften vil ikke dette ha noen direkte vekt for tolkning av forordningen.

For å illustrere en bransjenorm på informasjonssikkerhetsområdet anvendes også en standard i denne oppgaven.

1.3 Fremstillingen videre

Kapittel 2 inneholder en diskusjon av behandlingssikkerhet som grunnleggende personvernrettslig prinsipp i andre kilder enn GDPR. I kapittel 3 blir det gitt en presentasjon av innholdet i plikten til behandlingssikkerhet etter GDPR, samt betydningen av innebygget personvern etter artikkel 25 og vurdering av personvernkonsekvenser ved høy risiko etter artikkel 35.

Kapittel 4 inneholder en illustrasjon av hvordan plikten til behandlingssikkerhet etter GDPR artikkel 32 kan etterleves i praksis. Dette blir illustrert gjennom to ulike praktiske eksempler som innebærer ulik risiko for personopplysningssikkerheten. Videre følger plikten til å melde fra om brudd på personopplysningssikkerheten i kapittel 5.

Kapittel 6 inneholder avsluttende bemerkninger om plikten til behandlingssikkerhet etter GDPR.

2 Behandlingssikkerhet som grunnleggende prinsipp for behandling av personopplysninger

2.1 Hva menes med behandlingssikkerhet for personopplysninger?

Schartum definerer behandlingssikkerhet som «sikkerhet ved behandling av personopplysninger»[24]. I denne oppgaven menes det med dette begrepet hvilken risiko for brudd på personopplysningssikkerheten som behandlingen innebærer og hvilke slike risikoer det bør tas i bruk tiltak for å beskytte individet mot, samt hvilke tiltak som kan være egnet i det enkelte tilfellet.[25]

I GDPR er «Brudd på personopplysningssikkerheten» definert slik: «et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet»[26].

«Behandling» er tolket vidt i forordningen. Etter artikkel 4 nr. 2 omfatter dette: «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke.» Dette kan blant annet være «innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, … sletting eller tilintetgjøring».[27]

Personvernforordningen legger videre opp til en vid forståelse av begrepet «personopplysning». Personopplysning er i forordningen definert som: «enhver opplysning om en identifisert eller identifiserbar fysisk person ('den registrerte')», som videre defineres som «en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator.» [28]

Behandlingene av personopplysninger kan dermed være svært ulike med mange forskjellige formål, og en personopplysning kan være det aller meste av informasjon som kan knyttes til en fysisk person.

Rettspraksis etter direktivet tolket begrepet «personopplysning» vidt. I Breyer-saken ble en dynamisk IP-adresse ansett som en personopplysning, og i Nowak-saken ble en anonym eksamensbesvarelse regnet som en personopplysning.[29]

[24] Schartum (2018) s. 166

[25] Se også For 2016/679 EU art. 32

[26] For 2016/679/EU art. 4 nr. 12

[27] For 2016/679/EU art 4 nr. 2

[28] For 2016/679/EU art 4 nr. 1

[29] C-582/14 Breyer og C-434-16 Nowak

2.2 Behandlingssikkerhet i personverndirektivet

I GDPRs forgjenger, direktiv 95/46/EF, var ikke prinsippet om behandlingssikkerhet eksplisitt nevnt som et eget prinsipp for behandling av personopplysninger.[30]

Behandlingssikkerhet var imidlertid inntatt som et generelt krav til behandling av personopplysninger. Av artikkel 17 fremgikk det: «Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing».[31]

Videre fremgikk det av artikkelen: «Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected».[32]

Ved søk etter avgjørelser fra EU-domstolen om denne artikkelen, var det ingen saker der behandlingssikkerhet ble drøftet inngående. Sakene der denne artikkelen ble nevnt er derfor vurdert å ha liten interesse for behandlingssikkerheten i GDPR, og de blir ikke presentert ytterligere.

Mye av denne bestemmelsen er blitt videreført i GDPR artikkel 32.

2.3 Behandlingssikkerhet som grunnleggende prinsipp utenfor EU-regulering

Behandlingssikkerhet ble ansett som et grunnleggende prinsipp for personvernet lenge før GDPR trådte i kraft. Dette prinsippet fremgår blant annet av Convention 108 fra 1981 artikkel 7. I konvensjonens artikkel 7 fremgår det: «Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."[33]

Prinsippet om behandlingssikkerhet er også blitt innfortolket i EMK artikkel 8 av EMD. For betydningen av behandlingssikkerhet etter denne artikkelen er saken I v. Finland fra den

[30] Dir 95/46/EC art 6 og Skullerud (2018) s. 78

[31] Dir 95/46/EC art. 17 nr. 1

[32] Dir 95/46/EC art. 17 nr. 1

[33] Bygrave (2014) s. 164 og Convention 108 art. 7

europeiske menneskerettighetsdomstolen illustrerende. Her ble viktigheten av å ha på plass tilstrekkelige organisatoriske og tekniske tiltak for behandlingssikkerhet fremmet. Finland ble her dømt for brudd på EMK, for ikke å ha gitt en kvinnes helseopplysninger god nok sikkerhet.[34]

Saken gjaldt en HIV-positiv helsearbeider som opplevde at hennes kollegaer fikk uberettiget innsyn i hennes egne helseopplysninger om HIV-diagnosen. Kollegaene fikk her tilgang til opplysningene fordi de ikke var sikret mot at ansatte på sykehuset uten legitimt behov søkte dem opp. I tillegg var det ingen tilstrekkelig oversikt over hvem som hadde vært inne og sett på opplysningene, men kollegaenes oppførsel antydet at de hadde snoket i Is helseopplysninger. [35]

Domstolen fastholdt her at det forelå en plikt for Finland som stat til å fremme behandlingssikkerhet. EMD fremhever: «The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in article 8 of the Convention». Domstolen innfortolket dermed en positiv forpliktelse for staten til å ha slike tiltak at personopplysningene ble beskyttet. [36]

Kvinnen hadde etter lovverket mulighet til å få kompensasjon for skaden, men domstolen hevdet at dette ikke var tilfredsstillende. Domstolen uttaler: «What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place».[37]

2.4 Andre personvernprinsipper som får betydning for prinsippet om behandlingssikkerhet

2.4.1 Ansvarlighetsprinsippet

Prinsippet om ansvarlighet (ansvarlighetsprinsippet) fremgår av GDPR artikkel 5 nr. 2, og er formulert slik: «Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes (”ansvar“)».[38]

Artikkel 5 nr. 1 inneholder de grunnleggende personvernprinsippene som er nedfelt i forordningen, deriblant prinsippet om behandlingssikkerhet.[39]

Ved at ansvarlighetsprinsippet er tatt inn i forordningen på denne måten, er det den behandlingsansvarlige som sitter med plikten til å implementere tilstrekkelig behandlingssikkerhet.

[34] I. v. Finland

[35] I. v. Finland avsn. 6 til 9 og 43

[36] I. v. Finland avsn. 38

[37] I. v. Finland avsn. 47

[38] For 2016/679/EU art 5 nr. 2

[39] For 2016/679/EU art 5 nr.. 1 f)

Denne må sette seg inn i hva prinsippet innebærer og hva som skal til for å nå dette i bedriften. Den behandlingsansvarlige sitter dermed på et ansvar som ikke kan utkontrakteres eller skyves ned i systemet. Det at den behandlingsansvarlige selv må sette seg inn i dette, bidrar til en styrking av behandlingssikkerhet som prinsipp.

Det er store bøter for overtredelser av «de grunnleggende prinsippene for behandling i henhold til artikkel 5»,[40] opp mot «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».[41] Det at det kan ilegges høye bøter kan virke avskrekkende på behandlingsansvarlig, og det er derfor naturlig å anta at dette vil bidra til at disse overholder sine plikter etter artikkel 5.

2.4.2 Prinsippet om dataminimering

Prinsippet om dataminimering kan også få betydning for behandlingssikkerheten. Dette fremgår av GDPR artikkel 5 nr. 1 c), og innebærer at «personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».[42]

Peter Carey hevder i sin bok at å ikke behandle noen opplysninger, er den eneste måten å oppnå høyeste grad av sikkerhet. Videre hevder han derfor at, på grunn av dette, så er prinsippet om dataminimering spesielt viktig. Dersom det anvendes flere personopplysninger enn nødvendig, vil dette medføre en økt risiko for personopplysningene.[43]

Dette kan tas til inntekt for at det alltid vil være en risiko ved behandling av personopplysninger, uansett hvor gode sikkerhetstiltak som tas i bruk, eller hvor lite sensitive opplysningene er. En behandlingsansvarlig eller databehandler kan ikke helgardere seg mot dette, men må akseptere risikoen behandlingen bringer med seg.

Det er imidlertid viktig å påpeke at alle opplysninger som er nødvendige for å nå formålet med behandlingen skal innhentes for å få et korrekt beslutningsgrunnlag. Prinsippet om dataminimering er ikke til hinder for dette. Dette er viktig for at behandlingen skal være i samsvar med prinsippet om riktighet, som er nedfelt i GDPR artikkel 5 nr. 1 d), der det fremgår at «Personopplysninger skal være korrekte og om nødvendig oppdaterte».[44]

[40] For 2016/679/EU art. 83 nr. 5 a)
[41] For 2016/679/EU art. 83 nr 5
[42] For 2016/679/EU art. 5 nr. 1 c)
[43] Carey (2018) s. 88-90
[44] For 2016/679/EU art. 5 nr. 1 d)

3 Kravet til behandlingssikkerhet for personopplysninger i GDPR

3.1 Forankring, anvendelse og pliktsubjekter

3.1.1 Forankring

I forordningens artikkel 5 nr. 1 bokstav f) er behandlingssikkerhet nevnt som et grunnleggende prinsipp. Her settes det et krav om at personopplysningene «behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene». Etter artikkelleddet skal dette innebære «vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade.» For å oppnå dette skal det tas i bruk «egnede tekniske eller organisatoriske tiltak». Forordningen omtaler dette som prinsippet om «'integritet og konfidensialitet'.»[45]

Kravet til behandlingssikkerhet innebærer etter dette at det ved behandling av personopplysninger skal legges til rette for sikkerhetstiltak som sikrer et ønsket sikkerhetsnivå.[46]

Det at behandlingssikkerhet er tatt inn som et overordnet prinsipp, gir behandlingssikkerhet styrke som et av de sentrale prinsippene som forordningen ønsker å fremme. ENISA fremhever dette slik: «As a first point, it is important to note that security (in the sense of integrity and confidentiality) is established as one of the principles relating to personal data processing (Article 5 GDPR). This puts security at the core of data protection together with the rest of data protection principles, i.e. lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation».[47]

I den norske kommentarutgaven til GDPR er en mulig beskrivelse av fremhevelsen av prinsippet «et utslag av at den teknologiske utviklingen har medført betydelig økt risiko for brudd på konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger».[48] Videre fremheves det at personvernforordningen «forutsetter at teknologiens muligheter til å ivareta personvernet skal utnyttes.»[49] Dette belyser to sider av forholdet mellom teknologi og personvern.[50]

I fortalepunkt 39 utdypes prinsippet om behandlingssikkerhet, hvor det fremgår: «Personopplysninger bør behandles på en måte som gir tilstrekkelig sikkerhet og konfidensialitet, herunder

[45] For 2016/679/EU art 5 nr. 1 f)
[46] For 2016/679/EU art 5 nr.1 f)
[47] ENISA (2016) s. 12
[48] Skullerud (2018) s. 78.
[49] Skullerud (2018) s. 79
[50] Skullerud (2018) s. 200-201.

for å hindre ulovlig tilgang til eller bruk av personopplysninger og utstyret som brukes i forbindelse med behandlingen.»[51]

3.1.2 Forordningens formål og mål

Forordningens artikkel 1 angir dens formål og mål. Her fremgår det at «Denne forordning fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger.» Videre skal forordningen sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.» Til sist gjøres det klart at «Fri utveksling av personopplysninger i Unionen skal verken begrenses eller forbys av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.»[52]

I samsvar med den kontekstuelle- og formålsrettede tolkningen av EU-rett som beskrevet i kapittel 1.2.1, kan dette få betydning for tolkningen av resten av forordningen. Dette kommer jeg tilbake til i kapittel 3.2.

3.1.3 Forordningens saklige anvendelsesområde

Det saklige anvendelsesområdet til forordningen er definert i artikkel 2 nr. 1. Etter denne artikkelen omfatter forordningen behandling av personopplysninger dersom behandlingen er «helt eller delvis automatisert», og behandling som ikke er automatisert dersom denne behandlingen «inngår i eller skal inngå i et register».[53]

Hva som menes med «delvis automatisert» blir utdypet i kommentarutgaven til GDPR. Her nevnes at dersom flere behandlingsaktiviteter «skjer for samme formål, og derved utgjør én behandling,» så vil behandlingen være delvis automatisert dersom en behandlingsaktivitet er automatisert og én er manuell. Da får forordningen anvendelse på begge disse behandlingsaktivitetene.[54]

Det meste av behandling av personopplysninger som på grunn av den tekniske utviklingen er blitt automatisert, enten helt eller delvis, vil derfor være omfattet av forordningen.[55] Det samme gjelder annen behandling av personopplysninger som er omfattet av en form for register.[56] Etter

[51] For 2016/679/EU fortalepunkt 39
[52] For 2016/679/EU art. 1 nr. 1 til 3
[53] For 2016/679/EU art 2 nr. 1
[54] Skullerud (2018) s. 45
[55] For 2016/679/EU art 2 nr. 1
[56] For 2016/679/EU art 2 nr. 1

dette er det nærliggende at det meste av behandling av personopplysninger slik det utføres i dag vil omfattes av forordningen.

Artikkel 2 nr. 2 inneholder et par unntak fra dette utgangspunktet, blant annet dersom behandlingen gjøres «i forbindelse med utøvelse av en aktivitet som ikke omfattes av unionsretten»[57]. Denne bestemmelsen har ikke noen parallell i den norske personopplysningsloven, slik at den norske personopplysningsloven gir forordningen virkning også utenfor EØS-avtalens virkningsområde.[58]

Forordningen får videre ikke anvendelse dersom behandlingen gjøres «av en fysisk person som ledd i rent personlige eller familiemessige aktiviteter»[59]. Dette utdypes i fortalen: «Personlige eller familiemessige aktiviteter kan omfatte korrespondanse og føring av adresselister eller aktiviteter på sosiale nettverk samt aktiviteter på internett i forbindelse med slike aktiviteter.»[60] Etter den norske kommentarutgaven er det ikke klart hvor langt en videre kan strekke unntaket. [61]

Unntaket i GDPR artikkel 2 nr. 2 kan dermed tas til inntekt for at dersom Peder lager en perm med navn, adresse og telefonnummer til familiemedlemmene sine, som han skal bruke til å sende dem postkort fra ferier, er denne behandlingen dermed ikke omfattet av forordningen. Det samme må gjelde dersom han lager en gruppe på Facebook med kontaktinformasjon til vennene sine i forbindelse med en hyttetur.

Forordningen inneholder også andre unntak i artikkel 2, blant annet ved gjennomføring av strafferettspleie og straffeforfølgning, som er regulert sammenliknbart i personopplysningsloven, der saksgang i sammenheng med rettspleielovene er unntatt.[62] Disse unntakene er ikke av særskilt interesse for reguleringen av behandlingssikkerhet i GDPR, og blir derfor ikke problematisert videre her.

3.1.4 Forordningens geografiske virkeområde

Forordningens geografiske virkeområde er regulert i artikkel 3. Forordningen har et svært bredt virkeområde.

[57] For 2016/679/EU Art. 2 nr. 2 a)
[58] Personopplysningsloven § 2
[59] For 2016/679/EU art. 2 nr 2. c)
[60] For 2016/679/EU fortalepunkt 18
[61] Skullerud (2018) s. 46
[62] For 2016/679/EU art. 2 nr. 2 d) og personopplysningsloven § 2 (2) b)

For det første får forordningen «anvendelse på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Unionen, uavhengig av om behandlingen finner sted i Unionen eller ikke».[63]

I de offisielle språkversjonene er det et krav om etablering; «establishment», som brukes i den engelske versjonen. Etter en sammenstilling av ulike språkversjoner konkluder den norske kommentarutgaven at det springende punktet er hvorvidt «den behandlingsansvarlige eller databehandleren er eller befinner seg i "Unionen"». Dette skal videre forstås i samsvar med etableringskriteriet slik det kommer frem i de offisielle språkversjonene av GDPR.[64]

I den engelske versjonen er dette formulert som «in the context of the activities of an establishment of a controller or a processor in the Union»[65].

For å fortolke denne bestemmelsen i tråd med EU-rettslige tolkningsprinsipper skal dermed etableringskriteriet tolkes likt i den norske versjonen som i de offisielle språkversjonene, i tråd med EU-rettslig tolkning.

Vilkåret om etablering er en videreføring fra personverndirektivets artikkel 4, og rettspraksis fra denne får dermed betydning.[66]

Google-Spain- saken er relevant i denne sammenheng. Denne saken gjaldt en spansk statsborger, Mr. Costeja González. Navnet hans ble koblet til et tvangssalg på grunn av trygdegjeld som fant sted for mer enn 12 år tilbake, ved søk i Googles søkefunksjon. Gjelden var tilbakebetalt og han mente at dette ikke lenger var relevant for han som person. Han ønsket derfor dette slettet, eller linken mellom han og denne saken i søkeresultatet endret. [67]

Google hadde en egen spansk side, som ble styrt gjennom Google Inc., som befinner seg i USA.[68]

Domstolen fremholdt at behandlingen ble «carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary

[63] For 2016/679/EU art. 3 nr. 1
[64] Skullerud (2018) s. 49-50
[65] For 2016/679/EU art. 3 nr. 1
[66] Skullerud (2018) s. 49-50
[67] C-131/12 Google avsnitt 14-16
[68] C-131/12 Google avsnitt 43

which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.»[69] Etter dette vil forordningen dermed også få anvendelse i slike tilfeller.

Nytt med forordningen er imidlertid at også databehandlers plassering får betydning, da det til sammenlikning kun gjaldt behandlingsansvarlige, eller «the controller» i det tidligere direktivet.[70]

Etter artikkel 3 nr. 2 kan forordningen også få anvendelse «på behandling av personopplysninger om registrerte som befinner seg i Unionen, og som utføres av en behandlingsansvarlig eller databehandler som ikke er etablert i Unionen»[71].

Dette gjelder kun hvis «behandlingen er knyttet til»[72] enten «tilbud av varer eller tjenester til slike registrerte i Unionen, uavhengig av om det kreves betaling fra den registrerte eller ikke»[73] eller «monitorering av deres atferd, i den grad deres atferd finner sted i Unionen.»[74]

Dermed, hvis det foregår en behandling av personopplysninger om en person som oppholder seg i EU, så kan GDPR få anvendelse på dette selv om den behandlingsansvarlige eller databehandleren ikke befinner seg i EU, dersom denne behandlingsansvarlige tilbyr varer eller tjenester til personer som den registrerte i EU, eller dersom databehandler eller behandlingsansvarlig monitorerer atferden til den registrerte, hvis denne atferden foregår i EU. [75]

Ved vurdering av hva som anses som monitorering «bør det bringes på det rene om det skjer sporing av fysiske personer på internett, herunder en mulig påfølgende bruk av teknikker for behandling av personopplysninger som innebærer profilering av en fysisk person, særlig med det formål å treffe avgjørelser om vedkommende eller analysere eller forutsi vedkommendes personlige preferanser, atferd eller holdninger.»[76]

[69] C-131/12 Google avsnitt 60
[70] Dir 95/46/EC art. 4 og For 2016/679/EU art. 3
[71] For 2016/679/EU art. 3 nr. 2
[72] For 2016/679/EU art. 3 nr. 2
[73] For 2016/679/EU art. 3 nr 2 a)
[74] For 2016/679/EU art. 3 nr. 2 b)
[75] For 2016/679/EU art. 3 nr. 2
[76] For 2016/679/EU fortalepunkt 24

Til slutt kan forordningen også få «anvendelse på behandling av personopplysninger som utføres av en behandlingsansvarlig som ikke er etablert i Unionen, men på et sted der en medlemsstats nasjonale rett får anvendelse i henhold til folkeretten.»[77]

Dette innebærer i følge Voigt at forordningen «applies to data processing within diplomatic or consular representations of a Member state».[78]

Forordningen har dermed et vidt virkeområde, og kan få anvendelse også der behandlingen av personopplysninger skjer utenfor EU, eller der den behandlingsansvarlige ikke befinner seg innenfor EU.[79]

Angivelsen av virkeområdet for personopplysningsloven og forordningen i den norske personopplysningsloven er en parallell av forordningens artikkel 3, bortsett fra at etableringskravet og kravet til plassering av den registrerte knytter seg til Norge, mens behandlingskravet knytter seg til EØS-området. [80] Dette gir forordningen i grove trekk det samme anvendelsesområdet som etter forordningen selv. Dette blir derfor ikke utdypet videre her.

3.1.5 Pliktsubjekter

Det er den behandlingsansvarlige og databehandleren som har plikter etter GDPR artikkel 32, 33 og 34.

Etter forordningen er behandlingsansvarlig definert som «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ», «som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes» i artikkel 4 nr. 7.[81] En databehandler er videre definert som «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige».[82]

Det at databehandler direkte har egne plikter var ikke tilsvarende regulert i det tidligere personverndirektivet. I direktivet var det regulert at databehandlers plikter skulle fastsettes i en

[77] For 2016/679/EU art 3 nr. 3
[78] Voigt (2017) s. 22
[79] For 2016/679/EU art. 3
[80] Personopplysningsloven § 2 og For 2016/679/EU art. 4
[81] For 2016/679/EU art. 4 nr. 7
[82] For 2016/679/EU art. 4 nr. 8

databehandleravtale, men denne hadde ikke direkte plikter knyttet til behandlingssikkerhet i direktivet. Databehandler kan nå også bli sanksjonert etter artikkel 83.[83]

Der det brukes databehandler, vil denne ofte være den som er nærmest behandlingen, da det er denne som behandler opplysningene. At plikter er blitt lagt på både behandlingsansvarlig og databehandler direkte tilsier derfor en styrking av kravet til behandlingssikkerhet etter GDPR artikkel 32.

Artikkel 24 angir den behandlingsansvarliges plikter. Her fremgår det at denne skal: «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.» Videre fremgår det av artikkel 24 nr. 2 at «Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.»[84]

3.2 Innholdet i plikten til behandlingssikkerhet etter GDPR artikkel 32

3.2.1 Generelt

Hovedkravene til behandlingssikkerhet i personvernforordningen er inntatt i artikkel 32. Denne artikkelen gir holdepunkter for vurdering av kravene til behandlingssikkerhet, i det den presenterer hvilke hensyn som skal ivaretas gjennom kravet til behandlingssikkerhet, og hvilke tiltak som må vurderes for å oppnå et tilfredsstillende nivå.

I det følgende vil det gis en oversikt over innholdet i plikten til behandlingssikkerhet i artikkelen.

3.2.2 Vurderingstema

Utgangspunktet for vurderingstemaet er at både behandlingsansvarlig og databehandler plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen».[85]

Etter dette danner risikoen utgangspunktet for vurderingen, og også rammen for hvilke tiltak den behandlingsansvarlige og databehandleren er pliktige å innføre for å oppnå et tilstrekkelig sikkerhetsnivå. Disse tiltakene skal både gjelde det tekniske i systemer, i tillegg til det

[83] Carey (2018) s. 178, Dir 95/46/EC art 17 nr. 3 og For 2016/679 EU art. 83

[84] For 2016/679/EU art. 24 nr. 1 og 2

[85] For 2016/679/EU art 32 nr. 1

organisatoriske i organisasjonen. Gjennom disse tekniske og organisatoriske kravene gir forordningen holdepunkter for hvordan databehandler og behandlingsansvarlig skal utføre behandlingen av personopplysninger, slik at de på en tilfredsstillende måte kan møte de aktuelle risikoene på en passende måte.[86]

3.2.3 Vurdering av risiko

Artikkel 32 nr. 1 gir ikke konkrete holdepunkter for risikovurderingen, men gir noe veiledning. Risikoen kan være av «varierende sannsynlighets-og alvorlighetsgrad», og det gjelder risikoen for «fysiske personers rettigheter og friheter». Etter sin ordlyd legger artikkelen opp til at det skal anvendes et vidt risikobegrep. Alle risikoer for «fysiske personers friheter og rettigheter» skal etter ordlyden inkluderes.[87]

Formålet i artikkel 1 nr. 2 om at forordningen skal sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger»[88], kan tas til inntekt for at personopplysninger skal gis særskilt vern, og at denne risikoen bør prioriteres. Samtidig trekker dette formålet i retning av at risikobegrepet bør tolkes vidt, og at mange ulike risikoer skal beskyttes av artikkel 32.

Schartum fremhever at risikoen nevnt i artikkel 32 gir veiledning når den behandlingsansvarlige skal finne ut av hvor strenge tiltak som bør benyttes. Et høyt risikonivå krever strengere tiltak enn det et middels eller lavt nivå vil gjøre. For å vurdere risikoen nevnt i artikkel 32, skal rettigheter utover «personvern i snever forstand» vektlegges når risiko skal vurderes. For eksempel hevder Schartum at når det gjelder «rettslige beslutningssystemer i offentlig forvaltning vil særlig hensynet til rettssikkerhet måtte tillegges stor vekt, i tillegg til det klassiske personvernet».[89]

Risikoen gjelder videre «risikoer av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter», som kan føre med seg «fysisk, materiell eller ikke- materiell skade». Videre lister fortalepunktet opp 40 momenter som skal inkluderes når denne vurderingen skal tas.[90]

[86] For 2016/679/EU art 32 nr. 1

[87] For 2016/679/EU art. 32 nr. 1

[88] For 2016/679/EU art. 1 nr. 2

[89] Schartum (2018) s. 165

[90] For 2016/679/EU Fortalepunkt 75

Det vil gi et oppramsende preg å inkludere alle disse her. Noen av momentene er hvor sårbar den enkelte personen er, eller om behandlingen skjer i stort omfang, enten det gjelder antallet personopplysninger eller det er mange registrerte som vil påvirkes.[91]

Andre momenter som skal tas med i vurderingen er hvorvidt behandlingen kan medføre «forskjellsbehandling, identitetstyveri eller -bedrageri». Hvorvidt behandlingen kan medføre «økonomisk tap, skade på omdømme, tap av konfidensialitet for taushetsbelagte personopplysninger,» eller «uautorisert oppheving av pseudonymisering eller andre betydelige økonomiske eller sosiale ulemper», skal også tas med i vurderingen.[92]

Etter dette må det anvendes et vidt risikobegrep for vurdering av risiko etter artikkel 32. Risikoene kan være svært ulike.

Viktigheten av å gjennomføre en risikovurdering kan illustreres gjennom Helse Sør-Øst saken. Høsten 2017 fikk ni ulike helseforetak i Helse Sør-Øst pålagt et overtredelsesgebyr på 800 000 hver, for blant annet å ikke ha utført nødvendige risikovurderinger. [93]

I denne saken fremgår det av vedtaket gitt til Oslo universitetssykehus HF at det ikke var mulig å bekrefte eller avkrefte at personopplysningene hadde havnet på avveie, fordi den behandlingsansvarlige ikke hadde mulighet til å se hva som var blitt gjort i systemet, og det var heller ikke mulig å finne ut av om leverandørens tilgang til personopplysninger hadde vært berettiget eller ikke.[94] Noe av kjernen i saken var at det ble valgt en underleverandør i Bulgaria, og at det for dette, ikke ble utført slike risiko-og sårbarhetsanalyser som var nødvendige etter regelverket. [95]

3.2.4 Særlige holdepunkter for vurdering av egnet sikkerhetsnivå

GDPR artikkel 32 nr. 2 fremhever momenter som er viktige for vurderingen av hva som er et passende sikkerhetsnivå. Her 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.»[96]

[91] For 2016/679/EU Fortalepunkt 75
[92] For 2016/679/EU Fortalepunkt 75
[93] Datatilsynet (2017b)
[94] Datatilsynet (2017a) s. 12.
[95] Datatilsynet (2017a) s. 3
[96] For 2016/679/EU art. 32 nr. 2.

Av artikkel 32 nr. 2 kan det dermed utledes hvilke typer risiko som skal prioriteres. Det skal gjøres en vurdering av både de risikoene som er ulovlige, som da vil medføre et regelbrudd, og de mer tilfeldige hendelsene. Schartum fremhever at dette kan være tilfeldige hendelser, «først og fremst sikkerhetsspørsmål som er knyttet til ikke-villede hendelser og konsekvenser».[97]

Slike utilsiktede hendelser kan for eksempel være feil i systemene som medfører at personopplysninger slettes, eller feil i programmeringen av adgangskontroll slik at uvedkommende tilfeldig får adgang til opplysninger.

For ulovlige hendelser fremhever Schartum at dette først og fremst er «villede hendelser og konsekvenser».[98] For disse hendelsene vil den personen som står bak i første rekke ha et ønske om å oppnå denne risikoen. Derfor kan det være nærliggende å si at disse hendelsene og konsekvensene sannsynligvis ofte kan medføre større skade.

Samtidig taler mye for at det gjennom uaktsomhet ved bruk at systemer med systemfeil, lett tenkes at det kan oppstå ulovlige følger uten at personen som står bak dette har ønsket denne følgen.

3.2.5 Vurdering av hva som er «egnet»

For vurderingen av «risikoene av varierende sannsynlighets-og alvorlighetsgrad»[99] i artikkel 32 nr. 1, gir forordningens fortalepunkt nr. 76 veiledning.

Når risikoenes grad av sannsynlighet og alvorlighet skal vurderes, er etter dette punktet «behandlingenes art, omfang, formål, og sammenheng de utføres i», momenter som skal tas hensyn til. For å komme frem til om den aktuelle behandlingen involverer en risiko, og om denne eventuelt er høy, bør det legges til grunn en objektiv vurdering.[100]

3.2.5.1 Den tekniske utviklingen

Ved at vurderingen av hva som er egnet skal inkludere «den tekniske utviklingen», legger artikkelen opp til en dynamisk utvikling av kravet til behandlingssikkerhet. De passende tiltakene skal følge den tekniske utviklingen, slik at hva som anses som egnet, vil være under kontinuerlig utvikling.[101]

[97] Schartum (2018) s. 168
[98] Schartum (2018) s. 168-169
[99] For 2016/679/EU art 32 nr. 1.
[100] For 2016/679/EU Fortalepunkt 76
[101] For 2016/679/EU art 32 nr. 1

3.2.5.2 Gjennomføringskostnadene og behandlingens art

For tolkning av "gjennomføringskostnadene og behandlingens art" eller, i den engelske versjonen "the state of the art, the costs of implementation" uttaler ENISA: «It is important to note that the reference to the "state of the art and cost of implementation" should not be interpreted as an excuse not to act, but rather as a call to all the stakeholders to simplify and reduce the costs, in order to spread the adoption of security measures. In that sense approaches towards simplification of the notion of risk and adoption of appropriate measures are key to the proper implementation of this article.»[102]

Videre fremhever Schartum, for betydningen av at «behandlingens art» skal tas med i vurderingen, at dersom «behandlingens art» er en myndighetsutøvelse, tilsier dette «strengere tiltak enn om det f.eks kun gjelder informasjon og formidling av enkle tjenester».[103]

Det kan riktignok også tenkes at det kan være mye som ikke er en myndighetsutøvelse, men som likevel vil kunne få store konsekvenser for individet, og at det derfor kreves strenge tiltak for å få bukt med dette.

Hvilken betydning opplysningenes sensitivitet har, fremheves i den norske kommentarutgaven til GDPR. Her fremgår det at: «For eksempel må det etableres sterkere sikkerhetstiltak ved behandling av helseopplysninger i en pasientjournal enn ved behandling av kontaktopplysninger i kunderegisteret til et bilverksted.»[104]

3.2.5.3 Behandlingens omfang

Som nevnt innledningsvis vil behandling av et stort omfang personopplysninger medføre større risiko enn dersom få opplysninger behandles.

I den norske kommentarutgaven til GDPR fremheves det at mange enkeltopplysninger om en person som på egenhånd skulle tilsi et lite behov for beskyttelse, kan få et økt beskyttelsesbehov dersom mange slike opplysninger kan sammenstilles, sånn at det gjennom disse opplysningene for eksempel er mulig å gi en prognose for individets handlinger og reaksjonsmønstre i fremtiden. De trekker her frem nettbutikker eller sosiale medier som eksempler.[105]

[102] ENISA (2016) s. 12

[103] Schartum (2018) s. 165

[104] Skullerud (2018) s.201

[105] Skullerud (2018) s. 201

Schartum fremhever på sin side at «omfang» også bør vurderes i samsvar med hvor komplekse opplysningene er. «Stort volum og høy grad av kompleksitet, f.eks på grunn av komplekse rettsregler som er programmert inn i systemet, tilsier strenge tiltak», hevder han.[106]

3.2.5.4 Formål

Etter artikkel 32 nr. 1 er formålet med behandlingen et moment som skal tas hensyn til for å finne egnede tiltak.

For at tiltakene skal være egnede må de tilpasses formålet med behandlingen, fordi den kan si noe om hva som er viktigst med behandlingen, og hvilke tiltak som best vil møte risikoene den enkelte behandling medfører.

3.2.5.5 Sammenhengen behandlingen utføres i

Etter artikkel 32 nr.1 er behandlingens sammenheng et relevant moment for hvilke tiltak som er egnet.

Hvilken sammenheng personopplysningene behandles i får etter Schartum betydning på den måten at «behandling av opplysninger som produserer eller videreformidler personopplysninger til andre behandlingsansvarlige og beslutningsrutiner, krever strengere tiltak enn behandling som skjer isolert fra omgivelsene».[107]

Det er imidlertid nærliggende at dette må ses opp mot hvilke opplysninger som eventuelt blir videreformidlet, slik at hvilken type personopplysninger det er snakk om, er med på å påvirke hvor mye det har å si at opplysningene produserer eller videreformidler opplysninger.

3.2.6 Egnede tiltak

Artikkel 32 lister opp en ikke-uttømmende liste over tiltak databehandler og behandlingsansvarlig kan være pliktig å utføre for å nå det tilfredsstillende sikkerhetsnivået. Dette må etter artikkelen ses opp mot hva som er passende i det enkelte tilfelle.[108]

At listen ikke er uttømmende, tilsier i følge Schartum at databehandler og behandlingsansvarlig må undersøke om også andre tiltak kan være egnet. Dersom andre tiltak er egnet i det enkelte tilfelle, vil databehandler og behandlingsansvarlig måtte iverksette slike andre tiltak. Tiltakene eksplisitt nevnt i artikkel 32 nr. 1 bokstav a-d, er obligatorisk for databehandler eller behandlingsansvarlig å vurdere egnetheten av. Dersom et slikt tiltak ikke vil være egnet for å møte

[106] Schartum (2018) s. 165
[107] Schartum (2018) s. 165
[108] For 2016/679/EU art 32 nr. 1

sikkerhetsrisikoen, vil databehandler og behandlingsansvarlige dermed ikke være pliktig å ta disse tiltakene i bruk. Dermed skal en databehandler eller behandlingsansvarlig alltid ta stilling til hvilke av tiltakene i artikkel 32 nr. 1 bokstav a-d som vil være egnet for å møte sikkerhetsrisikoen, og i tillegg hvilke, eller om det eventuelt er, noen andre tiltak som vil være egnet.[109]

I det følgende gis det en presentasjon av de ulike foreslåtte tiltakene, som følger av artikkel 32 nr. 1 bokstav a-d. [110]

3.2.7 Tekniske tiltak[111]

3.2.7.1 Krav til system og tjeneste

I artikkel 32 nr. 1 b fremmes «evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene»,[112] som et mulig tiltak for å oppnå et tilfredsstillende nivå av behandlingssikkerhet. Gjennom dette tiltaket fremmes dermed viktigheten av å kunne fremme konfidensialitet over tid, slik at opplysningene ikke deles med uvedkommende. Ved at det stilles krav til integritet sikres det at opplysningene er korrekte. Kravet om tilgjengelighet sikrer at opplysningene er tilgjengelig når det er behov for dem. Gjennom kravet om robusthet sikres at løsningene som brukes tåler påkjenning og trusler som melder seg i disse situasjonene.

I den norske kommentarutgaven til GDPR fremheves det i denne sammenheng at: «I for eksempel helsesektoren er det avgjørende at pasientopplysninger ikke kommer på avveie, men det er minst like viktig at opplysningene er tilgjengelige når de er nødvendige for å gi helsehjelp.»[113]

3.2.7.2 Krav om gjenopprettelighet

I artikkel 32 nr. 1 bokstav c) er gjenopprettelighet nevnt som et tiltak som kan bidra til tilfredsstillende sikkerhetsnivå. Dette kravet er formulert som «evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.» Gjennom kravet til gjenopprettelighet fremheves dermed viktigheten av det å ha mulighet til å finne igjen opplysninger, dersom de blir mistet på grunn av noe som oppstår. Forordningen fremhever også viktigheten av at disse opplysningene finnes igjen raskt i de tilfellene dette er nødvendig, slik at opplysningene er tilgjengelige når de trengs.[114]

---

[109] Schartum (2018) s. 168

[110] For 2016/679/EU art 32 nr. 1 a)-d).

[111] Fordelingen mellom tekniske og organisatoriske tiltak er her hentet fra ENISA (2016) s. 33-46

[112] For 2016/679/EU art 32 nr. 1 b)

[113] Skullerud (2018) side 200

[114] For 2016/679/EU art 32 nr. 1 c)

I følge Schartum er det mest nærliggende å tolke kravet om «rett tid» dithen at det skal vurderes etter hva formålet eller formålene med behandlingen er, slik at hva som vil være «rett tid» vil være forskjellig i ulike tilfeller. Han fremholder løpende saksbehandling som et eksempel der gjenopprettelse må kunne skje raskt, og personopplysninger som lagres til å brukes en gang i fremtiden, som et eksempel på opplysninger som kun må være gjenopprettet på dette tidspunktet. .[115]

3.2.7.3 Pseudonymisering og kryptering

Et av tiltakene som er nevnt, er «pseudonymisering og kryptering av personopplysninger.»[116]

Det følger av artikkel 4 nr. 5 at det med pseudonymisering menes «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger». Det forutsettes videre at slike tilleggsopplysninger «lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person», for at de skal anses som pseudonymiserte.[117]

På denne måten endrer pseudonymisering personopplysningene, slik at det ikke lenger er mulig å identifisere personen opplysningene omhandler, med mindre en har andre opplysninger som kan sammenstilles med de pseudonymiserte, og dermed gjør identifisering mulig. Det kreves videre at denne informasjonen som gjør det mulig å finne frem til personen de pseudonymiserte opplysningene omhandler, lagres på et annet sted enn de pseudonymiserte, og at det tas i bruk slike tiltak for beskyttelse av opplysningene som gjør at de ikke kan kobles til den registrerte.[118]

Kryptering er ikke eksplisitt nevnt i forordningen, men en vanlig forståelse av dette er å «omforme (data) slik at de blir uleselige for uvedkommende»,[119] eller «å omforme opplysninger slik at de blir uleselige for andre enn dem som besitter en krypteringsnøkkel.»[120] Kryptering av personopplysninger gjør dermed at personopplysningene ikke blir leselige og tilgjengelige slik de opprinnelig er.

---

[115] Schartum (2018) s. 167

[116] For 2016/679/EU art 32 nr. 1 a

[117] For 2016/679/EU art 4 nr.5

[118] For 2016/679/EU art 4 nr.5

[119] Det norske akademis ordbok (udatert)

[120] Skullerud (2018) s. 202

Krav om kryptering etter den tidligere norske personopplysningsloven ble behandlet i sak PVN-2014-01 Skan-Kontroll. Denne saken gjaldt datatilsynets pålegg om at Skan-Kontroll måtte få på plass databehandleravtaler, betale overtredelsesgebyr og innføre informasjonssikkerhetstiltak gjennom å «avslutte sin praksis med å sende personopplysninger med behov for konfidensialitetsbeskyttelse over ukryptert e-post»[121].

I denne saken ble det om sending av bilder av personer på e-post uttalt at når «bilder ikke i tilstrekkelig grad er anonymisert, må de anses som personopplysninger som kan være sensitive. Slike bilder må sikres på en tilfredsstillende måte for eksempel ved kryptering, basert på en konkret vurdering av behovet for konfidensialitet.»[122]

Selv om denne dommen ikke har direkte rettsvirkning på forordningen, illustrerer den hvordan kryptering kan bidra til å bedre informasjonssikkerheten i et praktisk tilfelle.

3.2.8 Organisatoriske tiltak

Dersom tekniske tiltak ikke fungerer, kan det avhjelpes med organisatoriske tiltak. Det er imidlertid mye mer tidsbesparende og effektivt å benytte tekniske tiltak i mange tilfeller. Eksempelvis vil det, dersom personopplysningene ikke kan adgangskontrolleres i elektronisk system, være en løsning å oppbevare disse på fysisk papir i et arkiv med låst dør og kodelås for å komme inn. Dette vil være upraktisk for den behandlingsansvarlige og databehandler, og det illustrerer slik viktigheten av innebygget personvern, som muliggjør for overholdelse av forordningens plikter i systemene. Dette kommer jeg tilbake til. I andre tilfeller, som i det følgende, vil organisatoriske tiltak være nyttig.

3.2.8.1 Retningslinjer for adgangskontroll

Retningslinjer for adgangskontroll er et viktig tiltak for å sikre konfidensialitet i organisasjonen, samt å hindre at det blir utlevert personopplysninger til uautorisert personell eller at personer som ikke har behov for å ha tilgang til opplysningene, får det. Dette tiltaket må gjennomføres gjennom tekniske systemer for adgangskontroll, slik at det blir implementert i systemene bedriften bruker.[123]

I den tidligere nevnte saken I v. Finland, fikk klageren medhold fordi hun ikke hadde fått «practical and effective protection to exclude any possibility of unauthorised access occurring»[124]. Ut av dette kan man trekke at dersom Is opplysninger hadde vært beskyttet med

[121] Personvernnemda (2014) punkt 2 og 3

[122] Personvernnemda (2014) punkt 6-5

[123] For 2016/679/EU art 32 nr 1 b) og nr 2, samt ENISA (2016) s. 35.

[124] I v. Finland avsnitt 47.

adgangskontroll, så kunne kravene etter EMK artikkel 8 vært oppfylt. Dette kunne vært utført ved at sykehuset hadde tatt i bruk organisatoriske tiltak for å hindre at personer som ikke skulle ha tilgang til opplysningene, fikk det, og gjennomført dette i tekniske tiltak, så ville I mest sannsynlig hatt en slik beskyttelse som domstolen setter krav om.

Andre organisatoriske tiltak som kan være egnet for å oppnå tilstrekkelig behandlingssikkerhet, kan være å ha «clearly defined and documented responsibilites, roles and a need to know basis (which are regularly reviewed and redefined)»[125]. Det kan også være tiltak tilknyttet menneskene som arbeider i bedriften, slik som at personellet er egnet, og at de får den opplæringen de har behov for. [126]

3.2.9 Testing av tiltakenes effektivitet

Videre fremheves viktigheten av med jevne mellomrom å kontrollere sikkerhetskravenes effektivitet i forordningen. Dette er formulert som «en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.» En slik prosess vil dermed kunne fremme at behandlingsansvarlig og databehandler stiller seg kritiske til egne sikkerhetstiltak etterhvert som tiden går, slik at en får oppdaget det dersom enkelte tiltak som tidligere ga tilstrekkelig sikkerhetsnivå, nå ikke gjør det lenger. Gjennom en vurdering av tiltakenes effektivitet får en også stilt seg kritiske til egne tiltak, og kanskje få tatt tak i og endret tiltak som er mindre effektive, slik at disse kan byttes til andre som er mer effektive.[127]

I følge Schartum er det mest nærliggende å forstå denne bestemmelsen slik at den rutinen man har for regelmessig testing, også skal formes av hvilke hendelser som har oppstått, og som kan illustrere hvor effektive de sikkerhetstiltakene som allerede er i bruk er.[128] Av dette kan det utledes at behandlingsansvarlige da får, gjennom hendelser som allerede har oppstått, et innblikk i om tiltakene faktisk er egnet for å møte den aktuelle risikoen. Dette bør behandlingsansvarlige ta med seg videre i vurderingen av om tiltakene er effektive og fungerer til sitt bruk, eller om de bør endres.

Samtidig kan denne bestemmelsen neppe forstås slik at en bedrift som ikke har hatt datainnbrudd automatisk kan legge seg på et lavere nivå enn en som har hatt det. Spesielt viktig er det å se hen til sikkerhetstrusler som er gjeldende for den enkelte bransje man selv er i. Dette kommer jeg tilbake til i kapittel 4.

---

[125] ENISA (2016) s. 34

[126] ENISA (2016) s. 38-39

[127] For 2016/679/EU art 32 nr. 1 d)

[128] Schartum (2018) s. 167

3.2.10 Betydningen av godkjente atferdsnormer

I Artikkel 32 nr. 3 fremgår det at «Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.»[129]

Dette kan være med på å gjøre opprettholdelse av kravene til behandlingssikkerhet lettere. Ved å vise at man opprettholder en viss standard slipper man å alltid vurdere tilfredsstillende nivå i det enkelte tilfelle.

I fortalepunkt 77 spesifiseres hvordan veiledning til behandling i samsvar med forordningen bør gjøres. Slik veiledning «kan særlig gis ved hjelp av godkjente adferdsnormer, godkjente sertifiseringer, retningslinjer fra Personvernrådet eller anvisninger fra et personvernombud.» [130]

Schartum fremhever i sin bok viktigheten av at det etter artikkel 40 (1) kan utvikles egne adferdsnormer til ulike bransjer. Slik kan disse bransjenormene spesifisere hvordan de ulike kavene i forordningen skal etterleves i de ulike bransjene som anvender personopplysninger etter forordningen. [131]

Schartum utdyper dette videre, ved at han skriver: «Bransjenormer kan imidlertid bare legges til grunn dersom de er utarbeidet i samsvar med artikkel 40 (5), noe som både krever fremleggelse av utkast for den kompetente tilsynsmyndigheten, dialog med myndigheten, og til slutt godkjenning og offentliggjøring av adferdsnormen».[132]

3.2.10.1 Betydningen av ISO/IEC 27001:2013

ISO/IEC 27001 er en samling av ulike standarder for informasjonssikkerhet. Det er mulig for ulike bedrifter å bli sertifisert etter disse.[133]

Slike standarder, som ISO/IEC 27001:2013 som er blitt brukt av ENISA for å illustrere hvilket informasjonssikkerhetskrav som vil samsvare med tiltak de foreslår i håndboken for å møte ulike sikkerhetsrisikoer[134], er ikke det samme som en slik sertifisering som vil komme på plass

[129] For 2016/679/EU art 32 nr. 3
[130] For 2016/679/EU Fortalepunkt 77
[131] Schartum (2018) s. 169
[132] Schartum (2018) s. 169
[133] ISO (udatert)
[134] ENISA (2017) s. 55-66.

etter GDPR artikkel 42. Sistnevnte vil være en personvernsertifisering,[135] mens standardene i ISO/IEC 27001-familien er standarder for informasjonssikkerhet.[136] ENISAs henvisninger[137] kan imidlertid tas til inntekt for at ISO sine krav i enkelte tilfeller vil overlappe med det som vil være kravene etter GDPR, og at samsvar med ISO sin standard vil bidra til bedre behandlingssikkerhet.

Carey fremhever imidlertid at det ikke er noen automatikk i dette, der han fremhever at det «should be noted that compliance with ISO 27001 will not necessarily mean that the organization will not fall foul of the data security requirements in data protection law».[138]

3.2.11 Personer som handler for den behandlingsansvarlige eller databehandleren.

Artikkel 32 nr. 4 gir veiledning for de krav som stilles til personer som handler for den behandlingsansvarlige og databehandleren. Her fremgår det at både behandlingsansvarlig og databehandler «skal treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.»[139]

Etter denne artikkelen er det dermed en plikt for databehandler og behandlingsansvarlige til å påse at tredjepersoner behandler opplysningene tilfredsstillende.

3.2.12 Overholdelse av artikkel 32.

Etter ansvarlighetsprinsippet i artikkel 5 nr. 2 har den behandlingsansvarlige som nevnt i kapittel 2.1.4 ansvar for at prinsippet om behandlingssikkerhet slik det fremkommer i artikkel 5 nr. 1 f) overholdes, og for å dokumentere dette.[140] Etter artikkel 24 blir denne plikten utdypet til å gjelde hele forordningen, ved at behandlingsansvarlige skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning».[141] Etter dette utvides dokumentasjonsplikten, slik at plikten til å dokumentere etterlevelse gjelder alle plikter etter forordningen.[142]

[135] For 2016/679/EU art 42 nr. 1
[136] ISO (udatert)
[137] ENISA (2017) s. 55-66
[138] Carey (2018) s. 97
[139] For 2016/679/EU art 32 nr. 4
[140] For 2016/679/EU art. 5 nr. 1 f) og nr. 2
[141] For 2016/679/EU art. 24 nr. 1
[142] For 2016/679/EU art. 24 nr. 1

3.3 Behandlingssikkerhet og innebygget personvern

En viktig forutsetning for at behandlingsansvarlig og databehandler skal kunne møte kravene i artikkel 23-33 om behandlingssikkerhet, er at de systemene som benyttes, åpner for personvernvennlige løsninger. Her får forordningens artikkel 25 betydning.

Artikkel 25 har tittelen «Innebygd personvern som standardinnstilling». Her fremgår det blant annet at «Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles.» Videre fremgår det at «Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.»[143]

Artikkelen fremhever dermed at det er de personvernvennlige løsningene som skal være standard når det behandles personopplysninger.

Carey fremhever hvordan prinsippet om innebygget personvern skal implementeres, og viktigheten av at personvernet tas i betraktning gjennom hele prosessen når nye systemer utvikles; "In particular, when designing systems and technologies, controllers should build in privacy from the outset rather than bolting it on at the end – that is, they should adopt "privacy by design"(…) approach".[144]

Artikkel 25 nr. 3 fremholder: «En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.»[145]

Kravet til innebygd personvern gjør at systemutviklerne må ha disse løsningene innebygget i systemene sine. De utviklerne som ikke følger dette, vil ikke kunne tilby behandlingsansvarlig og databehandler systemer som muliggjør de tekniske kravene i artikkel 32. Dersom man benytter systemer som ikke gjør tekniske tiltak for å minske risiko mulig, vil man måtte løse dette med organisatoriske tiltak. Dette innebærer flere manuelle prosesser som vil ta lang tid og ikke gi de ansvarlige mulighet til effektivt å etterleve kravene i artikkel 32.

[143] For 2016/679 EU art. 25 nr. 2

[144] Carey (2018) s. 95

[145] For 2016/679 EU art. 25 nr. 3

Forbindelsen mellom behandlingssikkerhet og innebygget personvern er beskrevet slik i fortalepunkt 78: «For å påvise at denne forordning overholdes bør den behandlingsansvarlige vedta interne retningslinjer og gjennomføre tiltak som særlig overholder prinsippene om innebygd personvern og personvern som standardinnstilling. Nevnte tiltak kan blant annet omfatte å minimere behandlingen av personopplysninger, pseudonymisere personopplysninger så raskt som mulig, sikre at behandlingen og formålene med den er åpen, gjøre det mulig for den registrerte å kontrollere behandlingen samt gjøre det mulig for den behandlingsansvarlige å iverksette sikkerhetsfunksjoner og å forbedre dem.»[146]

Videre fremgår det av fortalepunktet: «Ved utvikling, utforming, valg og bruk av programmer, tjenester og produkter som er basert på behandling av personopplysninger, eller når personopplysninger behandles for å oppfylle disses funksjon, bør produsenter av nevnte produkter, tjenester og programmer oppmuntres til å ta hensyn til retten til vern av personopplysninger ved utvikling og utforming av nevnte produkter, tjenester og programmer». Videre bør disse også «idet det tas behørig hensyn til den tekniske utviklingen, sikre at behandlingsansvarlige og databehandlere kan oppfylle sine forpliktelser med hensyn til vern av personopplysninger. Det bør også tas hensyn til prinsippene om innebygd personvern og personvern som standardinnstilling i forbindelse med offentlige anbud.»[147]

Det er nærliggende å anta at det vil være en stor konkurransefordel for utviklere å kunne tilby løsninger som ivaretar personvernet. Dette hjelper behandlingsansvarlige og databehandler å enklere oppfylle kravene etter forordningen. De produktene som ikke muliggjør kravene til sikkerhet etter personvernforordningen, vil dermed, dersom forordningen får god gjennomslagskraft, ikke bli etterspurt.

3.4 Vurdering av personvernkonsekvenser ved høy risiko

Artikkel 35 i forordningen har tittelen «Vurdering av personvernkonsekvenser». Denne legger opp til et annet vurderingstema enn det som presenteres i artikkel 32. For sammenhengens skyld er det nyttig å forklare sammenhengen mellom de to artiklene, da disse fra et overordnet synspunkt tilsynelatende kan likne på hverandre.

Den risikovurderingen som artikkel 32, 33 og 34 legger opp til er forskjellig fra en slik vurdering av personvernkonsekvenser som skal utføres etter GDPR artikkel 35, som kalles en «DPIA» eller «data protection impact assessment». Den risikoen som gjøres i sistnevnte inkluderer flere personvernrettslige faktorer for risikovurderingen som ikke er sikkerhetsrelatert.

[146] For 2016/679/EU fortalepunkt 78

[147] For 2016/679/EU fortalepunkt 78.

Den vurderingen som illustreres etter artikkel 32 flg. vil derfor være relevant for vurderingen etter artikkel 35, men de vil ikke sammenfalle, og sistnevnte vil inneholde en bredere vurdering enn det som er tilfelle etter artikkel 32.[148]

En DPIA gjelder videre en behandling som det «er sannsynlig at … 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»[149]. Forordningen setter dermed kun krav til at en DPIA gjennomføres i enkelte tilfeller.[150] Den risikovurderingen som må utføres etter GDPR artikkel 32 for å finne et egnet sikkerhetsnivå skal på sin side utføres for alle behandlinger som omfattes av forordningen.

En risikovurdering etter artikkel 32 skal gjøres for all behandling av personopplysninger etter GDPR, mens det kun er krav om at en DPIA utføres der «det er sannsynlig at en type behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter»[151]. Blant annet skal det i en DPIA tas med «en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.»[152] Her skal det da illustreres lovligheten av behandlingen, sammenliknet med artikkel 5 nr 1 c (prinsippet om dataminimering). Dette er en vurdering som faller på utsiden av artikkel 32. Vurdering av tilstrekkelig sikkerhet etter artikkel 32 gjøres etter at det er vurdert at behandlingen er lovlig i første omgang. Det er kun hvilke sikkerhetstiltak som skal sikre behandlingen som er av interesse.

[148] ENISA (2016) s. 17
[149] For 2016/679/EU art. 35 nr. 1
[150] For 2016/679/EU art. 35 nr. 1
[151] For 2016/679 EU art. 35 nr. 1
[152] For 2016/679 EU art. 35 nr. 7 b)

4 Behandlingssikkerhet i praksis

4.1 Hvordan kan man i praksis oppnå et tilstrekkelig nivå av behandlingssikkerhet?

I dette kapittelet beskrives og illustreres hvordan kravene til behandlingssikkerhet i GDPR artikkel 32 skal etterleves i praksis. Hvordan risikoen for behandlingen skal vurderes, og hvilke sikkerhetstiltak som kan være egnet presenteres i kapittel 4.2.

ENISA (European Union Agency For Network and Information Security) har gitt ut flere veiledende publikasjoner for behandlingssikkerhet etter GDPR og hvordan en risikoanalyse i disse tilfellene bør utføres. [153] I dette kapittelet får «Guidelines for SMEs on the security of personal data processing» fra 2016[154] og «Handbook on Security of Personal Data Processing»[155] fra 2017 stor betydning.

ENISAs håndbok fra 2017 forholder seg til GDPR[156], og her slås det fast at retningslinjene fra 2016 også vil være passende når det skal vurderes risiko etter forordningen.[157]

ENISA fremhever at deres vurderinger av praktiske hendelser kun er en illustrasjon av hvordan deres retningslinjer kan anvendes i det praktiske liv. Dette er dermed ingen illustrasjon av om disse behandlingene er tillatt etter GDPR, eller om de foreslåtte tiltakene vil være tilstrekkelig etter forordningen. [158]

Det gjelder også den videre illustrasjonen av risikovurdering og mulige sikkerhetstiltak som presenteres i det neste delkapittelet. Dette er kun en presentasjon av risiko og sikkerhetstiltak nevnt i GDPR artikkel 32 og hvordan disse i samsvar med ENISAs veiledende dokumenter kan anvendes på faktiske hendelser, men det er ingen fasit. Denne vurderingen vil dermed kun forsøke å være illustrerende, ikke direkte rettledende for hva etterlevelse av forordningen innebærer.

Eksemplene i det følgende er inspirert av ENISAs oversikter over liknende praktiske scenarioer i håndboken fra 2017. Disse har gitt nyttige holdepunkter for hvordan risikovurderingen skal

[153] ENISA (2016), ENISA (2017)
[154] ENISA (2016)
[155] ENISA (2017)
[156] ENISA (2017) s. 9
[157] ENISA (2017) s. 6
[158] ENISA (2017) s. 17

utføres,[159] men vurderingen her er løsrevet fra de vurderingene som ble illustrert i håndboken, ved at vurderingen av risiko og egnede sikkerhetstiltak er gjort ut fra ENISAs håndbok, men eksemplene er vurdert uavhengig av de konkrete eksemplene i håndboken.

ENISA anbefaler i sin håndbok at «The data controller is advised to start with the examples provided and further carry out the assessment based on her specific data processing context and environment».[160]

For å illustrere vurderingen beskrevet overfor blir det her tatt utgangspunkt i hvordan denne kan utføres på et lite helseforetak og en nettbutikk der det selges klær.

4.2 Risikovurdering og egnede tiltak

Som nevnt i kapittel 3 er risikoen utgangspunktet for vurderingen av om nivået for behandlingssikkerhet er tilstrekkelig.

I ENISAs rapport fra 2016 ble det gitt retningslinjer for hvordan risiko for behandling av personopplysninger skal vurderes, der dette ble delt opp i 4 steg.[161] I ENISAS «Handbook on Security of Personal Data Processing» fra 2017 ble denne vurderingen tillagt et femte steg, der egnede tiltak for å møte risikoene ble inkludert.[162] Disse stegene vil bli beskrevet i det følgende. Den fremgangsmåten som er beskrevet i disse publikasjonene danner rammen for drøftelsen i dette kapittelet.

ENISAs rapport er begrenset til «SMEs» - «Small and Medium sized Enterprises»[163]. Illustrasjonen i dette kapittelet er derfor også begrenset til å fokusere på ulike SMEs.

Disse vil ofte ha mindre ressurser til å bruke på sikkerhetstiltak enn de største bedriftene, men dette fritar dem ikke for ansvar for beskyttelse av personopplysningene.[164]

Videre i dette kapittelet blir det gitt en kort oversikt over fremgangsmåten beskrevet av ENISA, og en illustrasjon av denne med praktiske eksempler. På grunn av denne oppgavens begrensede størrelse, vil kun hovedtrekkene i ENISAs retningslinje og håndbok bli omtalt.

[159] ENISA (2017) s. 26-28, 28-30 og 39-41
[160] ENISA (2017) s. 17
[161] ENISA (2016) s. 17.
[162] ENISA (2017) s. 16
[163] ENISA (2016) s. 7
[164] Carey (2018) s. 92

Oppbygningen i det følgende er hentet fra ENISAs retningslinje og håndbok.[165]

4.2.1 Første steg – «Definere behandlingsoperasjonen og dens kontekst»[166]

I denne delen av rapporten lister ENISA opp et minstekrav med spørsmål som må stilles. De fremhever også viktigheten ved at disse spørsmålene forstås på en god måte av behandlingsansvarlig og databehandleren.[167]
Disse spørsmålene er:

1. «Hva er behandlingsoperasjonen for personopplysninger?»[168]
2. «Hvilke typer personopplysninger blir behandlet?»[169]
3. «Hva er formålet med behandlingen?»[170]
4. «Hvilke midler brukes til behandling av personopplysninger?» [171]
5. «Hvor foregår behandlingen av personopplysninger?»[172]
6. «Hvilke kategorier er de registrerte?»[173]
7. «Hvem er mottakere av dataene?»[174]

Noen av disse spørsmålene blir i det følgende presentert nærmere for å illustrere behandlingen i de to eksemplene.

1. «Hva er behandlingsoperasjonen for personopplysninger?»[175]
Dette helseforetaket, en liten klinikk eller legekontor, utfører enklere fastlegetjenester, slik som undersøkelser, små kirurgiske inngrep eller veiledning.

Nettbutikken sender ut nyhetsbrev til tidligere registrerte kunder. Her innhentes navn, telefonnummer, e-post, kjønn og fødselsdato. Behandlingen av personopplysninger er her en tenkt oppbevaring og utsending av informasjon til kundene ved tilbudskampanjer eller liknende.

---

[165] ENISA (2016) s. 17-32 og ENISA (2017) s. 10-16
[166] Min oversettelse av ENISA (2016) s. 17.
[167] ENISA (2016) s. 17.
[168] Min oversettelse av ENISA (2016) s. 18
[169] Min oversettelse av ENISA (2016) s. 18
[170] Min oversettelse av ENISA (2016) s. 18
[171] Min oversettelse av ENISA (2016) s. 18
[172] Min oversettelse av ENISA (2016) s. 19
[173] Min oversettelse av ENISA (2016) s. 19
[174] Min oversettelse av ENISA (2016) s. 19
[175] Min oversettelse av ENISA (2016) s. 18

2. "Hvilke typer personopplysninger blir behandlet?"[176]
ENISA spesifiserer at dette spørsmålet har betydning for risikovurderingen på to måter. Dette kan gi et bilde av behandlingsoperasjonen, samtidig som det kan illustrere hvilket risikonivå behandlingen er på.[177]

Dette kan for eksempel illustreres hos helseforetaket. Her kan en tenke seg at kontaktinformasjon og informasjon om tidligere sykdomshistorie oppbevares i samme system. Det vil da være forskjell på risikovurderingen for kontaktinformasjon og sykdomsinformasjon, fordi sykdomsinformasjon er sensitive personopplysninger etter GDPR artikkel 9, mens kontaktinfo ikke er det.

Helseforetaket innhenter navn, opplysninger om helse, fødselsnummer, blodtype, og lagrer det i et IT-system. Helseforetaket behandler dermed særlige kategorier av personopplysninger etter GDPR artikkel 9 nr. 1.

Nettbutikken behandler informasjon om navn, adresse, kontaktinformasjon, fødselsdato og kjønn.

3. «Hva er formålet med behandlingen?»[178]
Formålet med behandlingen av personopplysninger hos helseforetaket er å sikre god og riktig helsehjelp.
Formålet med behandlingen av personopplysninger i nettbutikken er å gi kundene informasjon om tilbud, samt en smidig kjøpsopplevelse.

6. «Hvilke kategorier er de registrerte?»[179]
Hos helseforetaket er dette en stor variasjon av personer, både barn og voksne.
Hos klesprodusenten er dette kun voksne personer.

4.2.2 Andre steg – «Forstå og vurdere innvirkning»[180]

Det neste steget i vurderingen handler om hvilken innvirkning et mulig sikkerhetsbrudd for personopplysningene kan ha for den enkelte som rammes. Fordi kategorier av personopplysninger og behandlinger kan være veldig forskjellige, og fordi behandlingene kan være tilfeldige,

[176] Min oversettelse av ENISA (2016) s. 18
[177] ENISA (2016) s. 18
[178] Min oversettelse av ENISA (2016) s. 18
[179] Min oversettelse av ENISA (2016) s. 19
[180] Min oversettelse av ENISA (2016) s. 17

så kan man kun legge til grunn en kvalitativ tilnærming. [181] Hvor mange som kan bli utsatt for denne innvirkningen får derfor ikke betydning for nivået av innvirkning, det er kun graden av innvirkning den enkelte kan bli utsatt for som er av betydning.

For denne vurderingen er hvilken type personopplysninger det er snakk om, hvor viktig eller kritisk behandlingen av personopplysninger er, den enkelte karakteristikken den behandlingsansvarlige eller databehandleren har, og enkelte særtrekk med den registrerte viktige momenter.[182]

ENISA har laget en oversikt over hva som tilsvarer ulik grad av innvirkning, i samsvar med tidligere praksis på feltet[183]. Her oppdeles de ulike innvirkningsnivåene slik:

Lav: «Enkeltpersoner kan støte på noen få mindre ulemper, som de vil overvinne uten problemer (tid brukt på å skrive inn informasjon på nytt, ergrelser, irritasjoner osv.).»[184]

Medium: "Personer kan støte på betydelige ulemper, som de vil kunne overvinne, til tross for noen vanskeligheter (ekstra kostnader, nektelse av tilgang til forretningstjenester, frykt, manglende forståelse, stress, mindre fysiske plager etc.)."[185]

Høy: "Enkeltpersoner kan støte på betydelige konsekvenser, som de burde kunne overvinne om enn med alvorlige vanskeligheter (misbruk av midler, blacklisting av finansinstitusjoner, eiendomsskade, tap av sysselsetting, stevning, forverring av helse etc.)."[186]

Veldig høy: "Personer som kan støte på betydelige eller til og med irreversible konsekvenser, som de ikke kan overvinne (manglende evne til å jobbe, langsiktige psykiske eller fysiske plager, død etc.)."[187]

Videre kan disse ulike påvirkningene deles opp i tre. Dette er påvirkning ved tap av konfidensialitet, integritet og tilgjengelighet. Det er den av disse som kan gi høyest innvirkning for individet som skal vurderes som det endelige nivået for påvirkning. [188]

[181] ENISA (2016) s. 20.
[182] ENISA (2016) s. 21
[183] ENISA (2016) s. 20
[184] Min oversettelse av ENISA (2016) s. 20
[185] Min oversettelse av ENISA (2016) s. 20
[186] Min oversettelse av ENISA (2016) s. 20
[187] Min oversettelse av ENISA (2016) s. 20
[188] ENISA (2016) s. 23, ENISA (2017) s. 11

I det følgende vil vurderingen for grad av innvirkning presenteres gjennom de to tidligere illustrerte eksemplene.

4.2.2.1 Innvirkning hos helseforetaket

Tap av konfidensialitet kan her tenkes å føre til frykt og stress dersom personopplysningene kommer på avveie. Graden av innvirkning er etter ENISAs mønster derfor satt til middels.[189]

Tap av integritet kan her tenkes å få store konsekvenser. Dersom personopplysninger om en person blir endret, slik at pasienten står oppført med en annen kronisk sykdom enn den han eller hun har, eller en annen blodtype, kan dette få fatale følger. I verste fall kan det føre til død. Graden av alvorlighet for innvirkning blir dermed her satt til veldig høy i samsvar med ENISAs oversikt.[190]

Tap av tilgjengelighet kan i dette tilfellet være kritisk for pasientene. Dette kan føre til at han eller hun kan få mangelfull helsehjelp hvis for eksempel opplysninger om tidligere legebesøk er kommet på avveie. Graden av alvorlighet for innvirkning blir dermed satt til høy etter ENISAs oversikt.[191]

Etter ENISAs rapport er dermed innvirkningen veldig høy her, da det skal legges til grunn det høyeste nivået av de tre typene av innvirkning som kan oppstå.[192]

4.2.2.2 Innvirkning hos nettbutikken.

Tap av konfidensialitet kan her føre til at kundene må oppgi personopplysningene sine på nytt, eller at de vil bli kontaktet av andre gjennom den opprinnelige kontaktkanalen der personopplysningene er blitt oppgitt. For tap av konfidensialitet er derfor innvirkningen her vurdert til lav etter ENISAS mønster.[193]

Ved tap av integritet kan det oppstå irritasjon, ved at personen får reklame tilpasset et annet kjønn enn han/hun har spesifisert, eller at e-posten sendes til feil navn. Den registrerte kan også måtte bruke tid på å oppgi riktig informasjon på nytt til nettbutikken. Graden av innvirkning er derfor satt til lav etter mønsteret i ENISAs retningslinjer.[194]

---

[189] ENISA (2016) s. 20
[190] ENISA (2016) s. 20
[191] ENISA (2016) s. 20
[192] ENISA (2016) s. 20.
[193] ENISA (2016) s. 20
[194] ENISA (2016) s. 20

Ved tap av tilgjengelighet kan det være uforståelig for kundene at de ikke får nyhetsbrevet de har satt seg opp til, og det kan oppstå ekstra kostnader ved at de ikke får rabatter eller tilbud som de ville fått om informasjonen ikke hadde havnet på avveie. Innvirkningen av tap av tilgjengelighet blir derfor satt til medium her.[195]

Etter ENISAs mønster skal det høyeste nivået av innvirkning bli gjeldende, slik at det for nettbutikken er et middels innvirkningsnivå ved sikkerhetsbrudd.[196]

4.2.3 Tredje steg – «Definisjon av mulige trusler og vurdering av deres sannsynlighet»[197]

Det tredje steget for risikovurderingen er etter rapporten å definere de truslene som er mulige, samt å vurdere hva sannsynligheten for at slike trusler oppstår er. Dette ekskluderer konteksten av behandling av personopplysninger, som ble inkludert i steg 2. [198]

I rapporten deles ulike trusler opp i fire. Dette er «nettverk og tekniske ressurser»[199], «prosesser / prosedyrer relatert til databehandlingsoperasjonen»[200], «ulike parter og personer involvert i prosessoperasjonen»[201] og «bransjesektor og omfang av behandlingen»[202].

Videre skal hver av disse områdene vurderes til lav, medium eller høy sannsynlighet for at truslene oppstår. Lav sannsynlighet innebærer her at det er «usannsynlig at trusselen realiseres»,[203] medium risiko innebærer at det er «mulig at trusselen realiseres»[204], og høy risiko innebærer etter dette at «det er sannsynlig at trusselen realiseres».[205] Gjennom denne vurderingen av sannsynlighet for truslene fordelt på de ulike områdene, vil vurderingen gi et gitt trusselnivå.

[195] ENISA (2016) s. 20
[196] ENISA (2016) s. 20
[197] Min oversettelse av ENISA (2016) s. 17
[198] ENISA (2016) s. 24
[199] Min oversettelse av ENISA (2016) s. 24
[200] Min oversettelse av ENISA (2016) s. 25
[201] Min oversettelse av ENISA (2016) s. 25
[202] Min oversettelse av ENISA (2016) s. 25
[203] Min oversettelse av ENISA (2016) s. 29
[204] Min oversettelse av ENISA (2016) s. 29
[205] Min oversettelse av ENISA (2016) s. 29

Etter ENISAs veileder skal det gjøres en vurdering av risikoen fra 1-3, for hver av disse sektorene, som til slutt legges sammen, og trusselnivået settes da til omtrent gjennomsnittet av trusselnivået for disse undernivåene av trusler.[206]

Retningslinjene fra ENISA presenterer også en rekke spørsmål for denne vurderingen. [207]

4.2.3.1 Trusler for helseforetaket

«Nettverk og tekniske ressurser»[208], Momenter i denne vurderingen er at det er flere personer kan være inkludert, noe som åpner for menneskelige feil, og at dataene er lagret i IT-systemer[209]. Etter dette er trusselen satt til medium.

«Prosesser/prosedyrer relatert til databehandlingsoperasjonen»[210]
Her kan ikke personalet åpne systemet på eget teknisk utstyr. Det er også klart avgrenset hvem som har ansvar for behandlingen av personopplysningene, og de ansattes roller på dette punktet er tydelig definert. Dette er momenter som taler for lav risiko på dette punktet, og etter ENISAS retningslinje blir risikoen vurdert som lav.[211]

«Ulike parter og personer involvert i prosessoperasjonen»[212] Hos helseforetaket er det kun personer med lovlig behov som får se personopplysningene, og helseforetaket behandler alle personopplysningene selv. Dette er momenter som tilsier et lavt trusselnivå for denne vurderingen.[213] Etter dette blir trusselen lav for denne vurderingen.

«Bransjesektor og omfang av behandlingen»[214] For vurderingen av trusler tilknyttet bransjesektor, er det av betydning at helseforetak generelt har vært utsatt for trusler for sikkerheten til personopplysninger, slik som i Helse Sør-Øst[215] saken, eller i saken I v. Finland[216] som ble nevnt tidligere i oppgaven.

[206] ENISA (2016) s. 29-31.
[207] ENISA (2016) s. 25-29
[208] Min oversettelse av ENISA (2016) s. 24
[209] ENISA (2016) s. 25-26
[210] Min oversettelse av ENISA (2016) s. 25
[211] ENISA (2016) s. 26-27
[212] Min oversettelse av ENISA (2016) s. 25
[213] ENISA (2016) s. 27-28
[214] Min oversettelse av ENISA (2016) s. 25
[215] Datatilsynet (2017a) og Datatilsynet (2017b)
[216] I. v. Finland

Helseforetaket behandler også svært mye opplysninger om pasienten. Dette er momenter som trekker i retning av et høyt trusselnivå etter ENISAs retningslinje. [217]

Etter dette vurderes trusselsituasjonen til middels. Dette tilsvarer etter ENISA at muligheten for at trusselen oppstår er til stede, men det er verken usannsynlig eller overveiende sannsynlig at den oppstår. [218]

4.2.3.2 Trusler for nettbutikken

«Nettverk og tekniske ressurser»[219] Handel og innhenting av informasjon skjer på det ordinære, åpne internett, en faktor som i følge ENISA kan innebære en trussel for personopplysningene.[220] At bedriften styrer all sin behandling av personopplysninger i butikklokalene og i et åpent kontorlandskap sammen med personer fra andre bedrifter, kan bidra til en trussel for at uautorisert personell kan få tilgang til dette området og til personopplysningene. Dette innebærer i følge ENISA en trussel.[221] Etter dette blir trusselnivået for nettverk og tekniske ressurser vurdert til høy.

«Prosesser / prosedyrer relatert til databehandlingsoperasjonen»[222]: For eksempel kan det at de ansatte har mulighet til å bruke sine private elektroniske midler påvirke trusselen i følge ENISA.[223] At det føres en logg over hvilke ansatte som har vært innlogget i løsningen der personopplysninger behandles, og hvilke personopplysninger de har sett på, er i følge ENISA en faktor som senker trusselnivået.[224] Dette bidrar til at trusselsituasjonen settes til medium her.

«Ulike parter og personer involvert i prosessoperasjonen»[225] Personellet i bedriften har fått opplæring i hvordan de skal behandle personopplysningene på en sikker måte, slik at de har god kompetanse til å forstå de aktuelle truslene, noe som i følge ENISA er med på å holde et lavt trusselnivå. [226] Det at det ikke brukes databehandlere er også med på å holde et lavt trusselnivå i følge ENISA.[227] Etter dette blir trusselen lav her.

---

[217] ENISA (2016) s. 28-29
[218] ENISA (2016) s. 29
[219] Min oversettelse av ENISA (2016) s. 24
[220] ENISA (2016) s.25
[221] ENISA (2016) s. 25-26
[222] Min oversettelse av ENISA (2016) s. 25
[223] ENISA (2016) s. 27
[224] ENISA (2016) s. 27
[225] Min oversettelse av ENISA (2016) s. 25
[226] ENISA (2016) s. 28
[227] ENISA (2016) s. 27

«Bransjesektor og omfang av behandlingen»[228]. Det antas at denne bransjen typisk ikke er særskilt utsatt for trusler, noe som er med på å holde trusselnivået nede. [229] Det er imidlertid et stort antall kunder som er registrert, noe som kan utgjøre en trussel for personopplysningssikkerheten.[230] Etter dette lander nettbutikken på et middels trusselnivå.

4.2.4 Fjerde steg – «Vurdering av risiko»[231]

I den siste delen av en vurdering av risiko ved behandlingen, må annet og tredje steg kombineres. Dette gjøres ved at truslene og deres sannsynlighet multipliseres med den effekten et sikkerhetsbrudd kan ha for den enkelte. Slik får man da et bilde av risikoen. I ENISAs modell er det lagt til grunn det verst tenkelige scenarioet for innvirkning, og på grunn av dette blir nivået for innvirkning for individet vektet mer enn trusselnivået.[232]

Jeg har fulgt dette mønsteret for å vurdere risikoen for helseforetaket og nettbutikken.

Da ender helseforetaket, med veldig høy innvirkning og middels trusselnivå, på høy/veldig høy risiko, etter ENISAS modell.[233]

Nettbutikken med middels innvirkning og middels trusselnivå, ender på en middels risiko for sikkerhetsbrudd, etter ENISAs modell.[234]

4.2.5 Femte steg – «Sikkerhetstiltak»[235]

Dette femte steget skjer etter en vurdering av risikoen, der ulike tiltak som kan passe risikoen blir vurdert. De ulike tiltakene, som kan være tekniske eller organisatoriske, blir delt opp i tre ulike kategorier. Disse er fordelt etter risiko, slik at noen tiltak passer høy, andre passer middels og de siste passer lave risikoer.[236]

Her kan en se tilbake til det som ble nevnt under vurderingen av innholdet i pliktene i GDPR artikkel 32. Disse tiltakene vil som nevnt være avhengige av hvilken risiko de skal møte. Dette blir illustrert gjennom tiltakene i ENISAs retningslinjer.

---

[228] Min oversettelse av ENISA (2016) s. 25
[229] ENISA (2016) s. 28
[230] ENISA (2016) s. 29
[231] Min oversettelse av ENISA (2016) s. 31.
[232] ENISA (2016) s. 31
[233] ENISA (2016) s. 31.
[234] ENISA (2016) s. 31
[235] Min oversettelse av ENISA (2016) s. 33
[236] ENISA (2017) s. 16

4.2.5.1 Egnede tiltak

For å møte høy risiko kan det for eksempel komme på plass en god fordeling av roller, slik at tilgangen til personopplysningene kun blir gitt til de som trenger det for at formålet med behandlingen skal oppnås. [237]

For både helseforetaket og nettbutikken vil for eksempel det å trene personalet i sikkerhet for behandlingen være et egnet tiltak. I håndboken er det imidlertid lagt inn et krav om at det, for å møte en høy risiko, bør gjøres en årlig repetisjon av dette. For høy risiko er det også satt krav om at treningsplanen skal inneholde sikkerhetsmål. Det er dermed et mer spesifisert krav til trening på sikkerhet for behandling av personopplysninger ved høy risiko enn ved en middels. [238]

4.2.5.2 Egnede tiltak for helseforetaket

For å sikre seg mot den menneskelige risikoen som kommer med at det er flere personer som håndterer personopplysningene, kan for eksempel det å klart spesifisere hvem som skal ha tilgang til opplysningene tenkes å være et passende tiltak etter ENISAs oversikt.[239]

Videre kan to-faktor autentisering være et passende tiltak for å hindre at personell som ikke skal gå inn på opplysningene finner dem, og dermed hindre slike følger som en uautorisert utlevering kan føre til.[240]

Det å ha backup av informasjon kan også være et tiltak som kan bidra til et tilstrekkelig sikkerhetsnivå. Etter ENISAS håndbok bør disse bli lagret på et sikkert sted offline, og de bør krypteres.[241]

Slik kan tilgjengeligheten av disse opplysningene sikres, slik at man minsker risikoen for at de blir borte. Dette kan møte risikoen for at opplysninger om pasientene forsvinner, slik at de ikke får den helsehjelpen de trenger.

4.2.5.3 Egnede tiltak for nettbutikken

[237] ENISA (2016) s. 35
[238] ENISA (2017) s. 61 og s. 65.
[239] ENISA (2017) s. 65
[240] ENISA (2017) s. 65
[241] ENISA (2017) s. 66

Et mulig tiltak for å møte middels risiko for de nevnte risikoene hos nettbutikken, kan i samsvar med ENISAs håndbok være å opprette retningslinjer med krav til hvordan passord skal være. Hvilken lengde passordet skal ha, hvor ofte det skal skiftes og hvor mange feilede innloggingsforsøk som skal godtas bør med i disse tiltakene. [242]

I samsvar med ENISAs rapport kan det å unngå fjerntilgang til IT-systemene være et tiltak som nettbutikken bør vurdere.[243] Slik er det lettere å ha kontroll på hvem som er inne i IT-systemet der personopplysninger behandles, og når de er der.

To-faktor autentisering er i ENISAs rapport opplistet som et mulig tiltak for å treffe høy risiko[244], og nevnt som et mulig tiltak for å redusere risiko hos helseforetaket. Gjennom disse oversiktene får ENISA dermed illustrert hvordan de tenker at de ulike sikkerhetstiltakene kan tilpasses risiko. To-faktor autentisering illustreres som et virksomt tiltak, men som slik ENISA har illustrert det, ikke vil være nødvendig dersom risikoen er ansett å være lav.[245]

[242] ENISA (2017) s. 61
[243] ENISA (2017) s. 62
[244] ENISA (2017) s. 65
[245] ENISA (2017) s. 55 og 65

5 Plikten til å melde fra om brudd på behandlingssikkerheten etter GDPR artikkel 33 og 34

5.1 Hensyn og bakgrunn for melde-og underrettelsesplikt for brudd på personopplysningssikkerheten

Plikten til å gi beskjed om sikkerhetsbrudd er viktig fordi det sikrer at disse bruddene kommer frem i lyset og blir undersøkt med den styrken som er nødvendig. Det gir også tilsynsmyndigheten oversikt over de aktuelle sikkerhetsbruddene, slik at de kan bidra til å minske skadefølgene. At den registrerte får beskjed om brudd kan gi også denne mulighet til å minske skadefølgene.

Artikkel 29 gruppen har fremhevet at «et nøkkelelement i enhver datasikkerhetspolicy er, der det er mulig, å kunne motvirke databrudd og, hvis det likevel oppstår, å reagere i tide».[246]

Gruppen fremhever: «The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data."[247] Videre fremhever gruppen muligheten til å sanksjonere den behandlingsansvarlige etter artikkel 83 som en annen side av reguleringen av plikten til å melde fra om brudd på personopplysningssikkerheten. [248]

I det følgende vil det gis en presentasjon av plikten til å melde fra om sikkerhetsbrudd slik den fremgår av GDPR artikkel 33 og 34.

5.1.1 Hva innebærer det å melde fra om brudd på personopplysningssikkerheten?

Artikkel 33 og 34 hjemler plikt til å gi beskjed til henholdsvis tilsynsmyndigheten og den personen opplysningene gjelder, dersom det er skjedd et brudd på personopplysningssikkerheten.[249]

Plikten til å melde fra om sikkerhetsbrudd slik den fremgår direkte av GDPR artikkel 33 og 34, er ny i sitt anvendelsesområde. Direktivet GDPR erstatter hadde ikke noen slik plikt. Plikten er imidlertid ikke helt ny i personvernsammenheng. Flere datatilsyn i EU-land har oppfordret de behandlingsansvarlige til å melde fra dersom sikkerhetsbrudd oppstod. For noen vil plikten til å melde fra imidlertid være ny. [250]

[246] Min oversettelse av WP29 (2017) p. 6.
[247] WP29 (2017) s. 5
[248] WP29 (2017) s. 5
[249] For 2016/679/EU art 33 og 34
[250] WP29 (2017) side 5

I Norge hadde man plikt til å melde fra om enkelte sikkerhetsbrudd etter den tidligere personopplysningsforskriften §2-6 (3).[251]

5.1.2 Hva er et «brudd på personopplysningssikkerheten?»

Hva som menes med «brudd på personopplysningssikkerheten» i forordningen, er definert i artikkel 4 nr. 12, der dette er definert som «et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.»[252]

Etter Artikkel 29 gruppens retningslinje er det også et sikkerhetsbrudd hvis data kun er utilgjengelige for en liten tidsperiode og blir tilgjengelige igjen, så lenge dette ikke er en del av planlagt utilgjengelighet som følge av oppdateringer på systemer eller liknende. [253]

Med andre ord er det et brudd på behandlingssikkerheten dersom personopplysningene blir utsatt for behandling på en måte som ikke er i tråd med behandlingsansvarliges eller databehandlers tiltenkte og lovlige behandling etter forordningen, som følge av et brudd på sikkerheten.[254] Dette gjelder selv om dette kun er for en kort periode, slik at opplysningene er gjenopprettet når det oppdages. [255]

Artikkel 29 gruppen har delt mulig brudd på personopplysningssikkerheten opp i tre prinsipper, som de karakteriserer som anerkjente prinsipper for informasjonssikkerhet[256]. Dette er:

«"Konfidensialitetsbrudd"- der det foreligger uautorisert eller utilsiktet avsløring av eller tilgang til personlige opplysninger.
"Integritetsbrudd"- der det foreligger uautorisert eller utilsiktet endring av personopplysninger.
"Tilgjengelighetsbrudd" - der det foreligger et utilsiktet eller uautorisert tap av tilgang til eller ødeleggelse av personopplysninger."»[257]

Artikkel 29 gruppen fremhever at «et brudd kan vedrøre fortrolighet, integritet og tilgjengelighet av personopplysninger samtidig, samt enhver kombinasjon av disse.»[258]

---

[251] Personopplysningsforskriften (2000) § 2-6 (3)
[252] For 2016/679/EU art. 4 nr. 12
[253] WP29 (2017) s. 8
[254] For 2016/679/EU art. 32, 33 og 34
[255] WP29 (2017) side 9
[256] WP29 (2017) s. 7 WP29 (2014) del 1
[257] Min oversettelse av WP29 (2017) s. 7
[258] Min oversettelse av WP29 (2017) s. 8

I Datatilsynets veileder er disse generelle prinsippene for informasjonssikkerhet supplert med et fjerde– robusthet. I denne sammenhengen blir robusthet beskrevet som «at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser»[259].

Robusthet kan tenkes å påvirke de andre delene av informasjonssikkerheten, slik at både konfidensialiteten, integriteten og tilgjengeligheten for personopplysningene blir styrket. I artikkel 32 i forordningen er også robusthet tatt inn sammen med de andre prinsippene som ønskes ivaretatt under forordningen.[260]

Videre i dette kapittelet vil artikkel 33 behandles først i delkapittel 5.2. Etter dette følger en presentasjon av artikkel 34 i delkapittel 5.3

5.2 Plikt til å melde fra om brudd til tilsynsmyndigheten etter Artikkel 33

Kravene som stilles til den behandlingsansvarlige om varsling til tilsynsmyndigheten ved brudd på personopplysningssikkerheten er hjemlet i GDPR artikkel 33.[261]

5.2.1 Når meldeplikten utløses

Etter artikkel 33 nr. 1 skal behandlingsansvarlige melde fra om sikkerhetsbrudd hvis han «har fått kjennskap til det». Når den behandlingsansvarlige kjenner til at det er skjedd et sikkerhetsbrudd, så får han da en plikt til å melde fra om dette til tilsynsmyndigheten. Artiklene gir ikke videre veiledning for når den behandlingsansvarlige kan sies å ha denne kunnskapen.

En veiledning er blitt gitt av Artikkel 29 gruppen, der de fremholder at behandlingsansvarlige «"har fått kjennskap til bruddet" når den behandlingsansvarlige har en rimelig grad av sikkerhet for at det har oppstått en sikkerhetshendelse som har ført til at personopplysninger blir kompromittert».[262]

Dette kan forstås slik at der den behandlingsansvarlige har en viss begrunnet antagelse av at det er skjedd et sikkerhetsbrudd som har ført til negative følger for personopplysningene, så har han eller hun fått en plikt til å melde fra til tilsynsmyndigheten.

Artikkel 29 gruppen gir et eksempel på når behandlingsansvarlig etter deres mening kan sies å ha fått kjennskap til bruddet på personopplysningssikkerheten: «In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised

[259] Datatilsynet (2018) del 4

[260] For 2016/679/EU art. 32 nr. 1 b).

[261] For 2016/679/EU art. 33

[262] Min oversettelse av WP29 (2017) s. 10-11

persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.»[263]

Denne sammenhengen kan man tenke seg i flere tilfeller. Når det er vanskelig å oppdage om et brudd har ført til et brudd på konfidensialitet eller integritet, så vil det kanskje uansett være et brudd på tilgjengeligheten.

5.2.2 Tidspunkt for underrettelse

For meldeplikten etter artikkel 33 gjelder den relative tidsfristen «uten ugrunnet opphold». I de tilfellene det er mulig innebærer dette at det skal meldes fra innen 72 timer etter at behandlingsansvarlige «har fått kjennskap til» sikkerhetsbruddet. Hvis dette ikke er mulig, og det går lenger tid, skal det gis en begrunnelse for forsinkelsen.[264]

De tilfellene der den behandlingsansvarlige har brukt en databehandler, skal denne «uten ugrunnet opphold underrette den behandlingsansvarlige». [265] Dermed får den behandlingsansvarlige mulighet til å overholde pliktene sine etter artikkel 33. Etter ordlyden er det her ingen plikt for databehandleren til å vite følgene av bruddet før han melder fra. Databehandler har dermed en mindre omfattende plikt til å melde fra enn det behandlingsansvarlig har.

Når databehandler her får en slik plikt, kan det være med på å styrke retten til personvern, ved at den behandlingsansvarlige får informasjon om bruddet før den ville fått beskjed dersom databehandler måtte ha all informasjon før han ga beskjed til behandlingsansvarlige.

For at formålet bak bestemmelsene skal kunne opprettholdes vil det nok her være mindre rom for at databehandler somler med å gi videre beskjed om sikkerhetsbrudd enn det gjelder for behandlingsansvarlige. Databehandler har ingen absolutt frist slik som behandlingsansvarlige har, men i praksis vil nok også her opphold på mer enn 72 timer være lenger enn «uten ugrunnet opphold» etter artikkel 33 nr. 1.

Etter GDPR artikkel 28 skal databehandlers plikter overfor behandlingsansvarlige være underlagt en avtale, og databehandler skal bidra til at behandlingsansvarlige treffer målene sine etter forordningen, også artikkel 33.

[263] WP29 (2017) s. 11

[264] For 2016/679/EU art 33 nr. 1

[265] For 2016/679/EU art 33 nr. 2

Artikkel 29 gruppen fremhever at det i denne avtalen kan spesifiseres hvordan databehandler skal bidra til at behandlingsansvarlige når målene sine. I denne avtalen kan det også fastlegges en plikt for databehandleren til å melde fra om sikkerhetsbrudd etter GDPR artikkel 33 og 34, men gruppen fremholder at den rettslige plikten likevel vil være plassert hos den behandlingsansvarlige.[266]

Artikkel 29 gruppen fremhever videre at «Behandlingsansvarlig bruker databehandleren til å oppnå sine formål; Derfor bør behandlingsansvarlig i prinsippet betraktes som "kjent med" sikkerhetsbruddet når databehandler har informert om bruddet.»[267]

Fordi det ikke spesifiseres noen absolutt tidsfrist for å melde ifra om sikkerhetsbruddet, kom artikkel 29 gruppen med anbefalingen at dette skjer «omgående», og da slik at den videre informasjonen om bruddet kan gis trinnvis etter hvert som databehandler har den. Artikkel 29 gruppen fremholder videre at dersom den behandlingsansvarlige skal ha mulighet til å overholde 72-timers fristen som er spesifisert i artikkel 33 nr. 1, så er det viktig med en så kort frist for databehandler til å melde fra om sikkerhetsbruddet.[268]

5.2.2.1 Unntak fra meldeplikt

Plikten til å melde fra om brudd på personopplysningssikkerheten etter artikkel 33 nr. 1 gjelder ikke dersom «bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.»[269]

Her bygger artikkel 33 på en risikovurdering på samme måte som i artikkel 32, slik at der sikkerhetsbruddet ikke vil medføre en risiko, så trengs det ikke beskjed til tilsynsmyndigheten. I artikkel 32 og de tilhørende veiledende dokumentene fra ENISA[270] skal det lite til før et sikkerhetsbrudd utgjør en risiko. Ut fra dette kan en forstå det slik at de fleste sikkerhetsbrudd vil falle innunder hovedregelen om meldeplikt.

Artikkel 29 gruppen fremhever at et eksempel der det ikke vil være nødvendig å melde fra om sikkerhetsbrudd etter artikkel 33 nr. 1, «kan være hvor personopplysninger allerede er offentlig tilgjengelig, og utlevering av slike data ikke utgjør en sannsynlig risiko for den enkelte.»[271]

---

[266] WP29 (2017) s. 14.

[267] Min oversettelse av Art. 29 WP (2017) s. 13

[268] WP29 (2017) s. 14

[269] For 2016/679/EU art. 33 nr. 1

[270] ENISA (2016) og ENISA (2017)

[271] Min oversettelse av WP29 (2017) s. 18.

Dette kan for eksempel være tilfellet der den registrerte er en kjendis, og der dennes bosted allerede er alminnelig kjent.

Bevisbyrden for om unntaket for meldeplikt er oppfylt er det den behandlingsansvarlige som har, og det samsvarer således med ansvarlighetsprinsippet.[272]

5.2.3 Krav til innholdet i meldingen

Kravene til innholdet i meldingen om brudd på behandlingssikkerheten fremgår av artikkel 33 nr. 3. Artikkelen setter en rekke minstekrav til en slik melding.[273]

Det er et minstekrav at meldingen etter artikkel 33 nr. 3 bokstav a) skal gi en beskrivelse av hvilken art bruddet på personopplysningssikkerheten er. Dersom det er mulig, skal denne meldingen videre inneholde kategoriene av registrerte som berøres av bruddet, og hvor mange det gjelder. Dersom det er mulig skal meldingen også inneholde hvilke kategorier av personopplysninger det er tale om, og cirka hvor mange registrerte personopplysninger som blir påvirket.[274]

Videre skal det oppgis «navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes». Gjennom denne meldingen får tilsynsmyndigheten dermed vite hvem de skal henvende seg til for ytterligere informasjon. [275]

I tillegg skal meldingen «beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten». De følgene det er nærliggende at bruddet vil ha skal dermed være med i meldingen.[276]

Til slutt er det et minstekrav for meldingen at den må «beskrive de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.»[277]

[272] For 2016/679/EU fortalepunkt 85 og art. 5 nr. 2
[273] For 2016/679/EU art 33 nr. 3
[274] For 2016/679/EU art 33 nr. 3 a)
[275] For 2016/679/EU art 33 nr. 3 b)
[276] For 2016/679/EU art 33 nr. 3 c)
[277] For 2016/679/EU art 33. nr. 3 d)

5.2.4 Andre momenter for meldingen

Når det skal fastsettes mer spesifikke regler for formatet og hvordan man skal gå frem når det skal varsles, så skal det tas hensyn til omstendighetene rundt bruddet, og da også «om personopplysningene var omfattet av hensiktsmessige tekniske sikkerhetstiltak som på en effektiv måte begrenser sannsynligheten for identitetsbedrageri eller andre former for misbruk». I disse reglene og framgangsmåtene burde det tas «hensyn til de berettigede interessene til myndighetene med ansvar for håndheving av loven dersom en tidlig offentliggjøring i unødig grad vil kunne hindre etterforskning av omstendighetene rundt et brudd på personopplysningssikkerheten.»[278]

I den norske personopplysningsloven, der forordningen er gjennomført, er det etter dette innført et unntak. Den registrerte vil her ikke bli underrettet om brudd på personopplysningssikkerheten dersom en slik underretning vil gi informasjon som vil ha betydning for den nasjonale sikkerhet, som vil påvirke forebygging eller etterforsking av straffbare handlinger, eller som er underlagt taushetsplikt i lov eller med hjemmel i lov.[279]

5.2.5 Hvis det ikke er mulig å gi all informasjon til samme tid

Hvis det ikke er mulig at all informasjon blir gitt på samme tidspunkt, kan «den gis trinnvis uten ytterligere ugrunnet opphold.» Det spesifiseres dermed at hvis informasjonen som skal gis må gis i flere omganger, så kan hver utlevering av informasjon skje uten at noen av leveransene blir mer forsinket enn det er grunnlag for.[280]

Slik får man dermed muligheten til å gi beskjed selv om man ikke har nok informasjon til å oppfylle kravene til meldingen i artikkel 33 nr. 3, men den videre informasjonen må da gis kontinuerlig. Behandlingsansvarlige kan etter dette ikke gjemme seg bak at han ikke har informasjon nok til å melde fra i det hele tatt etter artikkel 33 nr. 3.

Kravene i nr. 3 er dermed ikke absolutte, det er mulig å melde ifra selv om man ikke har nok informasjon til å oppfylle disse kravene. Dette kan sies å bidra til forordningens formål, ved at den registrertes rettigheter beskyttes også der det vil ta lengre tid å ha nok informasjon til å gi en tilstrekkelig oversikt over bruddet og følger av dette.

5.2.6 Dokumentasjonsplikt for brudd på personopplysningssikkerheten

Det fremgår av artikkel 33 nr. 5 at «Den behandlingsansvarlige skal dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene

[278] For 2016/679/EU Fortalepunkt 88

[279] Personopplysningsloven §16 (4)

[280] For 2016/679/EU art 33 nr. 4

av det og hvilke tiltak som er truffet for å utbedre det. Denne dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere samsvar med denne artikkel.»[281]

Etter ordlyden gjelder dette dermed også dersom det er vurdert at bruddet ikke er meldepliktig etter artikkel 33 nr. 1., slik at også brudd som sannsynligvis ikke vil innebære en risiko skal dokumenteres på denne måten.

5.2.7 Vurdering av om det er skjedd et brudd på personopplysningssikkerheten.

For vurderingen av om det er skjedd et slik brudd på personopplysningssikkerheten at det skal meldes fra etter artikkel 33, gis det veiledning i fortalens punkt 87. For å vurdere om personopplysningssikkerheten er brutt, bør det etter denne gjøres en undersøkelse av «om alle tekniske og organisatoriske tiltak er blitt gjennomført». Gjennom denne vurderingen avklares det dermed også om den registrerte eller tilsynsmyndigheten skal varsles om bruddet. Videre skal det slås fast «om meldingen ble gitt uten ugrunnet opphold,» og i denne vurderingen skal det «tas særlig hensyn til arten og alvorlighetsgraden av bruddet på personopplysningssikkerheten og konsekvensene og skadevirkningene det har for den registrerte.» Når det er blitt gitt slik melding kan dette videre etter fortalepunktet medføre at tilsynsmyndigheten griper inn, dersom dette er en plikt den har i det enkelte tilfellet etter forordningen.[282]

Etter sammenhengen kan man da se hen til artikkel 32 for å se om tiltak for å møte risikoen er tilfredsstillende utført.

5.2.8 Følger av brudd på personopplysningssikkerheten

De ulike følgene av et brudd på personopplysningssikkerheten utdypes i fortalens punkt 85. Det fremgår her at hvis slike brudd ikke blir tatt hånd om på en passende måte og på riktig tidspunkt, kan brudd på personopplysningssikkerheten «påføre fysiske personer fysisk, materiell eller ikke-materiell skade.» Eksempler på slike skader kan etter fortalepunktet være «tap av kontroll over egne personopplysninger eller begrensning av egne rettigheter, forskjellsbehandling, identitetstyveri eller - bedrageri, økonomisk tap, uautorisert oppheving av pseudonymisering, skade på omdømme, tap av konfidensialitet for taushetsbelagte personopplysninger eller andre betydelige økonomiske eller sosiale ulemper for den berørte fysiske personen.»[283]

[281] For 2016/679/EU art 33 nr. 5

[282] For 2016/679/EU Fortalepunkt 87

[283] For 2016/679/EU fortalepunkt 85

5.3 Plikt til å gi den registrerte beskjed om brudd etter Artikkel 34

5.3.1 Når underrettelsesplikten oppstår

Ved brudd på personopplysningssikkerheten har den registrerte i enkelte tilfeller rett på beskjed om dette. Dette gjelder når «det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter».[284]

Terskelen for krav på underrettelse til den registrerte er dermed høyere enn for plikt til å melde fra om brudd på sikkerheten til tilsynsmyndigheten. Den behandlingsansvarlige vil dermed ha en plikt til å melde fra til tilsynsmyndigheten i flere tilfeller enn han vil ha en plikt til å gi beskjed til den registrerte.

Artikkel 29 gruppen fremhever at den høye terskelen for underrettelse av de registrerte vil hindre at de blir underrettet så ofte og for så ubetydelige sikkerhetsbrudd at de vil gå lei.[285] Ved å ha en høy terskel for når de registrerte skal underrettes, vil underrettelsene ha et alvor over seg og den vil innebære så høy risiko at det vil være forståelig for den registrerte at den får beskjed.

Artikkel 29 gruppen fremholder at risikonivået kan endre seg over tid, slik at risikonivået bør vurderes på nytt etter en stund. Slik kan det som var en lovlig avgjørelse om å ikke underrette den registrerte, med tiden endre seg slik at den registrerte skal ha beskjed.[286]

Dersom den registrerte har krav på underrettelse skal dette skje «uten ugrunnet opphold». Etter ordlyden gjelder det her ikke en slik absolutt tidsfrist som det gjelder etter artikkel 33.[287]

Tidsfristen for underrettelse utdypes i fortalepunkt 86, der det fremgår at underrettelsen bør skje «så snart det med rimelighet er mulig», og det bør skje «i nært samarbeid med tilsynsmyndigheten og i samsvar med retningslinjer utstedt av den eller av andre relevante myndigheter, f.eks. myndigheter med ansvar for håndheving av loven.» Det er flere forhold som kan påvirke tidsfristen for underrettelse. I fortalepunkt 86 utdypes det: «Behovet for å redusere en umiddelbar risiko for skade kan f.eks. kreve at de registrerte underrettes omgående, mens behovet for å gjennomføre egnede tiltak mot fortsatte eller lignende brudd på personopplysningssikkerheten kan berettige en lengre frist for underretning.»[288]

[284] For 2016/679/EU art 34 nr. 1

[285] WP29 (2017) s. 20.

[286] WP29 (2017) s. 22.

[287] For 2016/679/EU art 34 nr. 1

[288]For 2016/679/EU Fortalepunkt 86

5.3.2 Innholdet i underrettelsesplikten

I underretningen skal det gis «en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten og tiltakene nevnt i artikkel 33 nr. 3 bokstav b), c), og d).»[289] Det er dermed kun krav om at noen av opplysningene som skal gis til tilsynsmyndigheten skal gis til den registrerte. Etter dette er det færre krav til opplysningene som skal gis etter artikkel 34 enn etter artikkel 33.

Den registrerte skal få informasjon om navn og kontaktinformasjon til personvernombud eller relevant kontaktpunkt, en beskrivelse av bruddets sannsynlige følger, og hvilke tiltak den behandlingsansvarlige har tatt eller foreslår å ta for å ta hånd om sikkerhetsbruddet.[290]

Dette kan ha å gjøre med at den registrerte ikke har samme muligheter til å gjøre noe med bruddet som det tilsynsmyndigheten har. Opplysninger om «arten av bruddet på personopplysningssikkerheten … kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt»[291], som skal gis til tilsynsmyndigheten etter artikkel 33 nr. 3 bokstav a, vil typisk være mer interessante for tilsynsmyndigheten enn for den registrerte.

Plikten til å underrette den registrerte utdypes i fortalepunkt 86. Her fremgår det at meldingen skal gis «slik at vedkommende får mulighet til å treffe de nødvendige forhåndsregler». Den bør også «inneholde anbefalinger som den berørte fysiske personen kan følge for å begrense mulige skadevirkninger».[292]

5.3.3 Unntak fra underrettelsesplikten

I noen tilfeller er det mulig å gjøre unntak fra underrettelsesplikten i artikkel 34. Dette gjelder dersom vilkårene i bokstav a, b, eller c er oppfylt. Vilkårene er alternative.[293]

Den behandlingsansvarlige plikter ikke å underrette den registrerte om brudd dersom den «har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak», forutsatt at «disse tiltakene er blitt anvendt på personopplysningene som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, f.eks. kryptering».[294]

[289] For 2016/679/EU art 34 nr. 2.
[290] For 2016/679/EU art. 34 nr. 3 b-d.
[291] For 2016/679/EU art. 33 nr. 3 a)
[292]For 2016/679/EU Fortalepunkt 86
[293] For 2016/679/EU art 34 nr. 3
[294] For 2016/679/EU art 34 nr. 3 a)

Et annet unntak fra underrettelsesplikten gjelder dersom «den behandlingsansvarlige har truffet etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen for de registrertes rettigheter og friheter nevnt i nr. 1 vil oppstå».[295]Artikkel 29 gruppen nevner at dette unntaket vil være oppfylt der behandlingsansvarlige har innført tiltak for å stoppe den eller de som har fått tilgang til personopplysningene før de får gjort noe med opplysningene. [296]

Videre åpnes det for unntak fra underrettelsesplikten dersom «det vil innebære en uforholdsmessig stor innsats. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.»[297]

For eksempel kan dette være tilfellet der bruddet har ført til at de registrertes kontaktinformasjon har gått tapt.[298] Dersom et firma med mange registrerte, og der kontaktinformasjonen til de registrerte er blitt manipulert eller slettet, kan det dermed være enklere å gå ut med dette til allmennheten enn å bruke ressurser på å finne denne informasjonen igjen for å underrette den registrerte.

Dersom den behandlingsansvarlige ikke utfører pliktene sine etter artikkel 34, kan tilsynsmyndigheten i enkelte tilfeller kreve at den behandlingsansvarlige utfører et av vilkårene i nr. 3 bokstav c) eller underretter den registrerte dersom dette ikke er gjort. Dette gjelder etter at tilsynsmyndigheten har vurdert «sannsynligheten for at bruddet vil medføre en høy risiko».[299]

Dersom vurderingen som er gjort etter artikkel 34 ikke er forsvarlig, slik at det ikke er blitt underrettet i et tilfelle der det skulle vært det, kan det medføre sanksjoner etter forordningen.[300]

[295] For 2016/679/EU art 34 nr. 3 b)
[296] WP29 (2017) s. 22
[297] For 2016/679/EU art 34 nr. 3 c)
[298] WP29 (2017) s. 22
[299] For 2016/679/EU art 34 nr. 4
[300] WP29 (2017) s. 22. og For 2016/679/EU fortalepunkt 87

6 Avsluttende bemerkninger – hva er viktig for at forordningen skal få praktisk verdi?

Etter å ha gått igjennom det presenterte rettskildematerialet er det tydelig at forordningen bringer med seg praktiske utfordringer. Hvilken praktisk verdi får forordningen? Hva skal til for at den er med på å styrke behandlingssikkerheten for personopplysninger?

En stor endring for den norske rettstilstanden, er at forordningens krav til sikkerhet for behandling av personopplysningene er mye mer generell og overordnet enn det som var tilfellet tidligere.[301] Ved første øyekast kan dette synes å være en svekkelse av behandlingssikkerheten, men dersom forordningen tilnærmes på anbefalt måte, kan den i stedet utgjøre en styrking av behandlingssikkerheten. Det viktigste for å sikre etterlevelse av forordningen og for at den skal få en praktisk verdi, er at de behandlingsansvarlige forstår ansvarlighetsprinsippet og skaffer seg kompetanse til å utøve sin rolle på en tilfredsstillende måte. Slik kan forordningen bli den styrkingen av personvernet den er ment å være.

For å støtte den behandlingsansvarlige vil personvernombudene få en viktig rolle. ENISA fremhever at det er viktig at disse har både en god forståelse av behandlingssikkerhet, og at de har tilstrekkelig IT-kompetanse for å forstå moderne teknologi og de relevante «security best practices»[302] Det bør videre utarbeides en oversikt over hvilke ferdigheter og krav det bør settes til personvernombudene.[303]

Dersom det utføres en tilstrekkelig risikovurdering, vil elementer ved behandlingen som får betydning for risikonivået identifiseres, og gjennom de leddene som ble presentert i kapittel 4 får behandlingsansvarlig, dersom han tar ansvarlighetsprinsippet seriøst, en god forståelse for de ulike sidene av behandlingen som får betydning for sikkerheten for personopplysningene. Da er mye gjort.

ENISA fremhever at risikovurderingen vil være ulik for alle forskjellige behandlinger av personopplysninger, og at det derfor er viktig at behandlingsansvarlige har en god forståelse av behandlingen før han gjør denne vurderingen, slik at den kan tilpasses den enkelte behandlingen, og slik at sikkerhetstiltakene kan tilpasses dette.[304]

[301] Personopplysningsloven (2000) og personopplysningsforskriften (2000)
[302] ENISA (2017) s. 52
[303] ENISA (2017) s. 53
[304] ENISA (2017) s. 52

At det etter artikkel 83 kan ilegges høye bøter for overtredelse av forordningen[305], er en faktor som sannsynligvis vil bidra til at de behandlingsansvarlige ønsker å arbeide mot etterlevelse av forordningen.

ENISA fremhever viktigheten av at det må gis veiledning fra tilsynsorganer og EU-organer, slik at behandlingsansvarlig og databehandler får støtte til å kunne oppnå etterlevelse av forordningen. ENISA peker videre på at det nok ikke er mulig med retningslinjer som skal passe alle, men at de ulikhetene som følger med all databehandling må tas hensyn til.[306]

Viktigheten av sertifiseringsnormer for etterlevelse blir fremhevet av ENISA som viktig for at behandlingsansvarlige skal kunne oppnå og demonstrere hva passende sikringstiltak vil være, og etterlevelse i den enkelte situasjon. [307]

Det bør i følge ENISA også opprettes en metodikk for å vurdere både informasjonssikkerhetsrisiko og personopplysningsrisiko til samme tid. I utgangspunktet har disse to vinklingene på risiko forskjellige innfallsvinkler, da informasjonssikkerhetsrisikoen er en vurdering av hvilken risiko behandlingen vil ha for den behandlingsansvarlige, mens risikoen for behandling av personopplysninger, dreier seg om hvilken risiko for den registrerte behandlingen utgjør.[308]

Avslutningsvis bør det ses på som en fordel å være i samsvar med forordningen, slik at behandlingsansvarlige bør strebe etter etterlevelse som en konkurransefordel.[309] Det vil være en stor konkurransefordel å tilby løsninger som gjør etterlevelse av forordningen enklere for den behandlingsansvarlige. Det er likevel viktig å understreke at personvernrettslige systemer ikke i seg selv er nok. Den behandlingsansvarlige må ta ansvarlighetsprinsippet seriøst, og sikre etterlevelse i alle behandlingens ledd.

[305] For 2016/679/EU art. 83. nr. 1 og nr. 6.
[306] ENISA (2017) s. 52
[307] ENISA (2017) s. 53
[308] ENISA (2017) s. 54
[309] ENISA (2017) s. 54

7 Litteraturliste

7.1 Litteratur

Arnesen (2009) Arnesen, Finn og Are Stenvik. *Internasjonalisering og juridisk metode Særlig om EØS-rettens betydning i norsk rett*, Oslo: Universitetsforlaget, 2009.

Bygrave (2014) Bygrave, Lee A. *Data Privacy Law An international Perspective*, Oxford: Oxford University Press, 2014.

Carey (2018) Carey, Peter, Damien Welfare, Estelle Dehon mfl. *Data Protection A Practical Guide to UK and EU Law,* femte utgave, Oxford: Oxford University Press, 2018

Datatilsynet (2018) *Veileder internkontroll og informasjonssikkerhet*, 19.06.2018. [https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/] [31.10.2018]

Datatilsynet (2017b) *Ni helseforetak er varslet om gebyr.* (2017) https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/ [Sitert12.11.2018]

Det norske akademis ordbok (udatert) *kryptere*. (udatert), https://www.naob.no/ordbok/kryptere [Sitert 21.09.2018]

ENISA (2016) *Guidelines for SMEs on the security of personal data processing,* 2016. [DOI 10.2824/867415] [Sitert 3.10.2018]

ENISA (2017) *Handbook on Security of Personal Data Processing,* 2017. [DOI 10.2824/569768] [Sitert 3.9.2018]

The European Commission (2018). *THE ARTICLE 29 WORKING PARTY CEASED TO EXIST AS OF 25 MAY 2018.* (2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492 [Sitert 19.11.2018]

Fredriksen (2014) Fredriksen, Halvard Haukeland og Gjermund Mathisen. *EØS-rett,* 2.utgave, Bergen: Fagbokforlaget, 2014

Fredriksen (2018) Fredriksen, Halvard Haukeland og Gjermund Mathisen *EØS-rett*, 3.utgave, Bergen: Fagbokforlaget, 2018

Hotvedt (2017) Hotvedt, Signe Karin. *Hackere lammer datasystemer på sykehus.* (2017), https://www.nrk.no/urix/dataangrep-lammer-it-systemer-pa-sykehus-1.13514766 [sitert 24.11.2018]

ISO (udatert). *ISO/IEC 27000 family - Information security management systems* . (udatert), https://www.iso.org/isoiec-27001-information-security.html [Sitert 24.10.2018]

Schartum (2018) Schartum, Dag Wiese. *Digitalisering av offentlig forvaltning – Fra lovtekst til programkode*. Bergen: Fagbokforlaget, 2018.

Skullerud (2018) Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad mfl. *Personvernforordningen (GDPR) Kommentarutgave*. Oslo: Universitetsforlaget, 2018

Stemsrud (2015) Stemsrud, Odd. *EØS-rett i et nøtteskall.* (1. utgave) Oslo: Gyldendal Norsk Forlag AS, 2015.

Voigt (2017) Voigt, Paul og von dem Bussche, Axel. "Scope of Application of the GDPR" i *The EU General Data Protection Regulation (GDPR)* Cham: Springer, Cham, 2017, side 22, (sitert fra Springer link) DOI https://doi.org/10.1007/978-3-319-57959-7_2

WP29 (2014) Article 29 Data Protection Working Party (2014) *Opinion 03/2014 on Personal Data Breach Notification*, 25.03.2014. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf] [Sitert 11.11.2018] (693/14/EN WP 213)

WP29 (2017) Article 29 Data Protection Working Party. (2017) *Guidelines on Personal data breach notification under Regulation 2016/679,* 3 Oktober 2017 (sist revidert og vedtatt 6. Februar 2018). [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052] [Sitert 17.10.2018](18/EN WP250rev.01)

7.2 Lover og internasjonale rettskilder

EMK Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter Roma 4. november 1950

Convention 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981

Directive 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Personopplysnings-loven (2000)	Lov 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysnings-loven) (opphevet)
Personopplysnings-forskriften (2000)	Forskrift 15.12.2000. nr. 1265 Forskrift om behandling av personopplysninger (personopplysningsforskriften) (Opphevet)
For 679/2016/EU	EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR]
Personopplysnings-loven (2018)	Lov 15.06.2018 nr.38 Lov om behandling av personopplysninger (personopplysingsloven)

7.3 Internasjonal praksis, EU-praksis og forvaltningspraksis

I v. Finland,	Case of I v. Finland Application no. 20511/03, 17.07.2008
Case C-131/12 Google	Google Spain SL, Google Inc. v Agencia Española de Protección de datos (AEPD), Mario Costeja González ECLI:EU:C:2014:317.
Personvernnemda (2014)	Personvernnemda. (2014) PVN-2014-01 Skan-Kontroll, 27. oktober 2014. [https://www.personvernnemnda.no/pvn-2014-01] [Sitert 6.11.2018]
Case C-582/14 Breyer	Patrick Breyer v Bundesrepublik Deutschland ECLI:EU:C:2016:779.
Case C-434-16 Nowak	Peter Nowak v Data Protection Commissioner ECLI:EU:C:2017:994
Datatilsynet (2017a)	*Varsel om vedtak – overtredelsesgebyr – Oslo Universitetssykehus HF*, 24.10.17. [https://www.datatilsynet.no/globalassets/global/regelverk/avgjorelser-datatilsynet/2017/16-01531-51-varsel-om-vedtak--overtredelsesgebyr---oslo-universitetssykehus-hf-222949_4_1.pdf] [12.11.2018]