Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for lærerutdanning

Torstein Fjellingsdal

GDPR

Har den gjort nok for å beskytte brukerdata?

Bacheloroppgave i Arkiv- og samlingsforvaltning
Veileder: Ingeborg Stensrud

Mai 2019

NTNU
Norwegian University of
Science and Technology

Torstein Fjellingsdal

GDPR

Har den gjort nok for å beskytte brukerdata?

Bacheloroppgave i Arkiv- og samlingsforvaltning
Veileder: Ingeborg Stensrud
Mai 2019

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for lærerutdanning

NTNU
Kunnskap for en bedre verden

Innholdsliste:

1. Introduksjon til oppgaven.

Dette er en introduksjon til temaet «Har GDPR gjort nok for å beskytte brukerdata?» som er hovedtema for denne Bachelor-oppgaven. Det var et spørsmål som dukket opp i løpet av mine studier på NTNUs arkiv- og samlingsforvaltningslinje, det var en nysgjerrighet som har også blitt mer aktiv etter jeg har sett flere tilfeller av logging av aktivitet og offentlige skandaler som har omringet temaet om det nye lovverket som kom fra EU kalt GDPR – General Data Protection Regulation, og om denne reguleringen har gjort nok for å forebygge slike ting i fremtiden.

Denne oppgaven går ut ifra at leseren har litt grunnleggende kunnskap i hvordan arkiver fungerer, men det kommer til å bli forklart hva begrepene som er brukt betyr, og hvordan denne oppgaven har brukt dem. Dette er for å la flere lesere forstå hva som blir diskutert uten at det blir altfor teknisk.

Denne oppgaven går også ut ifra at leseren kan Norsk-Bokmål, om det brukes sitater fra engelske kilder så kommer det til å bli fulgt av en oversettelse, men jeg innser at noe av budskapet i teksten kan gå tapt og at forfatteren har sagt det best på sitt eget språk. Det er derfor at det originale sitatet er lett tilgjengelig slik at konteksten som den originale forfatteren brukte for sitt sitat er bevart.

Denne oppgaven er et litteraturstudium med et fokus på avisartikler. Dette er i hovedsak på grunn av at det finnes veldig få akademiske kilder om nettopp denne delen av temaet om GDPR. Den nye forordningen har vert i konsept-stadiet side 2016, men den ble ikke iverksatt før Mai 2018 og dermed har det vært ganske vanskelig å finne relevant data både for omfanget til GDPR og effekten den har hatt på arkivfaget. Jeg innser at mangelen på akademisk vekt i oppgaven er en betydelig svakhet for analysen, men jeg mener fortsatt at dette temaet er relevant. Det fins såpass lite om det, at en tidlig analyse av forordningen og omfanget det nye lovverket har er relevant, til tross for denne mangelen av akademiske kilder.

Hvor mye reguleringen påvirker faget generelt kan måles med mengden rettigheter individer får over data og informasjon som blir lagret om dem. Når jeg sier at det er ganske vanskelig å finne relevante akademiske kilder så mener jeg at jeg kan finne 15.000 treff på google scholar og studentbiblioteket hos NTNU om «hva» GDPR er og hvordan systemer skal sikres for å møte kravene, men svært få av disse kildene dokumenterer hva disse forandringene betyr i detalj og enda mindre om hvordan dets implementering påvirker arkiver.

I hovedsak kommer jeg til å prøve å finne akademiske kilder der jeg kan, men på grunn av hvor lite som fins av akademiske kilder om dette, så kommer mye av det til å være kilder i media.

Jeg valgte å skrive om GDPR og hvor omfattende den er, mest på grunn av omfanget av hva som ble påvirket av denne, for eksempel arkiver, eldre samlinger og håndteringen av personlig data via tredjeparter. Først var dette nytt og for mange ukjent siden folk flest vet kanskje ikke om hva GDPR står for, og potensielt enda mindre om hva som skjedde rundt opphavet til dette nye lovverket. Den gjennomsnittlige internett-brukeren fikk sikkert bare 10+ eposter om at flere nettsider og tjenester hadde oppdatert sin personvernspolicy som betydde at de måtte godta den nye policyen, og kanskje vis de leste litt så dukket opp ordene «I henhold til GDPR»

GDPR er et nytt og omfattende direktiv som påvirker måten tjenester og nettsteder lagrer informasjonen til brukerne sine. Dette var relativt banebrytende for vi hadde veldig få lover spesifikt for måten digital informasjon ble lagret på. EU og andre land hadde egne lover på hvordan personlig dokumentasjon skulle håndteres, men mye av det ga ingen spesifikke regler for hva som kunne lagres om hvem, hvor lenge det kunne lagres og potensielt hvem denne informasjonen ble delt med.

Når det gjelder digitale lovverk så er GDPR fortsatt nytt, og på grunn av måten den påvirker informasjon og data innenfor og utenfor EU så kan man trygt si at det digitale markedet kunne ikke ignorere det nye lovverket. Som en følge av dette ble GDPR ikke bare ansett som en veldig omfattende lov, men også en globalt anerkjent lov når det gjelder behandling av Data på grunn av Europas tilstedeværelse i den digitale økonomien.

Som en student i arkiveringsfaget virket dette som en veldig relevant del av utdanningen min. Det eneste problemet var bare at den er for ny til å være med i et offentlig pensum i mange tilfeller. Og dermed er denne Bacheloroppgaven et forsøk på et solid innblikk i det nye lovverket, og hvordan det kan påvirke arkivfaget i et globalt perspektiv, ved at den gir flere rettigheter til brukeren i forhold til dokumentasjon som lagres.

Med «Har GDPR gjort nok for å beskytte brukerdata?» så mener jeg i denne oppgaven: **hvordan var ting før GDPR dukket opp i forhold til beskyttelse av brukerdata, og hvordan har GPDR påvirket dette generelt?** Jeg skal se nærmere på opphavet til GDPR og omstendighetene som gjorde en slik lov nødvendig for å gi mer kontekst til denne problemstillingen.

Siden «gjort nok» kan være subjektivt er det noe rom for diskusjon angående hva som er et objektivt godt mål for at dette kriteriet har blitt møtt. Jeg kommer til å lage en konkret liste over forandringer som GPDR har påvirket, i tillegg til en forklaring på hvordan denne forandringen kanskje har påvirket arkivering generelt.

Først så må noen grunnleggende prinsipper diskuteres i forhold til implementeringen av GDPR. Dette er for å dokumentere objektive mål når man skal vurdere noe subjektivt som denne problemstillingen. Dette hjelper også til å etablere et startpunkt for vurderingen. Målet mitt er å gi leseren så mye informasjon om temaet som mulig, slik at de kan da ta en informert beslutning, med min egen konklusjon som en sum av det jeg har funnet ut.

Hovedtemaene er «Hva påvirker GDPR?», med dette spørsmålet mener jeg å kartlegge hva GDPR har en effekt på, det vil si hvor mye av arkivfaget påvirker den? I virken grad? og gi et generelt bilde over effekten av GDPR.

Det er også en del andre spørsmål som er diskutert når GDPR er nevnt, for eksempel er det temaet om «Grandfathering»? Det vil si: Hvordan håndterer GDPR systemer og arkiver som ble etablert før implementeringen av GDPR? Grandfathering er et begrep som betyr at en gammel regel eller lov fortsatt gjelder for eldre og eksisterende tilfeller, mens en ny lov gjelder for fremtidige tilfeller hvor regelen eller loven gjelder. Som regel er unntak som disse ganske små, eller ofte bare gjelder for en begrenset periode.

En annen målestokk for GDPR er temaet om det digitale sikkerhetsklimaet og problemet med uautorisert innsamling av data. Før implementeringen av GDPR var det ikke uvanlig at hackere hadde funnet en svakhet i et system og fått tak i flere hundre tusen, om ikke millioner brukeres data. Og ofte kom det fram på et senere tidspunkt at firmaet selv hadde solgt informasjonen til en ukjent tredjepart, og de kalte det for et ‘hackerangrep’ for å gi inntrykket av at de hadde ingen kontroll over dette, og at firmaet selv ikke kunne klandres.

Det er også mye snakk om at brukerne har fått flere rettigheter om informasjonen sin via GDPR. Blant annet er et stort tema er «retten til å bli glemt». Det vil si at brukeren selv kan ta kontakt med firma eller arkiv som har informasjon om brukeren og har nye rettigheter overfor hva som kan gjøres med denne informasjonen. Om denne retten har blitt brukt har firmaet opptil 30 dager å følge opp.

Arkivfaget i Norge er basert på konseptet å bevare arkiv som har kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon. Implementeringen av GDPR involverer en rekke nye regler, rettigheter og

ansvar, ikke bare for arkivene selv men også for brukerne av arkivene. Dette gjelder ikke bare private arkiver heller, dette angår i stor grad alle sektorer som arkiverer dokumentasjon om personer. Om GDPR har gjort nok for å beskytte brukerdata er en analyse av hvor mye GDPR faktisk har påvirket arkivfaget som vi skjenner det og hvordan det forandrer hvordan arkiver skal forholde seg til brukerdata. Brukerdata i denne konteksten er brukt for å beskrive all informasjon som angår en bruker av et system.

Det er også mange som ser alvoret med mangelen på lovverk som dette. Sjefen for Apple, Tim Cook, advarte om at personopplysninger er en lukrativ vare for internettgigantene da han talte på en konferanse i Brussel 24. oktober 2018. Det digitale markedet har vokst til et av de største markedene i verden, og hvordan vår personlige informasjon, fra det hverdagslige til det dypt personlige, brukes mot brukerne med militær effektivitet. Han peker også ut at dette er faktisk overvåkning, og at personopplysninger kun beriker de som samler dem inn. Til slutt sa han at det var på høy tid at resten av verden fikk lignende lovverk, inkludert Amerika. (NTB, 2018)

Det er også sitater fra andre kilder, for eksempel Samuel Greengards artikkel om GDPR kalt «Weighing the impact of GDPR» påpeker han at Alison Cool, en assisterende professor i antropologi ved University of Colorado, Boulder, sier at «There are a lot of questions and ambiguities that must be addressed, but it’s clear that the GDPR will significantly change the data landscape». (Greengard. 2018 S. 16)

Dette er spesielt relevant fordi det digitale markedet kommer bare til å vokse. Evnen og muligheten til å beskytte personopplysningene sine er farlig territorium, fordi alt kan gå for langt, det kan ha uforutsette konsekvenser dersom det ikke blir håndtert ordentlig, og dette kan ha enorme effekter på arkivfaget som vi skjenner det.

2. Hva er GDPR?

Denne definisjonen er hovedsakelig hentet fra boken «EU General data protection regulation (GDPR): an implementation and compliance guide» som ble skrevet av gruppen IT Governance Privacy Team. IT governance er en gruppe med direkte tilknytning til EU. (IT governance. U.Å)

EUs «General Data Protection Regulation» er en ny digital forordning. En forordning i EU er betegnelsen på reguleringer som har bindende virkning i medlemsstatene, fra det tidspunktet som er blitt bestemt. Det er ikke nødvendig for medlemstatene selv å gjennomføre denne i

lokalt lovverk, i motsetning til direktiver. GDPR trådte i kraft 25. Mai 2018 og er en omfattende regulering som skal beskytte data og personlig informasjon til alle innbyggere i EU og EØS (Europeiske økonomiske samarbeidsområde) i tillegg til strengere regulering om eksportering av denne dataen til land utenfor EU og EØS.

GDPR er en regulering som gjelder når en organisasjon samler inn data i noen form fra individer i EU, eller en organisasjon som samler inn data på vegne av noen andre. Men den gjør seg bare gjeldende dersom informasjonen tilhører en person fra EU-området. Flere tilfeller gjelder også reguleringen for organisasjoner utenfor EU, dersom de samler inn informasjon om personer som bor i EU-området. Dette gjelder kun for data samlet inn om en person for en aktivitet som er kun personlig, og ikke relatert til arbeid eller kommersiell bruk. Det vil si at loven er strengere i tilfeller der de har tenkt å bruke informasjonen din for å markedsføre produkter eller tjenester til deg, eller lignende.

Ifølge GDPR så er «Personlig Data» all informasjon som kan knyttes til en enkelt person. Det vil si all informasjon som er relatert til den personens private eller offentlige liv. Dette kan være alt fra en persons navn, vedkomnes adresse, et fotografi, en epost adresse, bank informasjon, ens aktivitet på sosiale medier, informasjon relatert til ens medisinske historie, eller en datamaskins IP-adresse. Den største forandringen GDPR har gitt til definisjonen av informasjon som kan brukes til å identifisere noen er at IP-adressen teller som slik informasjon, men dette sier litt om hvor omfattende GDPR er i forhold til eldre lover om beskyttelse av brukerdata.

Artikkel 5 av GDPR forklarer de grunnleggende prinsippene som skal brukes for all data som blir samlet inn i tilfellene der GDPR gjelder. Disse kommer i en lett liste, og igjen gir et godt inntrykk av hvor grundig denne reguleringen er.

Det første prinsippet er at all personlig data skal kun bli samlet lovlig og åpent. Dette er grunnen til at alle nettsteder som vil lagre informasjon om deg som bruker, gjør deg oppmerksom på at de vil lagre informasjon, men at du også må godta det. Riktig nok bruker de fleste dette som en betingelse for bruk av tjenesten. Men nå er de mye strengere om å være åpen med brukerne angående informasjonsinnsamling. Et godt eksempel på dette er hvordan alle nettsteder må be om samtykke for å bruke informasjonskapsler – eller «Cookies» som kan brukes til å identifisere brukeren. Dette gjelder spesielt når GDPR har bestemt at en IP-adresse teller som informasjon som kan brukes til å identifisere en bruker. (It Governance. 2017. S 100-107)

Prinsipp nummer to er at data skal kun innsamles for et spesifikt og lovlig bruksområde. Det vil også si at de må kunne forklare hva de skal bruke informasjonen din til, og nøyaktig hvilken informasjon de vil lagre. Dette knyttes også til prinsipp 1 i at de må fortelle hva de har tenkt å bruke informasjonen din til, om du godtar det. Informasjonen skal heller ikke viderebehandles på en måte som separerer informasjonen fra formålet den ble samlet in for. (It Governance. 2017. S 108-109)

GDPRs tredje prinsipp er at all informasjon må være relevant og begrenset til hva som behøves i forhold til bruksområdet. Dette knyttes til prinsipp 2 i mengden data som skal samles inn, og at datakontrollør må ikke bare vite hvor mye informasjon som skal lagres, men også at de må kunne forklare hvorfor hver del av data er relevant til bruksområdet. (It Governance. 2017. S 109-110)

Datakontrollør er begrepet brukt for å beskrive firma, organisasjoner eller andre enkeltgrupper som er påvirket av GDPR, og behandler data som lovverket har en effekt på. Datakontrollør er spesifikt brukt for å beskrive de som samler inn eller behandler data om brukere. Begrepet databehandlingsansvarlig har også blitt brukt av flere kilder, forkortet med «DBA»

Prinsipp fire er at all personlig informasjon skal være nøyaktig og oppdatert. Dette kan virke som et mindre poeng, men dette betyr at hvis informasjonen som har blitt samlet inn ikke er nøyaktig lenger, er den heller ikke lovlig å beholde. Dette er et prinsipp av loven som håndterer eldre systemer som ikke har blitt oppdatert til GDPRs regulering. (It Governance. 2017. S 111-112)

For å forklare dette litt bedre så betyr det at informasjon som lagres er ikke lenger er lovlig dersom det angår tilfeller der GDPRs regulering gjelder. For å gjøre denne informasjonen lovlig må de stemme overens med GDPR, i tillegg til at de trenger nytt samtykke fra brukeren som informasjonen gjelder for siden de må oppdatere brukerdataen slik at den er relevant. I tillegg må de kunne forklare hvilken informasjon de skal samle inn, hvilket formål denne informasjonen skal brukes til og de må begrense denne informasjonen til dette formålet.

Prinsipp fem av GDPR er at personlig data skal kunne brukes til å identifisere hvem denne informasjonen tilhører, men kun så lenge at dette er relevant til formålet bak innsamlingen av data. (It Governance. 2017. S 113-114)

Og til sist er det prinsipp seks, at all personlig data som innsamles, skal gjøres på en slik måte at den er sikret mot tilgang fra de som ikke har mottatt samtykke fra brukeren. Dette gjør også firma som samler inn data ansvarlig for å sikre seg at systemene deres er sikret, og at hvis de

skal samle inn informasjon via en tredjepart så må de forsikre seg om at denne tredjeparten også kan garantere sikkerhet av data. (It Governance. 2017. S 114-116)

Dette vil si at i tilfellet med hackerangrep eller lignende brudd i sikkerhet som har endt med at data om flere tusener brukere har kommet på avveie, som kan være alt fra personlig informasjon som adresser, telefonnummer og annen data, til mer ekstreme tilfeller der man ser kredittkortinformasjon og personnummer. Så er det firmaene som ble hacket som blir stilt ansvarlig i forhold til GDPR. Dette hjelper også til med å forebygge at informasjon og data blir lekket til tredjeparter med tanke på hvor alvorlig dette er hos organisasjoner som Interpol, som vurderer lekkasjer av informasjon og data i samme grad som hackerangrep. (It Governance. 2017. S 116-120)

Dette er kun hovedprinsippene i GDPR, men forskjellige artikler i GDPR gjør reguleringen mye mer omfattende, det er verdt å nevne i disse artiklene er artikkel 17, eller «Retten til å bli glemt», og dette gir brukere en lovlig rett til å kreve at informasjon om en skal slettes. For eksempel om man ikke lenger er kunde hos en tjeneste, har man en rett til å kreve at alle personopplysninger de har om deg skal fjernes. (It Governance. 2017. S 195)

I artikkel 20 er det også en rett til portabilitet, det vil si at du kan kreve at informasjonen din skal overføres fra en datakontrollør til en annen. Denne retten kan også brukes til å gjøre seg selv til sin egen datakontrollør, og dermed kreve at du får overført informasjonen til deg selv. (It Governance. 2017. S 200-201)

Det er også en egen artikkel om hvordan samtykke skal kunne gis på en forståelig måte. Du kan ikke lovlig gi samtykke om du ikke kan lese eller forstå avtalen du godtar. Dette har ikke gjort mye for å påvirke måten firma kan vise til et dokument på 20 sider om «sluttbrukeravtale» og en knapp som sier «godta» eller «ikke godta» på bunnen. Med denne artikkelen har en påvirkning på brukeren og på hvordan nettsteder kan samle inn informasjonen om han eller henne ettersom de er lovlig pålagt å motta samtykke fra brukeren i tilfellet med «Cookies» - en form for data som blir lagret som kan brukes til å identifisere systemet til brukeren. (It Governance. 2017. S 208-209)

Noe som er viktig å nevne er at når firma og databehandlingsorganer skal møte GDPRs regulering, så må de kunne demonstrere at alle systemene fungerer innenfor hva reguleringen tillater. Hvor omfattende dette har påvirket bedrifter og organisasjoner kommer helt an på hvor mye datainnsamling bedriften brukte, og hvor mye som var i strid med reguleringen. Og

med oppfølging så ser man at til tross for at ting kan være GDPR-godkjent så må de fortsette å følge reguleringen for å være tillat lovlig bruk av data fra EU.

Dette høres kanskje ikke så ille ut, helt til man innser at avvik fra reguleringen kan resultere i en bot fra EU kan være opptil 20 millioner euro, og en potensiell kriminalundersøkelse via Interpol eller en lokal myndighet. Dette er ansett som EUs metode for å stille datakontrollører ansvarlig for brukerdata som de samlet inn. Disse bøtene kan også være 4% av den globale omsetningen til et firma, dersom dette utgjør enda mer. For større internasjonale firma betyr dette at gebyr og bøter kan komme opp i milliardsummer. (It Governance. 2017. S 288-290)

Når EU kommer med en ny forordning vil det si at lokale regjeringer og myndigheter strengt tatt ikke trenger å innføre lokale lover som reflekterer EU-lovene, de trenger bare å sørge for at det er oppfølging av disse lovene lokalt. Det er mange medlemsland i EU som oversetter disse lovene til lokale lover og Norge er ikke ett unntak her. GDPR fikk Norge til å innføre en oppdatert lov om behandling av personopplysninger, eller Personopplysningsloven. Denne loven erstatter da den tidligere personopplysningsloven fra 14. April 2000, og fungerer som vår lokale implementering av GDPR. (Andersen, 2019)

«Ny lov om behandling av personopplysninger ble vedtatt 15. juni 2018 og trådte i kraft 20. juli 2018. Den nye loven gjennomfører EUs personvernforordning (GDPR) i Norge og gjør personvernforordningen til norsk lov. EU-direktiv 95/46, personverndirektivet, og personopplysningsloven fra 2000, er opphevet.» - (Kommunal- og moderniseringsdepartementet. 2018)

3. En analyse av opphavet til GDPR

GDPR som konsept er basert på eldre prinsipper som allerede fantes i EUs deltagerstaters lokale lover, men denne oppdaterte reguleringen av loven var et stort steg i rett retning. Guy Bunker, som jobber for itproportal.com, skriver at i 2016 viser mye data fra PwC – Pricewater HouseCoopers at det var ekstremt mye finansiell kriminalitet som foregikk på nettet. Så lite som 1 av 5 firma med digitale løsninger i UK gjennomførte sikkerhetsrutiner for å beskytte brukerne sine mot forskjellige typer farer, som for eksempel identitetstyveri og svindel i løpet av de siste 2 årene. Til tross for at slike typer cyberkriminalitet hadde blitt stadig mer og mer vanlig i det digitale markedet. (Bunker. 2017)

Pricewater HouseCoopers er et multinasjonalt «professional services» nettverksfirma. Det vil si de ansetter profesjonelle med spesialtrening i forskjellige typer arbeid, også kjent som

spesialister som kan gjennomføre arbeid og prosjekter som krever profesjonell lisens, for eksempel ingeniører, arkitekter, doktorer og advokater. PwC fungere altså da som et profesjonelt nettverk for spesialister og arbeidsgivere.

Cyberkriminalitet: En stadig mer vanlig form for kriminalitet som i hovedsak skjer online, men har veldig reelle og mulig katastrofale følger. Dette kan være alt fra å få et passord frastjålet, til noe veldig privat, dette kan ansees å være kanskje relativt mildt. Men i de verste tilfellene kan de få tak i spesielt sensitiv informasjon, for eksempel personnummeret til en bruker, og dette kan brukes av kriminelle.

For eksempel i april 2014 var et sikkerhetshull i alle OpenSSL-baserte nettsteder oppdaget, dette fikk mye oppmerksomhet på grunn av hvor omfattende denne skaden mulig var ettersom det ga uautorisert tilgang til data som folk trodde hadde vært sikret. Dette sikkerhetshullet fikk navnet «Heartbleed», på grunn av programvaren som ble brukt for å benytte seg av dette hullet. Det tok 6 dager etter oppdagelsen skjedde før det ble oppdatert, og selv dette trenger oppfølging av de enkelte nettstedene for å fjerne sikkerhetshullet. Men så mye som 45 dager etter implementeringen av koden som skulle fikse dette var det fortsatt over 800.000 populære nettsteder som hadde dette problemet. (Synopsis. 2014)

En stor del av dette handler om en stor hendelse i media angående et firma ved navn Cambridge Analytica, et underfirma av SCL gruppen – en større datainnsamlingsgruppe. Cambridge Analytica er et britisk IT firma som spesialiserte seg i forskning og «strategisk kommunikasjon», mens det var Cambridge som hovedsakelig ble avslørt i offentligheten som gruppen som stod bak det hele. SCL gruppen ble også fort oppdaget som firmaet Cambridge tilhørte og ble ikke spart for lovlige og offentlige konsekvenser.

Det mangler en god akademisk kilde som omfatter akkurat dette, men det eksisterer hundretalls artikler fra mange forskjellige nyhetsorganisasjoner som omtaler nettopp denne hendelsen. GDPR var fortsatt i planlegging og diskusjonsstadiet når hendelsene rundt Cambridge Analytica og SCL-gruppen skjedde, og det er kun spekulering om disse hendelsene framskyndet den nye reguleringen.

En av de mest omfattende artiklene som kartlegger det hele tilhører BBC – The British Broadcasting Corporation. Men igjen, mengden journalistikk gjort om denne saken kan hentes fra nesten alle nyhetsorganisasjonene på nettet. Via litt søk blant andre nyhetsorganer kan man se at det som BBC har skrevet samsvarer godt med informasjonen.

Grunnen til at jeg for fokusert på BBC sin artikkel er fordi at de er en av de største nyhetsorganene, og når alle sier det samme er det ikke mye rom for tolkning. Og en organisasjon som BBC kan ansees som en pålitelig kilde på grunn av nyhetsorganets lange historie og gode rykte når det kommer til objektiv observasjon av hendelser. Nyhetsorganet har i de siste årene (2016-2019) produsert mer sosialpolitisk innhold med en veldig klar bias, men dette ser ikke ut til å ha påvirket akkurat denne artikkelen.

Det hele startet i 2014 da Facebook ga ut en quiz som skulle la brukere finne ut sin personlighetstype. Denne quizen ble utviklet av Aleksandr Kogan ved Cambridge Universitet. Universitetet er ikke i relasjon til Cambridge Analytica. I seg selv virket ikke dette som noe spesielt brudd av troverdighet eller etikk, helt til Christopher Wylie som jobbet hos Cambridge Analytica ble oppmerksom på noe ekstraordinert, han fant ut at på grunn av mengden data som ble hentet inn fra de 270.000 brukerne som tok quizen, så ble informasjon til over 50 millioner brukere samlet inn i tillegg på grunn av metoden denne appen samlet inn data på ens sosiale nettverk av venner og bekjente. Problemet begynte, når ca 49.7 millioner brukere ikke hadde noen kontroll over at informasjonen deres ble samlet inn, og var ikke blitt gjort klar over at dette hadde skjedd heller.

Problemet ble større når det ikke fantes et solid regelverk for hvem firma som Cambridge kunne dele denne informasjonen med. Facebook fant ut om dette i ettertid, og har siden den gang fjernet appen, siden den åpenbart brøt med Facebooks eksisterende regler. Men skaden var teknisk sett allerede gjort, og dette endte med at Facebooks Mark Zuckerberg måtte gå til den amerikanske kongressen og sa at de ville implementere strengere krav for datasikkerhet for brukerne. Denne situasjonen fikk også lederne i det europeiske parlamentet til å undersøke om dataen som ble samlet inn her hadde blitt brukt for cyberkriminell aktivitet. (Kleinman. 2018)

Om selv-regulering og pragmatisme hadde fungert, så hadde vi ikke konstant sett på framsidene og på nyhetene om hvordan folk hadde blitt frarøvet seg nesten alt, og EU hadde ikke hatt et behov for GDPR, men som det var, så måtte de implementere dette for å beskytte befolkningen i EU. Så til tross for at GDPR i mange tilfeller kommer til å kreve stor forandring igjennom organisasjoner, kommer reguleringen til å sikre større beskyttelse for individuelle rettigheter i tillegg til å gi organisasjonene en bedre måte å få korrekt og relevant data for sitt eget bruk. Dette kommer til å gjøre ting lettere og mer kostnads-effektivt å navigere en stadig mer komplisert verden av data-sikkerhet. (Bunker. 2017)

Oversatt fra Guy Bunkers artikkel – noen konkluderende ord om opphavet og ikke minst behovet for GDPR i etterkant av det man kan se på som en stadig økende risiko for cyberkriminalitet.

4. Litt om Datatilsynet.

All informasjonen om Datatilsynet kommer fra deres egne sider.

Når det gjelder oppfølging av det nye lovverket i personopplysningsloven så er det Datatilsynet har det overordnede ansvaret for å påse at loven blir fulgt. Datatilsynet er et uavhengig forvaltningsorgan som først ble opprettet i 1980, de er administrativt underordnet Kongen og kommunal- og moderniseringsdepartementet, også forkortet til KMD. Med uavhengig betyr det at de ikke kan bli instruert i hvordan de skal gjennomføre vedtak eller avgjørelser, og gjør de bedre egnet til å gjøre avgjørelser i samsvar med loven uten forskjellig behandling for enkeltsaker.

Datatilsynets hovedrolle er altså å føre kontroll for personvernregelverket, og beskytte rettighetene til enkeltpersoner og forhindre at de ikke blir krenket gjennom bruk av disse opplysningen som kan knyttes til dem.

Datatilsynet har flere mål og oppgaver enn det som er strengt relevant for problemstillingen, men det er nesten alltid dette forvaltningsorganet som er i bildet når det gjelder personopplysningsloven og GDPR i Norge. (Datatilsynet. U.Å)

5. Hvordan GDPR påvirker arkiver.

GDPR og dets hovedprinsipper påvirker arkiver på en rekke måter, med i forskjellig grad i forhold til hvor langt de lå unna å være innenfor GDPRs hovedprinsipper. I arkiveringsprosessen er danningen av arkivet spesielt påvirket av GDPR, fordi allerede i dette steget så trenger arkivaren eller datakontrolløren samtykke fra de som informasjonen tilhører, og dette kan være en prosess i seg selv. (Datatilsynet. 2017)

Et eksempel er hvordan GDPR har hatt uventede konsekvenser for den offentlige sektoren. I dette tilfellet er det en internett-protokoll ved navn WHOIS – uttalt som spørsmålet «who is», er ikke en forkortelse av noe. Denne protokollen har blitt rammet av det nye regelverket. WHOIS er brukt av politietaten i en del land for å få tak i informasjon om hvem som eier en resurs på internett, for eksempel en webside. Denne informasjon kan brukes av politi, etterforskere og andre forskningsorganer for å bedømme hvor legitim denne resursen er. Dette

er veldig relevant for bekjempingen av Cyberkriminalitet, hvor man ofte hører om nettsider som gjerne ser like ut i forhold til en virkelig nettside, men er i virkelighet en kopi av denne nettsiden designet for å få tak i passord og brukernavn for alle som prøver å bruke denne nettsiden for å logge inn. Med WHOIS kan politi bedømme om den siden faktisk er legitim, eller om det er en falsk nettside, og i så fall hvem som eier den. (Emm. 2018)

Med GDPR så har flere domeneregistre, for eksempel GoDaddy, GostGator og BlueHost, det finnes flere tusen av disse, har bekreftet at å samle inn denne informasjonen om noen bryter GDPRs reguleringer, fordi denne informasjon kan brukes til å identifisere personer fra EU-området. Dermed kunne dette eksponere WHOIS til lovlige søksmål og enorme bøter fra EU om de fortsatte på samme måten som de gjorde. (Huey. 2018)

ICANN – «The Internet Corporation for Assigned Names and Numbers» er gruppen som overvåker WHOIS og har i ettertid bedt om tillatelse til å fortsette å samle inn denne informasjonen om personer som kjøper domenenavn og web-adresser mens de oppdaterer kontrakten sin for å følge GDPRs regelverk. Bedømmelsen om de får denne tillatelsen eller ei kommer til å bli avgjørende om ICANN kan fortsette med tjenesten de tilbyr politietater, om organisasjoner som EPGA ikke trenger å følge opp med denne informasjonen lenger er dette et virkelig hinder for politiets evne til å håndtere flere typer cyberkriminalitet. (Emm. 2018)

Dette vil si at lignende registreringsprosesser må også følge hovedprinsippene til GDPR for å kunne fortsette med driften, siden det er nå etablert en lovlig presedens for dette. Dette vil også stille større krav til f.eks spørreundersøkelser om informasjonen kan brukes overhodet til å identifisere de som har deltatt.

Et lokalt eksempel på dette er fra Oslo universitetssykehus, eller OUS. Datatilsynet ga et overtredelsesgebyr på 400.000kr for ulovlig innsamling, bruk av blodprøver og helseopplysninger fra pasienter. I dette tilfellet må OUS informere alle som har blitt involvert og dermed hatt personopplysninger behandlet av OUS om at dette har skjedd. I tillegg til at for at disse blodprøvene og opplysningene skal være lovlige i forhold til personopplysningsloven, så må pasientene gi et klart samtykke for at OUS skal få beholde profilene. Hvis ikke så må opplysningene slettes. (Datatilsynet. 2017)

Årsaken til gebyrets størrelse var på grunn av en kontroll som ble gjennomført av Datatilsynet hos Janusbanken, spesifikt i kreftregisteret hos OUS i 2016. Denne kontrollen avdekket at OUS hadde tatt ekstra blodprøver fra 1200 pasienter uten samtykke. Disse skulle bli brukt for framtidig kreftforskning, men dette lovbruddet ble desto verre når det viste seg at

kreftregisteret hadde hentet inn pasientlister fra flere deler av OUS internt og deretter brukt disse listene for å hente ut blodprøver fra Janusbanken. Dette er et brudd på taushetsplikten som gjelder for helseforetaket. Disse listene skulle ikke ha blitt delt med mindre et nytt samtykke hadde blitt samlet inn, og dette samtykke hadde kun vært gyldig dersom innsamling spesifiserte hvilke organisasjoner som de skulle dele opplysningene med. (Datatilsynet. 2017)

Dette er spesielt relevant for langtidslagring av dokumentasjon og arkivmaterialet fordi dersom dette nye samtykket ikke kan bli innsamlet, eller at pasientene ikke samtykker med dette som følge av alt som har skjedd, så må Janusbanken slette opplysningene som ble ulovlig innhentet, i tillegg til destruering av materialet selv. (Datatilsynet. 2017)

Dette kan være farlig territorium siden dette omhandler at eldre arkiver som mottar nytt materialet angående personer som allerede har fått samtykke, men om dette nye materialet ikke har blitt godkjent av personene opplysningene gjelder kan det også bety at de kan bestemme at arkivet skal fjerne alle opplysninger disse arkivene har om personen.

6. Retten til å bli glemt

GDPR har mottatt mye kritikk fra både media og andre kilder, for eksempel i en artikkel fra adresseavisa, for påstanden om at personopplysningsloven og datatilsynet «i sin iver» sletter spor som ‘vi’ etterlater oss og fjerner vår kollektive kunnskap i sanntid, at i sitt forsøk på å styrke personvernet så har de svekket rettsvernet. (Andersen. 2019)

«Ifølge en høringsuttalelse om nye bevarings- og kassasjonsbestemmelser for pasient- og journalopplysninger i kommunale og fylkeskommunale helse- og omsorgstjenester, 27. februar 2019, gir nemlig datatilsynet uttrykk for noen generelle betraktninger om arkivbevaring som er oppsiktsvekkende og bekymringsfulle.» (Andersen. 2019)

Spesifikt nevnes delen i artikkel 5 hvor behandling av personopplysninger skal begrenses «til det som er nødvendig for formålet». Dette kan ansees som et godt standpunkt når det gjelder begrensede formål. For eksempel at sykehjem nødvendigvis må ha opplysninger om beboere, og at arbeidsgiver trenger opplysninger om ansatte for å kunne utbetale lønn. Men dette også gjelder i forhold til arkivverkets bevaringsvurdering. Og forfatteren kritiserer med «at datatilsynet ikke har skjønt arkivverkets samfunnsoppdrag». (Andersen. 2019)

Forfatteren peker også ut at dette kan gjøre eldre loggføring og registrering ulovlig, og at slike kilder av informasjon kan brukes til mye mer enn det de originalt var lagd for. For eksempel hvordan kirkebøker fra 1600-tallet ble lagd for å gi en oversikt over datidens medlemmer og

kirkelige handlinger, men de kan nå brukes til slektsgranskning og arvelighetsforskning. (Andersen. 2019)

Det har kommet flere unntak til den nye personopplysningsloven. Dette tilfellet gjelder et unntak for lagring av personlig informasjon dersom det har et formål knyttet til vitenskapelig eller historisk forskning for å ivareta arkiver som kan inneholde informasjon som ellers ville vært beskyttet av loven, dette er for å beskytte «allmenn interesse» (Andersen. 2019)

Mye av kritikken av personopplysningsloven og GDPR kommer fra de som ikke ser ut til å helt forstå hva denne loven innebærer med «retten til å bli glemt». Som nevnt ovenfor fins det flere unntak for dette. Men i hovedsak gjelder bare retten til sletting, eller «retten til å bli glemt» for personlige opplysninger som kan brukes til å identifisere en fysisk person.

Datatilsynet har en egen liste over når denne retten kan brukes, og når den ikke gjelder. Du – brukeren, kan kreve at informasjonen din slettes dersom du benytter din rett til å protestere mot bruken av personopplysningene dine. Retten til å protestere kan brukes mot enhver virksomhet, og du trenger ikke å begrunne protesten din. Virksomheten er pålagt i henhold til lov og forskrift å svare på protesten din innen en måned, med mindre de kan dokumentere gyldig grunnlag til dette. Det fins få unntak til å bruke retten til å protestere og det er for eksempel dersom virksomheten trenger opplysningene dine for å utføre en avtale du har med dem, eller om de er pålagte i lov og forskrift, for eksempel et lån, eller en leiebilavtale, å behandle informasjonen din. Virksomheten må i så fall kunne bevise at det finnes «tungtveiende grunner» til at protesten din er ugyldig om unntakene ikke gjelder i ditt tilfelle.

Virksomheter trenger først samtykke for å lovlig samle inn informasjon om brukeren, men dette samtykket kan trekkes tilbake av brukeren uten gitt grunn, dette betyr at retten til sletting gjelder. (Datatilsynet. 2018)

Dersom brukeren er mindreårig og saken angår bruken av en digital tjeneste, slik som sosiale medier trenger man heller ikke begrunne slettingen forøvrig. (Datatilsynet. 2018)

Om brukeren kan vise til at det ikke er nødvendig for å beholde opplysningene om dem, at formålet er oppnådd, kan du også kreve sletting av opplysningene dine. (Datatilsynet. 2018)

Om opplysningene dine ble innsamlet ulovlig, som i tilfellet at du ikke ga samtykke til å begynne med, har du klar rett til sletting. Dette er også tilfellet om virksomheten har sletteplikt etter loven. (Datatilsynet. 2018)

Dette er Datatilsynets liste over de mest vanlige grunnene til at retten til sletting gjelder, men det finnes også en rekke unntak hvor grunnene nevnt ovenfor ikke gjelder. Det vil ikke si at du ikke kan kreve sletting, men da har ikke virksomheten noen lovlig binding for å gjøre dette. (Datatilsynet. 2018)

For eksempel opplysninger som skal brukes i en journalistisk ytring dekkes av ytrings- og informasjonsfriheten. Det vil si at man kan ikke personlig sensurere en avis eller nyhetsredaksjon. Riktig nok har ytringsfriheten sine grenser via andre lover, for eksempel krenking av privatlivets fred gjennom en ytring kan føre til straff og erstatningsansvar. (Datatilsynet. 2018)

Som nevnt ovenfor er også lagring for arkivering i allmenhetens interesse. Vitenskapelige eller historiske forskningsformål eller statistiske formål beskyttet av loven. Dette unntaket gjelder bare dersom sletting i alvorlig grad vil hindre disse målene. Artikkel 89 krever også at tiltak og garantier må eksistere for å vareta enkeltpersoners personvern. (Datatilsynet. 2018)

Dersom en virksomhet har lagringsplikt etter loven, i listens eksempel, bokføringsplikt, kan ikke retten til sletting bli brukt. I tillegg til dette er lagring innenfor enkelte deler av helsetjenesten nødvendig og dermed kan ikke slettes. (Datatilsynet. 2018)

Retten til å bli slettet gjelder heller ikke dersom lagring er nødvendig for å fastsette, gjøre gjeldene eller forsvare rettskrav. (Datatilsynet. 2018)

Dette viser bare at det er ikke enkelt å få tilgang til eller å få slettet personopplysninger om en, dersom de havner i offentlige organer eller i journalistiske organisasjoner, med mindre de bryter andre lover ved bruken av disse personopplysningene. Men det er fortsatt uten tvil at enkeltpersoner har fått mye mer mulighet til å kontrollere hvem som har tilgang til opplysningene sine, og hvem som får *beholde* dem.

Noe å nevne er også retten til innsyn, at du – brukeren, kan få en kopi av all informasjon en virksomhet har om deg, og dette skal være tilgjengelig gratis. Virksomheten kan kreve et administrasjonsgebyr, men du kan fortsatt få flere kopier gratis av dette dersom du trenger flere kopier. Informasjonen du får fra retten til innsyn kan også fortelle deg om ikke bare hvilken informasjon de har lagret om deg, men også hva de bruker den til. Dette kan brukes som et redskap til å finne ut om formålet er strengt lovlig. Du kan også bekrefte om informasjonen de har om deg er nøyaktig, eller i verste fall om de har ulovlig samlet inn mer enn det de trenger. De må også kunne fortelle deg om de har delt informasjonen din med noen

andre, og få en komplett liste av hvem som har informasjonen din dersom de har delt den. (It Governance. 2017. S 191-193)

7. Oppfølging av GDPR/personopplysningsloven

Når det gjelder oppfølging av personopplysningsloven er det i hovedsak Datatilsynet som er kontaktet når det er en offentlig sak om brudd på den nye loven. Dette har ført til en enorm mengde arbeid for en proporsjonalt liten avdeling og dette er kanskje mye av grunnen til mangelen på oppfølgning for systemer og virksomheter siden loven ble iverksatt.

Løsningen Datatilsynet har kommet med er «Internkontroll» eller i bedre forklart: et planlagt og systematisk styringssystem som virksomheter må etablere for å oppdage brudd på gjeldende regler. Ifølge Datatilsynet er dette en kontinuerlig prosess, og at virksomhetene selv skal håndtere avvik, i tillegg til å kontrollere at rutiner og tiltak brukes og fungerer etter hensikten. Etter at internkontroll har blitt etablert og forankret, må man sørge for at den gjøres kjent og etterleves blant de ansatte i virksomheten. (Datatilsynet. 2018)

Dette er altså en løsning som krever at virksomhetene selv etablerer et system som skal oppdage brudd på regler og håndtere oppdagete avvik fra regelverket. Dette betyr også at det er opp til virksomhetene selv å kontrollere hvordan de skal håndtere disse avvikene, og hva som i så fall rapporteres videre til Datatilsynet. Det kan se ut som at det er nesten ingen direkte oppfølgning fra myndighetene når det gjelder disse sikkerhetssystemene, og utenfor en sikkerhetsrevisjon av egenkontroller, internrevisjon og revisjon av eksterne parter. (Datatilsynet. 2018)

Hvis man ser nærmere på Datatilsynets sider bekrefter de dette. Rapporter for «avvik» trenger kun å sendes til Datatilsynet dersom det er et brudd på personopplysningssikkerheten i virksomheten, og det er sannsynlig for at bruddet vil medføre en risiko for de registrerte sine rettigheter og friheter, (Datatilsynet. U.Å)

Denne sikkerhetsrevisjonen er også kontrollert av virksomheten selv, noe som kan ha betydelige konsekvenser siden dette åpner mange muligheter for uærlige virksomheter til å fortsette ubemerket med mindre de blir rapportert av en tredjepart. Hvorav virksomhetene selv kan bruke god internkontroll for å forsikre seg mot falske anklager på grunn av all oppfølgingen når det kommer til innsamling og behandling av data. Det er ekstra ansvar for virksomheten, men alternativet er fortsatt mye verre dersom det skulle skje noe.

Et tilfelle av at dette kan ha gått galt er i tilfellet med NASDAQ – The National Association of Securities Dealers Automated Quotations, er et internasjonalt aksjemarked med hovedbase i Amerika men som har noen norske brukere via en bransje i Oslo. NASDAQ fikk mye publisitet over skandalen rundt Einar Aas, hvor nesten 3 milliarder kroner forsvant i løpet av noen få dager. Det er kun i ettertid at det ble klargjort at Einar Aas i dette tilfellet hadde godkjente stedfortredere som kunne handle i hans navn, men dokumentasjonen viste kun at det var en av disse stedfortrederne som hadde gjort «systematisk handel» gjennom Einar Aas sitt medlemskap. Denne saken fikk først mye oppmerksomhet når finanstilsynet selv kritiserte mangelen på lokal internkontroll, at rutiner og policyer var dårlige på et lokalt nivå. (Helle. 2019)

Dette er kanskje det mest offentlige tilfellet av at internkontroll har fortsatt langt igjen å gå i Norge, og at internkontroll som løsning er mangelfull i seg selv dersom det er ingen offentlig kontroll over at internkontroll har blitt etablert. Dette gjelder ikke bare i finans-sektoren av markedet, men av alle større bedrifter som behandler personopplysningene til hundretusener av norske innbyggere.

Som en del av forskningsdelen min besøkte jeg et middels stort helseforetak i Norge, der spurte jeg ut av nysgjerrighet om hvordan GDPR hadde blitt involvert i prosedyreverket. Svaret jeg fikk var at til tross for at det nesten har vært et helt år etter at GDPR og den nye personopplysningsloven ble iverksatt, så er ikke GDPR nevnt som ord/begrep i det hele tatt, ikke referert til eller brukt i noen sammenheng. Dette betyr ikke nødvendig vis at prosedyrene ikke er innenfor rammeverket til personopplysningsloven eller at det er noe mindre lovlig på gang, men det var litt spesielt. (Anonym. 17. April, intervju)

8. Diskusjon og Drøfting

Ved starten av Bacheloroppgaven la jeg ut noen objektive målestokker for argumentet «har GDPR gjort nok?» etter det jeg har begrunnet tidligere i oppgaven kan jeg diskutere disse målestokkene i større grad:

Grandfathering: GDPR omfatter mange deler av hvordan informasjon skal håndteres, men hovedprinsipp 4 av Artikkel 5 i GDPR forklarer at all informasjon skal være nøyaktig, men også oppdatert. Dette vil si at alle arkiver som har eldre dokumenter og informasjon om en bruker må i så fall oppdatere denne informasjon for å forbli lovlig, om arkivet eller datakontrolløren har tenkt å fortsette. Ifølge det første prinsippet av GDPR må nytt samtykke bli bekreftet fra en bruker. Dette betyr i så fall at enten så krever GDPR at du som bruker

samtykker til innsamlingen, men også at den nye informasjonen er relevant til det de trenger denne informasjonen til, og må potensielt slette deler av informasjonen din dersom den ikke stemmer overens med hva reguleringen krever. (It Governance. 2017. S 111-113)

Sikkerhetsklimaet: GDPR innførte mange nye regler som omfatter hvordan informasjon skal samles inn, i tillegg til hvordan det er databehandlers ansvar at denne informasjonen ikke kommer på avveie. Dette betyr at det er mye strengere for databehandlere om det er oppdaget avvik fra regelverket eller uhell som har latt hull i sikkerheten bli utnyttet av en tredjepart.

Når det gjelder den nye personopplysningsloven og Datatilsynet så virker «Internkontroll» som en veldig svak løsning til problemet om oppfølging av den nye loven. At sikkerhetskontroller skal gjennomføres av firmaene selv høres ut som en dårlig løsning, internkontroll er et godt redskap et firma kan bruke til å beskytte seg selv om de blir rapportert, men om alle firma skal rapportere selv så begynner problemet i virke litt mer åpenbart. (It Governance. 2017. S 116-119)

Generelt i forhold til hvor mye som har forandret seg med implementeringen av GDPR og Personopplysningsloven ser vi at rettighetene og ansvarene til alle involvert i lagringen av personopplysninger har blitt mer inkluderende, spesielt i tilfellet hos brukerne hvor slike rettigheter ikke fantes før.

I et punktvis perspektiv ser vi hvordan de fundamentale prinsippene i GDPR gjelder, hvor jeg skal også peke ut noen svakheter jeg mener er tydelige. I denne listen refererer jeg til Artikkel 5 og de 6 hovedprinsippene i samme rekkefølge som de har blitt diskutert tidligere og i boken fra IT Governance.

Prinsipp 1. Lovlig, rettferdig og åpent: når det gjelder innsamlingen av informasjon så må de ha samtykket fra brukeren, og de må forklare for brukeren hva slags innsamling vil bli gjort (åpent), at innsamlingen skal stemme overens med beskrivelsen (rettferdig), og at innsamlingen må være i henhold med det som er tillat innenfor reguleringen (Lovlig).

De spesifiserer at innenfor «rettferdig» eller «Fairness» så kreves det av datakontrollør at de er ærlige om identiteten sin, de kan ikke utgi seg for å være noe annet. De kan også kun samle inn informasjon fra de som kan gi samtykke til dette, det betyr også at man kan ikke samtykke på en annens vegne med mindre du har en form for lovlig fullmakt. Datakontrollør skal også kun behandle dataen på en slik måte en kan forvente «innen fornuft», og de skal heller ikke bruke dataen på en slik måte at det kan påvirke brukeren negativt «uten grunn».

Først er det et par problemer her – Ordbruken er veldig opp til tolkning her, «Innen fornuft» kan være veldig mye forskjellig avhengig av tjenesten. og de skal kunne forklare hva de bruker informasjonen til. Problemet oppstår i hvordan de gjennomfører dette siden det er sjelden en bruker får mer enn en lenke til et langt dokument som sikkert har en lang liste over ting de **kan** finne på å bruke informasjonen til, men kun 1 knapp for å godta det.

I «Åpent» eller «Transparency» viser de til at data kontrollør er påkrevd å fortelle åpent hvordan de skal bruke en brukers data. «med mindre det er opplagt». Eksempelet gitt i boken fra IT Governance er at vis man får et telefonabonnement ved et firma så kan de ikke sende den informasjonen til et søsterfirma som selger feriepakker siden dette ville vært utenfor hva som ville vært opplagt. Denne delen er litt mer spesifikk og kan brukes til å definere brudd av rettferdig bruk av dataen siden dette ville utenfor det man kunne ha kalt «innen fornuft», men det er fortsatt veldig opp til tolkning av reguleringen.

Den siste delen av Prinsipp 1 er at datainnsamlingen skal stemme i henhold til loven, og denne innsamlingen er kun lovlig dersom 1: samtykke ble gitt først. 2: innsamlingen er nødvendig for å fullføre en kontrakt mellom datakontrollør og bruker. 3: innsamlingen er nødvendig for å være i henhold med en annen lov, for eksempel politiet kan samle inn informasjonen din uten samtykke dersom det er et behov for det. 4: innsamlingen er nødvendig for å beskytte data som har stor verdi for brukeren eller for en annen person. 5: innsamlingen blir gjort i bevarelsen av allmenhetens interesse 6: at innsamlingen blir gjort på grunn av legitim interesse hos datakontrolløren eller en tredjepart, med mindre dette målet er direkte motsetning til rettighetene til brukeren, spesielt vis brukeren er et barn. nummer 6 er ansett som en underparagraf og gjelder ikke for offentlige myndigheter og arbeidet deres.

Prinsipp 2. Databehandler må begrense informasjonsinnsamlingen til det de skal bruke den til. Det står at dokumenter som «Terms and conditions» og sluttbrukeravtaler skal gi full kontekst til all data som skal innsamles slik at det ikke blir lagt igjen noe til tolkning og alt skal bli redegjort på i henhold til prinsipp 1.

Dette er et problem i utføring fordi brukeren får generelt bare en knapp og et par lenker til 40-sider lange brukeravtaler som den gjennomsnittlige brukeren ikke kommer til å lese og kanskje ikke heller forstår. Dermed har ikke forandret seg mye fra hvordan det var. Dette burde ha blitt diskutert i dannelsesstadiet av GDPR siden det er en tydelig svakhet i forordningen.

Det burde ha vært et krav å gjøre informasjonen lettere tilgjengelig og skulle ikke trenge en advokat til stedet for å tolke en brukerpolicy, til tross for at Artikkel 5 av sier at brukeren skal kunne forstå hva de har samtykket til.

Prinsipp 3. Begrensning av innsamlet informasjon: Dette betyr at innsamlet informasjon skal begrenses eller minimeres slik at en datakontrollør kun har informasjon relevant for grunnen de samlet den inn for. Dette legger et sterkere krav til at et arkiv må kunne definere hva de skal med den informasjonen og knyttes opp mot prinsipp 2.

Prinsipp 4. all informasjon skal være nøyaktig og oppdatert: Som nevnt ovenfor er dette en effektiv måte å ta seg av eldre systemer eller noen form for «grandfathering» som kunne oppstå. Å ha korrekt og oppdatert informasjon er også god praksis for et arkiv som aktivt brukes, f.eks i forhold til markedsføring, eller kanskje pasientjournaler. Det hadde ikke vært første gang at en artikkel om post og markedsføringsmaterialet har blitt sendt til en familie som sørger over tapet av et familiemedlem. Dette kan nå unngås fordi et oppdatert arkiv må i så fall kunne få med seg en slik forandring. Om noe lignende skjer i fremtiden kan det være grunnlag for lovbrudd og mulig oppfølging fra myndighetene. Men lovverket sier fortsatt at informasjon burde oppdateres på en månedlig basis, og de burde da slette informasjon som da ikke stemmer.

Prinsipp 5: Informasjon skal kunne brukes til å indentifisere hvem dataen tilhører. Dette er en god løsning for at GDPR skal kunne gjelde så å si all informasjonen som blir samlet inn, siden GDPR kun gjelder dersom informasjonen kan brukes til å identifisere en borger fra EU, EØS-land eller internasjonalt dersom det gjelder innbyggere fra EU og EØS.

Prinsipp 6: Sikkerhet, kontroll av tilgang og en full oversikt over hvem som har tilgang. Ganske enkelt og legger ansvaret hos databehandler dersom det blir offentliggjort at noe har skjedd. Dette hjelper til med å motvirke avslappet sikkerhet hos databehandler siden det er de som blir stilt ansvarlig i tilfellet av et hackerangrep.

Fra å ha lest og analysert det jeg har funnet ut om temaet vil jeg si at dette er veldig i tråd med andre lover som har kommet ut fra EU. De prøver å gjøre mye med denne loven, men det virker som at mye av det spesifikke er ikke grundig gjennomtenkt, for eksempel: Hvordan definerer man «samtykke» i denne loven? Hvor informert må en bruker være for at dette samtykket skal være gyldig? For eksempel hos leseren: Når var det sist gang du leste en brukerpolicy grundig fra start til slutt før du trykket «ja» når du ble bedt om å godta en policy

for å bruke en tjeneste? Eller er dette ikke et spesielt viktig poeng siden samtykket kan trekkes tilbake når brukeren føler for det?

Eller i den norske personopplysningsloven, hvordan definerer vi «Allmenhetens interesse»? Hvem avgjør dette, og hvordan kan noe objektivt bevises at noe er «allmenhetens interesse»? Det er opplagte ting som personregister, ja. Men om noen har samlet inn informasjon om deg, informasjon som du påstår er privat, men motparten påstår at det er ansett som «Allmenhetens interesse». Hvordan kan det avgjøres hvem som har rettigheter her?

Ord som kan tolkes på vidt forskjellige måter svekker lovverket. De tillater at loven kan tolkes på uønskede måter, og kunne vært unngått dersom lovverket hadde vært mer spesifikt om hva de mente. Eksemplene nevnt ovenfor er bare noen få av de som kan brukes. Og hvis GDPR eller personopplysningsloven skal bli mer anvendelig trenger den mer spesifikk ordbruk. Enkelte punkter som «all informasjon skal være oppdatert og korrekt» mener jeg er veldefinert siden den gir en klar beskjed til leseren.

I artikkelen «Weighing the impact of GDPR» påpeker Samuel Greengard at det er usikkert hvordan implementeringen av GDPR kommer til å påvirke lagring av informasjon. Men det er åpenbart når en spørreundersøkelse viser at i Amerika så mener 93% av voksne at det er viktig for dem å kontrollere hvem som har tilgang til PII – Personally identifiable informasion, og at 90% mener at det er viktig å kontrollere hva slags informasjon om dem som kan samles inn, og at det er lignende meninger verden over. (Greengard. 2018.)

Han viser også til hvordan Amerika og andre land har en «opt-out» policy. At det er opp til brukeren å informere et firma om at de ikke vil at informasjon skal samles inn om dem. Dette er jo i sterk kontrast til hvordan det har nå blitt i EU med GDPR. Norge med den nye Personopplysningsloven er det er nå isteden blitt et Opt-in system hvor man må ha samtykke før noe som helst annet kan samles inn. Han påpeker at dette systemet har også tatt dette konseptet til et enestående og utestet nivå hvor brukerne har nesten komplett kontroll over sin informasjon. (Greengard. 2018.)

Dette er veldig i tråd med hvordan reaksjonen har vært i Norge med Torkel Thime og hans kommentar om hvordan dette truer vår kollektive hukommelse siden brukere kan kreve å bli slettet fra nesten alle former for digitale databaser. Og dette er fortsatt sant, men hovedsakelig for den kommersielle sektoren hvor det er firma som har mindre statlige beskyttelser for innsamlet data. Offentlige arkiver er fortsatt beskyttet av loven til mer eller mindre samme grad som før. (NTB. 2018)

9. Konklusjon

Noe som er verdt å nevne først er at GDPR og personopplysningsloven er ganske forskjellig på enkelte punkter, personopplysningsloven har klarere definisjoner av for eksempel «allmenhetens interesse». Og dette ser ut til å være litt av grunnen til at vi har implementert GDPR på en slik måte istedenfor å bare oppfølge den nye reguleringen lokalt.

Denne forordningen har delt debatten veldig på midten. Noen mener dette var nødvendig, andre mener dette gikk altfor langt og burde ikke ha blitt implementert slik som den var, og burde heller ha gått gjennom mer drøfting og etablert mer konkrete regler og betydning for begrepene som blir brukt. Når jeg analyserte det grunnleggende av forordningen så var det opptil flere svakheter i ordbruken eller i gjennomførelsen av hovedprinsippene som definitivt viser til at begge sidene av denne debatten har gode poeng.

Med tanke på Grandfathering, en av målestokkene for problemstillingen så gjør GDPR en utmerket jobb, hovedprinsippet om nøyaktig data motvirker at foreldet informasjon kan lovlig brukes uten et nytt samtykke fra brukeren.

Når det gjelder sikkerhetsklimaet så gjør GDPR også en fenomenal jobb, hovedprinsippet om sikkerhet legger ansvaret hos datakontrolløren uansett hva som skjer, og da syns jeg ansvaret for datasikkerhet ligger der det skal være. At størrelsen på bøtene kan ha en motvirkende effekt på de som prøver lykken, er ikke nødvendig vis negativt

Alt i alt virker det som at denne forordningen bruker en del ord som høres bra ut, men har veldig subjektiv tolkning. Slik ordbruk er farlig i lovverk ettersom at dette kan medføre at loven kan feiltolkes, eller i verste tilfelle utnyttes.

GDPR er et godt steg i rett retning, men personlig ville jeg ikke ha sagt at loven har gjort nok. Denne loven kunne vært håndhevet med mikroskop over hvert enkelt tilfelle og fortsatt ha gått feil i mange tilfeller, mangelen på oppfølging gjør dette bare verre.

Den nye personopplysningsloven er et svært omfattende lovverk så arbeidsmengden som kreves for bedre oppfølging av denne er uten tvil en enorm oppgave i seg selv, men kontrollering om systemer er oppdaterte i henhold til den nye personopplysningsloven gjør jobben enda større. Veldig få lover var perfekte når de først kom, det er derfor man hele tiden ser hvordan lovene har fått tillegg og nye paragrafer som kan gjøre dem bedre. GDPR er fortsatt nytt, så det kommer nok flere oppdateringer til denne forordningen som kan gjøre den mer relevant, men veien er fortsatt lang før dette er tilfellet.

10. Referanseliste

Andersen. E. (2019, 01. Mai). Datatilsynet truer vår kollektive hukommelse. *Adressa*. Hentet fra https://www.adressa.no

Bunker. G (2017. 07. August) *The raison D'être behind the new regulation.* Hentet fra: https://www.itproportal.com

Datatilsynet. (Ingen årstall) *Om datatilsynet*. Hentet fra: https://www.datatilsynet.no

Datatilsynet. (Ingen årstall) *Håndtere Avvik*. Hentet fra: https://www.datatilsynet.no

Datatilsynet (2017. 20. Desember) *Gebyr for ulovlig innhenting av personopplysninger*. Hentet fra: https://www.datatilsynet.no

Datatilsynet (2018. 19. Mars) *Rett til sletting.* Hentet fra: https://www.datatilsynet.no

Datatilsynet (2018. 18. Juni) *Etablere Internkontroll.* Hentet fra: https://www.datatilsynet.no

Emm. D. (2018. 23. Juli) *The negative impacts of the GDPR.* Hentet fra: www.itproportal.com

Greengard. S. (2018). Weighing the impact of GDPR. *Communications of the ACM 61*(11) 16-18. Hentet fra https://dl.acm.org/citation.cfm?doid=3289258.3276744

Helle. B. T. (2019. 10. Januar) Finanstilsynet kritiserer NASDAQs internkontroll etter Einar Aas-skandalen. *Dagens Næringsliv.* Hentet fra: www.dn.no

Huey. C. (2018. 09. Mai) *the impact of gdpr on threat intelligence analysts*. Hentet fra: https://www.itproportal.com

IT Governance (Organization), & European Union. (2017). EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide (Andre utgave). Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Hentet fra http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1593800&site=ehost-live

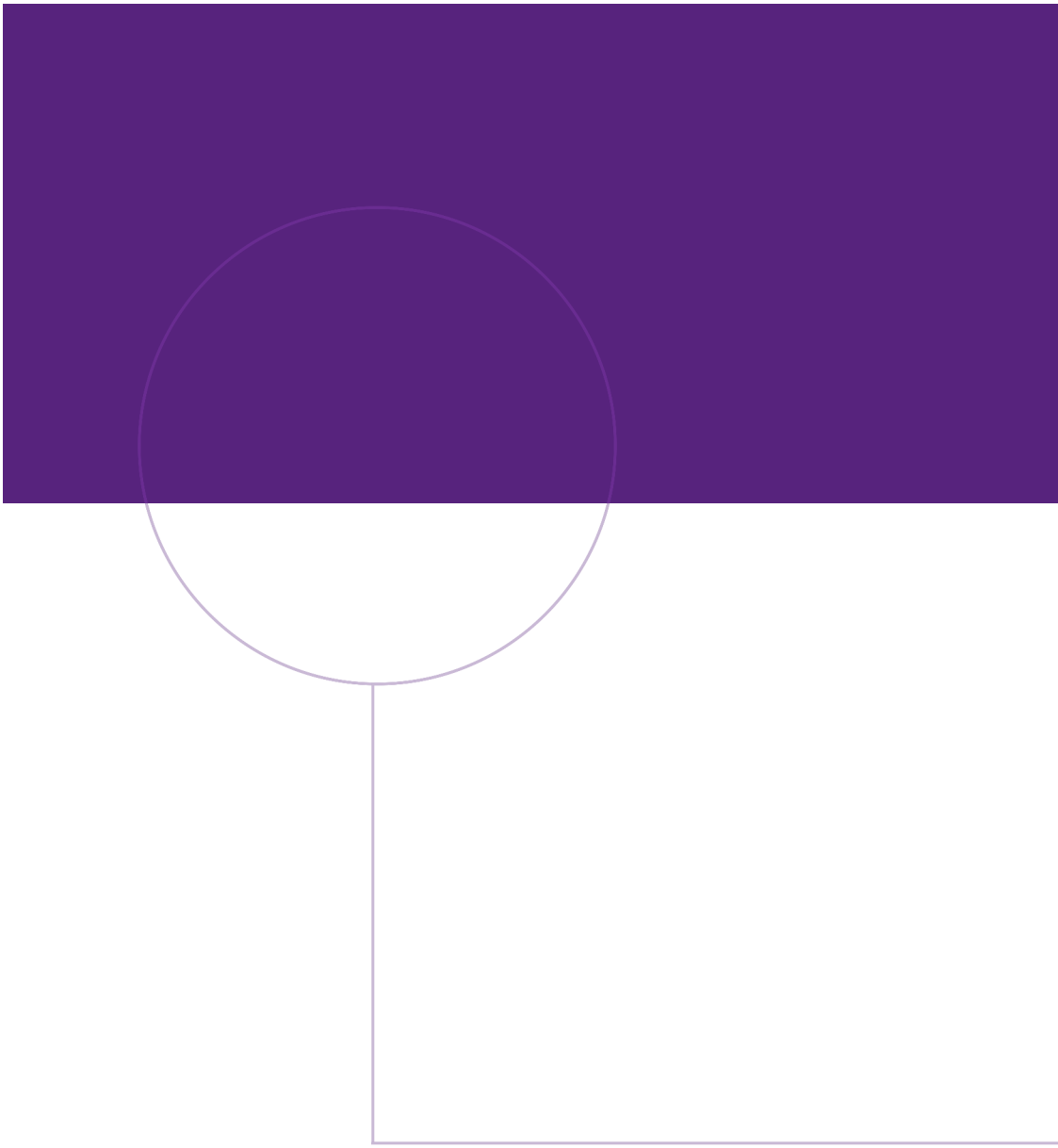
IT Governance (Uten Årstall) Hentet Fra: https://www.itgovernance.eu/en-ie

Kleinman. Z. (2018. 21. Mars) Cambridge Analytica: the story so far. *BBC.* Hentet fra: https://www.bbc.com

Kommunal- og moderniseringsdepartementet. (2018). *Ny personopplysningslov*. Hentet fra www.Regjeringen.no

(NTB) NTB-AFP-AP (2018, 24. Oktober) Apple-sjefen advarer: personopplysninger brukes som våpen. *Adressa.* Hentet fra https://www.adressa.no

Synopsis. (2014. 29. April) *The heartbleed bug*. Hentet fra: www.heartbleed.com



NTNU
Norwegian University of
Science and Technology