Arkiv Information Teknik

Nr 1
2020

GDPR 2 år senare

Efter GDPR: Problemet med att inte få skriva ner folks namn

Illustration: Henrik Wahlström

Utgivningsinformation

Arkiv Information Teknik, nr 1 2020

Chefredaktör: Alexandra Meija
Redaktör: Anders Hedman
Formgivare: Karin Appell
Utgivare: ArkivIT AB
Första numret: 2018
Land: Sverige
Språk: Svenska

Tryck: Drukatava, Lettland

Officiell webbplats: www.arkivinformationteknik.se

Målet med Arkiv Information Teknik är att bjuda in till en bredare diskussion med olika perspektiv och tankar kring informationshantering utifrån dagens förutsättningar. Det finns också en ambition att skapa en diskussion som breddar bilden av vad informationshantering kan vara. Skribenterna ansvarar själva för de åsikter och de fakta som förmedlas i artiklarna. Innehållet i tidskriften speglar inte nödvändigtvis ArkivIT:s uppfattning.

Medverkande skribenter i detta nummer:
Alexandra Meija
Roger Broberg
Viktoria Nordström
Isak Nyberg
Per Lövgren
Herwig Zaczek
Raimondas Andrijauskas
Mats Burell
Carine Spång
Anders Hedman
Constance Bell Dahlbäck
Roland Lycksell
Charlotte Arnell
Alicia Bergli
Johan Dressler
Johan Eriksson
Fia Ewald

Bildmaterial:
Karin Appell
Skribenternas egna
pixabay.com
unsplash.com
metmuseum.org
Henrik Wahlström

Innehåll

Ledare

Dataskyddsförordningen – 2 år senare

De av oss som var med när det begav sig minns den hets och den stress som ledde fram till den 25 maj 2018. Ute på uppdragen som arkivkonsult kunde man nästan ta på spänningen och osäkerheten och det kändes som att det raderades information till höger och vänster, det inventerades register med personuppgifter och i många fall kom troligen gamla skelett fram ur garderoben.

Nu har två år gått och saker bör ha stabiliserat sig. Eller? Vi kan fortfarande läsa om information som gallras på lite skakiga grunder, om klasslistor (som Anders Hedman skrivit en krönika om i detta nummer) som försvunnit men nu kommit tillbaka. Det tycks fortfarande infinna sig en viss nyans av panik i folks ögon när frågor kring personuppgiftshantering dyker upp, och en osäkerhet om vad man får göra och inte göra. Det är även många som i vissa fall verkar falla tillbaka i gamla vanor och skapar register som man sedan glömmer bort att redovisa i registerförteckningen eller hanterar personuppgifter på ett sätt som inte längre är tillåtet.

Vi har i det här numret valt att titta på hur det ser ut där ute, och första gången i tidningens historia (även den är två år gammal) har vi artiklar från Datainspektionen, inte bara Sveriges utan även Litauens och Österrikes, där alla tre berättar om hur arbetet bedrivits sedan 2018. Det som kraftigt betonas i artiklarna är samarbetet inom den Europeiska unionen och arbetet med att ensa arbetssätten. När det gäller Sverige verkar inte samarbetet ha varit detsamma och det känns som att många kommuner och myndigheter kämpar på egen kammare med samma problem. För att ta reda på hur det är ställt med det har vi frågat våra svenska kommuner hur de har arbetat med frågan. Men vi har även ställt lite grundligare frågor till några av dem för att höra hur arbetet har drivits, vilka fallgropar de stött på men även vilka lärdomar de fått med sig på vägen.

Det intressanta med dataskyddsförordningen är att den skapat en helt ny yrkesgrupp. Det tidigare PUL-ombudet hade en ibland anonym roll medan en DSO (dataskyddsombud) kliver in och pekar med hela handen. Idag har de flesta en DSO bland sina anställda men för mindre organisationer kan det ibland löna sig att köpa in den tjänsten. Samtidigt är det viktigt att även den övriga verksamhet beaktar frågan om dataskydd. Därför har vi i detta nummer en artikel där vi får tips om vad som är viktigt att tänka på vad gäller dataskyddsarbete och hur er verksamhet kan tänka när ni planerar ert år enligt dataskyddsförordningen.

”Det tycks fortfarande infinna sig en viss nyans av panik i folks ögon när frågor kring personuppgiftshantering dyker upp.”

Vi på ArkivIT stöter på de här frågorna flera gånger i veckan, då vi måste ta ställning, fundera och tänka efter. Ibland är det lite klurigt men ofta är lösningen att ta ett steg tillbaka, andas, läsa på, höra med dem som kan och sedan känna att man lärt sig något nytt. För ofta är det i ny kunskap man hamnar. Det okända och det man inte vet något om känns alltid läskigt och överväldigande, men sakta tar man några stapplande steg in i en främmande och annorlunda värld, för att ta några till och några till och till slut inser man att man går i maklig takt och t.o.m. hinner stanna till på vägen och njuta och ta in omgivningen. Vi i redaktionen hoppas att det här numret kan vara ett steg på vägen mot en ökad villighet att ta sig an det okända som i dagligt tal benämns GDPR och eller dataskyddsförordningen (kärt barn har många namn) och bidra till ökad kunskap i ämnet för dem som redan kommit en bit på vägen.

Trevlig läsning!

Alexandra Meija
Chefredaktör

Dataskyddsombudet

– Att skapa mervärden samtidigt som man skyddar

Att följa förordningar brukar mest generera kostnader. Jag har, tillsammans med många organisationer, istället använt det som en språngbräda för en värdeskapande verksamhetsutveckling. I det att en organisation börjar få en bättre bild av sin information och dess flöden, finns här en möjlighet till effektivisering och ett bättre skydd.

Dataskydd eller skyddande av data är reglerat i ett flertal lagar och förordningar. dataskyddsförordningen (GDPR), patientdatalagen och socialtjänstlagen är de mest kända. Lagar är bra, men ett känt faktum är att de är reaktiva. De tillkommer som svar på otillbörliga handlingar som inte accepteras av samhället. I en verklighet där allt mer av våra liv hanteras eller publiceras digitalt, behöver man ställa sig frågan om dessa regleringar räcker.

Hur ska vi lära oss att vara sunda och försiktiga med hur vi hanterar data? Dataskyddsombud, ett ombud för de registrerade, är vissa organisationer skyldiga att ha enligt dataskyddsförordningen som trädde i kraft i maj 2018. Ombudets roll är att ge råd och stöd samt granska att organisationen följer förordningen. Det är myndigheter, kommuner och organisationer som hanterar större mängder eller mycket känsliga personuppgifter som har krav på att ha ett ombud. Men det finns även organisationer som anlitar ett dataskyddsombud, utan att ha kravet, för att få professionell hjälp mad att följa förordningen.

Trots att dataskyddsförordningen inte är särskilt komplicerad och att vi i princip haft samma lag genom PUL sedan 1996, finns ett flertal organisationer som inte riktigt kommer i mål med att hantera personuppgifter på ett korrekt sätt. Det är nog i många fall här som det går lite tokigt. Vad är ett korrekt sätt? Jurister har skrivit spaltkilometrar med hur man ska tolka lagen. Tyvärr blir man oftast inte klokare, då de endera behandlar något mycket speciellt fall eller så väcker artiklarna nya frågeställningar och konstaterar att man varken kan säga bu eller bä. Men juridiken är bara en sida av myntet. Den andra, informationssäkerheten, hanteras oftast av helt andra delar i organisationen. Det är här som ett bra ombud kan göra en värdeskapande insats – genom att hjälpa till att samordna verksamhetsutvecklingen på ett sätt så informationssäkerheten ökar och att den är anpassad till förordningen. Enligt förordningen kan kraftfulla sanktionsavgifter utdömas till organisationer som inte följer den. Dessa döms oftast ut för att man brustit i säkerheten.

Vår syn på ett dataskyddsombud

Ombudet ska ha en god kunskap och förståelse för de lagar och regler som verksamheten styrs av. Ombudet är väl förtrogen med informationssäkerhetsarbete och de standarder och metoder som finns. Ombudet har en ledande roll och kan kommunicera i alla delar av organisationen. Ombudet är pedagogisk och kan förmedla vad som behövs på ett sätt som kan förstås och hanteras. Ombudet är pragmatisk och fastnar inte i detaljer utan försöker ha fokus på att organisationen har en fortsatt utveckling framåt. Sist men inte minst, det är inte ombudet som ska göra verksamhetsutvecklingen. Det är organisationen, verksamhetens jobb. Ombudet ska ge råd, stöd och granska. Ombudet är även kontaktperson gentemot tillsynsmyndigheten. Ordet systematiskt har en central betydelse. Det betyder planerat och kontinuerligt. Det kan uttryckas med exempelvis årshjul eller handlingsplaner.
Om du är ett ombud eller jobbar med förordningen i er organisation och inte känner igen dig i beskrivningen ovan, finns det en risk att ert arbete inte blir så värdeskapande som det skulle kunna bli.

”Information är ofta en av de viktigaste tillgångar som en organisation har för att kunna verka med en god kvalitet. Personuppgifter är också information. Planera för ett helhetstänk kring dataskyddet.”

Det räcker inte med att du vet vad som står i lagen. Du måste kunna omsätta det till verksamheten. Alla medarbetare måste förstå principerna och vara väl införstådda i hur just deras arbetsmoment påverkas. Jag trycker särskilt på att trots att det är samma lag ska instruktionerna till de olika delarna av verksamheten vara specifika. Regler och instruktioner ska vara riktade till den mängd och typ av personuppgifter som hanteras. Det är då det blir lättare för var och en att veta vad som gäller. Många organisationer väljer att göra en stor regelsamling på intranätet. Det kan fungera i vissa fall. Allt beror på vilka man riktar informationen till och vilken typ av personuppgifter man hanterar. Många organisationer hanterar i princip bara kontaktuppgifter eller publika uppgifter, undantaget HR. Där är skyddsvärdet lågt och man behöver generellt bara uppfylla minimikraven i förordningen.

Hur samverkar informationssäkerheten med dataskydsförordningen?

I förordningen förekommer på några ställen ordet ”lämplig säkerhet”. Betydelsen är lika diffus som det låter. För att veta vad som är lämplig säkerhet gäller det att man har kontroll på vilka personuppgifter man hanterar, var man hanterar dem, hur de lagras, vilka som hanterar dessa med mera. Det är här som informationssäkerheten kommer in i bilden. Organisationen ska och behöver ha kontroll på hur och var information hanteras i verksamheten. Information är ofta en av de viktigaste tillgångar som en organisation har för att kunna verka

med en god kvalitet. Personuppgifter är också information. Det betyder att dataskyddsförordningen ingår i informationssäkerhetsarbetet. Därför finns det ett flertal standarder och regelverk som verksamheten kan följa för att uppnå denna kontroll. Tyvärr finns inte dessa standarder framtagna specifikt till förordningen än. Men man kan lätt med en smula flexibilitet använda de vedertagna standarder och metoder som finns för informationssäkerhet för att följa upp sitt arbete med förordningen. Genom att kontinuerligt följa upp var man har sin information, inklusive personuppgifter, klassificera dessa och ge dem ett lämpligt skyddsvärde har organisationen gjort den viktigaste biten i förordningen. Kontroll och god dokumentation är honnörsorden för informationssäkerhet, detsamma gäller efterlevnaden av dataskyddsförordningen. Förordningen innehåller dessutom några specifika regler som bara finns där. Ett exempel rör integritetspolicy och personuppgiftsbiträdesavtal. Men de är ofta mer av engångskaraktär och ska bara revideras om behov finns.

Den värdeskapande samordningen

Det första organisationen behöver göra är en analys av vilken information som hanteras i verksamheten. Utifrån den analysen, samt en omvärldsanalys, kan man göra en bedömning av värdet och riskerna med informationen. I omvärldsanalysen ingår bland annat hot, lagar och regler. Med dessa analyser bestäms ”lämplig säkerhet” för respektive informationsklass. Att skilja hanteringen av personuppgifter från hantering av all annan information är kontraproduktivt och kan tvärtom vara riskabelt. Vad som menas med det är, att om hantering av personuppgifter sker i en del av verksamheten och informationssäkerheten i en annan del, och dessa inte är samordnade, finns det uppenbara risker. När vi pratar om värdeskapande samordning menas att man genom att utveckla och förstärka informationssäkerheten, kommer att öka kvaliteten. Om man inom ramen för detta kvalitetsarbete belyser dataskyddsförordningen och anpassar verksamheten efter denna, kommer det arbetet inte att vara belastande utan tvärtom värdehöjande. Planera för ett helhetstänk kring dataskyddet. Öka medvetenheten hos alla medarbetare i att information är en viktig tillgång som inte får missbrukas eller förstöras. Ansvariga i verksamheten ser över att det är korrekt, laglig information som samlas in och sparas. Rutiner och riktlinjer skapas för att det ska vara enhetligt och tydligt. Information som inte fyller något syfte tas bort.

Och framför allt: Det här är en kontinuerlig process.
Börja med en hygglig nivå som sedan kan förbättras.

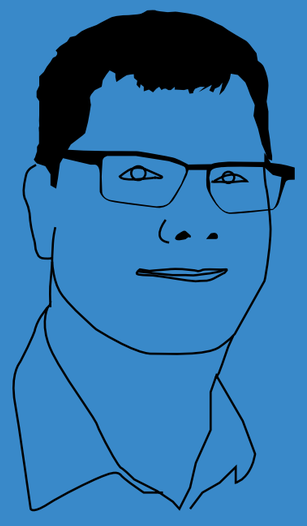
Jag kan inte nog poängtera detta:

Varje person har ett ansvar att behandla data på sunt och försiktigt sätt. Detta gäller såväl privat som på jobbet. Tro mig, hoten är många och det finns alldeles för många personer i världen som har som sin näring att lura personer som inte förstår bättre. Att ha en normal sund skepsis räcker långt. Men bättre är att alltid ifrågasätta varför någon vill ha dina uppgifter och alltid ifrågasätta säkerheten (om inte annat i tanken).

Vad händer framöver?

Fler och fler länder och regioner utanför Europa kommer med motsvarigheter till GDPR. Samtliga är anpassade till den verklighet och lagstiftning som gäller nationellt. Men här finns även inslag av att nationell lagstiftning, i tillämpliga delar, anpassas till skydd av personuppgifter. Detta öppnar för så kallad Code of Conduct eller hänvisning till motsvarande lagstiftning.

De europeiska tillsynsmyndigheterna börjar att få igång sitt samarbete och ett flertal vägledande domar och sanktionsavgifter har utdömts. Prognosen är att under 2020–2021 kommer ett flertal sanktionsavgifter att utdömas på redan prövade avsteg från förordningen. Med det menas även att förutsägbarheten för sanktionsavgift kommer tydliggöras. GDPR börjar sakta att vävas in i verksamheterna. Framöver kommer inte GDPR bara ses som en lag, utan efterlevnaden kommer att vara en del av den trovärdighet man vill visa för sina kunder och leverantörer. Det kommer att vara en konkurrensfaktor lika naturlig som kvalitet och miljö.



ROGER BROBERG

Arbetar på ArkivIT med dataskydd. Främst som dataskyddsombud, men med stor vikt på informationssäkerhet. Utöver lång erfarenhet inom IT i olika roller driver jag även utbildningar och seminarier inom dataskydd. Jag är dataskyddsombud (DSO) på ett stort antal organisationer. I denna artikel vill jag ge min syn på hur man kan tänka kring det professionella dataskyddsarbetet.

Att förvalta sitt dataskydd

– Ett kontinuerligt arbete som kräver en plan

För att lyckas med det praktiska arbetet med dataskyddsfrågor räcker det inte att kunna manövrera rätt i den snåriga juridiken. Det krävs också en bra plan. Det finns en stor risk att arbetet med dataskyddsfrågorna blir ineffektivt och tidsödande om man inte har en övergripande strategi för hur arbetet ska bedrivas.

Inför den 25 maj 2018, och i viss mån den närmaste tiden därefter, lade företag, myndigheter och organisationer över hela Sverige oändligt många projekttimmar på GDPR. Hur ska man med lite distans till detta säkerställa att allt arbete som lagts ner inte varit förgäves?

Det är knappast ett kontroversiellt påstående att förutsättningarna för arbetet förändras över tid hos de flesta verksamheter. Det kan till exempel handla om nya IT-system, digital utveckling och nya affärsmöjligheter, men också om organisatoriska förändringar och omgjorda arbetsprocesser. Allt sådant leder till att personuppgifter kan komma att behandlas på nya sätt. Dessutom sker saker i omvärlden som påverkar vad man behöver och vill göra i sin verksamhet, det har vi inte minst sett under coronapandemin. Dataskyddslagstiftningen i sig kan naturligtvis förändras den också. Att säkerställa ett gott dataskydd kräver därför mer än en engångsinsats i projektform. För att kunna efterleva lagkraven behöver dataskyddsarbetet bedrivas kontinuerligt, med översyn och uppdateringar.

Många verksamheter har kommit längre

Datainspektionen konstaterar i sin årsredovisning från 2019 att många företag, myndigheter och andra organisationer har kommit till en ny nivå i sitt dataskyddsarbete. Såhär beskriver Datainspektionens generaldirektör förändringen:

Om 2018 för många präglades av intensiva förberedelser inför dataskyddsreformen och att få grundläggande processer och rutiner på plats, så har 2019 snarare kännetecknats av att få strukturerna att fungera i praktiken, och utmaningar i form av mer komplexa rättsliga frågor och tolkningar.

Det är också tydligt att medborgarna har allt högre förväntningar på att deras persondata hanteras på ett korrekt, säkert och transparent sätt.

Datainspektionen framhåller samtidigt att behovet av vägledning och stöd från dem i mer komplexa rättsliga frågor är fortsatt stort. Många kan säkert skriva under på att det väldigt ofta saknas tydlig praxis för specifika situationer, eftersom det inte gått tillräckligt lång tid för att tillsynsmyndigheter och domstolar ska ha haft tid och tillfälle att över huvud taget ta ställning i många frågor.

Att dataskyddsarbetet har mognat och gått framåt i många verksamheter är något som också vi på Draftit kan konstatera. Vår verksamhet erbjuder digitala verktyg och tjänster inom dataskyddsområdet och de senaste åren har vi haft kontakt med många verksamma dataskyddsombud och GDPR-ansvariga. Det råder ingen tvekan om att kompetensen totalt sett har ökat. Från att ha handlat om grundläggande frågor med svartvita svar har våra kunders frågeställningar börjat vara alltmer branschspecifika och komplexa. Ett flertal olika aspekter och lagstiftningar samspelar. Allt oftare kommer också frågor om granskning och revision upp. För när alla grundläggande delar i en organisations ”dataskyddsmaskineri” är på plats är det dags att gå vidare till förvaltningsfasen.

Med rutiner för revision och internkontroll går det att göra förvaltningen av GDPR till en del av den dagliga verksamheten.

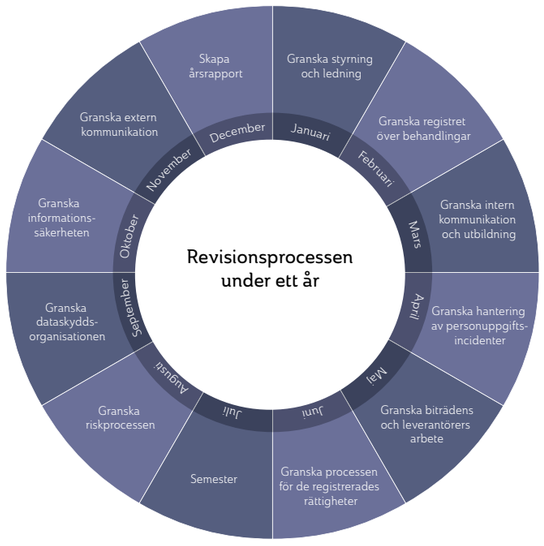
Det kan låta klyschigt och kanske rent av överambitiöst. Men faktum är att först då kan dataskyddsarbetet upprätthållas och förbättras, både så att man successivt får ett allt bättre integritetsskydd, men också ur ett kostnadsperspektiv. Redan utfört arbete går inte förlorat, och allt blir mycket effektivare!

Ett systematiskt dataskyddsarbete fördelat över hela året

Hur ska då organisationer hitta sätt att arbeta långsiktigt med GDPR med löpande omvärldsbevakning och uppföljningar, strukturerade revisioner med mera? För att underlätta revisionsprocessen och för att inte alltihop ska kännas ogreppbart och luddigt är det en bra idé att bryta ner arbetet i mindre delar. Att systematiskt ta en sak i taget, helt enkelt. Ett sätt att göra detta på är att utgå från ett årshjul.

Med hjälp av ett årshjul ser man till att olika delar av dataskyddsarbetet får uppmärksamhet i tur och ordning medan verksamhetsåret löper på. Året kan exempelvis börja med att adressera frågor som rör styrning och ledning. Finns det stöd och mandat från styrelse/verksamhetsledning att fortsätta möta kraven i GDPR? Har de ansvariga personerna inom dataskydd tillräckliga resurser till sitt förfogande?

Nästa steg kan exempelvis vara att se över registret över alla personuppgiftsbehandlingar. Finns samtliga behandlingar av personuppgifter dokumenterade, även sådana som tillkommit eller förändrats i närtid? Är informationen komplett och korrekt, med utgångspunkt i lagstiftningens krav (främst artikel 30 GDPR)? Låt fokus ligga på att granska och uppdatera registret om det behövs. Först när det är gjort, gå vidare till nästa steg, som skulle kunna vara att se över vilka kommunikationsinsatser som skett inom organisationen. För varje månad väljer man ett nytt fokusområde. Sett över ett helt år skulle det kunna se ut som i illustrationen nedan.



Som ett sista steg i slutet av året sammanställer man förslagsvis en rapport. Observera att det inte finns specifikt reglerat i dataskyddslagstiftningen i vilken form eller med vilken frekvens som revisioner ska redovisas för ledningen. Hur de som arbetar med dataskydd i praktiken informerar och rapporterar resultat internt är något som till stor del beror på hur den egna verksamheten är uppbyggd. Exakt vad som ska ingå i en årsrapport beror på vilka områden som varit i fokus under året, vilka problemområden och riskfaktorer som behöver lyftas, hur ofta och på vilken detaljnivå rapporteringen ska göras och så vidare. Hur genomförda granskningar sammanställs och rapporteras är kort sagt valfritt, men det behöver göras i någon form. Att presentera en årsrapport blir ett naturligt sätt att flagga för risker, synliggöra problem och föreslå åtgärder.

Flera fördelar med årshjul som involverar alla

Det finns flera fördelar med att arbeta utifrån ett årshjul eller motsvarande upplägg. Förutom att arbetet blir konkret, genomförbart och lättare att ta sig an så kan ett årshjul också bidra till att dataskyddsombudets roll som objektiv granskare tydliggörs och förstärks, om det finns ett dataskyddsombud i organisationen. Naturliga rapporteringsvägar skapas så att dataskyddsombudet inte riskerar att missa viktiga saker eller anklagas för att ha brustit i sitt uppdrag som informatör. Frågan om dataskyddsombudets personliga ansvar har kommit upp i media vid flera tillfällen under det gångna året. Vi kan konstatera att det ska mycket till för att ett dataskyddsombud ska kunna hållas personligt ansvarig av sin arbetsgivare i Sverige. Men för att undvika att hamna i riskzonen gäller det att alltid vara uppriktig och tydlig med vilka brister man ser. Hur då? Jo, genom att säkerställa att allting dokumenteras och rapporteras till ledningen.

Dessutom finns en skyldighet enligt dataskyddsförordningen att som organisation kunna visa att man följer reglerna. Utförlig dokumentation är därför ofta avgörande.

De olika fokusområdena över året tydliggör också hur olika delar i organisationen blir involverade i olika faser. Det visar på vikten av att involvera olika enheter. Förändringsarbetet kan visserligen ledas av ett dataskyddsombud eller en ansvarig projektgrupp, men det kan aldrig i praktiken utföras av en liten klick som jobbar ensamma på sin kammare, utan det måste ske ute i verksamheten – på IT-avdelningen, i kundtjänst, hos ledningen och så vidare – genom ett medvetet förhållningssätt och rutiner som införlivats hos alla anställda. När det kommer till att granska att personuppgiftsbiträden såsom IT-leverantörer lever upp till krav och överenskommelser behövs IT-kompetent personal. När det gäller att upptäcka nya behandlingar av personuppgifter så behövs stöd från hela verksamheten. När informationsinsatser ska utvärderas och granskas behöver kanske HR- och informationsavdelningen involveras och svara på frågor. När det kommer till regler för webbplats, utskick och nyhetsbrev, cookies med mera behöver marknadsavdelningen sannolikt bidra. För att ta några generella exempel.

Genom att arbeta löpande och systematiskt med dataskyddsfrågorna på ett förhållandevis konkret sätt signalerar man en strävan att faktiskt koppla lagstiftningen till den egna verksamheten i praktiken. I och med detta uppnår man förhoppningsvis också en ökad förståelse för att dessa frågor bidrar till förbättringar.

Kom ihåg att de allra flesta i en organisation inte är dataskyddsombud eller GDPR-ansvariga med integritetsfrågorna för ögonen varje dag. I slutänden är en verksamhets främsta mål troligtvis något annat än att uppnå hundraprocentig efterlevnad av GDPR. Men de som lyckas göra dataskyddsfrågorna till en integrerad del i vardagen på sin arbetsplats kan skapa en kultur där integritetsaspekterna inte uppfattas som ett nödvändigt ont, utan något som till och med kan stödja bredare strategiska mål.

Att förvalta GDPR-arbetet handlar i praktiken om att övervaka den egna organisationen över tid och se till att verksamheten fortsätter följa gällande dataskyddslagstiftning, även när det sker förändringar. Och förändringar sker hela tiden, antingen i den egna verksamheten eller i omvärlden. Genom att arbeta utifrån ett årshjul kan man säkerställa att man fortsätter ha kontroll. På lite sikt går det förhoppningsvis till och med att dra fördel av att allt är i ständig förändring.

VIKTORIA NORDSTRÖM

Är examinerad språkkonsult i svenska med ett stort intresse för att göra juridik och komplexa informationsmängder tillgängliga för en bredare målgrupp. Hon arbetar som produktägare och innehållsspecialist hos Draftit som tillhandahåller digitala verktyg, tjänster och kompetensstöd inom dataskyddsjuridik. Under de senaste åren har hon arbetat tillsammans med erfarna dataskyddsexperter och konsulter för att utveckla och förvalta ett omfattande kompetensstöd för GDPR som både förklarar det juridiska regelverket i sig och vägleder i den praktiska tillämpningen av det.

Skellefteå kommun testar ansiktsigenkänning

Hur kan man använda nya tekniska lösningar för att minska lärarnas administrativa uppgifter i klassrummet? I ett unikt pilotprojekt har Anderstorpsgymnasiet i Skellefteå kommun testat automatisk elevregistrering genom taggar, telefonappar och ansiktsigenkänning i samarbete med Tieto. Reaktionerna på projektet har varit positiva från både elever och lärare.

Varje år lägger lärarna på Anderstorpsgymnasiet i Skellefteå 17 280 timmar, motsvarande tio heltidstjänster, på att närvaroregistrera elever på lektionerna. Registreringen är en förutsättning eftersom lagstiftningen ställer krav på att skolan ska följa upp frånvaro och att skolor därför varje dag måste rapporteratill vårdnadshavarna hur närvaron ser ut på varje enskild lektion.

– Med automatisk registrering behöver inte eleverna längre oroa sig för att läraren tar fel på person eller glömmer bort att ge dem närvaro. Läraren kan dessutom komma igång med sina lektioner direkt, utan att bli störd av eftersläntrare. Vi ville hitta sätt att höja kvaliteten på skolan genom att lösa de här problemen, berättar Tommy Lindmark, IT-strateg, Skellefteå kommun.

Anderstorpsgymnasiet beslutade att skolan skulle delta i ett pilotprojekt tillsammans med Tieto där möjligheterna att införa automatisk registrering undersöktes. En klass valdes ut som testgrupp och de fick under åtta veckor genomföra försöket ”Future classroom”.

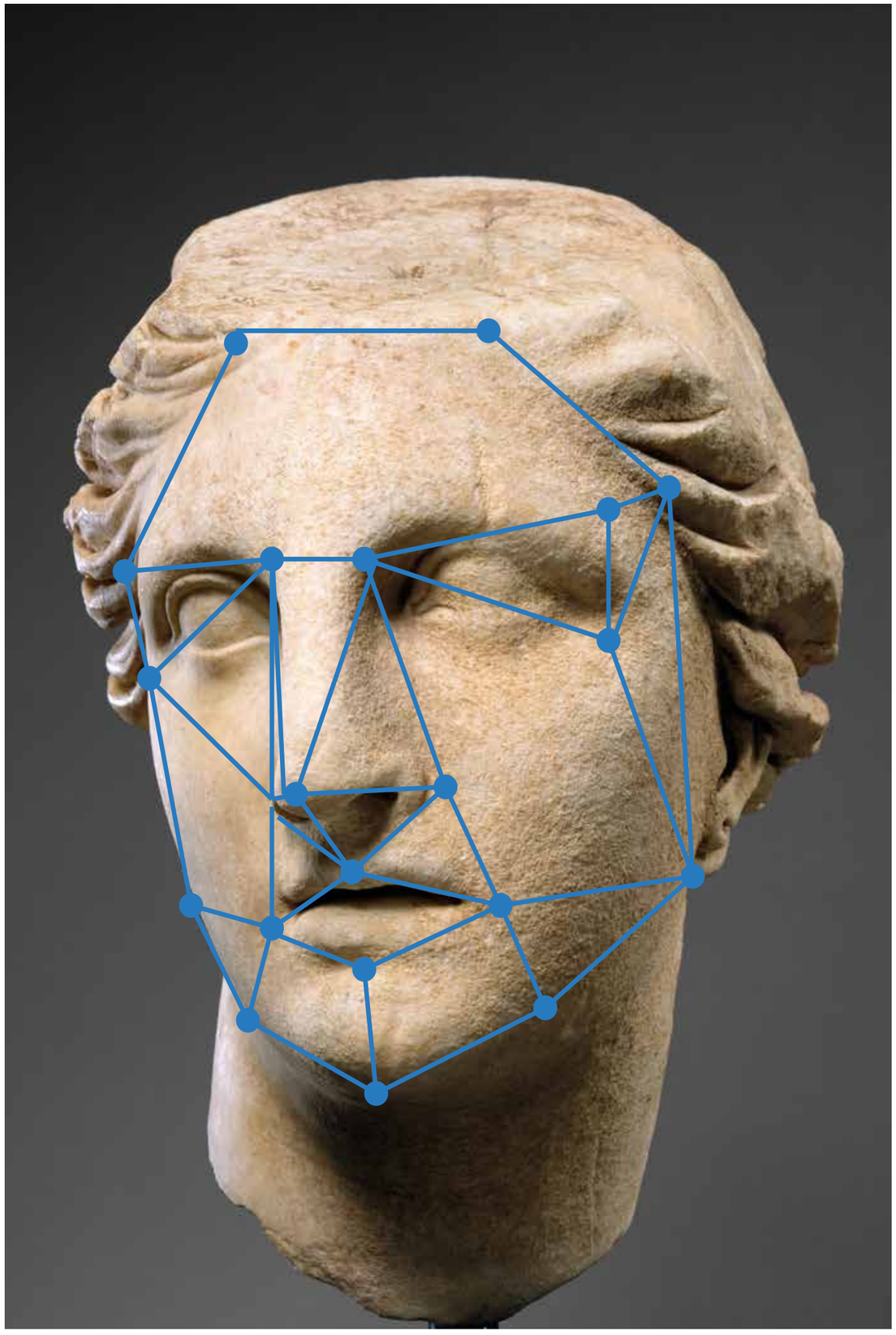
Elever och föräldrar fick ge sitt samtycke till personuppgiftsbehandlingen och man gick grundligt igenom säkerheten och rådgjorde med kommunens dataskyddsombud.

Flera olika tekniska lösningar undersöktes, bl.a. en smartphone-app, taggar som skulle registrera närvaron i en Raspberry pi (en minidator) och ansiktsigenkänning. Appen uteslöts tidigt eftersom det visade sig att de flesta elever hade Iphone och appen var enbart utvecklad för Android.

Taggen som användes var i form av ett kreditkort, fast tjockare, och registreringen gjordes via en inlåst mikroprocessor i klassrummet som känner av taggen på cirka 2 meters avstånd. Den kräver inget annat av eleven än att denne har med sin tagg. Det visade sig att det inte var helt lätt att komma ihåg att ta med sig taggen och vid testets andra vecka hade 60 % av eleverna glömt att ta med den till skolan. Detta gjorde att ansiktsigenkänning seglade upp som ett bättre alternativ.

Ansiktsigenkänningen hanterades med en enkel webbkamera som kopplades med en kabel till en inlåst minidator. Eleven fotograferas med ett antal bilder och med hjälp av en mjukvara lagras mätvärdena i minidatorn. När eleven passerar objektivets synfält jämförs bilden av eleven mot de mätpunkter som identifierar eleven. När punkterna överensstämmer till en viss procent tänds en grön lampa som indikerar att eleven är närvarande. Tekniken visade sig fungera bra och hanterar även avvikelser från den inlästa datan som skägg, glasögon eller keps. Utvärderingen av dessa lösningar gav vid handen att det som fungerade bäst var ansiktsigenkänning eftersom den var oberoende av tekniska hjälpmedel som att ett kort måste tas med eller att appen endast fungerar på Android.

En fördel med ansiktsigenkänning som eleverna har nämnt är att man inte behöver ha med sig något för att bli registrerad – man kan inte glömma sitt ansikte hemma. Skolan och kommunen kommer nu att utvärdera resultatet för att se om man vill gå vidare med automatisk registrering som en permanent lösning.



Den tekniska lösningen var relativt enkel och krävde ingen dyr utrustning i det här fallet även om en fortsättning på projektet kan komma att innehålla betydligt mer avancerad utrustning. Det var en billig kamera som användes och en framtida lösning kommer sannolikt att använda utrustning av högre kvalitet och tillförlitlighet.

Projektet fick stor uppmärksamhet både i branschmedia och i riksnyheter och uppmärksammades också med ett pris. Branschföreningen IT SMF Sverige tilldelade projektet pris för bästa ”It Service Management-projekt” med motiveringen ”Med ett pragmatiskt förhållningssätt och användandet av moderna IT-teknologier och metoder så har initiativet tagit ett problem och löst det på ett innovativt sätt”.

Projektet uppmärksammades också av Datainspektionen som tyvärr inte ansåg att fördelarna med förbättrad kvalitet och säker närvaroregistrering motiverade personuppgiftsbehandlingen. Datainspektionen påbörjade i stället en tillsyn där de inledningsvis ställde ett antal frågor om hur projektet hade hanterat bestämmelserna i dataskyddsförordningen bland annat den rättsliga grunden för behandlingen, om kommunen hade gjort en konsekvensbedömning och varför inte ett förhandssamråd hade begärts.

Skellefteå kommun besvarade frågorna som ställdes i samband med tillsynen och antog att det endast handlade om en formell tillsyn med frågor som skulle besvaras och att Datainspektionen skulle nöja sig med det gediget genomförda förarbetet som gjorts med eventuellt några anmärkningar rörande detaljer som kunde ha gjorts bättre.

Men Datainspektionen gjorde en helt annan bedömning än kommunen och i det beslut som fattades var budskapet att kommunen hade brutit mot tre artiklar i dataskyddsförordningen:

artikel 5 dataskyddsförordningen genom att behandla elevers personuppgifter på ett för den personliga integriteten mer ingripande sätt och omfattat fler personuppgifter än vad som är nödvändigt för det angivna ändamålet (närvarokontroll),

artikel 9 genom att ha behandlat känsliga personuppgifter (biometriska uppgifter) utan att för behandlingen ha ett giltigt undantag från förbudet att behandla känsliga personuppgifter och

artiklarna 35 och 36 genom att inte ha uppfyllt kraven på en konsekvensbedömning och inte ha kommit in med ett förhandssamråd till Datainspektionen.

Datainspektionen ansåg att elever inte kan lämna ett samtycke till personuppgiftsbehandlingen eftersom de är i en beroendeställning till skolan och därför sannolikt inte gjort detta frivilligt. Enligt Datainspektionens anvisningar är samtycke inte möjligt att göra i offentlig sektor eftersom den enskilde alltid är i beroendeställning gentemot det allmänna och kan därför inte användas som grund för personuppgiftsbehandling. Det innebär att personuppgiftsbehandlingen enligt deras förmenande saknar laglig grund. De anser också att eftersom det handlar om ny teknik måste både konsekvensbedömning och förhandssamråd genomföras. Gymnasienämnden, som är personuppgiftsansvarig för behandlingen, beslutade att överklaga beslutet med följande motiveringar:

”Kommunen delar inte heller uppfattningen att det handlar om ny teknik eftersom ansiktsigenkänning som metod har användsoch de senaste tio åren fått en allt större spridning.”

Eleverna och elevernas vårdnadshavare har lämnat sitt samtycke och delar uppenbarligen inte Datainspektionens uppfattning att de är i en beroendeställning gentemot skolan vilket framgår av intervjuer med eleverna men också av att det var sju av 29 elever som valde att inte delta i försöket.

Eftersom Datainspektionen i sitt tillsynsbeslut hade skrivit att det var osannolikt att eleverna skulle ha lämnat sitt medgivande frivilligt och kommunen inte delade den uppfattningen kändes det viktigt att fånga in elevernas uppfattning på nytt och ta med deras synpunkter i det överklagande som lämnades in till förvaltningsrätten i Stockholm.

Kommunens dataskyddsombud och projektledare tog kontakt med skolan för att genomföra intervjuer med de elever som hade varit med i projektet. Klassen besöktes och eleverna fick svara på frågor om hur de upplevt försöket med ansiktsigenkänning.

Klassen som helhet var positiv och bekräftade de synpunkter som hade kommit fram i försöket. Det vill säga att de tyckte att det var intressant att vara med. De kände sig trygga med registreringen med hjälp av en optisk lins där de faktiskt kunde se att de blev närvaroregistrerade eftersom en lampa blinkade grönt när de passerade genom klassrumsdörren. De kände inte att de var tvingade att delta eller att det skulle ha fått konsekvenser om de valt att avstå.

Därefter valdes slumpmässigt tre elever ut för att genomföra individuella intervjuer. Det resultatet skilde sig inte från det som hela gruppen vittnat om.

Nedan följer citat från besöket som genomfördes:

Elev 1 –
”Jag ville vara med men jag kunde inte, mina föräldrar bor i annan kommun och kunde inte skriva på samtycket.”

Elev 2 –
”Det var ju frivilligt, man kunde vara med eller inte och om man valde att vara med skulle föräldrarna skriva på.” ”Det var ingen påverkan, både jag och resten av klassen tyckte att det skulle vara roligt att vara med.” ”Man hade ju ett val om man ville vara med eller inte – man fick ju säga nej.”

Elev 3 –
”Det var flera som sa att de inte ville vara med – men det spelade ingen roll för mig, jag ville vara med.”

Elev 4 –
”Jag var en av eleverna som sa nej och jag kände mig inte tvingad. Tieto var väldigt tydliga i att om du vill vara med så får du vara med och om du inte vill vara med så behöver du inte vara med.” ”Om jag skulle få frågan idag så skulle jag vilja vara med för jag tycker det är en intressant teknik och det underlättar arbetet för lärarna.”

Elev 5 –
”Dom som inte ville vara med sa det direkt och då var dom inte med liksom.” ”Det var en kul grej som man ville vara med på för att se vad som skulle hända.”

Elev 6 –
”Det var väldigt mycket information från projektet och även en och en. ”Jag kände inte att man var tvungen och jag var inte med från början för jag hade glömt att lämna in mitt medgivande och kom in med det senare för att jag ville verkligen vara med Den information som getts har också varit tydlig både muntligt och skriftligt där det framgått att det är frivilligt att vara med och att de som inte vill delta är fria att avstå utan att det får några konsekvenser.”

Det finns också stöd för uppfattningen att det är möjligt att delta i frivilliga integritetskänsliga projekt om informationen är tydlig. Detta har Justitieombudsmannen fastslagit i ett beslut som visserligen inte rör ansiktsigenkänning men frivilliga drogtester som också är känsliga personuppgifter. Dessa uppgifter har minst lika hög grad av känslighet ur dataskyddslagstiftningens synpunkt och de är därtill också sekretessbelagda i enlighet med offentlighets- och sekretesslagen.

Den blankett som användes för samtycke såg ut så här:

SAMTYCKE FÖR DELTAGANDE I PROJEKT
FRAMTIDENS KLASSRUM ANDERSTORSPS
GYMNASIUM SEPTEMBER TILL DECEMBER 2018

Jag har tagit del av informationen kring studien och är medveten om hur den kommer att gå till.

Jag/Mitt barn deltar i denna studie helt frivilligt och har blivit informerad om vad syftet med deltagandet är.

Jag ger mitt medgivande till Tieto Sweden AB att lagra och bearbeta den information som insamlas under studien under den angivna studieperioden.

Elevens namn
Elevens signatur
Vårdnadshavarens Namn (för elever under 18 år):
Vårdnadshavare signatur (för elev under 18 år):

Kommunen delar inte heller uppfattningen att det handlar om ny teknik eftersom ansiktsigenkänning som metod har använts och de senaste tio åren fått en allt större spridning.
En googling på ”facial recognition” visar att tekniken användes redan i mitten på 60-talet av den amerikanska militären och kan därför knappast anses som tekniskt revolutionerande även om det kanske är första gången den används just för det här ändamålet.

Förvaltningsrätten i Stockholm har fattat beslut i ärendet och har utan annan motivering än att förvaltningsrätten anser att det inte har kommit fram skäl att göra någon annan bedömning än den Datainspektionen gjort i det överklagade beslutet beslutat avslå överklagan. Datainspektionen har således enligt Förvaltningsrätten haft fog för sitt beslut och överklagandet ska därför avslås.

Om beslutet från Datainspektionen blir prejudicerande kommer det att få konsekvenser för möjligheten att förbättra kvaliteten i den offentliga sektorn med hjälp av ny teknik om biometriska data inte kan användas med samtycke som grund.SKR, som är intresseorganisation för Sveriges kommuner, Kommer därför att hjälpa till att granska beslutet och formulera en Ansökan om prövningstillstånd och ytterligare skäl för överklagan till Kammarrätten med motiveringen att det är av vikt för stor vikt för rättskipningen att beslutet tolkas. Det är första gången en myndighet får en sanktionsavgift enligt dataskyddslagstiftningen och det första gången frågan om samtycke inom den offentliga sektorn prövas.

Det skulle inte förvåna om det här går ända upp till Högsta förvaltningsdomstolen med tanke på ärendet principiella betydelse
för möjligheten att utveckla välfärden i offentlig sektor.

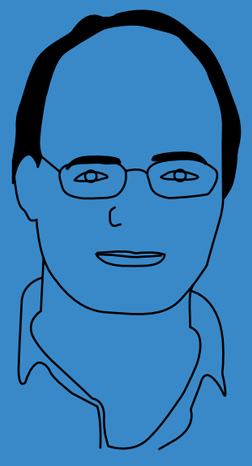
Skellefteå kommun ser fram emot att få ett avgörande i den här frågan som kommer att få stor betydelse både för kommunens möjligheter att utveckla välfärden med modern teknik men också genom att avgörandet får prejudicerande effekt för hela myndighetssverige.

Vidare läsning

https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

https://computersweden.idg.se/2.2683/1.723024/skellefteå-overklagar-gdpr-bot

https://www.bbc.com/news/technology-49489154



ISAK NYBERG

Beskriver sig själv som en äldre byråkrat i en större kommun vars huvudsakliga uppgifter är att arbeta med informationssäkerhet och dataskydd. Jag är också dataskyddsombud åt de flesta nämnder i Skellefteå kommun samt även åt en rad inlandskommuner (Vilhelmina, Åsele, Dorotea, Norsjö, Malå, Arjeplog och Sorsele).

Två år med GDPR

– Lagen som stärker skyddet för hur dina personuppgifter får hanteras

Dataskyddsförordningen, GDPR, trädde i kraft för två år sedan. Datainspektionen är den myndighet i Sverige som ska se till att företag, myndigheter och andra organisationer följer reglerna i GDPR. Här redovisar Datainspektionen vad som har hänt under de här två händelserika åren.

Den 25 maj 2018 trädde dataskyddsförordningen i kraft i Sverige. Ska man vara petig heter lagstiftningen egentligen den allmänna dataskyddsförordningen, vilket på engelska blir General Data Protection Regulation som i sin tur förkortas GDPR, en förkortning som ofta används även i Sverige.

GDPR är en EU-förordning som reglerar behandlingen av personuppgifter. Att det är en EU-förordning innebär att reglerna gäller som lag direkt och på samma sätt i alla EU:s medlemsstater, till skillnad från tidigare, då respektive land hade sin egen tolkning eller ”dialekt” på ett dataskyddsdirektiv från 1995. Den svenska tolkningen av direktivet var personuppgiftslagen, som alltså ersattes av GDPR för två år sedan.

I all korthet innebär GDPR en modernisering av lagstiftningen som reglerar hur personuppgifter får samlas in och användas. Den stärker rättigheterna för enskilda och höjer kraven på de företag, myndigheter och andra organisationer som hanterar personuppgifter.

För Datainspektionen har GDPR inneburit stora förändringar. Ett tydligt exempel är att myndigheten nästan fördubblat sin personalstyrka. 2017 hade myndigheten 57 medarbetare. 2019 arbetade 93 personer på myndigheten.

En stor nyhet i GDPR är att Datainspektionen nu kan utfärda så kallade administrativa sanktionsavgifter mot företag och andra organisationer som bryter mot reglerna i lagstiftningen. För företag är maxgränsen densamma i hela EU, 20 miljoner euro eller fyra procent av bolagets globala årsomsättning, beroende på vilket belopp som är högst. För offentliga verksamheter får sanktionsavgifter regleras nationellt, i Sverige är maxgränsen tio miljoner svenska kronor.

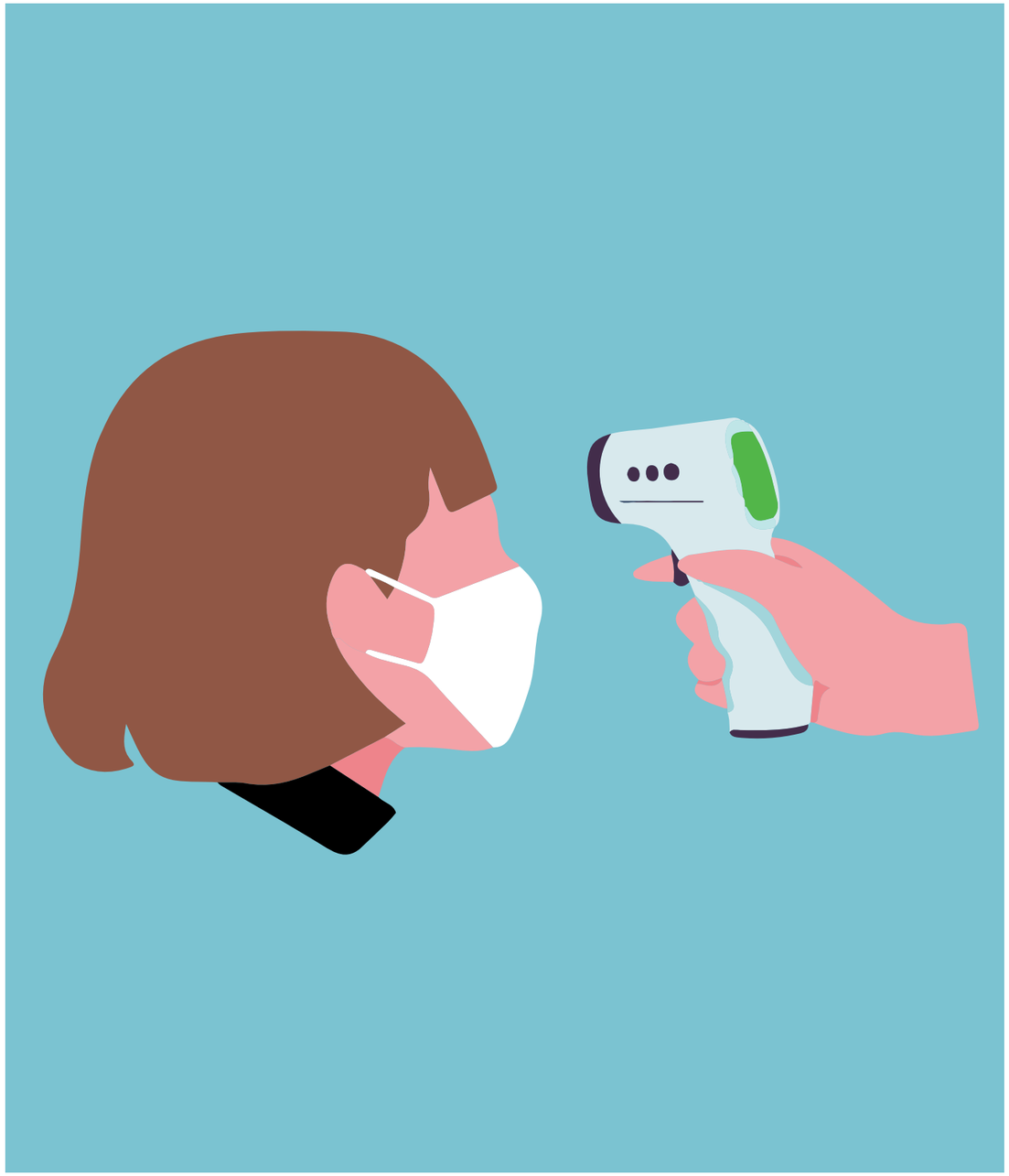
Under 2019 utfärdade Datainspektionen två administrativa sanktionsavgifter. I år har myndigheten hittills utfärdat tre sanktionsavgifter. Beloppen varierar från 120 000 kronor upp till 75 miljoner kronor.

En annan nyhet i GDPR är att företag och andra organisationer är skyldiga att anmäla vissa personuppgiftsincidenter till Datainspektionen. En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Det kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer.

Under 2018, från 25 maj och framåt, anmäldes drygt 2 250 incidenter till Datainspektionen enligt GDPR. Under 2019 anmäldes strax över 4 700 incidenter. Under 2019 har Datainspektionen inlett ett tiotal granskningar baserat på anmälda personuppgiftsincidenter.

Datainspektionen arbetar löpande med att producera rapporter där olika delar av ärendeinflödet till myndigheten beskrivs närmare. Syftet med rapporterna är att beskriva generella mönster och iakttagelser från inflödet till Datainspektionen samt att ge ett underlag som privata och offentliga verksamheter kan använda i sitt fortsatta dataskyddsarbete och bidra till en generell kunskapshöjning om integritet och dataskydd.

Hittills i år har Datainspektionen publicerat tre rapporter. En rapport går igenom de personuppgiftsincidenter som anmäldes 2019. En annan rapport analyserar specifikt de personuppgiftsincidenter som orsakats av olika former av it-angrepp som exempelvis så kallat nätfiske och spionprogram. Den tredje rapporten



beskriver de klagomål som myndigheten tagit emot som rör personsöktjänster, alltså sajter som masspublicerar personuppgifter. Närmare vart femte klagomål som Datainspektionen tagit emot sedan GDPR trädde i kraft rör personsöktjänster.

De här rapporterna är en del i Datainspektionens utåtriktade arbete. Under 2018 och 2019 har myndigheten satsat mycket på just utåtriktat arbete. Varje vardag finns jurister tillgängliga i myndighetens Upplysningstjänst för att svara på frågor via telefon och e-post från företag, myndigheter och andra organisationer men även från privatpersoner.

Och frågor ställs. Under 2019 besvarade Upplysningstjänsten över 8 300 telefonsamtal och tog emot över 5 100 frågeställningar via e-post.

Enligt Nationell Integritetsrapport som Datainspektionen publicerade i maj 2019 handlar ungefär en tiondel av alla frågor från medborgare om kamerabevakning.

Den 1 augusti 2018 trädde den nya kamerabevakningslagen i kraft. Enligt den är det Datainspektionen som är tillsynsmyndighet för den kamerabevakning som bedrivs i Sverige. Det är alltså Datainspektionen som ska kontrollera att företag och andra sköter sin kamerabevakning lagenligt. En nyhet med lagen är att det även är Datainspektionen som ska utfärda tillstånd för kamerabevakning. Tidigare gjordes det av landets 21 länsstyrelser.

”I kölvattnet av coronaviruset har det dykt upp en rad nya frågeställningar i samhället som rör hanteringen av personuppgifter.”

I början av 2019 fattade myndigheten beslut i ett tiotal granskningar som rörde privatpersoners kamerabevakning av grannar. Datainspektionen konstaterade att en husägare inte får rikta sin bevakningskamera så att den övervakar andra grannars tomter eller hus.

Går det att skriva en artikel i juni 2020 utan att nämna det nya coronaviruset eller covid-19? Det känns knappast troligt. Coronapandemin har påverkat Datainspektionen på en rad olika sätt. En absolut majoritet av personalen arbetar numera på distans. Endast ett fåtal anställda är på plats på kontoret för att exempelvis hantera fysiska akter, ärenden med hög sekretess eller utlämning av allmänna handlingar.

Den sociala distanseringen har lett till att Datainspektionen i nuläget inte kan göra inspektioner på plats hos företag eller andra organisationer som ska granskas. I stället görs det som internt kallas för skrivbordstillsyn, då ett antal frågor skriftligen ställs till organisationen som ska granskas vilka organisationen är skyldig att besvara sanningsenligt.

I kölvattnet av coronaviruset har det dykt upp en rad nya frågeställningar i samhället som rör hanteringen av personuppgifter. Vad ska man tänka på vid distansundervisning? Får företag registrera uppgifter om att de anställda haft covid-19? Får jag som arbetsgivare informera anställda om att en kollega kan ha smittats av coronaviruset?

Datainspektionen har på kort tid tagit fram coronarelaterad information på sin webbplats som besvarar några av de vanligaste frågorna.

Som redan nämnts är GDPR en lagstiftning som gäller likadant inom hela EU. Det har lett till ett betydligt intensivare samarbete mellan dataskyddsmyndigheterna i EU än tidigare. Ett exempel på det är den Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB), som är ett oberoende europeiskt organ som ska bidra till en enhetlig tillämpning av dataskyddsreglerna inom hela EU/EES samt främja samarbetet mellan dataskyddsmyndigheterna.

Under EDPB finns ett antal arbetsgrupper som arbetar med vägledning och rekommendationer för att klargöra lagstiftningen och med att ta fram riktlinjer och praxis. Datainspektionens inriktning har varit att åta sig rollen att leda arbetet med riktlinjer som är särskilt angelägna för svenska företag och andra verksamheter. I dagsläget har myndigheten rollen som huvud- eller medrapportör för sammanlagt sju pågående arbeten med riktlinjer. Under 2019 deltog Datainspektionen i samtliga styrelsemöten och underarbetsgrupper inom EDPB, vilket inneburit sammanlagt nästan 90 möten.

Datainspektionen har under de två år som gått sedan GDPR trädde ikraft lagt mycket krut på utåtriktat arbete. En viktig del i det arbetet är de utbildningar och konferenser som myndigheten ordnar. Under 2019 höll myndigheten 19 egna utbildningar och deltog i över 40 föreläsningar som ordnades av andra aktörer.

I maj 2019 ordnade Datainspektionen konferenser i Stockholm, Göteborg och Malmö på temat ”Ett år med dataskyddsreformen”. På konferenserna deltog experter från myndigheten men även andra svenska och internationella talare.

I år var tanken att myndigheten skulle anordna en motsvarande konferens fast nu så klart på temat ”Två år med dataskyddsreformen”. Konferensen skulle gå av stapeln den 25 maj 2020, på tvåårsdagen av att GDPR trädde i kraft.

Pandemin tvingade myndigheten att ställa in konferensen. Eller åtminstone den fysiska konferensen i Stockholm. I stället publicerade Datainspektionen en variant av konferensen på sin webbplats i form av sju videofilmer som tar upp delar av det som nämnts i den här artikeln, som exempelvis myndighetens internationella arbete, hantering av personuppgifter i samband med coronapandemin och personuppgiftsincidenter som uppstått via it-angrepp.

Länkar

Videofilmerna från tvåårskonferensen
www.datainspektionen.se/utbildningar/tva-ar-med-dataskyddsreformen/

Personuppgifter och corona
www.datainspektionen.se/corona/

Prenumerera på Datainspektionens pressmeddelanden
www.datainspektionen.se/press/prenumerera-pa-pressmeddelanden/

Följ Datainspektionen på Twitter
@Datainspektion

Följ Datainspektionen på LinkedIn
www.linkedin.com/company/datainspektion/

PER LÖVGREN

Pressansvarig på Datainspektionen.

Datainspektionens huvuduppgifter är att:

- granska och verkställa tillämpningen av dataskyddsreglerna
- ge vägledning och stöd till myndigheter, företag och organisationer samt till allmänheten
- bidra till en enhetlig tillämpning av dataskyddreglerna inom EU
- utfärda tillstånd och genomföra tillsyn avseende kamerabevakning, inkassoverksamhet och kreditupplysning
- följa och rapportera om utvecklingen inom integritetsområdet

Experience of the Austrian data protection authority when enforcing article 83 GDPR

Since the GDPR became applicable, the Austrian Data Protection Authority, as the competent Supervisory Authority of Austria pursuant to Article 58 paragraph 2 (i) GDPR, has been tasked with the fining of violations of the GDPR in accordance with Article 83.

In this context, the Austrian Data Protection Authority (hereinafter Austrian DPA) has imposed 38 fines and 11 reprimands within the meaning of Article 58 paragraph 2 (b) GDPR. In total, the Austrian DPA has imposed fines totaling €18,106,700.00.

Pursued Infringements

In the following paragraphs, essential case constellations are presented which, from the perspective of the Austrian DPA, have played a central role in the enforcement practice.

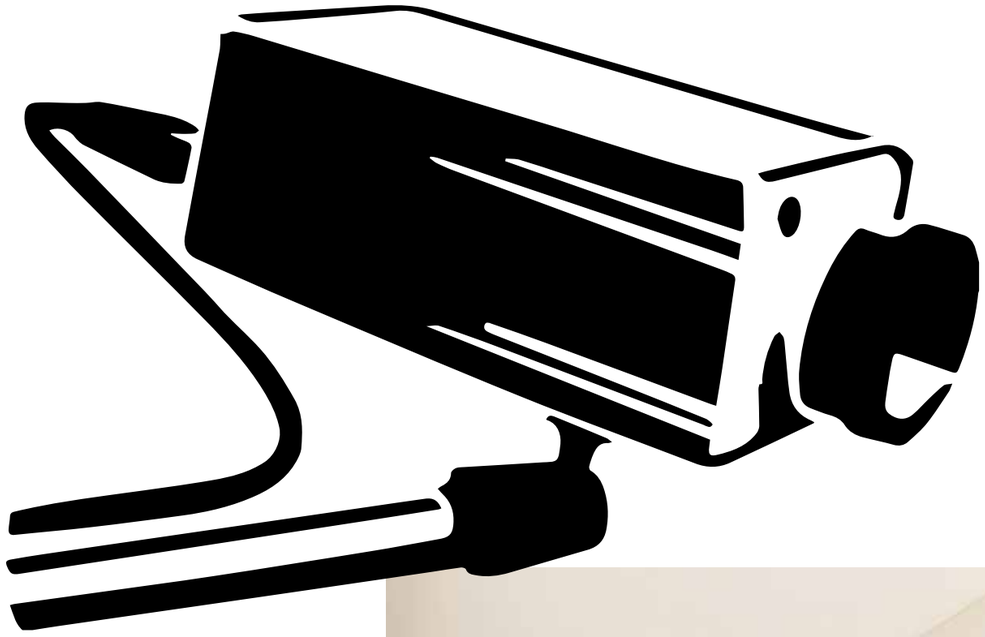
Image Processing

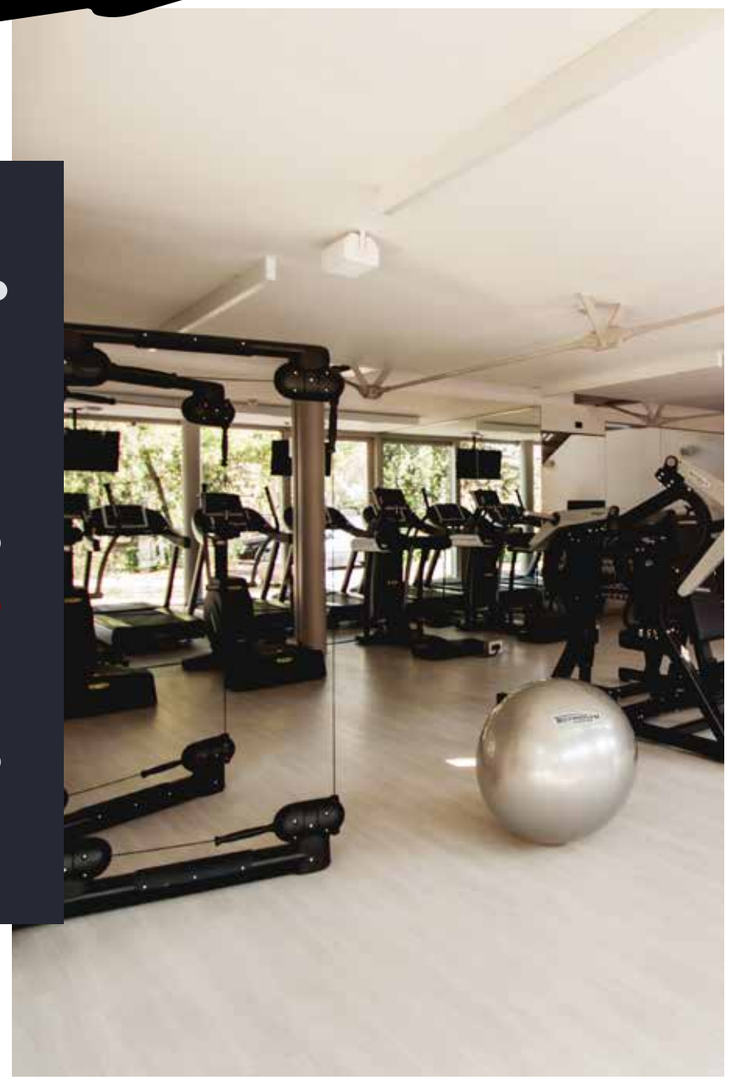
Particularly in cases of proceedings against private individuals, the (unlawful) operation of image processing systems, such as video surveillance systems in and on private buildings, and camera systems installed in vehicles (dash cams), has been in the center when imposing fines in accordance with Article 83 GDPR.

It has been demonstrated time and again that many controllers are unaware that the use of video surveillance systems, such as those mounted for surveillance of the outside area of their home or apartment, could infringe the rights of data subjects. In particular, where the surveyed area includes (parts of) public areas (i.e. sidewalks and parts of streets) video surveillance systems could infringe both the data processing principles as foreseen in Article 5 para 1 GDPR as well as Article 6 para 1 GDPR. In addition, fines have been imposed on controllers who operated a dashcam in their car and recorded public street traffic, and thus other public street traffic users, over longer periods of time. In a particularly serious case, the Austrian DPA fined the coach of a women’s soccer team with € 10,000 (not final) for covertly filming two soccer players in the dressing room, while being naked and taking a shower.

Regarding the data protection qualification of image processing operations, a recent judgment of the European Court of Justice, hereinafter referred to as CJEU, (Case C-708/18 dated December 11, 2019) must be mentioned. Although the judgment was based on Directive 95/46 (Data Protection Directive, hereinafter referred to as Directive), it remains relevant for the assessment of the legality of image processing systems with regard to the processing principles and legal grounds. The subject matter was whether a video surveillance system operated in a multi-party apartment building – which had been instigated by the co-owners to protect the security of the residents and their property as a result of multiple cases of burglary and property damage – is in line with the requirements regarding the lawfulness of data processing operations under the Directive. According to the legal assessment of the CJEU, the operation of a video surveillance system can, in principle, be based on Article 7 (f) of the Directive (now Article 6 para 1 (f) GDPR]. Consent of the data subjects (= residents) is not necessarily required. However, the CJEU stressed that any data processing must comply with all principles of Article 6 of the Directive [now Article 5 para 1 GDPR] and with at least one of the legal grounds as regulated in Article 7 of the Directive [now Article 6 para 1 GDPR].

The objective which the controller essentially seeks to achieve when he or she installs a video surveillance system, namely protecting the property or the health and life of the





co-owners of a building, is likely to be characterized as a legitimate interest, as defined in the former Article 7 (f) of the Directive [now Article 6 para 1 (f) GDPR].

In regard to the legitimate interest(s), it must be stated that this/these must have arisen before and existed at the time of processing; they must not only be hypothetical at this point in time. However, it is not imperative that the security of people's property has previously been compromised: burglaries or property damage that occurred previously can in any case be taken as an indication of the existence of a legitimate interest.

"In a particularly serious case, the Austrian DPA fined the coach of a women's soccer team with € 10,000 (not final) for covertly filming two soccer players in the dressing room, while being naked and taking a shower."

The necessity of processing (the second prerequisite as per Article 6 para 1 (f) GDPR) requires that the objective cannot be achieved by using less interfering measures. Hence, and in line with the principle of data minimization pursuant to Article 5 para 1 (c) GDPR, it may be necessary to use a different method for providing the security of the building (e.g. security doors and improved locks).

In order to weigh the interests as per Article 6 para 1 (f) GDPR, the legitimate expectations of the data subjects must also be taken into account: residents of a multi-party residential complex in which burglaries and property damage have already occurred several times can reasonably expect that video surveillance is used in view of the incidents that have occurred. In strong contrast to this, for example, data subjects can trust that their privacy is guaranteed in places such as changing rooms or sanitary facilities and that in such places no video surveillance takes place.

The listed points, which result from the jurisprudence of the CJEU can be used as a guideline for the assessment of any form of image processing (stationary, mobile, dash cam). In any case, however, a case by case assessment is required, in which the interests of the controller and the legitimate interests of data subjects and their expectations are carefully balanced.

Direct Marketing und Data Brokering

The Austrian DPA imposed an administrative fine of 18 million Euros on Österreichische Post AG (ÖPAG – Austrian Post) following administrative fine proceedings with decision of 23 October 2019. After conducting an investigation and an oral hearing, the data protection authority considered it proven that ÖPAG had violated the GDPR by processing personal data on the alleged political affinity of data subjects. In addition, ÖPAG violated the law due to the further processing of data regarding the package frequency and the frequency of relocations for the purpose of direct marketing.

As these violations were committed unlawfully and with negligence, the Austrian DPA considers the abovementioned administrative fine as appropriate to prevent other or similar violations. The fine imposed is not yet final, as the controller filed an appeal to the Federal Administrative Court.

Other Infringements

In another decision, the Austrian DPA fined the operator of a medical center with € 50,000. In this case, the controller violated the GDPR in several respects, namely, among others:

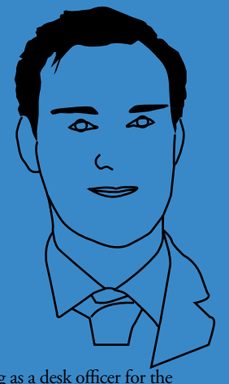
-by not designating a data protection officer as per Article 37 para 1 (c) GDPR and failing to meet the obligations under Article 37 para 7 to publish the contact details of the data protection officer and notify the DPA of these data;

-by not complying with the requirements for obtaining consent from patients as per Article 7 para 2 GDPR: items not subject to consent and items subject to consent were integrated into one written consent form, without a distinguishable separation thereof, giving the appearance that consent was required for all items; the declaration of consent failed to provide sufficient clarity for what the consent should be the legal basis; and

- by failing to meet the obligation to examine the need to carry out data processing impact assess ments in accordance with Article 35 GDPR with regard to data processing processes typically taking place in a health facility, such as the administration of medical reports and other patient data.

Coherent Union-Wide Enforcement

To achieve the objective of a coherent implementation of Article 83 GDPR across the Union, the Austrian DPA, together with the representatives of the supervisory authorities of the other Member States, is a member of the European Data Protection Board. The Board is set up as a body of the Union with legal personality according to Article 68 para 1 GDPR and independently fulfills the tasks assigned to it by the GDPR. The Board devises in various working groups, amongst other things, guidelines within the meaning of Article 70 para 1 (k) GDPR, which are adopted by resolution in plenary. These (non-binding) guidelines serve to further interpret individual provisions of the GDPR and are therefore also available online.



HERWIG ZACZEK

Lawyer, has been working as a desk officer for the Austrian Data Protection Authority in the department for imposing fines according to Article 83 GDPR since mid-2018. Before joining the Austrian Data Protection Authority, he worked as a lawyer in the Federal Ministry of Labor, Social Affairs, Health and Consumer Protection for six years.

A look at our neighbours

– How Lithuania work with GDPR

In Sweden we mostly hear about what happens inside our own boarders or when big fines are issued in another EU country. But we never hear about the everyday work in Lithuania and how the country prepared for the new regulation and how it changed the work regarding these questions there.

In Comparison with Sweden the Republic of Lithuania is a quite new state, born again after the resolution of the Soviet Union where they in many ways had to start from scratch, building a government. In many cases this means that they had the opportunity to build it without a legacy to carry and most often, as a cause of this, you find the old Baltic states among the countries who have developed an extensive technological environment for their public offices. To learn more about this we contacted personal data protection supervisory authority of Lithuania – the State Data Protection Inspectorate (Inspectorate) and had the opportunity to ask some questions about the data regulation to their head Raimondas Andrijauskas. We spoke about how the regulation changed how the country views issues concerning personal data and, of course, the fines.

We started our interview with perhaps the standard question these days: How has the work with personal data changed since the 25th of May 2018? Raimondas Andrijauskas says that during the run-up to the General Data Protection Regulation (GDPR), there was a stir in the data protection community in Lithuania. Furthermore, he says that even before the official starting day of application of the new regulatory framework of personal data protection the society felt a significant impact from the personal data protection reform. Since then, he explains, society itself has become more self-conscious and better informed about its rights and about the potential risks that are related to their personal data processing and organizations have begun to pay more attention to data protection. As a supervisory authority, Raimondas Andrijauskas explains, we have made organizational and activity changes within the institution.

In the run-up to the reform Raimondas Andrijauskas recalls that the financial and human resources were not the strongest part of the Inspectorate. Eventually additional funding was provided for supervisory authority and it increased from EUR 729 K in 2017 to 1111 K in 2018. Furthermore, the Inspectorate faced a major challenge in the brain drain of the Inspectorate's staff to the public and private sector. Raimondas Andrijauskas says that this was a result of the shortage of and the growing demand for personal data protection specialists that was required for filling in new data protection officer vacancies under the GDPR. However, thanks to a remaining strong core of the institution and a new staff committed to changes, the Inspectorate have been able to meet this extraordinary challenge. At the end of 2019 we received additional human resources and were able to increase the number of staff from 32 to 38 people working at the Inspectorate (there are also currently 4 unoccupied posts). Most of the employees are lawyers (23 of them), following with four IT specialists also such specialists as an accountant, HR and PR.

This year, Raimondas Andrijauskas goes on to tell, Lithuania celebrates the 30th Anniversary of the Restoration of Independence. Together with the restoration of independence, the history of human rights such as privacy and personal data protection in our country began. In 1996 the first law regulating the protection of personal data was adopted in Lithuania and the supervisory authority was set up in the same year. The approach to data protection strengthened when Lithuania became a member state candidate of the European

Union because Directive 95/46/EC was implemented in Law of Republic of Lithuania on Legal Protection of Personal Data in 2003. Following the implementation of the Directive, communication and cooperation were largely carried out with the other two Baltic states – Latvia and Estonia. We organized investigations in the same sectors on the processing of personal data, Raimondas Andrijauskas recalls, and we also shared experiences, good practices. Raimondas Andrijauskas says that it must be acknowledged that the GDPR has led to closer cooperation between all the EU member states and that undoubtedly one of the biggest impacts to data protection was caused by the GDPR.

As to the question about cooperation Raimondas Andrijauskas answers that has two aspects – one national and one international. At the national level, the Inspectorate is responsible for the supervision of GDPR, except when personal data is processed for journalistic, academic, artistic or literary purposes. The supervisory tasks for these purposes belong to the Inspector of Journalist Ethics. So we also cooperate with our colleagues at the national level. Concerning the cooperation at the level of the European Union, says Raimondas Andrijauskas;

"that is the essence of GDPR – to achieve the most uniform regulation of the processing of personal data in the EU."

–It´s is one of our priorities. After all, he continues, that is the essence of GDPR – to achieve the most uniform regulation of the processing of personal data in the EU to ensure the proper processing of personal data across borders and to create a well-functioning single market. As the Head of Lithuanian supervisory authority, I am a member of the European Data Protection Board (EDPB), other employees of the institution participate in the activities of EDPB working groups. Also, we resolve cross-border cases if necessary, we constantly consult and exchange information with the supervisory authorities of other EU countries.

We have to know, was it hard to implement the new regulation and could you see a difference between a non-governmental organization (NGO) or a state agency?

– As it often is with new legislation, when the rules are new and the practice is evolving, there will always be some difficulties. However, in general, I believe that the goals of EU data protection reform were achieved. There were some data controllers and data processors who did not give enough attention to new data protection requirements. However, this is one of the tasks of supervisory authority – to inform data controllers and data processors about their obligations and benefits of following the rules set in the GDPR. It would be hard to generalize to whom it was harder to implement the GDPR. I believe that it depends on specific NGO or state agency, their processing operations, resources, etc.

How many complaints have you received in concern to the GDPR from both state agencies, companies and the public? How many of them have led to an investigation?

Concerning the complaints from individuals, Raimondas Andrijauskas says that under the laws of Lithuania, the Inspectorate examines all complaints. In concern to the GDPR, they have already received 1716 complaints. He says that the number of complaints has almost doubled from 2017 to 2018 and that this is the effect of the GDPR. He continues to say that it is important to note that as a supervisory authority we also carry out investigations on our own initiative. Every year we have planned investigations on certain sectors, also investigations may be carried out when we receive information from the media or individuals and organizations about possible data breaches, etc.

	2017	2018	2019	2020 1st quarter
Complaints received by individuals	*480*	*859*	*880*	*281*
Investigated complaints	*490*	*619*	*995*	*260*
Investigations on our own initiative	*91*	*141*	*112*	*13*

As a result of the regulation Raimondas Andrijauskas tells us that in 2019 the Inspectorate issued six fines and that the first significant fine (EUR 61,5k) was for breaches of the GDPR imposed on a financial services company, following a personal data breach in the payment initiation service system, which, among other things, had not been reported to the Inspectorate. The sanctions were imposed for the breaches of Articles 5, 32 and 33 of the GDPR.[1]

We are also curious to know if you see a larger awareness in the Lithuanian society towards handling personal data? Raimondas Andrijauskas answers that the importance and rising awareness of personal data protection can be proved by numbers of the representative public opinion survey on personal data protection. According to this survey at the end of 2019 68 % (the same numbers in 2018) of the respondents gave an affirmative answer to the question whether they were aware of or believed to be aware of their statutory rights and duties in the area of personal data protection. Compared against 35 % in 2016 this demonstrates that from 2016 to 2018 and 2019 a proportion of people aware of their rights and duties around personal data protection grew almost twofold. By the way, these numbers between representatives of small and medium-sized businesses are even higher – 90 %. Raimondas Andrijauskas continues to say that this statistical information is very important to the Inspectorate and that it also shows our contribution to raising the awareness of various stakeholders. He brings up the example of the SolPriPa project – Promoting High Standards of Data Protection as a Fundamental Right and Central Factor of Consumer Trust in Digital Economy. It is partly funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020), where they partnered up with Mykolas Romeris University in Vilnius. In the project the target audiences are Lithuanian small and medium-sized businesses, especially in health care and media industries, start-ups, also youth and older people.

When researching this I came across the Data Protection Impact Assessment (DPIA) "blacklist", what can you tell our readers about it?Raimondas Andrijauskas says that the list means that some of the processing activities are considered to pose a high risk to the rights and freedoms of people but this list is not exhaustive. He explains that this means that even if the specific processing activity is not on this list, the data controller must assess the impact of processing operation onto the rights and freedoms of natural persons (for example, whether it could meet the Article 35(3) of the GDPR) and if such risk might be high, the DPIA must be made.[2]

When looking to more modern technology Raimondas Andrijauskas explains that the institution dealt with situations on processing biometric data even before GDPR came into effect. For example, one investigation was carried out in 2016–2017, in which the Inspectorate decided that a company could not process biometric data (fingerprints) of employees based on their consent. This decision was challenged at the courts. The Supreme Administrative Court of Lithuania also stated that consent is not appropriate legal basis for employees' biometric data processing. Even though this decision (2019) was made based on national law implementing Directive 95/46/EC, it does correspond with the rules set in the GDPR. Raimondas Andrijauskas further explains that the usage of biometric data is starting to be more and more common in fitness clubs (when entering them), and the Inspectorate decided to proceed with investigations on this matter in 2019. The investigation concluded that, yet again, it was stressed that biometric data of employees cannot be based on consent, but the consent might be used for customers' biometric data if there is an alternative for those who are not willing to provide their biometric data. Full report was published and can be found here [3] (in Lithuanian only). They also had a few complaints regarding the use of biometric data in work.

Looking in the future, it´s always hard to know what will happen but Raimondas Andrijauskas says that looking at the trends in the private and public sector and society, as a whole, it is quite clear that digitisation and digitalisation will continue, and therefore he explains, it is important to consider the issues of personal data protection. As more and more questions arise in this area it will be essential to provide guidance to the data controllers and data processors and where necessary pass sector specific legislation. When looking at which regulation will be coming in the near future, it will probably be ePrivacy regulation as electronic communication is an inseparable part of our daily lives. And looking further along the road, he says, everyone's eyes are on AI. It is widely discussed in society, the search to find out how to implement AI into the daily lives of private companies, how AI can help perform tasks of public institutions, law enforcement etc. So, the discussion must be had if there is a need for further regulation in this area and how it should look like. In this regard, a lot of attention should also be paid to the obligation to ensure transparency – to inform the public, etc. Raimondas Andrijauskas concludes that it is also worth mentioning that there should be discussions on how to make supervisory authorities' supervision more effective by making case handling procedures more harmonized across all the EU. If necessary, such harmonization could be achieved by legislative measures.

Vidare läsning

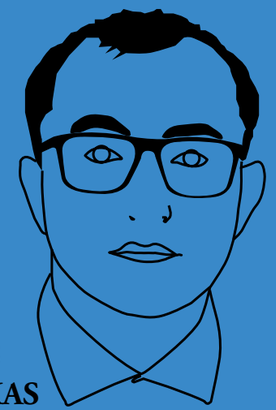
1 https://vdai.lrv.lt/en/news/first-significant-fine-was-imposed-for-the-breaches-of-the-general-data-protection-regultion-in-lithuania.

2 https://vdai.lrv.lt/en/news/list-of-data-processing-operations-subject-to-the-requirement-to-perform-data-protection-impact-assessment

3 https://vdai.lrv.lt/uploads/vdai/documents/files/Sporto_klubu_tikrinimai-biometriu_2019-05-29.pdf

ALEXANDRA MEIJA

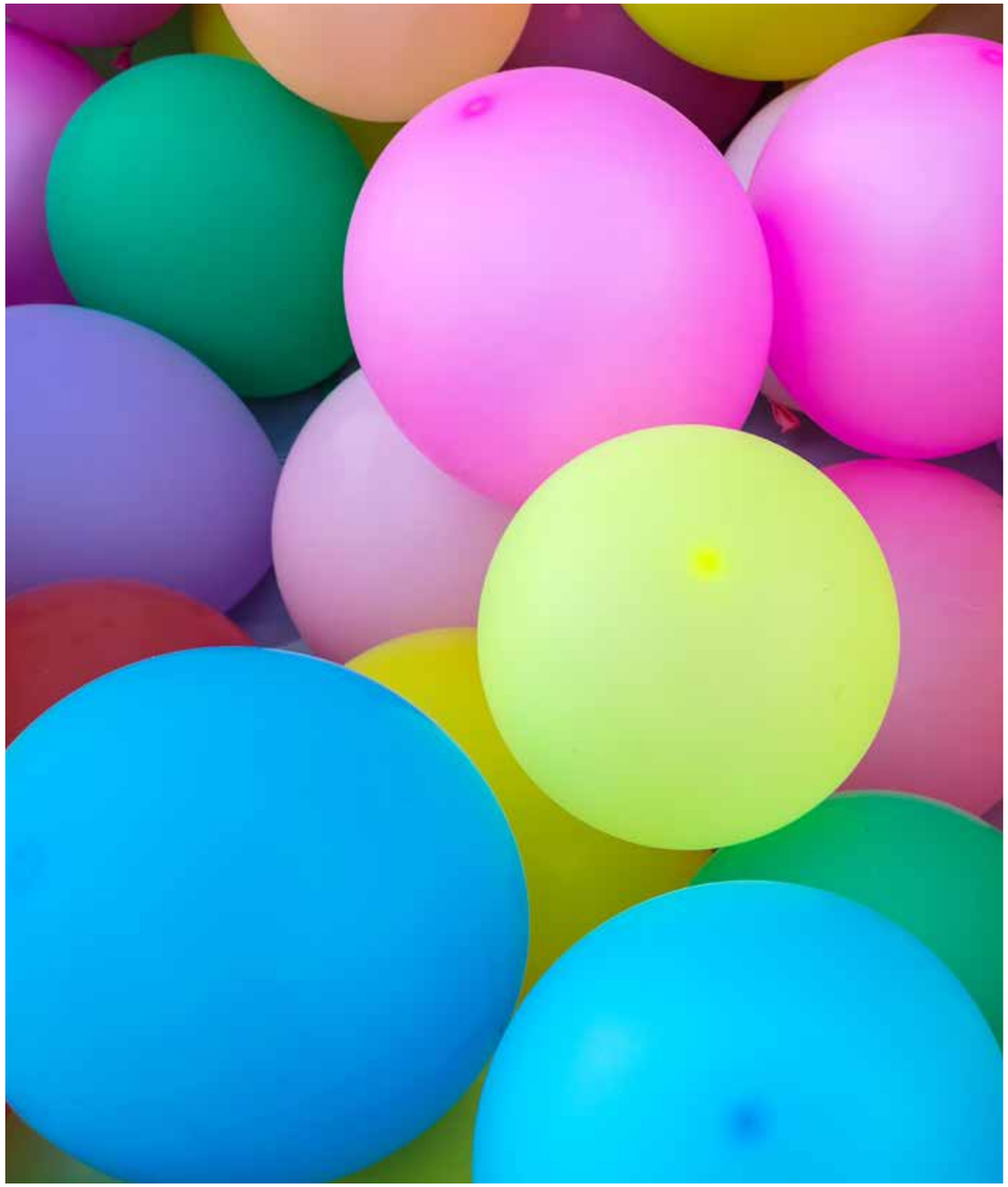
Satte sin fot i ett arkiv första gången som 16- åring, det var inte kärlek vid första ögonkastet, men nästan. Numera är hon chefredaktör för Arkiv Information Teknik, arbetsmiljöombud och arkivkonsult på ArkivIT i snart tre år. Vid sidan om konsultandet har hon genom åren skrivit artiklar och haft uppdrag som moderator på olika konferenser. Inom informationshantering är hon mest intresserad av processkartläggning och verksamhetsutveckling. Hon brinner för personlig utveckling, hos andra men även hos sig själv.



RAIMONDAS ANDRIJAUSKAS

Head of the State Data Protection Inspectorate of the Republic of Lithuania. Leader of changes in privacy and personal data protection, developer of a stable data protection supervision system in Lithuania, representative of Lithuania in the European Data Protection Board.

GDPR gratuleras på tvåårsdagen!



GDPR – EU:s dataskyddsförordning[1] – fyller två år i år. I hur stor utsträckning har frågetecknen om tillämpningen av GDPR på arkivverksamheten i Sverige rätats ut? Har vi blivit något klokare ännu?

Några reflexioner kan vara på sin plats kring i hur stor utsträckning vi kommit framåt med förtydliganden kring hur GDPR ska tillämpas i arkivverksamheten i Sverige.

Den tidigare personuppgiftslagen (PUL) var ju skriven för svenska förhållanden, även om den baserade sig på ett direktiv från EU. GDPR, skriven för att tillämpas rätt av i alla medlemsländer, introducerade en hel del begrepp och sammanhang, som inte så självklart var lätta att förstå vid införandet för två år sedan för oss arkivarier i Sverige. Så låt oss ta en titt på hur det har gått!

GDPR och offentlighetsprincipen

Om vi börjar med GDPR och offentlighetsprincipen, går det att läsa om stora förändringar i förhållandet till tryckfrihetsförordningen (TF) i ett bildspel som Riksarkivet tog fram 2017, i samband med ikraftträdandet:

”Grundläggande skillnad gentemot PUL för myndigheter enligt regeringen”.[2]

Det som åsyftas är att det av den nya lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen)[3] framgår att GDPR inte ska tillämpas om det strider mot bestämmelserna i tryckfrihetsförordningen (TF). I förarbetena till dataskyddslagen konstateras att regleringen i GDPR ger ett *ännu tydligare* stöd än det gamla dataskyddsdirektivet, som PUL baserades på, då den EU-rättsliga dataskyddsregleringen inte inkräktar på den grundlagsreglerade offentlighetsprincipen. Den sammanjämkning som GDPR kräver att medlemsländerna ska göra av behovet av dataskydd och offentlighetsprincipen gör vi i Sverige genom bestämmelserna i offentlighets- och sekretesslagen (prop. 2017/18:105 s. 43).[4]

Bedömningen att GDPR inte inkräktar på EU:s medlemsländers olika offentlighetsprinciper har också fått stöd av EU-kommissionens nationella expertgrupp i arkivfrågor, EAG (”European Archives Group”). I den vägledning som de publicerade ett halvår efter det att GDPR trädde i kraft uttrycker man det så här:

”It does not include rules regarding access to archives by the general public. The closing periods of documents containing personal data will remain the same.” [5]

GDPR:s förhållande till offentlighetsprincipen tydliggjordes ganska väl redan från början och frågetecknen att räta ut har varit färre här än på andra områden.

Arkivändamål av allmänt intresse

GDPR hindrar inte att personuppgifter bevaras för arkivändamål av allmänt intresse även om de ursprungligen samlades in för ett annat ändamål. Centralt för att tillämpa GDPR i arkivverksamheten är därför tolkningen av begreppet *”arkivändamål av allmänt intresse”*. Här rådde inledningsvis stor osäkerhet.

Regeringen kunde inte finna att begreppet definierats i GDPR och de konstaterade att det gamla dataskyddsdirektivet, som PUL byggde på, i stället använde begreppet ”historiska ändamål”. *”Det är oklart om någon skillnad i innebörd är avsedd”*, skrev regeringen inför införandet. Man konstaterade att den närmare innebörden av begreppet arkivändamål av allmänt intresse därför får klargöras i rättstillämpningen, särskilt i förhållande till begreppet historiska forskningsändamål (prop. 2017/18:105 s. 110).

Har vi blivit något klokare under dessa två år?

Kommissionens expertgrupp EAG menar att det nog ändå finns en förklaring till begreppet att läsa i GDPR. Av skäl 158 i GDPR framgår att det bör syfta på *”tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset.”*

Och ett år senare, i september 2019, återkommer Riksarkivet med denna förklaring till begreppet också i dess förslag till föreskrifter och allmänna råd om behandling av personuppgifter för arkivändamål av allmänt intresse inom den enskilda sektorn.[6]

Det är i alla fall för mig uppenbart att den arkivverksamhet som avses i GDPR, inte behöver sammanblandas med historisk forskningsverksamhet. Visserligen bedriver en del arkivinstitutioner även historisk forskning, men personuppgiftsbehandlingen för detta syfte behöver nog inte blandas ihop med behandlingen som görs för att förvärva, bevara och ge tillgång till uppgifter av bestående värde, på det sätt som

regeringen befarade inför införandet av GDPR.

Alldeles uppenbart är vi på väg i Sverige mot en större förståelse för begreppet än vad som var fallet inledningsvis. Det var inledningsvis också oklart om uppgifterna för de enskilda arkivorganen alltid är fastställda i enlighet med *svensk* rätt på det sätt som krävs för att GDPR ska vara tillämplig med dess stöd för att behandla personuppgifter för arkivändamål (prop. 2017/18:105 s. 112). Regeringen delegerade därför föreskriftsrätten till Riksarkivet i syfte att klargöra vilka *kriterier som ska vara uppfyllda* för att en enskild arkivverksamhet ska anses vara av allmänt intresse i GDPR:s mening.

EU-kommissionens expertgrupp EAG behandlar också frågan om de enskilda arkiven och GDPR, men betonar att detta med rättsligt stöd inte behöver tolkas så strikt att det måste finnas direkt lagstöd för verksamheten. Det borde helt klart räcka med stöd i ministeriers eller myndigheters föreskrifter, eller i regionala eller kommunala organs föreskrifter för att rättsligt stöd ska finnas för tillämpning av GDPR för arkiv inom enskild sektor, resonerar kommissionens expertgrupp.

Några beslutade föreskrifter från Riksarkivet har ännu i skrivande stund inte sett dagens ljus men kanske gör vi det lite krångligare än nödvändigt när vi landat i att det krävs särskilda föreskrifter på nationell nivå som uttryckligen pekar ut vilken enskild arkivverksamhet som ska ses som arkivändamål av allmänt intresse?

”Det är i alla fall för mig uppenbart att den arkivverksamhet som avses i GDPR, inte behöver sammanblandas med historisk forskningsverksamhet.”

Samtidigt finns uppenbart ett behov av tydliggörande så frågan är inte helt enkel att besvara med ett ja eller ett nej.

Gallringen av allmänna handlingar och rätten att bli glömd

En av de grundläggande rättigheterna i GDPR är rätten att bli glömd, även kallat rätten till radering. Den finns reglerad som artikel 17. Denna rättighet för var och en att få personuppgifter om sig själv raderade kan helt naturligt uppfattas stå i strid med den reglerade gallringen av allmänna handlingar med stöd av arkivlagens bestämmelser.
I bildspelet från Riksarkivet vid ikraftträdandet 2017 hävdas att *gallring* inte kan vara en konsekvens av *rätten till radering* i GDPR ”eftersom 2 kap TF tar över EU:s dataskyddsförordning.” Allmänna handlingar får, med ett sådant resonemang inte gallras och förstöras, enbart för att det finns en rätt för den enskilde att bli glömd.

Synen att 2 kap. TF ”tar över” GDPR tycker jag mig höra vara förhållandevis väl spridd bland arkivverksamma i landet. Jag kan dock finna att det även finns motargument mot detta resonemang. Både Datainspektionen och Kommerskollegium ifrågasatte bestämmelsens förenlighet med EU-rätten när förslaget lämnades att ta in det i dataskyddslagen. Regeringen bedömde dock ”att den unionsrättsliga dataskyddsregleringen även fortsättningsvis ger utrymme för bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.”(prop. 2017/18:105 s. 41f).

Det jag tänker är viktigt att notera är att regeringen i ovannämnda citat inte hävdat att TF ”tar över” GDPR, men däremot att GDPR *”ger utrymme för”* TF:s bestämmelser. Denna skillnad i tolkning av förhållandet mellan GDPR och TF påverkar också hur man ser på GDPR och bestämmelserna om gallringen av allmänna handlingar.
Av TF framgår att grundläggande föreskrifter om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande av sådana handlingar får meddelas i *lag* (TF 2:23). En naturlig konsekvens av synsättet att TF ”tar över” GDPR kan då bli att inte endast offentlighetsprincipen i snäv mening – bestämmelserna om rätten att ta del av allmänna handlingar – utan även myndigheters gallringsföreskrifter *går* före GDPR.

Men om TF inte *går före* GDPR utan i stället GDPR *ger utrymme* för TF blir ju detta resonemang inte lika självklart. GDPR behöver ju inte nödvändigtvis ”ge utrymme” för gallringsföreskrifter som inte tar hänsyn till GDPR:s krav på rätten till radering, bara för att de ger utrymme för TF:s bestämmelser om rätten att ta del av allmänna handlingar. Här kan jag således skönja en divergerande syn på GDPR och gallringen mellan olika aktörer i Sverige.

Hur har då utvecklingen gått under de två åren?

Arkivutredningen menar att synen på gallring delvis förändrats i samband med ikraftträdandet av GDPR (SOU 2019:58 s. 247).[7] Ett stort antal registerförfattningar har ändrats med anledning av genomförandet av dataskyddsreformen. Genomgående har lagstiftaren valt att ta bort de tidigare gällande bestämmelserna om gallring och ersatt dem med bestämmelser om längsta tid för behandling (SOU 2019:58 s. 259). Även om man bestämmer sig för linjen att TF inte ”tar över” GDPR utan det är GDPR som ”ger utrymme” för TF så har det ju ändå blivit en tydligare åtskillnad mellan gallringsbegreppet i arkivrättsliga regler och raderingsbegreppet i regler om dataskydd.

Jag kan fortfarande se olika synsätt och uppfattningar kring om detta också skulle innebära att en radering enligt GDPR inte får innebära sådan utplåning av information att den äventyrar tillämpningen av gallringsföreskrifter. Man kan resonera att TF inte ”tar över” GDPR, utan det är GDPR som ”ger utrymme för” bevarande om rätten till radering äventyrar tillämpningen av gallringsföreskrifter. Rätten till radering ska också enligt GDPR, artikel 17.3.d, inte gälla om behandlingen är nödvändig för arkivändamål av allmänt intresse om raderingen *sannolikt omöjliggör* eller *avsevärt försvårar* uppnåendet av syftet med sådan behandling.

Regeringen gjorde dock bedömningen att dataskyddslagen *inte* bör innehålla några generella undantag från den registrerades rättigheter vid behandling av personuppgifter för arkivändamål av allmänt intresse, trots att GDPR kan sägas ge utrymme för detta (prop. 2017/18:105 s. 119).

Vissa undantag har i stället tagits in i arkivförordningen men där begränsats till att endast avse arkivmyndigheters behandling av personuppgifter och *inte* behandlingen för arkivändamål hos arkivbildande myndigheter och förvaltningar. Rätten till radering har inte heller inkluderats bland de rättigheter och skyldigheter i GDPR som arkivmyndigheterna har blivit undantagna från genom arkivförordningens nya bestämmelser.

Regeringen motiverade dessa förhållandevis *begränsade* undantag från de registrerades rättigheter i syfte att stödja arkivverksamheten, med en allmän utgångspunkt att den nya svenska dataskyddslagen inte bör inskränka de registrerades rättigheter i större utsträckning än vad som gällde enligt den gamla personuppgiftslagen, PUL *(prop. 2017/18:105 s. 121)*.

”Man kan resonera att TF inte ”tar över” GDPR, utan det är GDPR som ”ger utrymme för” bevarande om rätten till radering äventyrar tillämpningen av gallringsföreskrifter.”

Om man kan säga att regeringen verkligen tog ställning aktivt för den svenska lagstiftningen om rätten att ta del av allmänna handlingar i förhållande till GDPR, så gjorde de det omvända vad gäller möjligheten till undantag från GDPR till stöd för den svenska lagstiftningen om bevarande och gallring. Regeringen prioriterade upprätthållandet av den rättighetsnivå som redan fanns enligt PUL, framför att utnyttja de ökade möjligheter som GDPR ger till stöd för att säkerställa ändamålen med arkivverksamheten i landet.

Detta kan jag ha stor förståelse för. Skulle rätten att bli glömd inte gälla så snart en handling konstateras vara en allmän handling skulle denna rättighet i princip helt sättas ur spel vad gäller personuppgifter inom offentlig sektor på ett sätt som i alla fall jag inte bedömer vara rimligt.

Rätten till radering ska samtidigt enligt GDPR, artikel 17.3.d, inte gälla i den utsträckning som behandlingen är nödvändig för arkivändamål av allmänt intresse om det *sannolikt omöjliggör* eller *avsevärt försvårar* uppnåendet av syftet med sådan behandling.

Att det inte uttalats tydligt ännu för svenska sammanhang att rätten att bli glömd inte ska tillämpas om den försvårar behandling för arkivändamål av allmänt intresse kan jag samtidigt tycka vara klart olyckligt.

Här behövs nog ett fortsatt arbete med att finna en lämplig balansgång mellan upprätthållandet av dataskyddets krav och hänsynen till arkivverksamhet.

Arkivändamålen för allmänt intresse enligt GDPR syftar ju, om man åter tittar på definitionen i skäl 158 på ”uppgifter av bestående värde för allmänintresset”.[8] Vårt svenska begrepp ”allmän handling” är ju betydligt vidare än så och innefattar ju även gallringsbara handlingar med enbart tidsbegränsat värde för allmänintresset.

En precisering att det undantag för arkivverksamhet från ”rätten att bli glömd” som kanske kan vara rimlig inom den offentliga sektorn i Sverige kunde vara att endast hänsyn får tas till bevarandet av de *icke gallringsbara* allmänna handlingarna i myndigheternas arkiv.

På området för gallring av allmänna handlingar och rätten till radering återstår nog således en del behov av klargörande kring tillämpningen i Sverige som skulle underlätta dialogen i myndigheter och företag mellan företrädare för arkivintresset och för dataskyddsintresset.

Några slutord

Nedslagen i tillämpningen av GDPR för arkivverksamhet visar helt klart att en del frågetecken rätats ut under de två år som gått sedan GDPR trädde i kraft. Men alla de frågetecken som förelåg när GDPR trädde ikraft har definitivt inte rätats ut. Och GDPR medför givetvis fler tillämpningsfrågor än de som jag tagit upp här. Jag tänker t.ex. på frågorna om behandling av känsliga personuppgifter för arkivändamål av allmänt intresse och skyldigheterna att lämna information om behandling av personuppgifter tillämpat på arkivverksamhet. Stort utrymme finns för fortsatt utrednings- och utvecklingsarbete på området.

1 https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1

2 https://riksarkivet.se/Media/pdf-filer/GDPR,%20dataskyddslag%20och%20myndigheters%20arkiv.pdf

3 https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20182218-med-komplet terande-bestammelser_sfs-2018-218

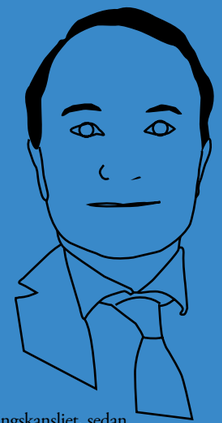
4 https://www.riksdagen.se/sv/dokument-lagar/dokument/proposition/ny-dataskyddslag_H503105

5 Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector. © European Archives Group Date: October 2018. https://ec.europa.eu/info/files/guidance-data-protection-archive-services_en

6 https://riksarkivet.se/Sve/Remisser/Dokument/Forfattning_utkast_5-juli_remiss.pdf

7 https://www.regeringen.se/4afb8a/contentassets/8e78a764094b4f60a1da3e444d7e42fa/hari fran-till-evigheten.-en-langsiktig-arkivpolitik-for-forvaltning-och-kulturarv-sou-201958.pdf

8 https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-beaktandesatser/



MATS BURELL

Är sedan 1999 anställd i Regeringskansliet, sedan 2010 som ämnesråd, och arbetat med bl.a. departementens och utlandsmyndigheternas arkiv. Mats har sedan 1980-talet arbetat med arkivfrågor vid statliga arbetsplatser och parallellt även undervisat i arkivvetenskap vid olika universitet och högskolor. Tillsammans med Carina Sjögren har han författat läroboken ”Information i verksamhet och arkiv”, som gavs ut 2018 av Föreningen för arkiv och informationsförvaltning (FAI). Han är sedan september 2019 och t.o.m. augusti 2020 utsänd nationell expert i arkivfrågor vid Europeiska unionens domstol i Luxemburg, med uppgift att bl.a. föreslå beslut om urval och gallring. I uppdraget ingår analys av dataskyddsfrågor och dess förhållande till domstolens arkiv.

Läs mer https://fai.nu/publikationer/bokutgivning/information-i-verksamhet-och-arkiv/

GDPR 2018–2020: Vad har hänt?

Hur tänkte man kring GDPR innan lagen trädde i kraft? Hur ser man på den nu? Vad har förändrats sedan den blev svensk lag? Representanter för tre professioner och artikelförfattaren själv reflekterar från sina skilda perspektiv över hur synen på GDPR har förändrats.

Dagen är här, det är den 25 maj 2018, den dag som vi arbetat så hårt för att ”hinna bli klara” till.

Så här i efterhand kan man undra ”vad som skulle hinna bli klart” egentligen, eftersom GDPR är en ständigt pågående process.

Som dataskyddsombud (DSO) är jag inbjuden till ett early-bird-möte med kommunikationschefen för att ”stämma av det sista” innan kommunens växel öppnar. Vi är helt övertygade om att hanteringen av personuppgiftsincidenter kommer att fylla stora delar av vår arbetsdag under lång tid framöver och att Datainspektionen kommer att knacka på dörren, redan innan sommaren.

Vi är taggade och redo.

Nu står vi på tå som aldrig förr! Växeln öppnar, kommunhusets dörrar slås upp för allmänheten, registrator öppnar funktionsbrevlådan, pressansvarig har sitt headset redan på plats och både jag och organisationens personuppgiftsansvarige kan inte undvika att snegla ut genom fönstret. Vi måste ju kunna upptäcka teamet från Datainspektionen i tid.
Men märkligt nog hör inte NÅGON av våra närmare 90 000 kommunmedborgare av sig! Det kommer inte en enda fråga från media och Datainspektionen lyser med sin frånvaro.
Det är en inte helt vanlig fredag i Europa, i Sverige och i vår kommun. Livet rullar i och för sig på som vanligt, men maj månad 2018 innehåller inte bara frågor om GDPR – Stockholm upplever den torraste maj månad sedan 1951 och värmerekordet från 1911 slås i Västmanland. Maj 2018 kommer förmodligen att gå till historien, men mer för sin värmebölja än för införandet av GDPR.

GDPR – EU:s dataskyddsförordning

EU beslutar att anta ett nytt regelverk för behandling av personuppgifter som ska tillämpas från och med den 25 maj 2018. EU:s förordning gäller direkt som lag i Sverige (och övriga medlemsstater i Europa och EES) och i Sverige ersätter förordningen den tidigare gällande Personuppgiftslagen (PUL). Datainspektionen får uppdraget att se till att reglerna följs.

Det övergripande syftet med förordningen är att skydda den enskildes grundläggande rättigheter och friheter, med särskilt fokus på skyddet av personuppgifter. Ett annat viktigt syfte är att fastställa regler för flödet av personuppgifter inom EU och därmed skapa en grund för en ökad digitalisering inom unionen.

Det var väl inte så många kommuner, myndigheter, företag eller föreningar som ”blev klara i tid”, även om både vilja och ambition fanns. Fortfarande, efter två år, pågår arbetet med att upprätta styrande dokument, öppna e-tjänster, samt utbilda medarbetare och medlemmar. Ännu är osäkerheten stor och tolkningar av förordningen är föremål för kontinuerlig diskussion.

GDPR har trots det blivit en del i det vardagliga arbetet. En hel del rutiner och metoder har producerats och den samlade erfarenheten har vuxit. Men fortfarande kan man få höra: ”Det där får man inte göra på grund av GDPR”.

Tröjan är framtagen av:
Kristian Luoma och Daniel Åkerlund
https://www.copydaniel.com/gdpr

Vad tycker kommunregistratorn, advokaten och DSO:n?

Jag tycker att inställningen till och kunskapen om GDPR har förändrats. I början såg många en framtid bestående av kontroll, förbud och stora sanktionsavgifter. Ingen visste riktigt vad den nya förordningen innebar: Skulle den bli en lagstiftning för juristerna att tolka eller skulle den uppfattas som ytterligare en pålaga?

Jag frågar några personer som möter lagen i sitt dagliga arbete om hur synen på GDPR har förändrats sedan den där soliga fredagen i maj 2018.

Vad är den största förändringen tycker du, under den tid GDPR har varit i lag i Sverige och Europa?

DSO:n: ”Den största förändringen är att organisationerna har tagit frågorna om hur vi hanterar informationen på allvar. Även om man inte har haft råd att tillsätta resurser alltid. Sedan kan det vara summan det kostar att inte sköta sig som är drivkraften men oavsett det så har det hänt rätt mycket när det gäller det.”

Advokaten: ”Medvetandegörandet av dataskyddsreglerna i det offentliga och privata Sverige/Europa samt hos privatpersoner. Plötsligt fick persondataskydd och integritetstänk en helt ny arena. Personuppgiftslagen i Sverige fanns visserligen innan GDPR men jag upplevde inte att någon tog den riktigt på allvar.”
Kommunregistratorn: ”GDPR är mera strikt jämfört med PUL beträffande personidentiteten och säkerheten på internet”.

Hur tycker du att svenska folket verkar förhålla sig i frågan om GDPR? Bryr man sig?

DSO:n ”I början tyckte jag att folk brydde sig men sedan har det förändrat sig lite på grund av att regelverket uppfattades som detaljstyrning och att det var svårt att alltid följa det. Men det hör av sig mer folk nu om synpunkter på att informationen hanteras på ett felaktigt sätt. Jag tycker att folket bryr sig mera än innan”.

Advokaten: ”Jag tror att gemene man anar vad reglerna handlar om och att det är något positivt, men få vet egentligen vad reglerna innebär. Ryktesspridningen är stor, till exempel i skolor och kommuner om till exempel möjligheten att ta skolfoton. Mest där jag tror att gemene man bryr sig i form av egenintresse, till exempel om man önskar att radera uppgifter till exempel på sociala medier.”
Kommunregistratorn: ”Flertalet medborgare visste inte vad PUL var, som hade funnits länge, man hade glömt bort innebörden. När nu hela Sverige och Europa har talat så mycket om GDPR och informerat innan den 25 maj 2018 så är medborgarna mer insatta men en del missuppfattar GDPR, och hör av sig och vill att man raderar allt om dem.”

Tror du att man känner till innehållet i GDPR? Eller tror man att det är en lag som består av förbud?

DSO:n ”Många vet att GDPR finns men förstår inte riktigt allt utan kan ringa och fråga vad som menas med olika saker. Hur det ska tolkas med mera. För organisationerna uppfattas lagen mer som förbud än vad svenska folket uppfattar den som.”
Advokaten: *”Nej, det tror jag inte. De flesta har väl lärt sig bokstavskombinationen, men det är något de flesta bara 'slänger sig med' utan att riktigt förstå reglernas innebörd.”*

Kommunregistratorn: ”Trots att det gavs ut information och det fanns mycket information så var flertalet/många rädda och började ta bort och makulera personinformation i till exempel listor med namn, adresser och liknande hos föreningar och så vidare”

Du har ju arbetat med GDPR från ”första dagen”. Vad tycker du har varit den största utmaningen under de här två åren?

DSO:n: ”Största utmaningen har varit att implementera GDPR i organisationen med tanke på att det inte har tillsatts tillräckliga resurser. Informationen har ju legat rätt spridd i organisationen utan tanke på om det legat rätt eller inte. Men kommuninvånarna upplever jag har varit förstående.”

Advokaten: ”Att få till en faktisk och en reell tillämpning av bestämmelserna i GDPR, med samma värde som andra policyer på företag, till exempel kvalitets- och miljöpolicyer och etiska regler. Jag arbetar för att få reglerna att fästa i företagarnas medvetande; det ska ’ringa en klocka’ när personuppgifter behandlas – i alla sammanhang. Vi är inte riktigt där ännu.”

Kommunregistratorn: ”Efter två år är det fortfarande diskussioner vid arbetsplatser om hur man ska tolka och arbeta efter GDPR. Det är svårt att skriva rutiner. En kan tolka GDPR från två sidor om samma sak. En utmaning har varit att många varit ’rädda’ för att spara personuppgifter digitalt och istället skrivit ut till papper utan att förstå att GDPR ändå gäller. Fortfarande behövs det experter på GDPR som hjälper till.”

”Två år senare är det lätt att le vid tanken på de första dagarna med GDPR, i somliga stunder upplevdes de lika ödesmättade som millennieskiftet.”

Ska jag tolka svaren som ”same, same but different but still the same”? Att det saknas resurser, att man slänger sig med ”GDPR-uttrycket” och att organisationer tycker det är allmänt besvärligt? Eller kan det vara så att GDPR har förändrat vårt synsätt och medfört att du och jag och alla andra ”vanliga” människor har vaknat upp och insett att vi äger rätten till våra egna personuppgifter?

Avslutande reflektioner

Datainspektionen konstaterar i sin årsredovisning för 2019, publicerad den 21 februari 2020 under rubriken En ”andra våg” i GDPR-arbetet, att många företag, myndigheter och andra organisationer har kommit till en ny nivå i sitt dataskyddsarbete. Om 2018 för många präglades av intensiva förberedelser inför dataskyddsreformen och att få grundläggande processer och rutiner på plats, har 2019 snarare kännetecknats av att få strukturerna att fungera i praktiken, och utmaningar i form av mer komplexa rättsliga frågor och tolkningar. Det är också tydligt att medborgarna har allt högre förväntningar på att deras personata hanteras på ett korrekt, säkert och transparent sätt.
Under 2019 hanterade Datainspektionen totalt cirka 8 300 telefonförfrågningar och tog emot 18 700 ärenden. Av dessa var ungefär: […] 4 000 klagomål från enskilda individer, 4 800 var anmälningar där en privat eller offentlig verksamhet anmält att de haft en personuppgiftsincident”. (källa: En ”andra våg” i GDPR-arbetet, www.datainspektionen.se)
Min tolkning av årsredovisningen för 2019 är att medvetenhet och kunskap har ökat och att vi alla – organisationer, företag och privatpersoner – har större kännedom om vilka rättigheter, skyldigheter och krav GDPR medför. Vi förstår att vi äger rätten till våra egna personuppgifter.

Två år senare är det lätt att le vid tanken på de första dagarna med GDPR, i somliga stunder upplevdes de lika ödesmättade som millennieskiftet. Den där fredagen var en stor dag. Det var på riktigt. Det var på fullt allvar som vi väntade på allvarliga incidenter och Datainspektionens granskning.

Nu 2020, tvåårsdagen har nyss passerat och vi kan titta i backspegeln och se hur kunskap och medvetenhet har ökat. Du och jag och alla andra i hela Europa vet att vi i en viss mening äger rätten till våra egna personuppgifter. Vad som än händer äger jag rätten till min integritet.

Ändå kan man ställa sig frågan: Har GDPR slagit rot?
För var dag, varje ny händelse, varje ny lagstiftning är efterlevnaden av GDPR relevant och viktig.

Under våren 2020 pågår en pandemi. Ord som “lock-down”, “social distansering” och “digital smittspårning” har blivit vardag. Mobiloperatörer har resurser för att på begäran från myndigheter kunna rapportera om medborgares rörelsemönster i ivern att begränsa smittspridningen. Det finns ”appar” för digital smittspårning som används i flera av Europas länder. Det kommer förslag som får acceptans om tillfälliga regler, undantag, begränsningar och lagförslag för att skydda medborgaren mot smittspridningen.

Det får mig att fundera: Hur djupt har GDPR hunnit rota sig i Europa? Vem hävdar rätten till sin integritet när hotet om stor smittspridning kan mötas med en enkel “app” i mobilen?

Två år har förflutit sedan den soliga fredagen i maj 2018.

År 2021 byter Datainspektionen namn till det mer talande namnet Integritetsskyddsmyndigheten.

CARINE SPÅNG

Utbildades till IT-säkerhetschef i Försvarsmakten, redan 2002–03. Hon har tjänstgjort som IT-säkerhetschef i försvarshögkvarteret och som informationssäkerhetssamordnare i Botkyrka kommun. Hon har kunskaper och långa erfarenhet inom området i kombination med egenskapen att visa stor närvaro i allt hon gör. Sedan ett år arbetar hon som senior expert inom IT- och informationssäkerhet och dataskydd (DSO), vid ArkivIT. Carine har uppdrag som dataskyddsombud i flera kommuner och som informationssäkerhetssamordnare.

Vid sidan av arbetet hos ArkivIT har hon ett stort intresse för traditionell nordisk stickning, vandrar lika gärna i fjällen som gör en historisk stadsvandring eller runt Boglösas hällristningar och runstenar.

Jakten på klasslistan

– GDPR och skolan

Du som läser detta och inte är alldeles purung minns kanske hur det var när du gick i skolan: I början av varje läsår fick man en klasslista med namn, adress och personnummer på alla i klassen. Kort därpå brukade man få ett litet häfte med samma uppgifter, fast för hela skolans personal och elever. Under terminen besökte en fotograf skolan och fotade alla elever enskilt och klassvis. Dessutom fotades varje klass för en skolkatalog som alla kunde köpa. Kanske kom det även någon stencilerad produkt ifrån festkommittén, elevrådet eller liknande med tokroliga bilder och texter. På luciatåg och kabaréer fotades det och filmades friskt utan att någon ingrep eller tog anstöt.

Sedan kom GDPR.

Först försvann adresshäftet, sedan klasslistorna, sedan skolkatalogen, sedan – i många skolor – även de individuella elevfotona och klassfotona. Någonstans på vägen slutade festkommittén med sina skojiga häften och vem vågar idag ta en bild av luciatåget, utan att först ha fått samtliga föräldrars godkännande?

Om man i dag vill ha kontakt med en förälder, till exempel för att mejla ut inbjudningar till ett kalas eller för att ens barn vill leka, får man stora problem om man inte personligen fått uppgifter från föräldern. Klasslistor delas ju inte längre ut, telefonkatalogerna gick i graven innan gemene man ens kunde stava till Eniro.se och vem har för övrigt i dag ens koll på om nätets söktjänster har ens aktuella mobilnummer? Det finns inga sammanställningar över folks (ständigt ändrade) e-postadresser, och dristar man sig till att sända ett meddelande till någon man inte redan är ”vän” med på Facebook/Messenger hamnar det i en speciallåda vid sidan av den vanliga och upptäcks i bästa fall ett halvår senare.

När jag härom året bad om en e-postadress till en elev som min son ville bjuda på kalas, meddelade studierektorn att man ”på grund av GDPR inte får lämna ut e-postadresser”. När jag anförde att GDPR inte hindrar skolan från att följa sin lagstadgade skyldighet att lämna ut allmän handling fick jag svaret att han först måste tala med skolans jurister. Någon dag och något samtal med juristerna senare fick jag en klasslista med e-postadresserna i mejlen.

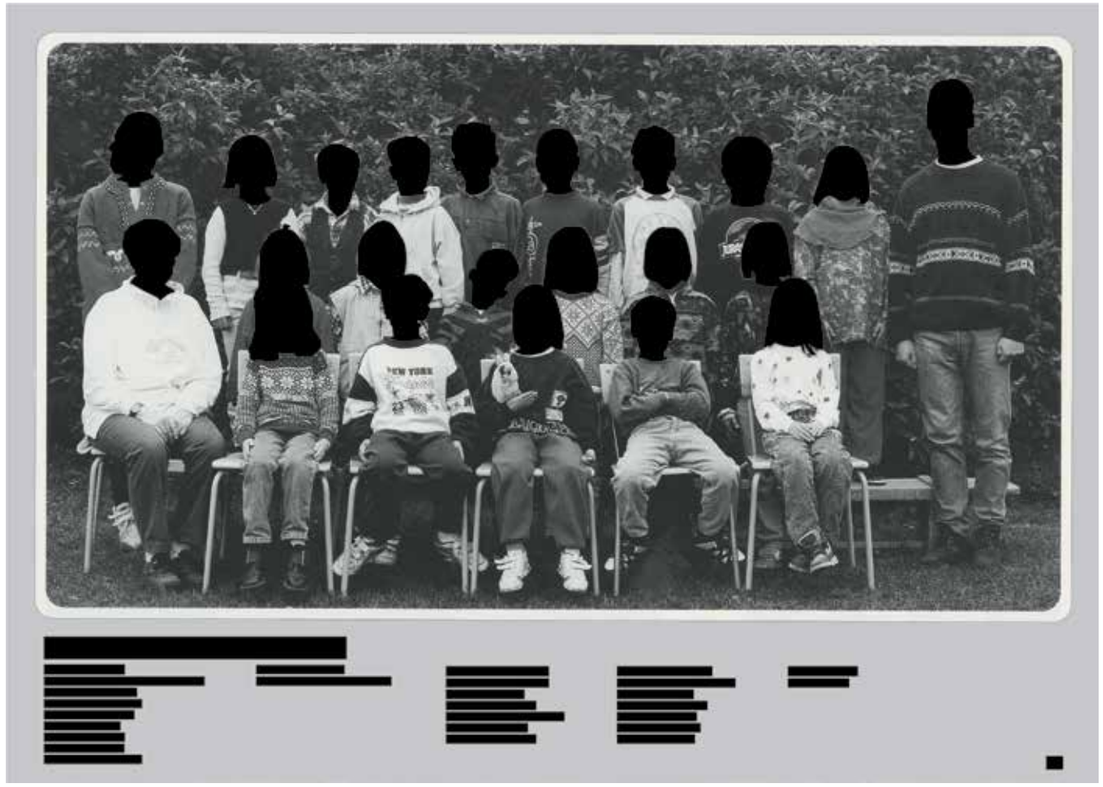
På min dotters fritids satt förra året en lista som vårdnadshavare kunde skriva upp sina namn, telefonnummer och e-postadresser på. Ett initiativ för att föräldrar skulle kunna kontakta varandra trots de avskaffade klasslistorna och adresshäftena. Jag tror inte någon avstod från att fylla i listan. I år fanns ingen lista. Troligen var man på skolan rädd för att ”behandlingen” ansågs allt för kränkande av GDPR.

”På luciatåg och kabaréer fotades det och filmades friskt utan att någon ingrep eller tog anstöt. Sedan kom GDPR.”

Episoden med sonens kalasinbjudan gick i repris härförleden när dottern skulle firas och vi behövde en adresslista för att kunna mejla ut inbjudningar. Det första som händer när jag ringer den nuvarande studierektorn är att han i strid med tryckfrihetsförordningen frågar varför jag är intresserad av den. Sedan lite slentrianmässigt tjafs om att skolan inte får lämna ut sådan information, varpå jag svarar det sedvanliga om TF och arkivlagen, sedan ytterligare lite tjafs om att det kan dröja några dagar innan han får tid att ta sig an mitt ärende, varpå jag påpekar lagens skyndsamhetskrav. Några timmar senare hade jag min klasslista i mejlen, visserligen med överstrukna sista siffor i personnumren, men dem hade jag ändå inget intresse av.

Frågan man ställer sig är, hur gör alla andra som vill kontakta föräldrar till sina barns klasskamrater? Ska man verkligen behöva vara utbildad arkivarie med koll på lagarna som styr handlingsoffentligheten och deras förhållande till GDPR för att kunna få en enkel klasslista med adresser? Borde inte skolans personal känna till ett så enkelt faktum som att arkivlagen och tryckfrihetsförordningen står över GDPR?

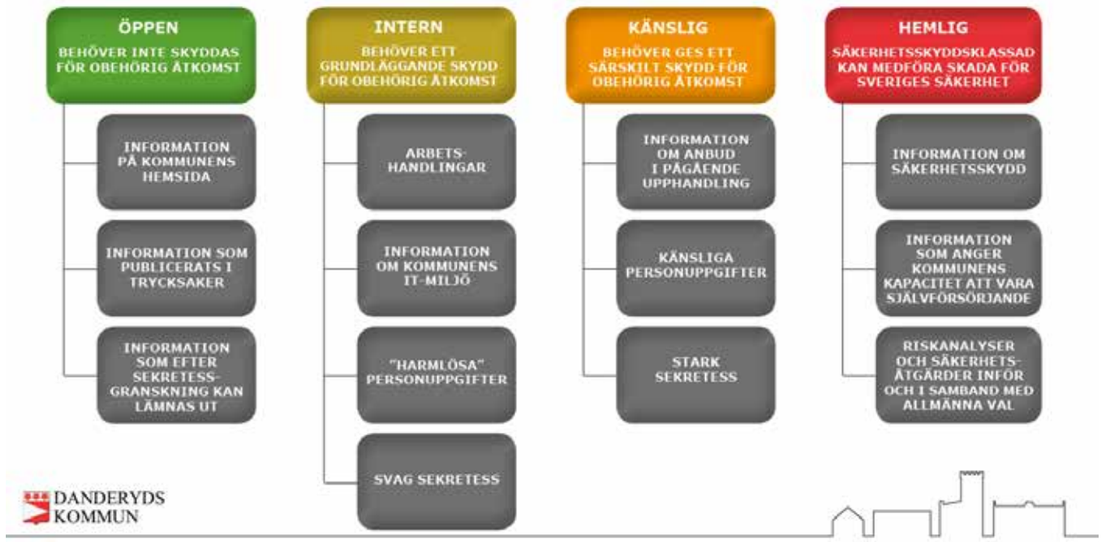
Dataskyddsförordningen var tänkt för att skydda människor från otillbörlig behandling av deras personuppgifter, speciellt av kommersiella krafter, och för att inte känsliga personuppgifter skulle spridas. Men handen upp alla som anser att en e-postadress är en ”känslig” uppgift och en utdelad klasslista en otillbörlig behandling! För övrigt har elever med skyddad adressuppgift alltid haft möjlighet att slippa vara med i både klasslistor och andra offentliga handlingar.



ANDERS HEDMAN

Arkivarie och litteraturvetare. Har arbetat i kommun, stat, stiftelse och privat sektor. Har medverkat i böcker om Gustaf Fröding och AC/DC. Är intresserad av e-arkivering och äldre handskrifter, i synnerhet nygotisk kursiv. Öppen för diskussioner om arkivteori, språkfrågor och annat spännande.

Resan med dataskyddsförordningen i Danderyds kommun



Den 25 maj 2018 började en ny EU-förordning att gälla och som nu efter drygt två år kanske äntligen börjat landa lite.

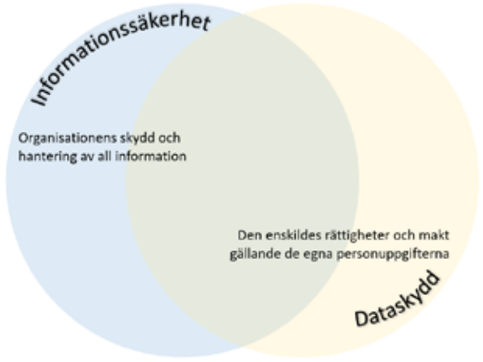
Dataskyddsresan hittills

Constance: ärligt talat så hade jag väldigt lite koll på vad dataskydd var för två år sedan. Det var något som hände ”above my pay grade”. Jag kommer dock ihåg känslan av brådska och osäkerheten i hela organisationen med den 25 maj som en mållinje. Inledningsvis kändes det konstant som att beslut fastnade på olika håll, man hörde endast brottstycken. Jag blev sen inblandad i implementeringsprojektet i mitt arbete som systemspecialist, och när dåvarande dataskyddsombud skulle byta arbetsplats förra året blev jag ombedd att ta vid. Det har varit en virvelvind av nya begrepp, nytt tänk och nya sätt att se på organisationens arbete.

Det jag har lärt mig sedan jag klev på som dataskyddsombud, och som jag inte hade greppat tidigare, är att dataskydd och informationssäkerhet bara delvis handlar om lagstiftningar och rutiner. Det är organisationens *kultur och värderingar* som måste stå i fokus, hur vi ser på vårt dagliga arbete och informationen vi hanterar varje dag. Dataskyddslagstiftningen är för krånglig, lång och omständlig för att minnas utantill, så förutom den grundläggande kunskapen kan det inte vara enbart själva lagen som implementeras, utan även *attityden till lagstiftningen.* Jag vill att mina kollegor ska känna sig trygga nog att ställa frågor när något inte stämmer, när något saknas, när de upptäcker något nytt. Hur de ska veta vad de ska fråga om? Där kommer jag in med utbildningar, informationsfilmer och besök.

Roland: Som konsult inom informationssäkerhet hade jag några tidspressade uppdrag inför 25 maj. Det var roligt och lärorikt. Jag försökte åstadkomma verksamhetsnytta med så kallade risk- och gap-analyser, incidenthantering och leverantörsstyrning. Jag samarbetade med IT-chefer, jurister, verksamhetsutvecklare, informationssäkerhetssamordnare och dataskyddsombud (DSO). Det var inspirerande och stressande att ta fram tillräckligt bra rutiner som skulle fungera i praktiken och samtidigt tåla en granskning.

Nu som heltids-CISO (Chief Information Security Officer) på kommunen har jag fått möjlighet att arbeta än mer strategiskt i att ta fram ett ledningssystem för informationssäkerhet (LIS) och ansvara för implementeringen. Det handlar framför allt om att klassa och hantera information på ett effektivt och säkert sätt digitalt. Vi har mognat i vårt dataskyddsarbete. Den slutsatsen kan man dra eftersom antalet rapporterade incidenter har ökat.



Jag har också fått möjligheten att lära mig mer om trygghets- och säkerhetsarbete i en kommun. Det handlar bland annat om bevakning, passersystem, brand, larm och beredskap.

Samarbetet är viktigt!

Informationssäkerhet och dataskydd har väldigt mycket gemensamt. Dataskyddsombudet har fokus på medborgarnas rätt att kontrollera sina egna personuppgifter och användningen av dem, informationssäkerhetssamordnaren har fokus på organisationens användning av information i alla situationer. Informationssäkerheten skyddar dessutom exempelvis Sverige (säkerhetsskyddslagen), IT-utrustning och ekonomiska värden. Oavsett vilket område det gäller håller vi därför kontinuerlig kontakt och ser till att den andra alltid vet vad som finns på agendan. Då kan vi alltid stötta varandra och bolla idéer och frågor, vilket är värdefullt när beslut ibland behöver tas med kort varsel.
Vi leder också ett nätverk med kontaktombud från de olika kommunala förvaltningarna. Kontaktombuden bidrar bland annat till att underlätta implementeringen av de policyer och riktlinjer som beslutats på högre nivå, och kan involveras operativt i dataskyddsarbetet. De underhåller också nämndernas behandlingsregister och samordnar hästjobbet som kallas inventering. De kan verksamheterna bättre än vad vi någonsin kommer att kunna och vet vilka oskrivna regler (för årligt talat, de finns) som styr deras dagliga arbete, vilket är oerhört värdefullt för att vi faktiskt ska kunna nå ut på riktigt.

Hur vi arbetar – tips!

Constance: För att kulturskiftena ska nå ut förbi den inre kretsen av dataskyddskunniga behöver man göra två saker: nätverka och kommunicera med alla samt konkretisera vad som behöver göras.

Nätverka och kommunicera

Låt dina kollegor lära känna dig! Visa att du är en människa av kött och blod som bryr dig om att verksamheten ska fungera. Be om fem minuter på APT, lägg upp en nyhet på kommunens interna nyhetskanaler, boka in en timme med nyckelpersoner och be dem förklara hur de arbetar och förklara sen vad ditt jobb går ut på, fika i olika fikarum under veckan, skriv om arbetet på Linkedin. Hitta också andra inom samma arbetsområde genom att gå med i nätverk, så att du alltid har någon att bolla tankar med, och mentorer som du kan lära dig av.

Ledningen får man heller inte glömma i kulturskiften, förändring måste ske i alla led. Ledningen har dock hand om precis allt övergripande och viktig information kan ibland försvinna i flödet. De behöver stöd i att veta hur och när de kan vara behjälpliga. Rapportera regelbundet och ofta, be att få komma och berätta om viktiga punkter, förtydliga vilka aktiviteter som konkret måste förankras och när i tiden det behöver ske. Avdramatisera prat om dataskydd och personuppgifter, det är en del av det vardagliga arbetet och ska behandlas som så.

Konkretisera

Ja, hela lagstiftningen ska följas. Men att slänga lagtexten på någon och säga ”De här 150 kraven måste ni följa, vi ses om en månad” har nog aldrig fungerat. Om mina kollegor inte förstår vad som gäller förstår de inte heller vad de ska göra, och hur ska det då gå med den sanna efterlevnaden? Börja med de absoluta grunderna, och gå inte vidare förrän de faktiskt förstått. Jag har till exempel gjort om de grundläggande principerna till frågor när jag utbildar, för att ingen ska kunna gömma sig bakom tanken att dataskydd är ”above my pay grade” som jag gjorde. ”Ändamålsbegränsning” kan viftas bort som ”för krångligt, någon annan får göra det”. Frågan ”Har vi ringat in varför vi använder uppgifterna?” kan däremot diskuteras, bollas runt och besvaras.

Det viktiga första steget är att hitta good enough-nivån. Vad MÅSTE vi ha på plats varje dag? Det måste konkretiseras först. Sen kan man fortsätta bygga på, och alltid återkomma till att alla ska förstå innan man går vidare. Jag ser mycket hellre att

det tar längre tid, och att alla är med på tåget, än att vi slänger ihop något som ser snyggt ut men som bara blir en hyllvärmare. Det varken skyddar registrerades rättigheter eller underlättar för verksamheterna.

Roland: Det gäller att ha tillräckligt bra register över personuppgiftsbehandlingar och avtal med leverantörer samt att hålla dem uppdaterade. Då har man en gällande överblick över behandlingarna och leverantörerna.

Satsa på utbildning, både lärarlett och e-learning. Nanoutbildning, en kort intensiv utbildning, kan vara effektivt. Diskutera nuvarande arbetssätt, ifrågasätt och arbeta med ständiga förbättringar.

Praktik

Det finns många utbildningar, bl.a. inom informationssäkerhet, där praktik på arbetsplatser är en viktig del. Sådan praktik (lärande i arbete) är ofta mycket givande för båda parter, ger nya perspektiv och en bra relation. Den studerande får insikt i och kunskap om det praktiska informationssäkerhetsarbetet, samtidigt som hen får möjlighet att pröva de kunskaper som erhållits. Den studerandes uppgift bör vara tydlig och avgränsad. Handledaren måste finnas tillgänglig för stöd.

”Det är organisationens kultur och värderingar som måste stå i fokus, hur vi ser på vårt dagliga arbete och informationen vi hanterar varje dag.”

IT

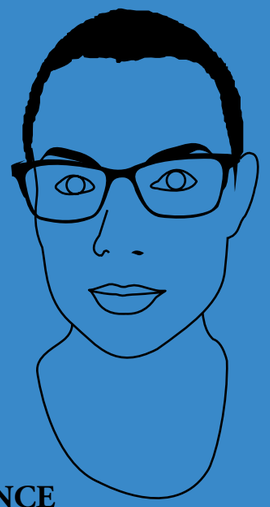
Ingenting fungerar bra och säkert utan bra och säkra it-lösningar. Sätt dig in i hur it-lösningarna fungerar på en övergripande nivå och i praktiken. Studera informationens livscykel från skapande och klassning, till användande och gallring. Skapa bra nätverk och beslutsforum med it-chefer, it-säkerhetsansvariga, lösningsarkitekter, systemförvaltare och it-tekniker. Glöm inte bort arkivarien.

Vad händer nu?

Constance: Tvåårsstolpen innebär att vi nu kan börja arbeta på allvar med dataskydd, med sanna kulturskiften i organisationerna. Den första paniken har (förhoppningsvis) lagt sig, prejudikat börjar komma in från hela EU och nätverk har börjat formas så att alla som arbetar med området kan stötta och rådfråga varandra. Lagstiftningen ÄR krånglig, så att fler EU-gemensamma riktlinjer kommer ut regelbundet är guld värt. Men vi behöver strukturera upp hur vårt arbete ska se ut nationellt. 2020 har blivit ett viktigt år som ger oss riktningen för hur arbetet ska fortgå. Ett bra exempel är vårens pandemiläge, där vi fick uppleva hur dataskyddsarbetet appliceras under stress, med frågor om hur och när man får offentliggöra känsliga personuppgifter, och att insamling av personuppgifter har samma krav oavsett om det är kris eller ej.

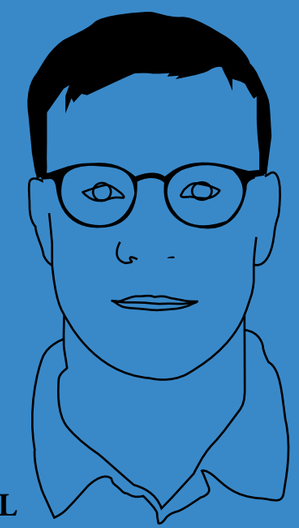
Eftersom jag själv jobbar i en kommun ser jag fram emot fler riktlinjer uppifrån gällande hur kommuner, med flera myndigheter i samma organisation, ska navigera mellan de olika lagstiftningarna. Det känns dumt att alla kommuner gör olika och konstant försöker uppfinna hjulet på nytt. ”Dataskydd är inte ett ensamarbete”, säger jag regelbundet till mina kollegor, ”inte ens för mig”.

Roland: Coronaviruset har tvingat oss att ta det digitala språnget som vi pratat om så länge. Mycket av mitt arbete nu handlar om säkert distansarbete och säker distansundervisning, att vi kan hantera information lika säkert när vi inte är på plats på jobbet eller i skolan.



CONSTANCE BELL DAHLBÄCK

är dataskyddsombud och informations- och processförvaltare på Danderyds kommun. Hon är beteendevetare inom socialpsykologi i grunden, och har tidigare jobbat inom projektledning och systemadministration.



ROLAND LYCKSELL

är informationssäkerhetssamordnare på Danderyds kommun. Han är civilingenjör inom teleteknik och har de senaste åren arbetat som konsult inom informationssäkerhet, dokumenthantering och kvalitetssäkring.

Hur kan GDPR tillämpas för att skapa samklang med andra lagregler?

I skrivande stund är det drygt två år sedan den nya dataskyddsförordningen[1] trädde i kraft, till vardags ofta kallad GDPR. För de flesta som på något sätt hanterar personuppgifter, finns ett före och ett efter GDPR. Materiellt innebar GDPR egentligen inte så många nyheter, men den kräver ett helt annat arbetssätt med dataskydd, och integritetsskydd har blivit en fråga på agendan för de flesta organisationer. Ibland kan det åtminstone upplevas som att regler i dataskyddsförordningen (eller annan dataskyddslagstiftning) går stick i stäv med en del andra lagregler och principer.

Resonemangen i den här artikeln bygger på en kommuns verksamhet, och de regelverk som gäller för kommuner

Lagstiftningen

Dataskyddsförordningen gäller som lag i alla EU:s medlemsländer, i exakt samma lydelse (så kallad direkt effekt). Eftersom det är en EU-lagstiftning gäller den också före de allra flesta nationella lagar, exempelvis arkivlagen, offentlighet- och sekretesslagen och förvaltningslagen.

Däremot lämnar förordningen inom vissa områden utrymme för nationell lagstiftning. Den nationella lagstiftningen blir då ett komplement till dataskyddsförordningen. Exempel på detta är behandling av känsliga personuppgifter (exempelvis uppgifter om en persons hälsa eller genetiska uppgifter), där grundläggande bestämmelser finns i dataskyddsförordningen[2], och kompletterande bestämmelser i dataskyddslagen.[3]

Inom vissa områden finns också undantag för tillämpningen av GDPR. Exempelvis gäller inte förordningen för avlidna personer[4] och den får heller inte hindra den enskilde att utöva sin yttrande- och informationsfrihet.[5] Det innebär exempelvis att för journalistiska ändamål gäller inte dataskyddsförordningen.

Dataskyddsförordningen i förhållande till annan lagstiftning och andra intressen

Ofta hävdas att dataskydd handlar om skyddet för den registrerades integritet, och det är så klart inte felaktigt. Problemet är bara att samma individ också har en rätt till exempelvis lättillgänglig service och smidiga tjänster från det offentliga. Den har också ett berättigat intresse av att den skatt den betalar används på ett kostnadseffektivt sätt, utan att för den skull göra avkall på skyddet för sin integritet. Och medarbetare i exempelvis en kommun har all rätt att förvänta sig ett modernt digitaliserat verktyg för medarbetarutveckling och personaladministration, men inte till priset att förlora sin integritet som enskild person och anställd.

I dataskyddsförordningens skäl 4 uttrycks behovet av avvägning mellan olika intressen på ett, enligt mig, väldigt bra sätt.

”Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. (…).”

Jag tycker att formuleringen tydliggör vad tillämpning av dataskyddsförordningen i praktiken väldigt ofta handlar om, nämligen en avvägning mellan olika intressen. Ett annat exempel där intresseavvägningen[6] tydliggörs är i art. 85 p. 1 där det anges att rätten till integritet ska förenas med yttrande- och informationsfriheten. Det är alltså inte så enkelt som en fråga om lagstiftningshierarki eller vilka undantag som finns. Det handlar många gånger om att balansera intressen mot varandra. Målet är att nå effekten som nämns i skälets första mening: Personuppgiftsbehandlingen ska *tjäna* människor.

Konkreta exempel

Ett exempel på en situation när det inte är helt givet hur de olika intressena ska förenas är förhållandet mellan förvaltningslagen[7] och GDPR. Förvaltningslagen gäller för alla myndigheter och den beskriver bland annat vad som är ”grunderna för god förvaltning”. Det anges bland annat att kontakterna med enskilda ska vara smidiga och enkla, att en myndighet ska vara tillgänglig och att ärenden ska handläggas så enkelt, snabbt och kostnadseffektivt som möjligt med bibehållen rättssäkerhet. Dessa krav är så klart formulerade bland annat utifrån att det ligger i den enskildes intresse att på ett enkelt sätt kunna ha en smidig kontakt med myndigheter, att kunna ta tillvara sin rätt, och för att skattemedel, som i det yttersta kommer från den enskilde i någon form, ska användas på ett effektivt sätt.

Ett exempel på en funktion som skulle kunna skapas utifrån motiven och reglerna i förvaltningslagen är om man som boende i Sverige skulle kunna komma åt alla sina kontakter med myndigheter från ett och samma ställe, och genom att skriva in sitt personnummer och logga in en gång. Utifrån ett strikt förvaltningslagsperspektiv vore sannolikt detta ett bra sätt att gå tillväga. Dock skulle en sådan lösning kunna ha en betydande påverkan på enskildas integritet. En sådan lösning skulle, även omgärdad med omfattande avgränsningar och säkerhetsåtgärder, innebära en sårbarhet för individen eftersom den riskerar en stor exponering av sitt privatliv, i det fall en sådan tjänst skulle missbrukas eller tekniska fel skulle uppstå.

I teorin är lösningen på ovan beskrivna dilemma förhållandevis enkel eftersom GDPR gäller framför förvaltningslagen.
I praktiken är dock lösningen inte lika enkel. Den enskilde, som båda lagstiftningarna är till för, har ju både ett intresse att få lättillgänglig service och att få sin integritet skyddad.

”Utifrån ett strikt förvaltningslagsperspektiv vore sannolikt detta ett bra sätt att gå tillväga. Dock skulle en sådan lösning kunna ha en betydande påverkan på enskildas integritet.”

Ett område som ibland omnämns som en ”krock” är den mellan utlämning av allmänna offentliga handlingar och dataskyddsregler. Det svenska regelverket kring allmänna handlingar, dess offentlighet och utlämningen av dessa, oftast benämnt som offentlighetsprincipen, ger en omfattande öppenhet och insyn i myndigheters verksamhet. För en kommun innebär det för det mesta att öppenhet om verksamheten också innebär en öppenhet avseende de personer som är del av verksamheten, både i form av anställda och invånare. Den öppenheten behöver inte alltid stämma överens med individens intressen om skydd för sin integritet.

När det gäller uppgifterna som sådana finns det en särskild sekretessregel, för det fall att det går att anta att uppgiften kommer att behandlas i strid med bland annat GDPR.[8]
Det ställs relativt höga krav för att sekretess ska kunna tillämpas, men det är viktigt att inte glömma bort den.

Ett annat exempel som relativt ofta aktualiseras är när uppgifter och handlingar ska lämnas ut, och frågan uppstår *hur* de får lämnas ut. Oftast handlar frågan om ifall det är förenligt med GDPR att mejla uppgifterna till den som begärt ut dem.

Tryckfrihetsförordningen stadgar att en myndighet är skyldig att lämna ut allmänna offentliga handlingar.[9] Däremot är myndigheten inte skyldig att lämna ut kopior i ett särskilt format, utan endast kopior i något format, alternativt en möjlighet att läsa handlingen på plats. Det allra vanligaste sättet idag som en allmän handling önskas utlämnad är via e-post. Därför kan det sannolikt antas att gemene mans uppfattning om en ”smidig och enkel” kontakt, såsom förvaltningslagen stadgar, i ett sådant fall skulle vara en digital utlämning.

Samtidigt kan en sådan utlämning innehålla stora mängder av, eller känsliga/extra skyddsvärda, personuppgifter (exempelvis en lönelista, eller en mejlkonversation med nedsättande uppgifter om personer), och en utlämning med vanlig e-post riskerar därför att sprida personuppgifter på ett otillåtet eller olämpligt sätt.

Jag vill nog hävda att det alltid handlar om en bedömning i det specifika fallet eftersom alla unika omständigheter måste vägas in. Det finns exempel när lösningen, i syfte att följa GDPR, har blivit, i mitt tycke, orimligt krånglig. Exempelvis där en enstaka personuppgift i den begärda handlingen gör att myndigheten bestämmer att utlämnandet ska ske på vanligt papper som skickas per post. Ett sådant tillvägagångssätt anser jag vara tveksamt i förhållande till förvaltningslagen och oproportionerligt utifrån ett dataskyddsperspektiv eftersom de personuppgifter som är aktuella fortfarande är offentliga och del av en allmän handling som vem som helst kan begära ut.

Å andra sidan finns exempel på stora volymer av personuppgifter, exempelvis en fil med löneuppgifter, som på grund av själva volymen, kan anses olämpligt att skicka med e-post. Anledningen är att just volymen är så stor att det har bedömts som osäkert att skicka en så omfattande samling av extra skyddsvärda uppgifter med vanlig e-post.

Ett exempel där ett ”förenande” av lagregler ökar genomslagskraften för flera lagstiftningar handlar om gallring av information och handlingar.[10] En av hörnstenarna när det kommer till skydd av personuppgifter handlar om att inte lagra information som inte behövs. I praktiken kan det handla om att rensa e-post eller gallra handlingar och uppgifter i ett verksamhetssystem. Gallringarna i en kommun styrs av informationshanteringsplaner och gallringsbeslut. Så länge dessa anger att lagring ska ske, finns generellt en rättslig grund för att behandla personuppgifterna i systemen. I risk- och konsekvensbedömningar avseende själva personuppgiftsbehandlingen får därför rensnings- och gallringsfrågan en central betydelse. I Västerås stad är det tydligt att den frågan har fått betydligt mycket mer uppmärksamhet och även personer som vanligtvis inte arbetar med den typen av frågor är numera angelägna om att exempelvis informationsplaner är uppdaterade och följs.

Ett annat positivt exempel handlar om sekretessbelagda uppgifter i vanlig e-post. Sedan länge är det känt att sekretessbelagda uppgifter inte får skickas med vanlig e-post (bland annat genom JO-beslut). Med dataskyddsförordningens inträde blev det ytterligare fokus på frågan och det blev också en tydligare riskbild, det vill säga att en myndighet där sekretessklassat material skickats med vanlig e-post skulle kunna drabbas av sanktionsavgifter. Min bild är därför att användandet av olika typer av säkra e-postlösningar har ökat och de flesta är mer observanta på vad som skickas med e-post.

CHARLOTTE ARNELL

Arbetar som dataskyddsombud och digitaliseringsjurist i Västerås stad. Arbetet spänner över alla stadens verksamheter och över de allra flesta förekommande rättsområden men den röda tråden är att verka för en hållbar digitalisering. Brinner för att en god dataskyddskultur ska utgöra och betraktas som ett verktyg för att skapa bra verksamhet och största möjliga nytta.

Sammanfattning

Att balansera kraven i GDPR mot krav i andra lagstiftningar är många gånger inte lätt och i de flesta fall saknas det en tydlig inriktning. Det positiva med osäkerheterna är att det i de flesta fall driver utveckling. Min erfarenhet är att det överlägset bästa sättet att balansera olika intressen, göra bedömningar och hitta lösningar på problem är genom dialog med intressenterna i det specifika ärendet. Det kan krävas lite tragglande, kan ta lite tid och det krävs tålamod och ett öppet sinne hos de involverade. Men när man går i mål har man inte bara lagt grunden för ett väl genomarbetat och förberett beslut, utan man har också skapat ett mervärde. Ett mervärde i form av ökade kunskaper, ökad förståelse och ökad insikt om varandras verksamheter och förutsättningar.

Dataskydd, även på mycket konkret och praktisk nivå, är komplext och svårt. Därför är det lockande att ta fram generella hanteringslösningar för att göra bedömningarna och hanteringen enklare. Vi kan dock se att de generella, förenklade lösningarna oftare leder fel än leder rätt. Därför har vi valt arbetssättet att vi tar oss tid att resonera och diskutera mycket med våra uppdragsgivare kring de aktuella frågorna och ärendena som uppstår. I början tar det längre tid än att skriva rutiner och manualer. Men på längre sikt är det ett effektivare arbetssätt. Dels för att det arbetet vi lägger ner nu leder till att vi oftare gör rätt, och att göra rätt från början är ett av de bästa sätten att effektivisera. Dels skapar vi lärande bland våra kollegor genom att ta oss tiden att möta dem och det gör att hela organisationen blir mer kompetent och självständig i de här frågorna. En högre kunskapsnivå kommer även i sin tur driva på utvecklingen av bättre anpassade IT-lösningar, vilket är en nödvändig komponent för en hållbar digitalisering.

1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

2 GDPR, artikel 9

3 Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, allmänt kallad dataskyddslagen, 3 kap. 5 §

4 GDPR, skäl 27

5 GDPR, art. 85, p. 1

6 Begreppet intresseavvägningen ska i detta sammanhang inte förväxlas med en av de rättsliga grunderna för personuppgiftsbehandling som kallas samma sak.

7 Förvaltningslag (2017:900)

8 Offentlighets- och sekretesslag (2009:400), 21 kap. 7 §

9 Tryckfrihetsförordningen (1949:105), 2 kap. 1 §

10 Dataskyddsförordningen och Arkivlag (1990:782)

Svenska kommuners arbete med GDPR

När dataskyddsförordningen trädde i kraft rådde hos många verksamheter stor förvirring rörande hur man på bästa sätt skulle kunna leva upp till och inkorporera bestämmelserna i sin verksamhet. Nyfiken på hur andra verksamheter hanterade arbetet? Vi skickade ut en enkät till Sveriges kommuner där de anonymt kunde besvara hur de hanterade GDPR-arbetet, vilka utmaningar som de stötte på och hur de har påverkats av införandet.

Dataskyddsförordningen (GDPR) påverkar i princip alla verksamheter, men eftersom alla verksamheter fungerar olika kan hur man arbetar med GDPR-frågor och försöker leva upp till bestämmelserna i förordningen skilja sig mellan verksamheterna. En enkät skickades till Sveriges samtliga kommuner där de anonymt kunde besvara frågor kring deras arbete med GDPR. 85 kommuner svarade. I denna text har deras svar sammanfattats.

Hur har ni gjort för att hantera kraven i GDPR?

Detta är första frågan som respondenterna möts av när de trycker sig in i enkäten. En väldigt vag och bred fråga, men intressant nog har majoriteten ändå gett liknande svar. Utbildat, tillsatt dataskyddsombud och infört nya/uppdaterade rutiner/riktlinjer är de vanligaste svaren. Någon har angett att det är ”chefer och nyckelpersoner” som erbjudits utbildning, men en klar majoritet verkar ha utbildat medarbetare överlag.Och självklart tas registerförteckningarna som har skapats upp. Många verksamheter visar sig även ha skapat organisationer med GDPR-ansvariga eller samarbetat med andra, genom exempelvis arbetsgrupper eller nätverk. Införandeprojekt verkar också ha varit ett vanligt sätt att arbeta på för att hantera kraven som GDPR medförde, och en kommun skriver följande:

[Vårt] arbete med att hantera kraven i GDPR inleddes med ett omfattande införandeprojekt som alla förvaltningar deltog i. Projektet avslutades under hösten 2018 och sedan dess ansvarar respektive förvaltning för att kraven i förordningen efterlevs. Kommunens dataskyddsombud följer upp arbetet med GDPR två gånger om året genom granskningar som resulterar i åtgärdslistor. Dessa listor stäms av vid nästa granskningstillfälle.

Detta är enda svaret som nämner interna granskningar och åtgärdslistor, en metod som känns som ett bra sätt att säkerställa att arbetet sker kontinuerligt och ständigt förbättras istället för att GDPR-arbetet görs en gång och sedan glöms bort. Ett par svarande anger att deras verksamheter sen tidigare arbetade aktivt med personuppgiftslagen och att då kraven inte var så olika behövdes bara vissa anpassningar göras. En annan person anger däremot att de hade ”[a]rbetat med frågorna i projektform för att i ett första läge nå PUL:s krav. Sedan har vi försökt öka arbetstakten med de nya frågeställningarna.” Alla verksamheter levde alltså inte ens upp till föregående lagstiftning, vilket kan förklara varför att mer arbete krävdes.

Vilka har varit de största utmaningarna?

Som så ofta när det kommer till förändringsarbete framkommer av svaren att återkommande utmaningar var att förändra medarbetares beteenden och att få dataskyddsarbetet att genomsyra verksamheten. Respondenterna berättar att alla anställda inte upplever att de berörs av den nya lagstiftningen, att det är viktigt att ”få all personal att se nyttan med lagen och inte bara merjobbet” och att det är en utmaning att försöka undvika att GDPR-arbetet endast blir en ”pappersprodukt”. En av de svarande beskriver följande som den största utmaningen:

Att få medarbetare på alla nivåer att förstå att GDPR är vår nya vardag. GDPR kommer in på så många olika sätt i vår verksamhet, att maila personnummer innebär nya sätt att skicka, bilagor kan innehålla känslig information. Att höja medvetenheten om att vi inte kan göra som vi alltid gjort är en utmaning.

Andra återkommande svar är, som så ofta inom alla verksamheter, tidsbrist och resursbrist, likväl som att det är svårt att förstå GDPR då förordningen kommer med nya begrepp, och rättspraxis ännu saknades, varför egna tolkningar behöver göras. Ytterligare svar som angavs var att det var svårt att skapa intresse för lagstiftningen efter införandet och att få verksamheterna att prioritera frågan. I vissa fall verkar det till och med ha varit svårt att få stöd från ledningen, vilket skulle kunna vara en bidragande faktor till varför tid inte avsätts – arbetet prioriteras inte av ledningen. En respondent skriver att ”alla var vansinnigt trötta på GDPR efter maj 2018... svårt att hålla liv i frågan. DSO har för lite tid avsatt för att driva på frågan internt”, vilket visar på både intresse- och tidsbristen i verksamheten.

Har några rutiner lagts om eller ändrats?

Som vi redan sett från svaren på första frågan är införandet och uppdatering av rutiner ett vanligt sätt för verksamheterna att hantera förordningens krav, och detta speglas även i svaren på denna fråga. En klar majoritet svarar ”ja” på enkätfrågan, men antalet förändringar verkar variera då det ibland anges ”många”, ibland ”flera” och i vissa fall uppräkningar av vilken eller vilka rutiner som har förändrats. Flera gånger nämns rutiner kring e-post och personuppgifter, men även rutiner för registerutdrag och incidentrapportering tas upp som sådana som har behövts införas. En av respondenterna anger att det är med rutinarbetet som ”den största arbetsinsatsen [har] varit”.

Fascinerande nog verkar inte rutiner ha ändrats i alla verksamheter. Svar som ”Inte alls”, ”Nej, inte direkt”, ”Nej, inte vad jag vet” och ”Nej, inte i någon större utsträckning” förekommer också. Några kanske är samma respondenter som tidigare skrev att de hade ett så bra PUL-arbete sen tidigare att inga större förändringar behövdes göras, men det var bara två personer och här är det fler än två. En av dem som har svarat anger att rutinerna inte har ändrats i den utsträckning som de skulle ha behövt ändras, vilket är intressant eftersom det visar att de vet om att större förändringar egentligen krävs. Detta skulle kunna hänföras tillbaka på den brist på tid och resurser som påtalats i flera svar.

Vilken är den största skillnaden jämfört med innan GDPR:s införande?

På frågan om vad som är den största skillnaden jämfört med tidigare är det främst fyra svar som återkommer: en högre medvetenhet vid och om personuppgiftsbehandling (”alla känner till GDPR och vet ungefär vad som gäller”), sanktionsavgifterna, att GDPR är administrativt krävande och att ”missbruksregeln”[1] försvann. Den högre medvetenheten kan förklaras med att den utbildning som vi såg i svaren på första frågan var vanlig. I flera av svaren nämns även en rädsla för GDPR, vilket kan förklaras med högre medvetenhet, avsaknad av rättspraxis och hotet om sanktionsavgifter. En svarande anger att ”[d]et har blivit mer tung-arbetat genomgående. GDPR har skapat en stor osäkerhet bland medarbetarna för vad som är ok eller inte och de mest triviala saker så som t.ex. namnskyltar kan ha blivit ett problem”. Alla vet att förordningen ska efterlevas och att höga sanktionsavgifter kan bli resultatet om man misslyckas, men är osäkra på hur de ska göra för att helt följa den.

1 Missbruksregeln innebar enklare regler för personuppgifter i ostrukturerat material.

”Fascinerande nog verkar inte rutiner ha ändrats i alla verksamheter. Svar som ”Inte alls”, ”Nej, inte direkt”, ”Nej, inte vad jag vet” och ”Nej, inte i någon större utsträckning” förekommer också.”

Tidigare nämndes att två personer angav att de inte behövde göra några större förändringar då de redan arbetat aktivt med PUL, vilket andra inte verkar ha gjort. En möjlig förklaring till detta kan ses i följande respons: ”GDPR ställer tydliga krav på kontinuerlig efterlevnad, inte bara vid ett visst tillfälle som lagstiftningen gäller. PUL kändes som att man gjorde jobbet och när det var klart så var där inga tydliga kontrollmekanismer.”

Är ni färdiga eller vilka utmaningar kvarstår?

En klar majoritet av respondenterna var överens om att GDPR-arbetet är menat att ständigt pågå: ”Man blir aldrig färdig, detta är ett förändrat arbetssätt som ständigt måste vara levande.” Vissa verkade dock vara av uppfattningen att de var i princip klara, med svar som ”för det mesta färdiga”, ”saknas fortfarande en del pub-avtal” och ”[r]utinerna finns på plats men det går alltid att bli bättre”. Det behöver såklart inte tolkas som att de inte håller med om att det är ett ständigt pågående arbete, utan kan även tolkas som att de stora arbetena är färdiga och vardagliga, mindre saker, som fortsatt ifyllande av register över personuppgiftsbehandlingar, inte uppfattas som någon stor utmaning.

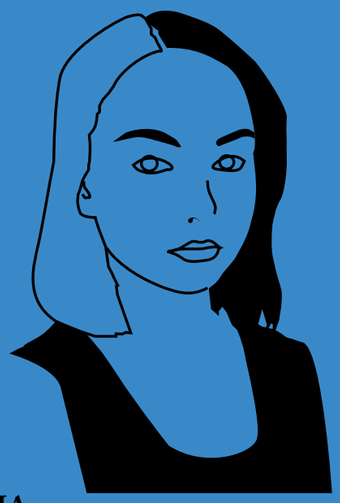
Hur har införandet av GDPR påverkat dig?

Flera meddelar att de efter införandet av GDPR arbetar som dataskyddsombud och att arbetet med GDPR tar upp mycket tid och arbetsuppgifter. Några nämner att det belastar det övriga arbetet, då ingen tid har frigjorts för uppdraget. En person skriver att GDPR-arbetet ”har lett till väldigt mycket merarbete som mestadels har försvårat för medarbetarna utan att leda till någon uppenbar nytta för organisationen eller medborgarna”. Ett av svaren på första frågan angav att det var en utmaning att få medarbetarna att se nyttan i GDPR-arbetet och i citatet kan vi se att respondenten endast ser GDPR-arbetet som onödigt merarbete. Detta kan naturligtvis vara ett resultat av att resurser och tid inte har satts av till arbetet eller att man har svårt att tolka förordningen, varför man ser negativt på detta ”tidskrävande krångel”.

Att arbete med GDPR därutöver är mer administrativt krävande än arbetet med personuppgiftslagen tas upp många gånger och jag vill igen koppla till de personer som angav att inga stora förändringar hade behövts göras i verksamheten när GDPR infördes, då de sedan tidigare hade en bra grund i PUL-arbete. Det är svårt att utan mer insyn i verksamheterna veta om de personerna underskattar GDPR:s krav eller om de faktiskt hade rutiner sen tidigare som till stor del levde upp till de nya kraven. En skillnad i hur administrativt krävande arbetet framstår är dock tydlig i dessa två fall.

Men även om arbetsbelastningen och den tillhörande tidsbristen är de vanligast förekommande svaren ses inte införandet av GDPR av alla som någonting negativt. Den utbildning som respondenterna anger har skett i verksamheterna har gett effekt då flera konstaterar att de har mer kunskap kring personuppgiftsbehandlingar, integritet och informationssäkerhet än tidigare och likaså att verksamheterna nu har bättre koll på personuppgiftsbehandlingarna överlag. Men även om några skriver att införandet har varit ”positivt” och ”till det bättre” finns det också de som menar att införandet ”inte alls” eller ”inte speciellt mycket” har påverkat dem. Detta är intressant då resten av svaren i enkäten tycks visa på att GDPR har krävt mycket mer arbete, att det har skett utbildningar och att det har förändrat de vanliga arbetsrutinerna väldigt mycket. Det tydliggör om inte annat hur stor skillnad det är från verksamhet till verksamhet.

Jag vill avsluta artikeln med ett svar som lämnades på den sjätte frågan: ”som gammalt PUL-ombud som numer är DSO så har rollen fått ökad status och tydlighet och större mandat”. Kontentan verkar vara att även om vissa anser att GDPR mest inneburit onödigt arbete tas åtminstone lagstiftningen seriöst och verksamheter anstränger sig för att utbilda, inventera och skapa rutiner (även om det beror på hotet från sanktionsavgifter). Betydligt mer tid och resurser behöver däremot avsättas för att arbetet ska kunna göras ordentligt oavsett hur man har arbetat med GDPR-frågan, om man ska tro de svar som har lämnats in på enkäten.



ALICIA BERGLI

Är arkivkonsult på ArkivIT, med en masterexamen i ABM med inriktning arkivvetenskap i ryggen.
Hon skyller sitt val av arbete på sitt historieintresse, och riskerar att hamna med näsan i gamla arkivhandlingar lite väl länge om ingen stoppar henne.

Avanzas resa med GDPR

På Avanza vill vi att våra kunder ska känna sig trygga oavsett vilka regler som styr verksamheten. EU:s dataskyddsförordning GDPR började tillämpas våren 2018, men för Avanza började resan redan 2016 när förordningen fastställdes. För vår del handlar förordningen om våra kunders ökade rättigheter när det gäller deras personuppgifter och våra skyldigheter kring hanteringen av dessa. Vi ser positivt på GDPR, då förordningen skyddar våra kunder.

Avanza startades med en enkel idé – vi ville bygga ett företag där vi själva skulle vilja vara kunder. Vår affär bygger på ett starkt kundfokus och visionen är att skapa en bättre framtid för miljoner människor, genom ett billigare, bättre och enklare erbjudande. Vi vill engagera och skapa förståelse för sparande genom utbildning, information och enkla beslutsstöd. Vi vill samtidigt uppmuntra och inspirera till ett hållbart sparande. Ambitionen är att skapa det bästa verktyget för våra kunder för att lyckas med ekonomin. Avanza har mer än 1 miljon kunder med över 400 miljarder kronor i totalt sparkapital. Det motsvarar 4,4 procent av den svenska sparmarknaden. Förra året vann Avanza Svenskt kvalitetsindex (SKI) utmärkelse Sveriges nöjdaste sparkunder för tionde året i rad samt blev årets bank för andra gången.

Utmaningarna dök upp tidigt i analysfasen och gällde tolkningen av artiklarna i förordningen. Vi arbetade tillsammans inom Avanza, men även inom branschen för att komma fram till gemensamma tolkningar och en gemensam förståelse av innebörden, för att få en så bra start som möjligt. Detta arbete var viktigt och tog tid. Utfallet av tolkningarna kom senare att ligga till grund för beslut om de åtgärder som skulle implementeras i koncernen. Här underlättade det verkligen att vi hade en gemensam förståelse från början. Parallellt med detta genomförde vi en kartläggning av väsentliga delar som behövde komma på plats, så att vi tidigt kunde resursplanera vilken kapacitet som behövdes under projektet.

Analysarbetet kokade ned till fyra övergripande områden som vi behövde arbeta vidare med: ”kundens rättigheter”, ”incidentrapportering”, ”utbildning” och ”skydd av uppgifter”.

Kundens rättigheter innebär att kunden ska ha möjlighet att, få information om vilka personuppgifter vi behandlar, begära rättelse eller radering av uppgifterna, eller begränsning av behandlingen, samt kunna invända mot behandlingen. Utöver allt detta ska det finnas möjlighet att föra över personuppgifter till ett annat företag. Dessa krav har funnits i tidigare lagstiftning så här handlade det primärt om att säkerställa att vi kunde leva upp till samtliga delar och fastställa på vilket sätt det skulle göras.

För att möta kraven utvecklade vi ett verktyg där kunderna själva kan se och hantera sina uppgifter, via Avanzas digitala plattform, utan att behöva kontakta vår kundservice. Det var viktigt för oss ur ett kundperspektiv samtidigt som vi byggde en skalbar lösning som inte riskerade att skapa en belastning på organisationen i takt med att vi växer. Redan första året hade vi tusentals nedladdningar av personuppgifter via vår digitala plattform.

”Utfallet av tolkningarna kom senare att ligga till grund för beslut om de åtgärder som skulle implementeras i koncernen.”

Kundens rättigheter omfattar även information om hur Avanza använder personuppgifterna. Här eftersträvar vi att alltid ha transparent lättförståelig information på vår hemsida.

Incidentrapporteringen syftar till en skyndsam hantering om olyckan skulle vara framme och ett misstag från vår sida begås i personuppgiftshanteringen. Den ska säkerställa en grundlig analys om vilken eventuell påverkan incidenten kan få för kunderna och vilka åtgärder som behöver vidtas. Incidentrapportering var redan etablerat hos oss, men för att uppfylla specifika krav i förordningen genomfördes vissa justeringar i hur vi internt skulle hantera incidenter och på vilket sätt rapporteringen skulle ske.

Utbildning och tydlig intern information har alltid varit viktigt för oss i syfte att skapa förståelse och engagemang hos våra medarbetare. Här har vi arbetat med att utveckla anpassade utbildningspaket för vår personal i syfte att öka kunskapen om GDPR och de krav som ställs på oss. Den ökade kunskapen utbildningarna har fört med sig, har också underlättat vårt utvecklingsarbete och skapat bra förutsättningar för alla som berörs. Skydd av uppgifter var det område som fick störst påverkan på oss då regelverket ställer stora krav på inventering, lagring och transport av information samt principer för hur länge uppgifterna behöver lagras och vilka leverantörer som har tillgång till personuppgifterna (där vi behövde se över och förnya våra avtal). För att framtidssäkra vår regelefterlevnad krävdes att vi anpassade våra processer för utveckling och inköp av system, något som omfattade samtliga applikationer i Avanzas digitala plattform och påverkade hela vår it- och utvecklingsorganisation. Tillgång till information är ett centralt område i GDPR. Här gäller det att varje medarbetare endast har tillgång till den information denne behöver utifrån sina arbetsuppgifter och inte har för vida behörigheter.

Eftersom vi har en omfattande hantering av personuppgifter omfattades vi också av kravet att tillsätta ett dataskyddsombud (DSO). Rollen tillsattes tidigt under 2017 och jag fick nöjet att axla den. I rollen som DSO var jag beställare av GDPR-projektet. På så sätt fick jag tidigt en djup förståelse för hur Avanza byggde upp sin hantering kring dataskyddsfrågor, vilket gav mig en heltäckande bild av våra styrkor och svagheter. I rollen, som både omfattar rådgivning och granskning av efterlevnaden, kunde jag vägleda företaget under resan.

När jag blickar tillbaka och ser vad vi kunnat göra annorlunda så är det främst två områden jag kommer att tänka på. Den första är förändringen i ett av våra inloggningsförfaranden. Den förändring vi införde gjorde det säkrare för kunderna, men den innebar också att våra kunder behövde logga in med hjälp av tvåfaktorsidentifiering vilket vissa av våra kunder upplevde som störande. Det i sin tur genererade en ökad belastning på vår kundservice. I backspegeln skulle vi ha infört förändringen under en längre tidsperiod så att alla involverade fick mer tid att anpassa sig till de nya förutsättningarna.
Det andra området är avtalsrelationer med leverantörer och samarbetspartner. I förordningen är det väldigt enkelt, nämligen att det är vi som ska upprätta avtal med leverantörer och samarbetspartner som behandlar personuppgifter för vår räkning. Detta fanns redan på plats genom tidigare lagstiftning, men i och med GDPR blev ansvaret för berörda parter större. Detta ledde till en omarbetning av avtalen, vilket tog lång tid och i vissa fall skapade komplikationer som vi inte hade räknat med.

Nu när två år har passerat sker den faktiska tillämpningen runt om i världen på riktigt. Dataskyddsmyndigheter genomför granskningar och utfärdar varningar och sanktioner. Granskningarna och sanktionsskrivelserna visar hur dataskyddsmyndigheter tolkar förordningen, vilket ger ytterligare insikter och möjliggör för oss att se över och eventuellt ändra vår hantering.

Idag arbetar vi liksom tidigare med kunden i fokus, men med en rad nya arbetssätt, rutiner och processer. Vi ser regelbundet över hur vi kan göra det ännu enklare för våra medarbetare och kunder, i allt från vägledning till nya verktyg, information och utbildningsinsatser.

Om jag ska blicka framåt tror jag att GDPR alltid kommer att handla om att i första hand skydda kundens rättigheter och i andra hand om att ha förmågan att upptäcka och hantera brister i den egna verksamheten. I takt med att nya tolkningar och tillämpningar genomförs blir omvärldsbevakningen en naturlig del för att säkerställa att vi uppfyller kraven även i framtiden.

Sammanfattningsvis har på ytan inte så mycket förändras efter GDPR. Det kan bero på att vi inte genomförde några större organisatoriska förändringar utan skapade möjligheter för alla medarbetare att anpassa sig till de nya förutsättningarna i sina befintliga roller. Vi är stolta över vår implementering. Förhoppningen är att även våra kunder uppskattar det vi gjort och känner sig trygga med att vi hanterar deras uppgifter på ett tryggt sätt med stor integritet.

JOHAN DRESSLER

Mitt namn är Johan Dressler och jag är dataskyddsombud på Avanza. 2017 utbildade jag mig inom dataskyddsförordningen och dataskyddsfrågor och är nu certifierad på området. Jag har arbetat på Avanza sedan 2011 där jag primärt har arbetat med informationssäkerhet, incidenthantering, riskhantering och kontinuitetshantering. Denna artikel är min berättelse om hur vi har hanterat GDPR från 2016 fram till idag.

Sjyst data för bättre affärer

Svenskarnas oro för hur deras personuppgifter hanteras har paradoxalt nog ökat efter införandet av GDPR. Osäkerhet och ovilja att dela data medför negativa konsekvenser för den växande digitala ekonomin. Kanske kan en kvalitetsmärkning öka tryggheten och samtidigt möjliggöra nya integritetsvänliga affärsmodeller? Det hoppas åtminstone deltagarna i projektet Sjyst data.

Forskningsprojektet Sjyst data har sedan hösten 2017 undersökt hur användares integritetskrav kan förenas med nytta för företag och offentliga verksamheter.

– Det finns en ökad oro över hur företagen använder kundernas personliga data. För att oron ska minska, måste det bli mer transparent och lättfattligt vilka data som sparas och i vilket syfte, säger Sara Leckner, universitetslektor vid institutionen för datavetenskap och medieteknik, Malmö universitet.

Tillsammans med tio partners från akademi och industri jobbar hon för att skapa trygga och lättbegripliga tjänster, trots ett minst sagt snårigt regelverk.

Den växande oron beror åtminstone delvis på större medvetenhet bland allmänheten. Våren 2018 kunde knappast någon undgå begreppet GDPR eller den hets som stundtals rådde bland företag och organisationer som plötsligt skulle uppdatera medgivanden, register och avtal. Den massiva uppmärksamheten och informationen har haft både goda och mindre goda konsekvenser, säger Sara Leckner.

– Att medvetenheten ökar är ju i grund och botten bra, men det främjar inte den digitala ekonomin att människor är negativa eller oroade för att dela sina data.

Ofta bygger oron dessutom på okunskap eller svårigheter att tolka lagstiftningen. Många är osäkra på vilka regler som gäller. Det kan göra att samhället går miste om potentiellt nyttiga innovationer.

– Den digitala ekonomin bygger på de användardata vi delar med oss av. Risken är att företag avstår från att utveckla innovationer som användarna faktiskt skulle kunna få nytta av.

Jonas Ledendal, som också deltar i projektet, är universitetslektor vid Institutionen för handelsrätt vid Lunds universitet. Jonas Ledendal menar att GDPR inom vissa sektorer redan har medfört en säkrare hantering av personuppgifter, men det råder stora skillnader mellan olika sektorer.

– GDPR är en komplicerad reglering som kräver specialistkompetens och ett systematiskt regelarbete, säger Jonas. Det stämmer inte med hur många små och medelstora företag eller ideella föreningar brukar vara organiserade. De större företagen och organisationerna klarar sig bättre, men även där finns förbättringspotential.

En möjlig lösning på problemen är dataskyddsförordningens (GDPR) skrivningar om självreglering via uppförandekoder och certifiering (artikel 40–43 i GDPR). En uppförandekod är tänkt att bestå av ett antal skräddarsydda och praktiska dataskyddsregler som tas fram gemensamt för organisationer i en viss bransch och som sedan godkänns av Datainspektionen. Hittills är det dock få som använder möjligheten att jobba med uppförandekoder. Enligt Malin Fredholm, jurist på Datainspektionen, har endast sex organisationer ansökt om godkännande av uppförandekoder. Än så länge har ingen godkänts.

Sjyst data siktar dock ännu högre: syftet är att åstadkomma en branschöverskridande integritetscertifiering av digitala tjänster. En certifiering gäller inte bara för en viss bransch, utan ska kunna garantera en allmän efterlevnad av GDPR och kanske även EU-direktivet e-privacy, lagen om elektroniska anslagstavlor (LEK) och andra relevanta regler och krav.

– Det krävs något som kortfattat och begripligt klargör hur din data hanteras när du besöker en sida, säger Sara Leckner. Något som upplevs som trovärdigt, ungefär som många nog tänker om Svanenmärkning på varor.

Att åstadkomma en fungerande och trovärdig märkning av ”Sjyst Data” är förstås inte gjort i en handvändning. Utöver att identifiera krav och analysera vad kraven i praktiken innebär för tjänsteutveckling och informationsarkitektur, förutsätter märkningen också inrättande av ett godkänt certifieringsorgan.

– Vi söker nu pengar och partners för nästa steg, säger Sara. Planen är då att implementera och etablera processen för certifieringsarbetet, vilket förväntas vara klart efter ca 3 år. Så det är fortfarande en lång process innan vi kan nå ut med en färdig certifiering eller märkning.

Läs mer
På projektwebben *sjystdata.se* kan den intresserade följa arbetet och även ladda hem projektets slutrapport och den praktiskt inriktade “Vägledning om EU:s dataskyddsförordning (GDPR): God integritet vid digital tjänste- och affärsutveckling”.

Fakta: uppförandekoder i Sverige

SÖKANDE	STATUS
Sveriges Åkeriföretag (AB Åkerikonsult)	***Beredning***
Säkerhetsbranschen	***Avslutad - ansökan avslagen***
Samtrafiken i Sverige AB	***Avslutad - avskrivning efter återkallelse***
Riksidrottsförbundet	***Beredning***
SRF Konsulterna	***Beredning***
Bildleverantörernas Förening, BLF	***Beredning***

Källa: Datainspektionen

JOHAN ERIKSSON

Är skribent, projektledare, föreläsare och utbildad arkivarie. Han är författare till ”Öppna Myndigheten” och jobbar bland annat med e-arkiv, tillgängliggörande av öppna data, läromedel, utredningar och kulturarvspedagogik. Kontakt: johan@kjfe.se

Allt kan förklaras. Widegrens jobbar med kunskaps-förmedling åt myndigheter, företag och ideella föreningar. Ritar processkartor, vässar formuleringar i utredningar, formger utställningar och förtydligar utbildningsmaterial. Producerar böcker, posters, webbplatser och så vidare. Formaten varierar, men kärnan i arbetet består: begriplig information. Vill du veta hur man gör? Låt oss förklara.

Ring Johan, 070 292 16 30,
eller e-posta: info@widegrens.com

Kurser om hur du skapar informationssäkerhet – på riktigt!

Du ska jobba med informationssäkerhet...men vad är det?
Det står att information ska klassas men hur gör jag det i praktiken?
Plötsligt är alla involverade – hur organiserar jag det och vem ska göra vad?

Känner du igen dig?

Kurserna är för dig som har ett ansvar för informationssäkerheten i din organisation och känner att du behöver utveckla din kompetens!

Praktis 1
Informationssäkerhet – vad är det?
Djurönäset på Värmdö

En grundkurs i informationssäkerhet som varvar informativa pass om informationssäkerhetens olika delar med praktiska övningar.

Kursen är lämplig för dig som vill ha en överblick över informationssäkerhetsområdet och få en känsla för hur arbetet med höja säkerheten går till i praktiken.

Praktis 2
Att införa och förvalta ett systematiskt informationssäkerhetsarbete
Djurönäset på Värmdö

Kursen ger dig konkreta verktyg för hur du lyckas med informationssäkerhetsarbetet i din organisation.

Vi fortsätter att ha en praktisk inriktning med fokus på konkreta frågor om planering, implementering och förvaltning av ett bestående informationssäkerhetsarbete.

Anmäl dig på www.fiaewald.se/utbildningar

Fia Ewald CONSULTING AB

6 snabba med Fia Ewald

FIA EWALD

Har en lång bakgrund inom arkiv, informationshantering och informationssäkerhet. Numera är hon konsult, skribent och leder utbildningar

Hej Fia Ewald, nu har det gått strax över två år sedan dataskyddsförordningen infördes, vilka är de största förändringarna som du kan se har kommit av den?

Att integritet har blivit en fråga för företags- och myndighetsledningar på ett helt annat sätt än tidigare. I alla fall på det sätt att man vill undvika sanktionsavgifter och badwill. Däremot så är jag osäker på om dataskyddsförordningen kommer att vara verkligt effektiv i det övervakningssamhälle vi allt mer har kommit att leva i.

Vilka frågeställningar kring dataskyddsförordningen upplever du var vanligast innan och sedan efter 25 maj 2018?
Innan den dataskyddsförordningen så var det väldigt många detaljfrågor som skulle lösas på relativt kort tid – man såg liksom inte skogen för alla träd. Nu överskuggar molnfrågan det mesta.

Upplever du att frågor rörande personuppgifter tas på större allvar nu?
Ja, det får jag nog säga. Jag tror att ledningar i företag och myndigheter har lärt sig en hel del om hur viktigt är att vara compliant till [följa] dataskyddsförordningen och det gör det lättare för dem som arbetar praktiskt med frågorna att nå fram.

Upplever du att det finns en tydlighet bland dem som berörs av dataskyddsförordningen rörande hur personuppgifter ska hanteras?
Nej, jag uppfattar att många organisationer, både privata och offentliga, har dålig kontroll över vilken information de faktiskt har. Av det följer att de har dålig kontroll över vilka personuppgifter som finns, hur de används och hur de får hanteras.

”Däremot så är jag osäker på om dataskyddsförordningen kommer att vara verkligt effektiv i det övervakningssamhälle vi allt mer har kommit att leva i.”

Vad har varit det mest positiva som kommit med införandet av dataskyddsförordningen?
Det tråkiga svaret är sanktionsavgiften. Även om summorna hittills varit blygsamma har det ett stort signalvärde när exempelvis Statens servicecenter blir ålagda att betala 200 000 kronor för ett felaktigt agerande. Det är också lärorikt för andra organisationer när en praxis utvecklar sig.

Vilka är de största missuppfattningarna runt dataskyddsförordningen som finns kvar nu två år senare?
Att dataskyddsförordningen skulle kunna lösa de frågor som finns gällande de stora molntjänsterna. Där tycker jag snarare att vi har gått baklänges och att det idag är svårare än någonsin att avgöra hur vi ska kunna arbeta med tillräcklig integritet i dessa tjänster.

För mig är det också litet torftigt att se integritet bara som en fråga om juridik. Integritet handlar ytterst om värderingar och människosyn och därför upplever jag det som en missuppfattning att juridiken ger alla svar.

I nästa nummer av
Arkiv Information Teknik, med tema

Och den ljusnande framtid är vår
– arbetsmarknaden för informationshanterare

som utkommer våren **2021**,
tittar vi på dåtid, nutid och framtid för
yrkesverksamma inom informationshantering.

Är du intresserad av att bidra med en artikel
eller har förslag på artikelförfattare får du
väldigt gärna kontakta redaktionen
info@arkivinformationteknik.se