VAGGERYDS KOMMUN

Redovisning Informationssäkerhet 2020

Ansvarig tjänsteman:
Ciso /Informationssäkerhetssamordnare

Beslutad av:

Innehållsförteckning

Bakgrund till kommunens informationssäkerhetsarbete 3
Sammanfattning 3
Hänt under 2020 4
Informationssäkerhet och Säkerhetsskydd 4
Nytt nationellt Cybersäkerhetscenter 4
Nya Föreskrifter och vägledningar 4
Antagande av Policy för informationssäkerhet 5
Fokus på Informationsförvaltning 5
Fokus på integritetsskyddsarbetet (GDPR) 6
Schrems II- domen i EU 6
Datainspektionen har bytt namn 6
Första rapporten från granskningsmyndighet IMY (integritetsskyddsmyndigheten) till regeringen 6
Kommunens informationssäkerhetsarbete kopplat till övergripande nationella mål, kommunfullmäktiges övergripande mål 6
Agenda 2030 7
Utmaningar kommande år 7
Fastställande av mål och styrning inom informationssäkerhetsarbetet 7
Styrning av olika kriterier kring informationstillgångar 8
IT systems inventering och dokumentation 8
Klassning av IT system och informationstillgångar 8
Gemensam Riskhantering 8
Rätt personuppgiftshantering 9
Kompetensförsörjning 9
Sammanfattning och rekommendation 9
Bilaga 1 Sammanfattning av IMY´s integritetsskyddsrapport 2020 10

Bakgrund till kommunens informationssäkerhetsarbete

Digitaliseringen är ett globalt fenomen och påverkar i stort sett alla delar av vårt samhälle. Det medför stora möjligheter, men också risker. Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet. Informationssäkerhet är idag en fråga som angår hela samhället. Alla behöver ta sitt ansvar för informationssäkerhetsfrågor för att vi ska uppnå en effektiv och säker hantering av information. Ingen kan ensam lösa säkerhetsutmaningarna och när det är många olika aktörer som arbetar på olika sätt och i olika sammanhang är det särskilt viktigt med samverkan och en gemensam riktning.

Inom Vaggeryds Kommun ska vi säkerställa den gemensamma nationella riktningen inom informations- och cybersäkerhet och ge förutsättningar för en säker hantering av information inom Vaggeryds kommun. Vaggeryds Kommuns styrdokument informationssäkerhetspolicyn har sin utgångspunkt i den nationella strategin för samhällets informations- och cybersäkerhet som i sin tur har sin utgångspunkt i målen för Sveriges säkerhet: att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter.

Vår styrning och arbete har även sin utgångspunkt i det it-politiska målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Regeringen presenterar i digitaliseringsstrategin, en strategi för hur digitaliseringspolitiken ska bidra till konkurrenskraft, full sysselsättning samt ekonomiskt, socialt och miljömässigt hållbar utveckling.

Vaggeryds kommun har tagit fram en informationssäkerhetspolicy inom området för att möjliggöra målsättningarna i den nationella strategin för information- och cybersäkerhet och ange, färdriktningar och arbetssätt för säker hantering av information i Vaggeryds kommun.

Information är en av Vaggeryds kommuns viktigaste tillgångar. Oavsett form och kanal har den en avgörande roll för kommunens verksamheter varje dag, året runt. Informationssäkerhet berör med andra ord alla. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i utan undantag. Informationssäkerhet handlar därmed om mer än att säkra informationssystem. Även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

Sammanfattning

Informationssäkerhet är en del av kommunens alla nämnders och styrelsers ordinarie arbete och inget som kan ligga vid sidan av. Målet är att informationssäkerhet blir en naturlig del i alla verksamheter till nytta både för det interna säkerhetsarbetet men också i ett bredare perspektiv. Det gäller att säkerställa trygghet och säkerhet i den kommunala verksamheten och de tjänster kommunen ska leverera till sina medborgare och samhället i stort avseende säker hantering av information. 2020 är första året det lämnas en officiell rapport inom informationssäkerhetsområdet.

2020 var ett år som påverkades stort av den världsomspännande pandemin. Den påverkar oss som individer men också Vaggeryds kommun som organisation. Vi stod inför utmaningen att driva ett stort förändringsarbete samtidigt som organisationen stod med stora utmaningar att kunna bedriva sin dagliga verksamhet. Utifrån ett informationssäkerhetsperspektiv har ändå pandemin satt fokus på grundläggande viktiga delar i säkerhetsarbetet. Vissa påstår att vi genom pandemin förflyttat vår digitala utveckling 7 år framåt i tiden. Detta har naturligtvis ställt oss inför många nya och utmanande situationer gällande genomförande men också med säkerheten i fokus. Vi har digitaliserat flera processer som tidigare varit analoga. Fysiska möten har blivit digitala. Frågor kring säkerhet har nu blivit en naturlig del i många olika forum.

Trots utmaningar har informationssäkerhetsarbetet under 2020 ändå nått viktiga milstolpar.

Hänt under 2020

Informationssäkerhet och Säkerhetsskydd

Arbetet har under 2020 fortsatt gällande säkerhetsskydd och följsamhet till ny säkerhetsskyddslag som kom 2019. Informationssäkerheten har en given plats i det arbetet och det gynnar även vårt interna arbete. Vi har utökat samarbete med länsstyrelsen, nätverk bedrivs inom informationssäkerhetsområdet, det lyfts och diskuterar olika slags säkra kommunikationslösningar samt att det erbjuds kompetensutveckling.

Nytt nationellt Cybersäkerhetscenter

2020 är också året då cybersäkerheten fått mer fokus beroende på förändrad hotbild för Sverige och även andra nationer gällande cybersäkerheten. Vi ser fler och fler intrångsförsök och sabotage även mot den kommunala verksamheten. På uppdrag av regeringen fick de stora myndigheterna Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen uppdraget att tillsätta ”nytt nationellt cybersäkerhetscenter”

Ett cybersäkerhetscenter syftar till att förstärka myndigheternas förmågor att lösa sina respektive uppdrag, samtidigt som det ger förbättrade möjligheter att höja den nationella förmågan att förebygga, upptäcka och hantera cyberangrepp och andra IT-incidenter som riskerar att skada Sveriges säkerhet. Detta har och kommer påverka även den kommunala verksamheten.

Stöd i form av Rapporten ”Cybersäkerhet i Sverige 2020 – hot, metoder, brister och beroenden har tagits fram” samt ”Rapporten Cybersäkerhet i Sverige 2020 - rekommenderade säkerhetsåtgärder” berör och påverkar även den kommunala verksamheten. Läs mer om nationellt cybersäkerhetscenter och ta del av aktuella rapporter (MSB)

Nya Föreskrifter och vägledningar

MSB har identifierat behov av tydligare styrning av statliga myndigheternas informationssäkerhetsarbete. Därför har MSB givit ut ett föreskriftspaket som omfattar informationssäkerhet, IT-säkerhet och incidentrapportering för statliga myndigheter.

MBS:s uppdrag inom området cyber- och informationssäkerhet är bland annat att:

- analysera och bedöma omvärldsutvecklingen,
- vara regelgivande inom området,
- lämna råd och stöd i förebyggande arbete till andra statliga myndigheter, kommuner, regioner, företag och organisationer.

I detta arbete har MSB under åren givit ut föreskrifter med krav som statliga myndigheter ska följa. Redan 2009 gav MSB ut föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10). Dessa föreskrifter har uppdaterats och i föreskriftspaketet är kraven uppdelade i tre föreskrifter: informationssäkerhet, säkerhetsåtgärder i informationssystem (IT-säkerhet) och incidentrapportering.

I oktober 2020 kom MSB MSBFS 2020:6 nya föreskrifter om informationssäkerhet för statliga myndigheter. MSB har inte mandat att ge föreskrifter till kommuner men rekommenderar att föreskrifterna även bör användas av den kommunala verksamheten. Läs mer om MBS:s författningssamling, föreskrifter för informationssäkerhet

MSB stödjer och ger vägledning också till den kommunala verksamheten via t.ex. metodstöd för att införa ”Ledningssystem för informationssäkerhet (LIS) som i sin tur bygger på ISO standarden 27001. Ta del av MBSs stöd till kommuner och metodstöd för informationssäkerhet

Antagande av Policy för informationssäkerhet

20200622 beslutar kommunfullmäktige att anta Vaggeryds kommuns policy för informationssäkerhet, det innebär att kommunen kan fortsätta sitt arbete med att ta fram konkreta mål och nyckeltal samt övriga riktlinjer kring informationssäkerhet för att stödja förvaltningar och bolag. Övrigt styrande dokument gällande Informationssäkerhet i Vaggeryds kommun

Fokus på Informationsförvaltning

2020 är ett år då mycket av informationssäkerhetsarbetet haft fokus på informationsförvaltning. Information i alla dess former är en viktig tillgång i kommunen, samhället och behöver lämpligt skydd. Framväxten av en kommun och samhälle som i ökad omfattning bygger att information hanteras elektroniskt skapar behov av modeller och metoder för att lägga grunden till detta skydd. Om information ska utbytas och förmedlas säkert måste det finnas gemensamma modeller för att värdera information för att så långt det är möjlig skapa skyddsnivåer som överensstämmer. Arbetet med informationsförvaltning pågår parallellt med informationssäkerhetsarbetet. Det ena kan inte fungera utan det andra.

Det praktiska arbetet inom informationsförvaltningen är ett stort arbete för bolag och förvaltningar och det kommer att vara i fokus flera år framöver. Det är stora arbetet i våra administrativa miljöer och innefattat arbeten i funktioner för:

- Dokumentation/registrering och ärendehantering
- Systemförvaltning
- Dokumenthantering(Kod verk, Informationshanteringsplan, metadata på dokument)
- Informationsförflyttning (på vilket sätt bör vi förflytta information, e-post, kryptering, gemensam fildelning eller andra lösningar.)
- Arkivförvaltning

Samtliga förvaltningar och bolag har under 2020 startat upp och ska färdigställa informationshanteringsplaner med information som omfattar processer , information och IT system kopplat till dessa samt hänvisning till vilka arkiveringsregler som gäller. Dessa delar kan existera i en eller annan form även i en organisation som saknar en organiserad informationshanteringsplan men det är en omöjlighet att arbeta med ett strukturerat informationssäkerhetsarbete om vi inte har en systematiserad och strukturerad modell. Kommunstyrelsens informationshanteringsplan antogs och beslutades under 2020. Den hanteras som vägledande för övriga förvaltningar och bolag.

Fokus på integritetsskyddsarbetet (GDPR)

2020 fortsatte även arbetet med att få följsamhet till integritetsskyddslagstiftningen och personuppgiftshantering i alla våra verksamheter. Kartläggning går parallellt med arbetet kring informationshantering. Vi har ett fortsatt stort arbetet i att förflytta oss även under kommande år. Vaggeryds kommun står inför utmaningar som överensstämmer med de slutsatser som IMY, integritetsskyddsmyndigheten pekar på i sin rapport. IMY rapport 2021:1. Det handlar om inventering och analys av olika digitala lösningar, val av IT system med bedömning ”tillräcklig ”säkerhet, utmaningar med avtal, teknik, arkivering och lagring. Vårt ansvar att uppfylla den enskildes rättigheter och få följsamhet till dataskyddsprinciperna.

Schrems II- domen i EU

Vårt GDPR arbetet har och kommer även framöver att påverkas av den EU-dom Schrems II som kom sommaren 2020 – gällande Privacy shield och CLOUD Act. Schrems II-domen gällde i huvudsak lagligheten i att överföra personuppgifter till mottagare i USA under den s.k. Privacy Shield-överenskommelsen. Förenklat var Privacy Shield en överenskommelse mellan EU och USA som gjorde det möjligt att föra över personuppgifter mellan EU och USA nästan som om USA vore ett EU-land. Hitintills har Privacy Shield varit det huvudsakliga sättet på vilket vi löser att använda amerikanska IT-leverantörer, även om de inte fysiskt för över personuppgifter till USA. CLOUD Act innebar att allt som lagras hos en leverantör som lyder under amerikansk lagstiftning ska betraktas som överfört till USA.

Det påverkar oss i våra nuvarande avtal med leverantörer och våra kommande val av leverantörer och i sin tur leverantörens underleverantör som i många fall har support eller lagring i amerikanskägda bolag. Vår påbörjade och kommande IT- systems kartläggning innefattar personuppgiftsbiträdesavtal med leverantörer som då får uppge underleverantörer och säkerhetslösningar. Där efter får vi ta ställning till lämpligt eller icke lämpligt IT system eller planera för byte av leverantör.

Datainspektionen har bytt namn

Under 2020 har också tillsynsmyndighet Datainspektionen bytt namn till Integritetsskyddsmyndigheten IMY. www.IMY.se

Första rapporten från granskningsmyndighet IMY (integritetsskyddsmyndigheten) till regeringen

Regeringen gav under 2019 Datainspektionen i uppdrag att vart fjärde år redovisa utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik. Denna rapport utgör den första redovisningen enligt uppdraget. Eftersom Datainspektionen den 1 januari 2021 bytt namn lämnas rapporten i Integritetsskyddsmyndighetens (IMY:s) namn. Bilaga 1.Sammanfattning av rapporten av Ciso. Ta del av hela Integritetsskyddsrapporten

Kommunens informationssäkerhetsarbete kopplat till övergripande nationella mål, kommunfullmäktiges övergripande mål.

Vaggeryds kommuns yttersta målsättning med informationssäkerhetsarbetet är att vi får ett högt förtroende från medborgare och ett tryggt och säkert samhälle. Arbetet är viktigt för att kommunfullmäktiges övergripande mål samt att kommunens vision ska uppfyllas. Kommunfullmäktige målen avser hållbar tillväxt och samhällsplanering genom en säker digitalisering samt delaktighet, tillgänglighet och trygghet i att invånare upplever kommunen attraktiv och har ett förtroende för kommunens funktionalitet, effektivitet och kvalitet. Vårt arbete utgår från den Nationella strategin för informations- och cybersäkerhet och de it-politiska målen i Digitaliseringsstrategin.

Agenda 2030

Inom agenda 2030 kopplas informationssäkerheten främst mot mål16, att ha en gemensam brottsbekämpning då utifrån Cyberhot. Mål 9 och 11 handlar om vår digitala infrastruktur och vårt ansvar kring hållbar digital utveckling där informationssäkerheten är en förutsättning för trygga och säkra digitala lösningar.

Gällande Agenda 2030 är informationssäkerhetsarbetet kopplar bland annat till målen som handlar om att främja fredliga och inkluderande samhällen och gemensam brottsbekämpning. Cybersäkerheten är ett globalt problem som även blir ett lokalt problem för oss i Vaggeryds Kommun.

Målet kring hållbar infrastruktur för att främja informations- och kommunikationsteknik för alla samt effektiva och inkluderande institutioner på alla nivåer. Här är det den hållbara digitala infrastrukturen

Hållbar stadsutveckling omfattar hållbart byggande och hållbar planering av bostäder, infrastruktur, offentliga platser, transporter, återvinning och säkrare kemikaliehantering som i sin tur kräver ny teknik och samarbete mellan flera sektorer. Inkluderande och innovativ stadsplanering behövs för att göra städerna säkra och hållbara för framtiden. Den digitala infrastrukturen är en viktig angelägen del för kommunen vars utbyggnad ska ske på ett säkert sätt.

Utmaningar kommande år

2021 kommer till största delen innebära ett praktiskt arbete inom informationssäkerhetsområdet. Kommunen ska också fastställa ett flertal riktlinjer för att säkerställa styrning.

För att få så många aktiviteter som möjligt genomförda och påbörjade behöver vi kommande(nuvarande) år fokusera på:

Fastställande av mål och styrning inom informationssäkerhetsarbetet

Vaggeryds Kommun har ett stort arbete med att få riktlinjer på plats inom flera områden. Identifierade områden är Riktlinjer A Informationssäkerhet för medarbetare, B Styrning av informationssäkerhet, C Informationssäkerhet i verksamhetsnära förvaltning, D Informationssäkerhet i IT- miljö. Fokus 2021 blir riktlinjer för medarbetare och styrningen av informationssäkerhetsarbetet. Målet är att uppnå systematik i informationssäkerhetsarbetet och följsamhet med ISO 27001 standard.

Styrning av olika kriterier kring informationstillgångar

Kommunen behöver gemensamt bestämma definition av olika slags IT system. Vilka kriterier som ska uppfyllas för att bli benämnt t.ex. kommungemensamt, kriterier som ska gälla vid nyanskaffning/utveckling av system. Kriterier som ska beaktas vid säkerhetsbedömning. Gemensam resursfördelningsmodell för gemensamma system mm.

IT systems inventering och dokumentation

Ett arbete som fortsätter är det stora kartläggningsarbetet av kommunens IT system.
Det är nödvändigt för kommunen att ha kontroll på sina informationssystem. Ytterst handlar det om att kommunen måste ha ett strategiskt och transparent utvecklingsarbete kring digitalisering.

Genom att ha en standard dokumentation kring våra system kan vi hitta synergieffekter, ta strategiska beslut och använda resurserna på bästa möjliga sätt. Vi kan också digitalisera med ”tillräcklig säkerhet”. Vårt mål blir att ha rätt underlag för att kunna fatta rätt beslut som medför maximal nytta för våra invånare och de vi finns till för.

Varje system behöver en förvaltningsplan, dedikerade roller, handlingsplan, strategisk utvecklingsplan samt en informationssäkerhetsplan för att säkerställa rätt skyddsåtgärder kring systemet. Arbetet kommer pågå under flera år. 2021-2022 ska kommunens gemensamma IT system ha en förvaltningsplan.

Klassning av IT system och informationstillgångar

Kommunen ska klassa sina IT system, dvs bedöma vad konsekvenserna skulle bli om:

- informationen kom i orätta händer
- systemet inte skulle vara tillgängligt
- vi inte kunde lita på att informationen var korrekt och riktig i systemet
- eller om vi inte kunder spåra aktiviteter som utförts i systemet.

Denna bedömning ska ske utifrån perspektivet:

- Ekonomiskt
- Verksamhet
- Förtroende
- Individ

När vi har bedömt konsekvenser och fastslagit Klassning, ska ”rätt” säkerhetsåtgärder fastställas på systemet.

Vår konsekvensmatris, bör också den vara kommungemensam och användas vid andra risk- och säkerhetsbedömningar.

Gemensam Riskhantering

I vårt informationssäkerhetsarbete ligger grunden alltid i, att arbeta förebyggande och med riskfokus så att incidenter inte inträffar. Kritiska informationstillgångar ska ha riskbedömts och fått belyst sårbarheter för att planera säkerhetsåtgärder. Denna riskbedömning ska om möjligt vara densamma som används vi andra riskbedömningar inom kommunen. Ett verktyg som man känner igen sig i. En utmaning under året som kommer.

Rätt personuppgiftshantering

Kommunen har fortfarande stora utmaningar med att få följsamhet till GDPR lagstiftningen som började gälla i maj 2018. Naturligtvis påverkas även detta arbete av pandemin då verksamheternas fokus har varit på kärnverksamheten.

Utmaningen sitter också ihop med det stora arbetet kring informationsförvaltning, där kommunen hade utmaningar redan innan 2018.

Kommunens utmaningar gällande information kring våra IT system påverkar också arbetet då 80% av all vår informationshantering sker i något slags IT system.

Samtliga förvaltningar och bolag har utmaningar med att få §30 registret på plats (registerförteckningar). Förhålla sig till Schrems II domen och kartläggning av IT system. Arbetet ska färdigställas under 2021-2022. I arbetet ingår också att se över den enskildes rättigheter och att möta samtliga dataskydds principer. Vi behöver även här stärka upp med kompetensstöd.

Kompetensförsörjning

2021 kommer vara året då vi arbetar med att höja säkerhetskulturen. Att skapa säkerhetsmedvetande hos den enskilde medarbetaren och förtroendevalda, är i många fall avgörande för hur Vaggeryds kommuns resultat kommer att se ut gällande informationssäkerhetsarbetet.

I alla undersökningar gällande incidenter, sabotage och intrång har man kunnat härleda det till den enskilde individens handlande. Inte med ont uppsåt utan i brist på säkerhetstänk. Därför är det oerhört viktigt att ”säkert beteende” finns med som punkt vid introduktion av nya medarbetare/förtroendevalda samt upprepad kompetensinhämtning varje år.

Sammanfattning och rekommendation

Vaggeryds Kommun befinner sig i ett förändrings- och förbättringsarbetet som enligt min bedömning har motsvarighet när samhället gick från analog hantering av information till möjligheten som inträdet av datorerna gav oss. Det stora omställningsarbetet som följde var enormt för verksamheter. Vi genomförde kompetenssatsningar. Det påverkade vårt eget sätt att arbeta. Det blev stora förändringar av processer och ett annat sätt att hantera information på. Samhället i stort samt även kommunen och den enskilde medarbetaren fick obegränsade möjligheter att göra lite som man själv ville. Lagra information på ”mitt” bästa sätt. Döpa informationen på ”mitt sätt”. Skicka informationen på det sättet som ”jag” ansåg lämpligt. I flera organisationer fick man också välja teknik, den enskilda organisationen ägde teknik, man fick välja telefon, använda den lite som man ville, man valde system med liten IT kompetens och väldigt liten IT styrning. Allt detta har naturligtvis lett till de utmaningar vi står inför nu.

I vår kommun har man ändå varit framgångsrik i förändringen av IT strukturer och vi har numera sedan flertalet år tillbaka centraliserad styrning av teknik och olika digitala lösningar och därmed en uppstyrd säkerhet kring vår IT- säkerhet och drift. Vaggeryds Kommun var den första kommunen i Sverige som införde e-legitimation till alla våra medarbetare för att säkerställa säkerheten i bl.a. inloggning i vårt nätverk och åtkomsten till information. Men IT äger inte informationen. IT har ingen kunskap om leverantörer eller dennes säkerhet i de system eller lösningar verksamheterna själva väljer, appar eller molnet tjänster där IT inte ansvarar för drift. IT äger inte heller ansvaret för vilken

slags information som hanteras i våra system och hur känslig den informationen är. IT agerar på de krav som verksamheten ställer och med det kommer den stora utmaningen vi nu står inför.

Nu är vår utmaning att centralisera styrning av information och säkerställa säkerheten i hantering av informationen. Det är en omöjlighet att arbeta med informationssäkerhet om vi inte agerar på samma sätt inom informationshanteringen.

För att uppnå målsättningen inom informationssäkerhetsområdet bör våra satsningar vara likställda med föregående stora förändringsarbete som datorerna medförde. Liknande resurser behöver avsättas för att få styrning på information och säker hantering. Kommunens skyldighet är att tillse att känslig information får rätt skydd och att inte informationen tillgängliggörs för obehöriga. Att informationen vi hanterar är riktig, att ingen har förvanskat den samt att vi kan spåra aktiviteter som utförts på informationen…… men……..

Det stora arbetet gäller främst att förändra vårt beteende. Vi behöver ”tänka säkert”. I IMY´s analys, Säpos uttalanden, summeringar utifrån inträffade incidenter mm, nämns uteslutande att det är den mänskliga faktorn som orsakar de flesta incidenterna. Fel hantering av information, vi skickar information felaktigt, känslig information i e-post, vi skickar information till fel person. Vi klickar på länkar som har olika virus i sig där syftet är att förstöra vår information eller komma åt känsliga uppgifter. Vi blir lurade att på ett eller annat sätt lämna ifrån oss uppgifter, antingen om oss själva eller den organisationen vi befinner oss i.

Vaggeryds kommun ska göra ett stort arbete kring att höja säkerhetsmedvetandet hos våra medarbetare och förtroendevalda. Incidenter inträffar inte för att den enskilde medvetet vill sabotera utan i de flesta fall utifrån brist på kunskap.

Alla stora förändringsarbeten pågår under flera år, med ett strukturerat arbete uppdelat i hanterbara delar och avsatta resurser kommer Vaggeryds kommun att lyckas med ett systematiskt informationssäkerhetsarbete.

Annika Lagerqvist
Ciso (Informationssäkerhetssamordnare)
Vaggeryds Kommun

Bilaga 1 Sammanfattning av IMY´s integritetsskyddsrapport 2020

Sammanfattning av IMY´s integritetsskydds-rapport 2020

I januari 2021 lämnade Integritetsskyddsmyndigheten (tidigare Datainspektionen), IMY, över sin första integritetsskyddsrapport till regeringen. Rapporten är en del av IMY:s nya uppdrag att vart fjärde år lämna en redovisning av utvecklingen inom dataskyddsområdet till regeringen. IMY:s slutsats är att Sveriges ambitiösa digitaliseringspolitik behöver kompletteras med en tydlig och konkret integritetsskyddspolitik. I denna sammanfattning har Ciso i Vaggeryds Kommun tagit delar av rapporten och sammanfattat några av de viktigaste punkterna som IMY lyfter fram i sin rapport.

DIGITALISERINGSPOLITIKEN I EU OCH SVERIGE

I IMY´s rapport lyfts det fram att både EU och Sverige har en hög ambitionsnivå avseende tillvaratagande av digitaliseringsmöjligheter och digitaliseringspolitiken är högt upp på agendan. I Sverige har vi den nationella digitaliseringsstrategi och en nationell inriktning för AI. Inom EU märks det bland annat genom att det i februari 2020 presenterades flera strategiska dokument som anger inriktningen för EU:s digitala framtid: EU:s digitaliseringsstrategi, datastrategi och vitbok för AI.

VIKTIGA INITIATIV INOM EU - ETT ÖKAT SKYDD FÖR PERSONUPPGIFTER

För att möta den snabba tekniska utvecklingen och ökande insamlingen och delningen av personuppgifter infördes dataskydds-förordningen (GDPR) den 25 maj 2018. Genom den stärktes de enskildas rättigheter samtidigt som skyldigheterna för de verksamheter som

hanterar personuppgifter skärptes. Ett direktiv på det brottsbekämpande området, implementerades också i svensk rätt genom brottsdatalagen och brottsdataförordningen som trädde i kraft under 2018.

Genom dataskyddsförordningen inrättades också den Europeiska dataskyddsstyrelsen, EDPB. Styrelsen beslutar om yttranden och vägledningar men har även mandat att fatta beslut i gränsöverskridande ärenden.

Sedan GDPR trädde i kraft har EU-domstolen meddelat ett tiotal domar rörande integritetsskydd. I rapporten ges en kortfattad beskrivning av den praxis som hittills utvecklats. Rapporten tar bland annat upp EU-domstolens underkännande av Privacy Shield, målet där EU-domstolen klargör vad som gäller vid överföring av personuppgifter till tredje land (Schrems II).

DIGITALISERING OCH TEKNIKUTVECKLING

I rapporten beskriver IMY sexton olika teknikutvecklingsområden som tillsammans bidrar till utveckling och Sveriges förmåga att ta tillvara digitaliseringens möjligheter, men som samtidigt haft stor betydelse för den personliga integriteten.

Teknikutvecklingsområdena presenteras utifrån de olika sätt personuppgifter kan behandlas på (utifrån personuppgifternas livscykel).

TEKNIK FÖR ATT SAMLA IN DATA

Stora mängder data ger omfattande affärsmöjligheter vilket har skapat starka incitament för att utveckla teknik för att samla in data. Den ökande insamlingen av data om vårt beteende och rörelsemönster, dels på nätet, dels i den fysiska världen har påverkat och kommer även framöver att påverka den personliga integriteten. Ny teknik för att samla in data ger en mängd aktörer tillgång till en fullständig bild av våra liv, våra intressen, våra kontakter, vår hälsa, våra rörelsemönster, vanor och beteenden.

Risker för den enskilde individen med den ökande datainsamlingen handlar bland annat om att det blir allt svårare att upptäcka, kontrollera eller välja bort att data om oss samlas in. Det faktum att uppgifter delas mellan olika aktörer på ett sätt som ofta är svåröverblickbart både för den enskilde individen och för verksamheterna som delar data gör integritetsriskerna större. Det finns också en risk för ändamålsglidning, det vill säga att uppgifterna används för andra ändamål än de ursprungligen samlats in för.

Sensorer och sändare

Ett teknikutvecklingsområde som lyfts fram i den här delen är sensorer och sändare, Som exempel kan nämnas kroppsnära teknik som pulsklockor och träningsarmband och geospatial teknik för positioneringsdata.

Nya former för interaktion mellan människa och dator

På kort tid har röststyrningsteknik fått ett brett genomslag och spridits från mobiltelefoner och datorer till bland annat bilar, klockor, hörlurar och olika smarta prylar i hemmet som till exempel TV-apparater.

Internet of things (IoT)

Utvecklingen inom Internet of things, IoT, utgör ett särskilt riskområde ur ett integritets-perspektiv. IoT avser apparater, maskiner och fordon som har inbyggd teknik och internetuppkoppling, men typiskt sett inte ses som datorer. Det kan vara vardagsföremål som vitvaror, termostater, belysning, TV-apparater, elektroniska lås och larm, kläder eller bilar, men också utrustning i industri, infrastruktur eller vården. Utvecklingen går mot att IoT används inom allt fler samhällsområden och på allt fler geografiska platser för att samla in data. En stor andel IoT-enheter har visat sig ha bristande säkerhet. Forskare har till exempel visat hur man kan ta kontroll över en modern bil via ett trådlöst nät, eller via fjärrstyrning manipulera en pacemaker eller insulinpump.

Webbskrapning

Med teknik för webbskrapning som kombineras med artificiell intelligens, AI, är det förhållandevis enkelt att samla in och bearbeta mycket stora informationsmängder från nätet, exempelvis från sociala medier. Kännetecknande är ofta att informationsmängderna blir så stora att det blir oöverblickbart och kräver AI-teknik för bearbetning.

Biometrisk data

En särskild typ av datainsamling som i ökande utsträckning används inom allt fler samhällsområden handlar om insamling av biometriska uppgifter. Biometri innebär att mäta kroppens egenskaper (till exempel hand- eller fingeravtryck, mönster i ögats iris, ansikts- eller kroppsform och röstavtryck) eller individers beteenden (till exempel gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster) för att verifiera, autentisera eller identifiera individer. Användning av biometriska uppgifter kan skapa ökad bekvämlighet, snabbhet och säkerhet. Samtidigt medför den ökande användningen av biometriska uppgifter betydande integritetsrisker. En av de främsta riskerna handlar om att biometriska data (till skillnad från till exempel lösenord eller passerkort) inte kan bytas ut om uppgifterna skulle hamna i orätta händer. De biometriska uppgifterna är beständiga, vilket gör en integritetsförlust svår att reparera.

TEKNIK FÖR ATT BEARBETA OCH ANALYSERA DATA

De ökade möjligheterna att samla in data skulle i praktiken vara värdelösa om inte tekniken för att bearbeta och använda uppgifterna också tagit stora utvecklingssprång.

AI – artificiell intelligens
Utvecklingen av artificiell intelligens (AI) har haft avgörande påverkan på den personliga integriteten under de senaste åren. De möjliga nyttorna med AI är stora och den outnyttjade potentialen fortfarande stor. I dagsläget uppges ungefär fem procent av svenska företag och tio procent i offentlig sektor använda AI i sina verksamheter.
Samtidigt innebär AI integritetsrisker för den enskilde i form av bland annat bristande transparens, diskriminering, försvårat ansvarsutkrävande, missbruk och fientlig användning. Särskilda risker finns vid automatiserade processer i beslutsfattande, när ett beslut kan få stora konsekvenser för den enskilde.

Riskområde -Digitala annonsmarknaden
De komplexa och icke transparenta processerna som kan inkludera hundratals aktörer inom den digitala annonsmarknaden gör det i praktiken omöjligt för den enskilde att utnyttja sina rättigheter, till exempel att få information raderad. Affärsmodellerna gör det i praktiken också mycket svårt för företagen att ha kontroll och uppfylla sina skyldigheter när det gäller enskildas rättigheter. Såväl norska som brittiska myndigheter har i färska analyser kommit till slutsatsen att stora delar av den digitala annonsmarknaden systematiskt bryter mot dataskyddslagstiftningen.

TEKNIK FÖR ATT LAGRA DATA

För att kunna utnyttja fördelarna med insamling av stora mängder data och tekniken för att bearbeta och använda data behövs lämpliga lagringsmöjligheter. Utifrån detta lyfter IMY fram teknikutvecklingsområdena molnlagring och edge storage. En utmaning med bearbetning eller lagring i molntjänster är att marknaden för molntjänster idag domineras av amerikanska aktörer vilket kan medföra att lagringen, efter EU-domstolens avgörande i juli 2020 i det så kallade Schrems II-målet, inte är laglig.

Edge computing
Ett utvecklingsområde som kan innebära fördelar ur ett integritetsperspektiv handlar om var data bearbetas – i centrala datacentra och serverhallar eller lokalt. Teknik för edge computing medför att bearbetning av data nu allt oftare kan ske lokalt, i uppkopplade enheter med låg kapacitet eller i lokala servrar. Detta innebär att data i mindre utsträckning behöver transporteras och delas, vilket kan skapa bättre kontroll. Med utvecklingen inom IoT ökar också behovet av lagring och säkring direkt i enheterna utan att behöva transportera data i nätet. Sådan teknik benämns ofta edge storage och edge security, det vill säga att personuppgifter kan lagras och säkras direkt i de lokala enheter där de samlas in, exempelvis i en privatpersons smarta mobiltelefon.

TEKNIK FÖR ATT TRANSPORTERA DATA

Den stora mängden insamlad data och förmågan att bearbeta och använda denna data ställer inte bara krav på lagringsmöjligheter utan också på teknik för att transportera stora datamängder. I denna del lyfter IMY fram 5G och andra former av digital kommunikationsteknik.

5G är nästa generation av mobila nätverk med extremt hög kapacitet för att transportera data. För EU-kommissionen är utvecklingen mot 6G redan en prioriterad fråga. Ett centralt användningsområde för 5G och 6G kommer att vara IoT med till exempel uppkopplade enheter i industrin och i smarta städer. En integritetsrisk kopplat till 5G handlar om att geografisk positionering kommer vara möjligt med mycket med större precision än idag. Ett annat exempel på integritetsrisker som 5G medför är kopplat till en ökad insamling av högupplöst bildmaterial. Möjligheten att utan fördröjning överföra stora mängder högupplösta bilder kommer sannolikt utgöra en pådrivande faktor för en ökad direkt och indirekt insamling av biometrisk data.

Andra former av digital kommunikationsteknik som utvecklas tar sikte på kommunikation på nära avstånd, till exempel mellan enheter i ett och samma rum eller i chip som kan monteras i prislappar.

TEKNIK FÖR ATT SÄKRA DATA

Teknik för att säkra data behövs under hela livscykeln och den sammanlagda teknikutvecklingen har medfört ökade krav på digitala säkerhetslösningar. I rapporten diskuteras AI-baserad säkerhetsteknik och edge security, krypteringsteknik och blockkedjor som exempel på teknikutvecklingsområden vilka kan användas för att stärka integritetsskyddet.

TEKNIK FÖR ATT FÖRSTÖRA DATA

Teknik för att förstöra data skiljer sig från de andra delarna av personuppgifternas livscykel. Medan teknikutvecklingen inom övriga områden har drivit på varandra har utvecklingen av teknik för att förstöra data snarare gått i motsatt riktning. Genom att lagringskapaciteten har ökat har incitamenten för att förstöra data minskat. Det teknikutvecklingsområde som lyfts fram i den här delen av rapporten handlar istället om teknik för att återskapa raderad eller på annat sätt förlorad data.

DEN EXPONENTIELLA TEKNIKUTVECKLINGEN

IMY framhåller vid upprepade tillfällen i rapporten den snabba teknikutvecklingen. IMY poängterar att många av de teknikutvecklingsområden som beskrivs i rapporten utvecklas exponentiellt och att utvecklingen de kommande 100 åren, på grund av detta, kommer att motsvara 20 000 år av teknikutveckling. IMY påpekar också att de olika teknikutvecklingsområdena hänger ihop och påverkar varandra. Exempelvis har den ökade insamlingen av biometriska uppgifter i stor utsträckning möjliggjorts och påskyndats av utvecklingen inom till exempel IoT, sensorer och sändare, AI och big data och molnifiering av lagring.

INTEGRITETSSKYDDET IDAG – OCH I FRAMTIDEN

I rapporten diskuteras också vilken nivå integritetsskyddet har idag. IMY:s bedömning är att det generellt finns stora brister av grundläggande karaktär hos många verksamheter i samhället.

De närmare 500 sanktionsavgifter som hittills utfärdats inom EU visar att de vanligaste överträdelserna handlar om att de grundläggande principerna inte följs, att rättslig grund för behandlingen saknas, att enskildas rättigheter inte hanteras som de ska eller att säkerhetsåtgärderna varit otillräckliga. Av de drygt 11 000 personuppgiftsincidenter som anmälts till myndigheten beror majoriteten av fallen på den mänskliga faktorn, vilket betyder att det finns ett behov av mer och bättre utbildning för att öka kunskapen hos medarbetare. I rapporten presenteras att grundläggande kunskap om dataskyddsförordningen hos medborgarna är bra och att de flesta vet att personuppgifter används men att få vet hur personuppgifterna används, vilket har lett till att oron för hur uppgifterna används har ökat hos befolkningen.

AVSLUTANDE KOMMENTAR

I rapporten dras tre huvudsakliga slutsatser. För det första har människor idag viss kunskap om att data samlas in, men inte i vilken utsträckning det görs. Detta kan för många leda till en känsla av otrygghet. För det andra innebär utvecklingen med IoT att datainsamling och personuppgifts-hantering flyttar in i människors hem, vilket gör det ännu viktigare att hanteringen sker på ett lagligt sätt. För det tredje innebär den ökade insamlingen av biometrisk data att det krävs särskilda insatser för att öka säkerheten avseende användandet av sådana uppgifter. IMY pekar på vikten av att man tidigt i lagstiftningsarbetet gör en ingående integritetsskyddsanalys. Ju mer genomarbetad nationell lagstiftning som kompletterar dataskyddsförordningen är, desto enklare blir det för företag, myndigheter och andra organisationer att tolka och tillämpa dataskyddsreglerna. Vi får då också en lagstiftning som är homogen och heltäckande och ger verksamheterna det stöd de behöver för sin personuppgiftshantering.

//Annika Lagerqvist
Ciso, Vaggeryds Kommun