Databokslut 2021

Sibbo kommun

18.2.2022

SIPOO
SIBBO

Innehållsförteckning

1 Syftet med kommunens databokslut

Det här är Sibbo kommuns databokslut. Databokslutet är en sammanfattningsrapport som uppstår som ett resultat av den interna granskningen. Dess syfte är att ge en beskrivning av den nuvarande databehandlingen samt en bedömning av dataskyddets och datasäkerhetens förverkligande. I databokslutet kartläggs även utvecklingsbehov gällande dataskydd och datasäkerhet samt de åtgärder som dessa förutsätter. Databokslutets syfte är att ge en helhetsbeskrivning av hur databehandling, datasäkerhet och dataskydd förverkligas i kommunen. Det kan ses både som ett verktyg för ledningen och som en del av den personuppgiftsansvariges ansvarsskyldighet enligt EU:s allmänna dataskyddsförordning. Ansvarsskyldigheten betyder att verksamheten har följt lagar och varit förenlig med god databehandling och god informationshantering. Syftet med databokslutet är att öka transparensen och bygga upp förtroendet för en organisation som följer de i organisationen skapade principerna för datasäkerhet och dataskydd och behandlar personuppgifterna enligt dem. Ett välskött dataskyddsarbete inverkar även på konkurrenskraften och organisationens effektivitet. Databokslutets syfte är att fungera som en ledningsrapport som används internt i kommunen och att ge en beskrivning av databehandlingen för intressentgrupperna. Det stöder även planering, styrning av verksamhet, rapportering och ledningen.

2 Hur datasäkerhet och dataskydd genomförs i Sibbo kommun

Enligt dataskyddsförordningen (artikel 24) ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder, som säkerställer och även i praktiken visar att personuppgifterna behandlas i enlighet med förordningen. Med tekniska och organisatoriska åtgärder avses exempelvis utbildning för personalen, interna anvisningar och föreskrifter, avtal och förbindelser om sekretess, övervakning av konton och användning, kryptering av uppgifter, anonymisering eller pseudonymisering av uppgifter, revision av datasystem och register, distansförbindelser, användningsövervakning, tekniska begränsningar, kontroll- och övervakningssystem, processer kring databokslut samt användning av uppförandekoder och certifikat.

2.1 Behandling av personuppgifter i Sibbo kommun

Sibbo kommun ser till att de i dataskyddsförordningen angivna dataskyddsprinciperna hörsammas. Personuppgifter behandlas med respekt för följande krav:

- laglighet, korrekthet och öppenhet
- ändamålsbegränsning
- uppgiftsminimering
- korrekthet
- lagringsminimering
- integritet och konfidentialitet
- den personuppgiftsansvariges ansvarsskyldighet

Detta databokslut beskriver hur ovan nämnda principer efterföljs i kommunens verksamhet. Sibbo kommuns databokslut är i sin helhet en offentlig rapport.

2.2 Organisering av dataskydd och datasäkerhet samt anvisningar och utbildning

Sibbo kommun har en dataskydds- och datasäkerhetspolicy. Den senast uppdaterade versionen godkändes av kommunstyrelsen 12.3.2019. Ansvarsområden gällande allmän datasäkerhet respektive ansvarsområden i särskilda uppgifter beskrivs i dataskydds- och datasäkerhetspolicyn.

2.2.1 Tekniska och organisatoriska skyddsåtgärder för personuppgifter

Förvaltningen av datasystem som används för att behandla personuppgifter följer kommunens principer för datasäkerhet och dataskyddsanvisningar. Datasystemen och användargränssnitten är tekniskt skyddade bland annat med brandväggar, och datainnehållet i kritiska system säkerhetskopieras regelbundet.

Åtkomsten till informationssystem har med hjälp av användargrupperna begränsats så att varje användare har tillgång enbart till de uppgifter som hen behöver för att kunna utföra sina arbetsuppgifter. Övervakning av konton och användning genomförs med hjälp av logginformation som de olika datasystemen samlar samt med auditering av användarbefogenheterna som utförs vid behov. Kommunen införde år 2021 ett centraliserat system för hantering av användarnas identitet och befogenheter. Utvidgningen av åtkomsthantering till alla kommunala system pågår fortfarande, men målet är arbetet kan slutföras innan utgången av år 2022.
IT-tjänster ansvarar för den centraliserade förvaltningen av åtkomsträttigheter, medan systemägarna ansvarar för att införa åtkomsträttigheter för sina egna system. I samband med åtkomsträttighetsprojektet ska användarrättigheterna för informationssystem definieras och uppdateras utifrån användarens uppgiftsrelaterade användningsbehov (16 § i lagen om informationshantering inom den offentliga förvaltningen).

Enheten IT-tjänster ansvarar för anskaffning, ibruktagande och underhåll av arbetsstationer, mobilapparater, servrar, nätutrustning och andra datasystem. Installering av arbetsstationer har lagts ut på entreprenad. Anskaffningen av applikationer sker i samarbete med den enhet som använder applikationen, upphandlingsservicen och IT-tjänster. System används på distans via skyddade anslutningar.

2.2.2 Datasäkerhets- och dataskyddsrisker i kommunen

En anvisning har utarbetats för hantering av datasäkerhetsincidenter. En blankett med vilken anställda kan göra anmälan av datasäkerhetsincidenter togs i bruk 2019 och den används fortfarande. Datasäkerhetsincidenter som upptäckts eller kommit till kommunens kännedom antecknas och klassificeras på ett enhetligt sätt, varefter kommunens dataskyddsansvarige (från och med oktober 2021 en extern service som erbjuds av Privaon Oy) behandlar dem enligt en bestämd process. På detta sätt kan åtgärderna planeras, koordineras och dokumenteras på ett enhetligt och kompetent sätt. IT-tjänster hjälper vid behov.

En del av kommunens anställda arbetade på distans under största delen av 2021 på grund av covid-19-pandemin. Datasäkerhet, dataskydd och nätsäkerhet är lika viktiga när man arbetar på distans hemma, möjligen till och med viktigare än på den egentliga arbetsplatsen.

Distansarbete är förknippat med datasäkerhetsrisker. Anställda som arbetar på distans ska följa kommunens anvisningar om dataskydd och datasäkerhet och rapportera incidenter som eventuellt orsakar risk för datasäkerheten till sina chefer och till Datasäkerhetsteamet. Datasäkerhetsteamet publicerade våren 2021 närmare anvisningar om distansarbete och gemensamma förfaranden.

Kommunen ska se till att kommuninvånarna har tillgång till tjänsterna även under en pandemi. Detta är utmanande med tanke på datasäkerhetsarbetet. Det är viktigt att IT-miljön skyddas ordentligt vid distansarbete, och vi har satsat på detta. Även behovet av kontroll i anknytning till dataskyddet, så som kontroll av tillgången till systemen och övervakning av datakommunikation, har ökat under det gångna året.

Dataskyddsförordningen förutsätter att behandlingen av uppgifterna sker datasäkert och att den övervakas kontinuerligt. Kommunen har haft som uppgift att definiera och vidta tekniska och organisatoriska åtgärder för att säkerställa både personalens och klienternas uppgifter. Det här kravet är ännu viktigare nu när informationen flyter lättare över fysiska gränser. Kommunen ska också regelbundet testa, undersöka och utvärdera effektiviteten av åtgärderna för att säkerställa säkerheten.

Liksom tidigare år var det största hotet i cybervärlden 2021 nätfiske (phishing) riktat till organisationernas e-postkonton med syfte att få kontroll över anställdas e-postanvändarnamn och -lösenord. Sibbo kommun har stegvis tagit i bruk bland annat en e-posttjänst som baserar sig på molnteknologi. Tjänsten har använts sedan år 2018, och antalet phishingförsök för att få tag i användarnamn var 2021 igen högre än åren innan. Fenomenet framkommer även på nationell nivå, bland annat i varningar som Cybersäkerhetscentret publicerar.

Även de så kallade bluffsamtalen fortsatte under år 2021. Syftet med dessa samtal är också att få kontroll över kommunanställdas användarnamn och lösenord. Stulna e-postanvändarnamn och -lösenord används oftast för att få ekonomisk nytta genom att följa med organisationens betalningsrörelser. Lyckat nätfiske medför varierande risker som är kopplade till anseende och reglering. Nätfiske leder nästan varje gång till att skyddet för personuppgifterna äventyras, vilket förutsätter att man anmäler en personuppgiftsincident. Om risken bedöms vara hög ska man även kontakta de berörda personerna.

Ett skadligt program som går under namnet FluBot spred sig omfattande i Finland 2021. Programmets mål var att korruptera SMS-meddelanden och upp till 70 000 skadliga meddelanden skickades till finländare varje dag. Även Sibbo kommuns telefoner mottog ett stort antal dylika meddelanden. Upprepade varningar publicerade på kommunens intranät fungerade relativt bra och enbart ett fåtal anställda öppnade meddelandena. IT-tjänster kunde förhindra att skadeprogrammet spreds.

Sibbo kommun ger kontinuerlig vägledning och kommunikation om farorna med nätfiske, så att anställda inte bara i den kommunala miljön utan även utanför arbetet kan skydda sina personuppgifter. Kommunen tog redan år 2020 i bruk ett multifaktorautentiseringssystem (MFA) med vilket det är möjligt att avsevärt minska sannolikheten för lyckat nätfiske.

Riskbedömningar har visat att den största risken fortfarande ligger hos slutanvändaren. Personuppgiftsincidenter beror mer ofta på ett mänskligt fel än på ett fel i apparater eller programvaror. Denna sårbarhet utnyttjas också av brottslingar. Som regel är brottslingarnas försök därför inriktade på anställda snarare än på potentiella sårbarheter i programvaran. Vid utveckling av datasäkerhet bör således utöver det tekniska kunnandet även processernas säkerhet och den mänskliga sårbarheten beaktas. Därför har kommunen särskilt satsat på att informera och utbilda personalen och att utarbeta anvisningar.

2.2.3 Riskhantering och hantering av informationssäkerhetsincidenter

IT-tjänster gör årligen en riskbedömning av den egna verksamheten. Då bedömer man även riskerna förknippade med datasäkerhet och dataskydd. En konsekvensbedömning görs alltid när man tar i bruk ny teknologi, behandlar uppgifter som gäller särskilda kategorier av personuppgifter på ett omfattande sätt (artikel 9 och 10 i EU:s allmänna dataskyddsförordning) samt i övriga situationer, då bedömningen görs enligt av tillsynsmyndigheten utfärdade anvisningar.

Förberedelser för att hantera informationssäkerhetsincidenter beskrivs i dokumentet Anvisning för hantering av datasäkerhetsincidenter. Alla informationssäkerhetsincidenter antecknas i systemet.

2.3 Kommunens anvisningar

Dataskydds- och datasäkerhetspolicyn kompletteras av datasäkerhetsanvisningar, datasäkerhetsregler för personalen, anvisningar för datasäkerhet och dataskydd samt av utbildningsmaterial. Personalen förbinder sig till sekretess när de skriver under arbetsavtalet. Alla anställda ska även skriva under en separat datasäkerhetsförbindelse. Förbindelsen undertecknas elektroniskt. Om den anställda inte skriver under datasäkerhetsförbindelsen låses användarkontot. Sibbo kommun tog redan år 2020 i bruk en ”Sekretess- och dataskyddsförbindelse”. Alla utomstående köptjänster så som konsulter och projektledare samt andra personer som har tillgång till Sibbo kommuns data och datasystem ska i fortsättningen skriva under en separat ”Sekretess- och dataskyddsförbindelse”.

2.4 Kommunens dataskyddsutbildningar

Uppföljning och utveckling av personalens kunnande utgör en viktig roll, eftersom det globalt uppskattas att 50 % av datasäkerhetsincidenterna orsakas av mänskliga fel. Antalet dylika incidenter kan effektivt dras ner med hjälp av utbildningar och genom att öka personalens medvetenhet om ämnet. Det har ordnats både allmänna och enhetsspecifika utbildningar om dataskydd och datasäkerhet för personalen. Utbildningarna har ordnats kostnadseffektivt i samarbete med KUUMA-kommunerna.

Kommunen tog också redan år 2018 i bruk en nätutbildning om dataskydd och datasäkerhet, som hela personalen samt förtroendevalda ska gå igenom. Utbildningen är obligatorisk för samtliga anställda och förtroendevalda. I samband med introduktionen i arbetet förutsätts att den anställda går utbildningen om datasäkerhet och dataskydd och undertecknar datasäkerhetsförbindelsen. Användarnamnet låses om den anställda eller den förtroendevalda inte avlägger utbildningen. Ett meddelande publiceras i Intra innan kontona låses och de anställda ges en möjlighet att ta hand om sin plikt.

Under 2021 undersöktes nya lösningar för personalutbildning. De tidigare, mycket omfattande utbildningarna har uppfattats som tunga och deras rapporteringsfunktioner har uppfattats som svaga. Dataskyddet och säkerhetsfrågorna förändras också hela tiden. Det konstaterades att det borde vara möjligt att ge personalen anvisningar som uppdateras under hela året och på sätt ersätta eller stödja individuell och omfattande utbildning. Ett annat krav i sökandet efter en ny lösning är förmågan att möjliggöra det som kallas mikrolärande, dvs. förmågan att koncentrera och bryta ner anvisningarna till kortfattade delar av information som många människor har lättare att tillgodogöra sig i sin hektiska vardag än att läsa långa handböcker eller titta på webbseminarier, som givetvis också kommer att fortsätta att erbjudas.

2.5 Kommunen deltar i Projektet JUDO

År 2019 genomfördes flera utvecklingsåtgärder gällande datasäkerhet. Myndigheten för digitalisering och befolkningsdata har ett utvecklingsprogram för den digitala säkerheten inom den offentliga förvaltningen, Projektet JUDO. Projektet utvecklar ledningen och förvaltningen av den offentliga förvaltningens digitala säkerhet, personalens kunskaper om digital säkerhet samt tillhandahåller stöd för att utveckla säkrare tjänster. Digital säkerhet omfattar fem delområden: riskhantering, verksamhetens kontinuitet och beredskap, datasäkerhet, cybersäkerhet och dataskydd. Projektet JUDO stöder den offentliga förvaltningen i utvecklandet av säkra och tillförlitliga tjänster under 2019–2021. Genom att delta i detta projekt för digital säkerhet får Sibbo kommun tillgång till moderna metoder, verktyg och modeller som stöd för att utveckla den digitala säkerhetens ledning och hantering.

2.6 Av vem erhålls personuppgifterna och till vem överförs de?

Personuppgifter om personalen, kommuninvånarna och personer som hör till olika intressentgrupper erhålls i huvudsak av den registrerade själv eller av olika myndigheter.

Personuppgifter kan överföras till kommuninterna tjänster; till exempel personuppgifter som behövs för hanteringen av arbetsavtalsförhållandet och de anställdas personuppgifter kan överföras mellan kommunens olika system. Personalens personuppgifter lämnas ut till andra personuppgiftsansvariga enbart med den registrerades samtycke eller med stöd av lagstiftningen.

Kommunen överför i princip inte personuppgifter utanför EU eller det Europeiska ekonomiska samarbetsområdet (EES), dock med undantag av vissa personuppgifter som är nödvändiga för tjänsternas genomförande (bl.a. användarnamn, e-postadress och namn). Personalens uppgifter är synliga på kommunens offentliga webbplats, som också är tillgänglig utanför EU-området.

En närmare beskrivning av överföring av personuppgifterna finns i dataskyddsbeskrivningarna, som är tillgängliga på Sibbo kommuns webbplats.

2.7 Webbtjänster och andra ICT-tjänster

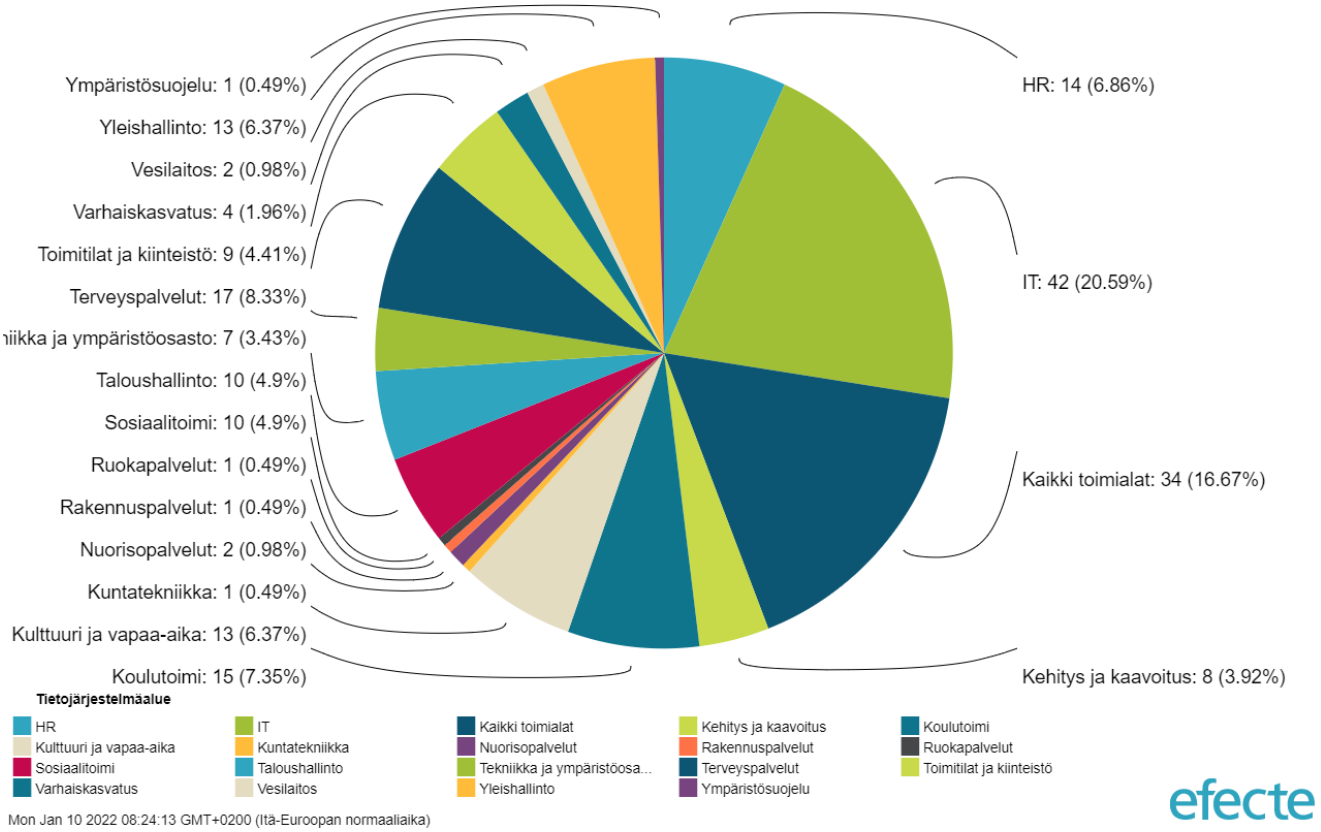
IT-enheten producerar infratjänster, kommunens gemensamma tjänster samt tjänster inom separata verksamhetsområden och/eller resultatenheter. Dessa tjänster är nödvändiga för kommunens verksamhet. Infratjänsterna består av följande helheter: tjänster för slutanvändare, datakommunikationstjänster, server- och kapacitettjänster samt användarförvaltning. Gemensamma tjänster samt tjänster inom separata verksamhetsområden består av applikationer och system.

Datasystem har skaffats från olika leverantörer och i olika tider, vilket gör att de inte bildar en arkitektoniskt enhetlig helhet. De datasystem som används i Sibbo klassificeras enligt systemets effekt och kravnivå. I klassificeringen är kriterierna som påverkar systemets effekter direkt kopplade till kritiskheten av kommunens olika processer.

Systemets kritiskhet:

Kritisk: Serviceverksamheten skadas betydligt eller hindras i sin helhet om systemet inte fungerar
Viktig: Serviceverksamheten skadas om systemet inte fungerar
Nyttig: Serviceverksamheten skadas något om systemet inte fungerar
Liten: Hjälp- eller stödsystem som effektiverar arbetet. Verksamheten skadas inte nämnvärt om systemet inte fungerar.

Datasystem har delats i olika kritiskhetsklasser, som dock varken är i korrelation med behandlingens omfattning eller antalet och kvaliteten av personuppgifter i systemet. Angående behandling av personuppgifter är klassen riktgivande och den beskriver datasystemens relation med processernas kritiskhet med tanke på kontinuitetskontrollen.



Karta över datasystem 2021

Datasystem i anknytning till respektive register definieras i registrets dataskyddsbeskrivning. Registret bildas av de informationshelheter och datareservrar, vilka behandlas på ett sätt som definieras i dataskyddsbeskrivningen. Registret är oberoende av teknologi, och det kan bestå av flera datareservrar. Till exempel kan ett register som innehåller uppgifter om personalen bestå av personaltjänsternas databas, arbetsavtal i pappersarkiv och, till exempel, interna arbetsskiftslistor. Det som är avgörande är att registrets uppgifter är organiserade och att uppgifterna behandlas i registrets olika former på ett enhetligt, i dataskyddsbeskrivningen definierat sätt.

Kommunen har lagt ut en stor del av sin serviceproduktion på entreprenad. Samtidigt har man också börjat utnyttja molnteknologi i allt större grad. Riskhanteringen får en ännu större betydelse speciellt då man övergår till att använda molntjänster.

2.8 Anskaffningar och dataskydd i avtal

Avtal som Sibbo kommun ingår med sina avtalsleverantörer är formbundna. I dem tas helheter i anknytning till datasäkerhet, dataskydd och kontinuitetskontroll i beaktande. Avtalsvillkor och bilagor preciseras vid behov beroende på den producerade tjänstens kvalitet, kritiskhet och värde.

Vid upphandlingar använder man allmänna, vid tidpunkten gällande krav som tillämpar den offentliga förvaltningen. Ett separat säkerhetsavtal förutsätts om leverantören behandlar kommunens sekretessbelagda information. Om leverantören behandlar personuppgifter å kommunens räkning eller å kommunens vägnar ska det i avtalet bifogas specialvillkor som grundar sig på EU:s allmänna dataskyddsförordning, dvs. den av Kommunförbundet rekommenderade bilagan för behandling av personuppgifter.

Leverantörernas avtalshandlingar granskas för att säkerställa att de innehåller tillräcklig information om datasäkerhet och dataskydd ur kommunens perspektiv.

Dataskyddsförordningen förutsätter att parterna ingår avtal om behandling av personuppgifter respektive upprättar någon annan handling med rättslig verkan som personuppgiftsbiträdet förbinder sig till. En ny anvisning om avtalshantering färdigställdes 2021 och under året såg man till att alla kontrakt uppdaterades för att överensstämma med gällande lagstiftning.

Sibbo kommun ansökte om och beviljades stöd för det digitala SaaSec-projektet av Finansministeriet hösten 2021. Andra KUUMA-kommuner anslöt sig också till projektet. Projektet går ut på att utveckla ett koncept och avtalsriktlinjer för upphandling och livscykel för SaaS-tjänster. På detta sätt har kommunerna i framtiden ett standardiserat sätt att garantera avtalens säkerhet och dataskydd inklusive revisioner. Under perioden 2021–2023 kommer projektet också att delta i gemensamma säkerhetsrelaterade projekt som samordnas av ministeriet.

2.9 Dokumenthantering och arkiv

Organisationer ska enligt lagen vara medvetna om vilka uppgifter de förvaltar över. För att uppfylla principerna av rättskydd och offentlighet ska organisationen beskriva vilka uppgifter den förvaltar över och hurdana principer den tillämpar i behandlingen av uppgifterna. Med en övergripande planering av informationshantering kan man säkerställa informationens användbarhet, integritet och kvalitet samt dataskyddet. Informationshanteringen genomförs med hjälp av en informationsstyrningsplan (ISP) och en informationshanteringsmodell samt med beskrivning av och anvisningar för dokumentförvaltning och arkivering.

Informationshanteringslagen ålägger offentliga myndigheter skyldigheter när det gäller beskrivningar, elektronisk arkivering samt tillgång till och användbarhet av uppgifter. Kommunen har arkiveringsskyldighet och den följer vissa lagenliga bestämmelser om informationsutbyte, vilket dock gör att det i kommunen fortfarande behandlas mycket information i pappersform. Kommunen övergår till elektronisk behandling av klientuppgifter i takt med att digitala lösningar utvecklas och godkänns med tanke på utförande av lagstadgade uppgifter. De ska också passa in i kommunens helhetsarkitektur. Det finns också fortfarande arbete att göra för att modernisera informationshanteringspraxisen och bryta med gamla vanor.

Som registeransvarig ser kommunen till att all information som behandlas är ändamålsenligt skyddad, både när det är fråga om datasystem och arkiv i pappersform. Lagrade uppgifter och användarrättigheter för servrar samt andra uppgifter som är avgörande för personuppgifternas säkerhet behandlas konfidentiellt och enbart av arbetstagare i vars arbetsbeskrivning det ingår.

Kommunen har utfört en intern utvärdering i vilken det konstateras att det finns behov av att utveckla arkiveringen. Målet med dokumenthanteringen är att avdelningarna får anvisningar om hur material ska hanteras och arkiveras och att anvisningarna uppdateras mer regelbundet än förr. Informationsavbrott, bristen på resurser för och grundläggande kunskaper i arkivering samt försämrad arkiveringspraxis som redan varit vardag för en längre tid på många avdelningar i kommunens organisation orsakar problem. Många avdelningar visar dock ett växande intresse för arkiveringsfrågor och arbetar för att förbättra sina rutiner.

Att tillämpa aktuella och fungerande praxis inom dokumenthantering och arkivering som en systematisk del av avdelningarnas vardag är ett långsiktigt mål. År 2021 har huvudfokus för avdelningarnas riktlinjer för arkivering legat på Social- och hälsovårdsavdelningen, där riktlinjerna har mottagits väl och många praktiska förbättringar har genomförts för att tillgodose de grundläggande arkiveringsbehoven.

Sibbo kommuns social- och hälsovårdstjänster överförs till Östra Nylands välfärdsområde från och med 2023. När det gäller informationshantering och arkivering inom social- och hälsovårdstjänster inleddes förberedelserna för övergången till välfärdsområdet hösten 2021.

Dokumentförvaltningen samarbetar kontinuerligt med IT-tjänster för att uppnå informationshanteringens övergripande mål. De viktigaste samarbetsområdena år 2021 var utvecklingen av en modell för informationshantering, förberedelser för elektronisk arkivering och digitalisering samt dataskyddsfrågor.

När kommunförvaltningen flyttade till nya lokaler 2020 rengjordes och flyttades en del av det gallrade närarkivmaterialet till det nya verksamhetsstället. Slutarkivet samt en del av det gamla närarkivmaterialet är dock fortfarande i de gamla lokalerna, där de väntar på att bli gallrade och eventuellt även digitaliserade. År 2021 fortsatte avdelningarna att gallra sina uppgifter i sina gamla verksamhetslokaler.

Det är viktigt att förbereda sig för att digitalisera materialet i så stor skala som möjligt, eftersom den årliga ökningen av mängden pappersmaterial som lagras permanent är konstant, men kommunen investerar för närvarande inte i byggandet av nya arkivlokaler. Man bör dock komma ihåg att en del av det viktigaste arkivmaterialet även i fortsättningen kommer att bevaras också i pappersform på grund av dess kulturella och historiska värde. Digitalisering i syfte att förstöra pappersversioner av materialet i slutarkivet kräver för tillfället ett förhandsgranskningsbeslut av Riksarkivet i enlighet med gällande bestämmelser. Ett förslag till gallring lämnades in till Riksarkivet hösten 2021 för en del av det material som nu finns i Sibbo kommuns slutarkiv och ett gallringsbeslut väntas under 2022.

Ett av de viktigaste besluten under 2021 när det gäller utvecklingen av arkiveringen var beslutet att köpa ett elektroniskt arkiv som möjliggör exklusiv elektronisk arkivering av permanent lagrat material inom kommunens alla verksamhetsområden. Det exakta datumet för införandet av det elektroniska arkivet är dock ännu inte känt.

Sibbo kommun tog 1.1.2021 i bruk en informationsstyrningsplan (ISP) som beskriver processernas nuvarande tillstånd och uppfyller SÄHKE2-kraven. Planen infördes i samband med att kommunen tog i bruk den nyaste versionen av ärendehanteringssystemet, Dynasty10. I och med att informationsstyrningsplanen togs i bruk upphävdes Sibbo kommuns arkivbildningsplaner (ABP), som i flera delar redan var föråldrade eller ofullständiga.

Informationsstyrningsplanen styr processerna i ärendehanteringssystemets bakgrund samt ger aktuella anvisningar i frågor som rör dokumentens förvaringstider och sekretess. Informationsstyrningsplanen är också en förutsättning för att kommunen kan ta i bruk elektronisk arkivering.

Införandet av informationshanteringsplanen och Dynasty10-versionen av ärendehanteringssystemet har tagit lite tid att vänja sig vid i organisationen, men har medfört positiva förändringar. Tack vare funktionaliteten i den nya versionen av ärendehanteringssystemet och den reviderade klassificeringen av uppgifter är organisationens ärendehantering nu mer strukturerad, informationen är lättare att hitta och det finns en större medvetenhet om offentlighets- och sekretessfrågor.

Informationsstyrningsplanen uppdateras kontinuerligt, dvs. avdelningarna meddelar dokumenthanteringen om eventuella uppdateringsbehov. Planen uppdaterades flera gånger särskilt i början av 2021. I framtiden kommer informationsstyrningsplanen att uppdateras ytterligare i enlighet med avdelningarnas behov. Arbetet med att utarbeta en beskrivning av handlingars offentlighet inleddes 2021. Målet är att beskrivningen av handlingars offentlighet färdigställs 2022.

3 Lagstiftning som påverkar databehandlingen

Sibbo kommun har i enlighet med personuppgiftslagen upprättat registerbeskrivningar om kommunens samtliga personuppgiftsregister. Registren har varierande användningsändamål. Dataskyddsförordningen kräver inte att kommunen upprättar beskrivningar per respektive register, utan att det upprättas en beskrivning om den personuppgiftsansvariges register över behandling samt att informationen om behandlingen av personuppgifter är transparent.

Därutöver har kommunen utarbetat ett register över behandling enligt artikel 30 i dataskyddsförordningen. Beskrivningar om behandling av personuppgifter har också publicerats/publiceras på kommunens webbsida.

Personuppgiftsbehandlingen styrs av bland annat följande dokument:

- Dataskydds- och datasäkerhetspolicy
- Riskhanteringspolicy
- Regler och anvisningar för datasäkerhet
- Dokumentmallar för dataskyddsbeskrivningar
- Anvisningar och dokumentmallar för konsekvensbedömningar
- Anvisningar och blanketter för begäran om uppgifter
- Personalmeddelanden och anvisningar i Intra

Central lagstiftning som styr personuppgiftsbehandlingen i kommunen:

- Lag om informationshantering inom den offentliga förvaltningen 906/2019
- Kommunallag (410/2015)
- Förvaltningslag (434/2003)
- EU:s allmänna dataskyddsförordning (EU 2016/679)
- Dataskyddslag (1050/2018)
- Lag om integritetsskydd i arbetslivet (759/2004)
- Lag om tjänster inom elektronisk kommunikation (917/2014)
- Lag om ändring av informationssamhällsbalken (68/2018)
- Lag om informationshantering inom den offentliga förvaltningen (906/2019)
- Lag om offentlighet i myndigheternas verksamhet (621/1999)
- Arkivlag (831/1994)

- Lag om offentlig upphandling och koncession (1397/2016)
- Bokföringslag (1336/1997)
- Arbetsavtalslag (55/2001)
- Arbetarskyddslag (738/2002)
- Diskrimineringslag (1325/2014)
- Lag om jämställdhet mellan kvinnor och män (609/1986)
- samt särskilda lagar för respektive verksamhetsområde

Det här kapitlet beskriver hur Sibbo kommun följer dataskyddsprinciperna laglighet, korrekthet och öppenhet i sin verksamhet.

4 Den registrerades rättigheter och hur de tillgodoses

Sibbo kommun samlar in och behandlar sina kunders personuppgifter enbart i den mån som det är nödvändigt för att producera respektive tjänst. Personuppgifter behandlas enligt registrets användningsändamål. Dataskyddsbeskrivningar som krävs enligt EU:s allmänna dataskyddsförordning har utarbetats av samtliga register. Kunden har rätt att veta vilka uppgifter om honom eller henne samlas in. Om det uppstår fel i uppgifterna eller om de är inkorrekta kan kunden kräva att felen rättas till.

Om uppgifterna samlas in med den registrerades samtycke kan kunden när som helst återkalla sitt samtycke och kräva att hans eller hennes uppgifter raderas. Största delen av kommunens verksamhet bygger dock på fullgörande av en rättslig förpliktelse, för att tillgodose ett allmänt intresse eller som ett led i avdelningens myndighetsutövning (ofta bland annat arkivering, statistik, utvecklingsprojekt). Kunden kan i dessa fall inte kräva att hans eller hennes uppgifter raderas.

Sibbo kommun strävar efter att följa principerna om öppenhet och korrekthet enligt förordningen (allmän dataskyddsförordning, artikel 5). För att uppfylla informationsplikten använder man fortfarande dataskyddsbeskrivningar. Godkända och aktuella dataskyddsbeskrivningar finns på kommunens webbplats (allmän dataskyddsförordning, artikel 13 och 14).

Sibbo kommun har öppnat en specifik sida om Dataskydd på sin webbplats för att informera de registrerade. På webbsidan finns blanketter för begäran om insyn respektive begäran om rättelse av registeruppgift, som baserar sig på de registrerades rättigheter (allmän dataskyddsförordning, artikel 15, 16).

En personuppgiftsincident ska inom 72 timmar anmälas till tillsynsmyndigheten om incidenten kan äventyra fysiska personers rättigheter och friheter. År 2020 var man tvungen att göra två (2) anmälningar om personuppgiftsincidenter till tillsynsmyndigheten.

En personuppgiftsincident ska utan oskäligt dröjsmål anmälas till den registrerade, om den sannolikt orsakar en hög risk för en fysisk persons rättigheter och friheter. Datasäkerhetsteamet bedömer huruvida man ska göra anmälan av en personuppgiftsincident (artikel 33). Den dataskyddsansvarige tar kontakt med de registrerade antingen per brev eller per telefon. Om personuppgiftsincidenten berör ett stort antal registrerade ska även ett meddelande om incidenten publiceras på kommunens webbplats.

5 Uppföljning och mätning

Datasäkerheten och dataskyddet samt IT-miljön år 2021 kan beskrivas med följande nyckeltal:

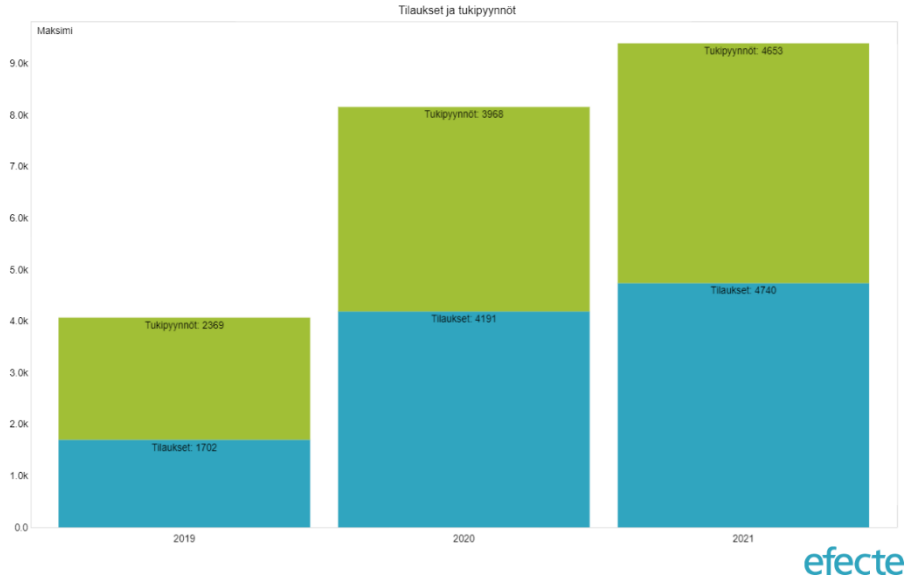


Bild 1 Beställningar och servicebegäranden

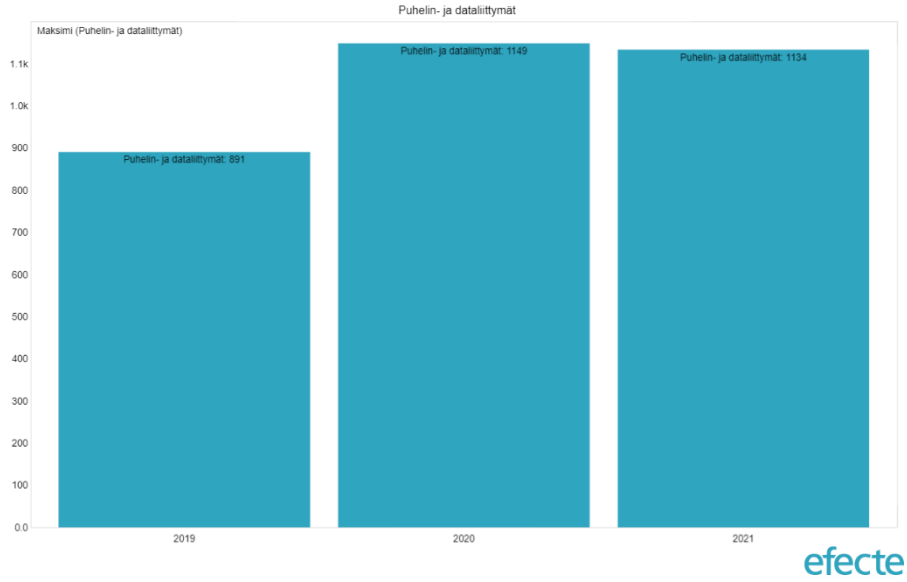


Bild 2 Telefonabonnemang och dataförbindelser

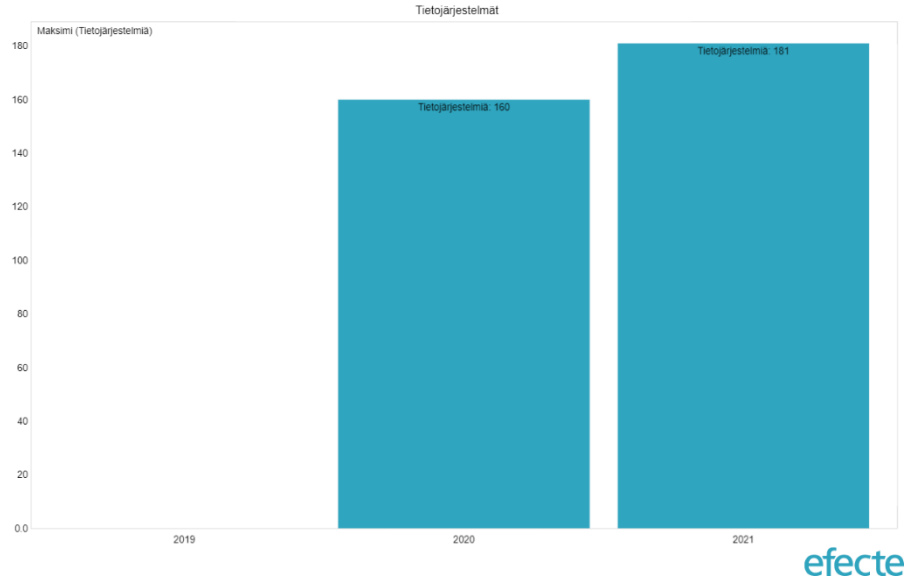


Bild 3 Datasystem

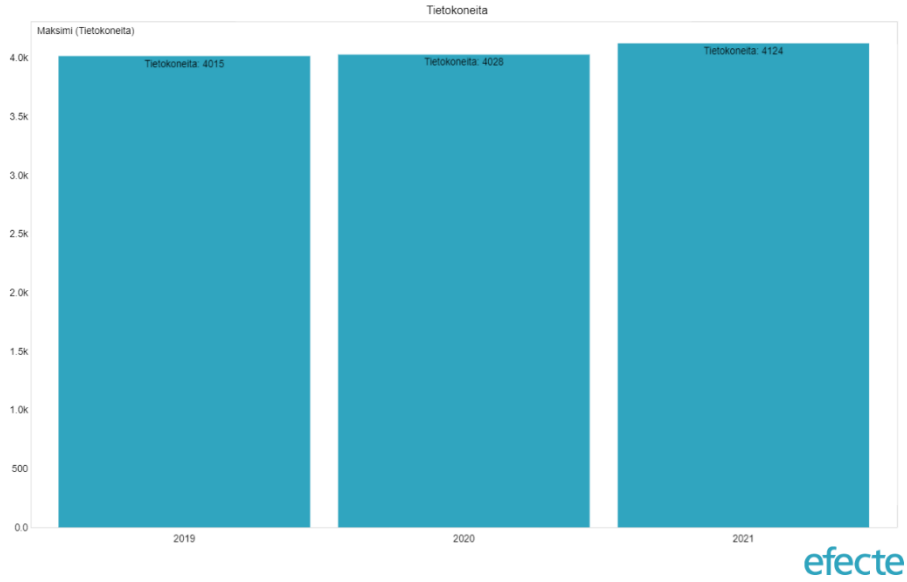


Bild 4 Antal datorer inklusive studerandenas datorer

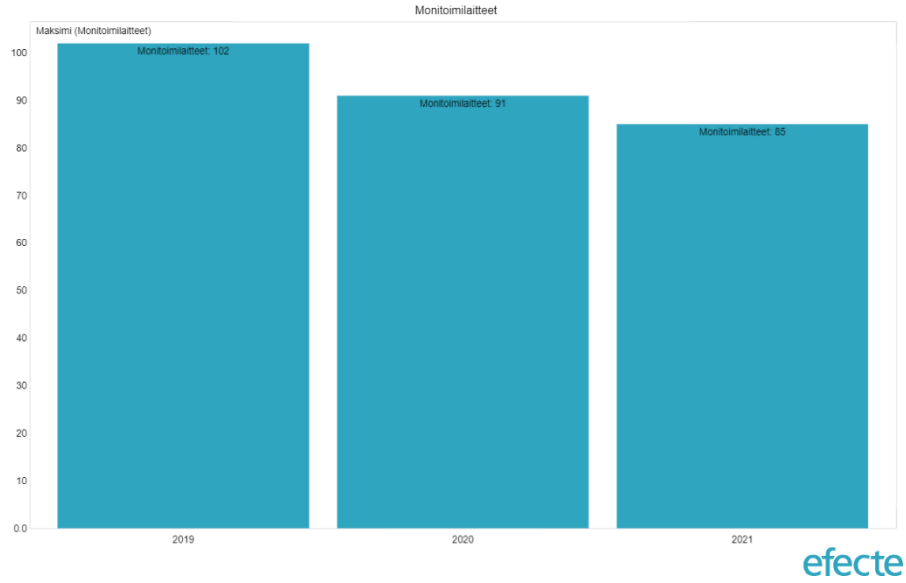


Bild 5 Multifunktionsapparater

Begäran om insyn, rättelse eller radering av uppgifter på grund av den allmänna dataskyddsförordningen:

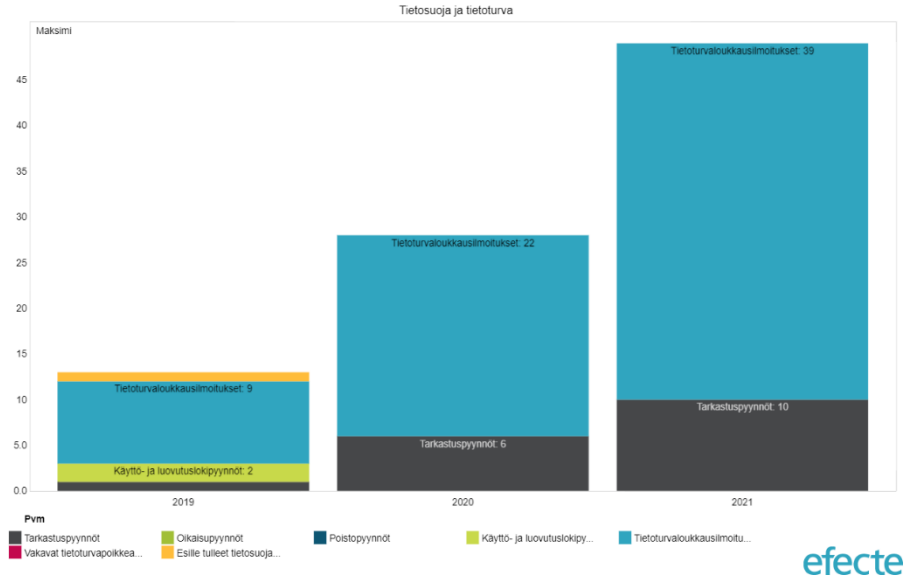


Bild 6 Dataskydd och datasäkerhet

År 2021 (bild 6)
Anmälan av personuppgiftsincidenter 40 st.
Dataskyddsincidenter: 4 st.
Allvarliga informationssäkerhetsincidenter: 0 st.
Framkomna bekräftade eller misstänkta datasekretessförbrytelser: 0 st.

Utförda utbildningar:

Webbutbildning för hela personalen, genomgått av cirka 95 % av personalen
Tilläggsutbildning för chefer, genomfört av cirka 90 % av cheferna
Dataskyddsutbildningar för personalen: 4 st.

6 Identifierade utvecklingsobjekt och blick på framtiden

EU:s allmänna dataskyddsförordning har tagits emot på ett förtjänstfullt sätt. Organisationen strävar efter att svara på de utmaningar som förordningen för med sig, men det finns saker att utveckla i flera delområden.
Det styrande dokumentet är dataskyddspolicyn och datasäkerheten som nämndes ovan.

Självbedömningen visar att efterlevnaden av förordningen på många områden igen har förbättrats jämfört med tidigare år, men att det fortfarande finns utrymme för förbättringar.

Gruppen för informationssäkerhet och dataskydd kommer att samordna utvecklingen i framtiden.

6.1 Rekonstruktion av datasäkerhets- och dataskyddsgruppen

Sibbo kommun hade tidigare en dataskyddsansvarig som arbetade på heltid och en datasäkerhetsansvarig som arbetade på deltid. Tillsammans bildade de kommunens Datasäkerhetsteam. Kommunens datasäkerhetsansvarig sade upp sig på sommaren och kommunens dataskyddsansvarig i oktober. I oktober beslutade kommundirektören och CDO att köpa dataskyddsansvariges tjänster av Privaon Oy, så att kommunen inte hamnar i en situation där det inte finns någon dataskyddsansvarig alls. CDO inledde rekryteringsprocessen för en ny dataskyddsansvarig i slutet av december.

I november inrättade kommundirektören en ny datasäkerhets- och dataskyddsgrupp som består av medlemmar som representerar kommunens olika verksamhetsområden. Medlemmarna utsågs av ledningsgruppen. Gruppen hann dock inte sammanträda i november–december. Datasäkerhets- och dataskyddsgruppens uppgift är att följa med hur dataskyddet genomförs och att ge utvecklingsförslag samt erbjuda stöd till dataskyddsansvariga och systemadministratörer inom olika verksamhetsområden. Gruppen ska med sex månaders mellanrum rapportera till kommunens ledningsgrupp om hur datasäkerheten och dataskyddet genomförs.

Expertis för att säkerställa och förbättra den tekniska säkerheten kommer att förvärvas genom Tiera.

6.2 Svar på kraven i den nya lagstiftningen

Informationshanteringslagen trädde i kraft 1.1.2020. I lagen föreskrivs bland annat om den offentliga förvaltningens allmänna förpliktelser när det gäller informationshantering och användning av datasystem, om den allmänna styrningen av informationshanteringen inom den offentliga förvaltningen, om skapande av och elektroniskt utlämnande av informationsmaterial, om de grundläggande kraven på informationssäkerhet inom den offentliga förvaltningen, om utnyttjande av tekniska gränssnitt samt om ärendehantering och förvaring av informationsmaterial. Det betydelsefulla med tanke på kommunsektorn är att syftet med lagen är att upphäva statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010), vilket betyder att kraven på datasäkerhet i fortsättningen grundar sig på informationshanteringslagen och förpliktar kommunaktörerna.

Dokumentationen i enlighet med informationshanteringslagen inleddes 2021. Dokumentationen har varit splittrad, vilket har gjort det omöjligt att sammanställa en modell för informationshantering i kommunen. I februari 2022 kommer man att införa en ny digital modell för säkerhet, Digiturvamalli (www.digiturvamalli.fi) för att göra det möjligt för alla verksamhetsområden att beskriva de enheter som krävs enligt informationshanteringslagen med hjälp av ett enkelt Teams-användargränssnitt. När miniminivån av beskrivningar har importerats till modellen kan informationshanteringsmodellen automatiskt laddas ner från tjänsten.

Den digitala säkerhetsmodellen kommer i framtiden att innehålla inte bara informationshanteringsmodellen utan också GDPR-kompatibel dokumentation som även kan publiceras på webbplatsen www.sibbo.fi. Den digitala säkerhetsmodellen kan också användas för att publicera nyheter och vägledning för personalen om informationshanteringsmodellen, GDPR-frågor och allmän informationssäkerhet och dataskydd.

Kommunen kartlade 2021 de SIEM-system (Security Information and Event Management) som finns på marknaden. Efter kartläggningen definierades de uppgifter som överförs till det centraliserade dataloggningssystemet i enlighet med kommunens loggningspolicy. SIEM-systemet och det tillhörande SOC (Security Operations Center) har köpts som en tjänst och tillhandahålls kommunen av Insta Defsec. SIEM övervakar organisationens informationssystem och nätverk och larmar när det upptäcker onormal aktivitet. Instas SOC-tjänst skyddar kritiska IT-system genom att identifiera attacker och andra hot som är svåra att avvärja. När eventuella avvikelser identifieras så tidigt som möjligt kan de åtgärdas snabbt, vilket minimerar skadan.

Systemet för identitets- och åtkomsthantering (Efecte IGA) togs i bruk 2021. Hanteringen av anställdas användarnamn och tillhörande åtkomsträttigheter kan nu genomföras i enlighet med de krav som ställs i informationshanteringslagen. Användarnamnens giltighet har säkerställts genom att koppla deras giltighet till de anställdas arbetsavtal. I IGA-systemet beviljas åtkomsträttigheter i enlighet med den anställdas arbetsuppgifter, antingen genom personens arbetsroll eller genom att beställa rättigheten separat. Även om det har funnits mycket motstånd mot förändringen börjar personalen förstå att syftet med identitets- och åtkomsthantering inte är att trakassera personalen eller minska IT-tjänsters arbetsbörda, utan att tillhandahålla ett nytt arbetssätt som krävs enligt lag och som kommer att öka IT-tjänsters och även Personaltjänsters arbetsbörda. Ett annat alternativ att sköta åtkomsthanteringen enligt lagen hade varit att varje avdelning manuellt skulle ha fört ett register och en logg över åtkomsträttigheter för varje anställd och system. Detta skulle dock ha tagit tio gånger så lång tid på hela kommunens nivå och processen skulle förmodligen aldrig ha nått den nivå som lagen kräver.

Sommaren 2021 installerades en ny brandvägg i kommunen och den gamla brandväggen togs ur bruk. När utrustningen var installerad tog det inte länge att definiera brandväggsinställningarna. Under hösten konfigurerades nya filter i brandväggen för att blockera åtkomsten från Sibbo kommuns nätverk till skadliga webbplatser på Internet. Tillgången till webbplatser med innehåll som är olagligt i Finland, t.ex. barnpornografi, sexhandel och droger, har blockerats helt och hållet. Brandväggen varnar användaren för webbplatser som inte är direkt olagliga, men som till exempel innehåller skadliga program, sex eller våld.

Utbildningsanordnare måste ta hänsyn till ett antal riktlinjer och bestämmelser bland annat om användning av personuppgifter, publicitet och personlig integritet. År 2021 införde Sibbo dataskyddstjänsten Luuppi för att hantera dataskyddet inom bildningsväsendet. Cloudpoint Oy:s dataskyddsexperter använder tjänsten för att kontrollera att de digitala tjänster som läroanstalterna använder uppfyller de gällande dataskyddsbestämmelserna och lagen om grundläggande utbildning. Tjänsten säkerställer att det inte finns några digitala tjänster med reklam eller annat olämpligt innehåll i undervisningen. Efter den första granskningen av tjänsterna kommer Luuppi att fortsätta att övervaka dataskyddet i de tjänster som utbildningsanordnaren använder, eftersom sekretessinställningarna för tjänsterna kan ändras.

Suomi.fi-identifieringen blev i fjol betydligt vanligare i olika myndighetssystem. År 2021 beslutade Sibbo kommun att betala för DVV-organisationskort för kommunanställda som regelbundet måste identifiera sig för olika tjänster i sitt arbete. Organisationskorten erbjuder också en möjlighet till elektronisk underskrift som uppfyller kraven enligt det som föreskrivs på den högsta nivån i EU:s eIDAS-förordning. Traficom ansvarar för en förteckning över leverantörer av betrodda tjänster, och Myndigheten för digitalisering och befolkningsdata hör till dem. Förutom organisationskortet infördes även mobilcertifikat i samband med bytet av operatör. Anställda som använder ett kommunalt telefonabonnemang även för personligt bruk har möjlighet att ta i bruk ett mobilcertifikat, som kan användas för autentisering i stället för personliga bankkoder. Användningen av mobilcertifikatet är gratis för den anställda. Att ta i bruk mobilcertifikatet förutsätter stark autentisering, men därefter behöver man bara telefonen för att använda certifikatet. Tack vare organisationskorten och mobilcertifikaten kan de anställda logga in till externa tjänster med stark autentisering.

6.3 Utveckling av övningsverksamheten

Genom övningar lär man sig att agera på ett säkrare och tryggare sätt. Det är effektivt att använda övningsverksamhet (till exempel TAISTO-övningar) för att utveckla personalens kunnande. Samtidigt säkerställs kontinuitetskontrollen. Därför är det motiverat att utveckla kommunens övningsverksamhet under den kommande rapporteringsperioden. Detta kräver både budgetering och personalresurser. För att få även våra tjänsteleverantörer att delta i övningsverksamheten ska man kräva att de förbinder sig till detta redan vid upphandlingsskedet eller när man ingår avtal med olika parter. Det är nödvändigt att planera övningsverksamheten på lång sikt för att säkerställa kontinuiteten i organisationens verksamhet.

6.4 Kontinuitetskontrollen

Med kontinuitetskontrollen avses en verksamhetsmodell med vilken en organisation bygger sin beredskap och sin förmåga att sköta de mest centrala uppgifterna oberoende av situation. Kontinuitetskontrollen är en process med vilken man identifierar riskerna för verksamheten och deras konsekvenser samt bygger upp en omfattande modell för hanteringen av verksamhetsförmågan. Kontinuitetskontrollen består av krishantering, planer för kontinuitet och återhämtning.

Kontinuitetskontrollen kan också beskrivas med följande åtgärder:
– Identifiera hot, risker, störningar och bundenheter i verksamheten.
– Bedöma hur olika hot kan påverka organisationen och dess aktörsnät.
– Organisera och genomföra praxis för störningssituationer.
– Säkerställa att kritiska partner behåller sin verksamhetsförmåga i en störningssituation.
– Skydda intressen för organisationens kärnverksamhet samt dess värdeproduktionsförmåga.

Kommunen ska kunna sköta sina kritiska funktioner och skydda invånarnas välmående oberoende av störningar, hot eller risker i den externa eller interna verksamhetsmiljön. I Sibbo styrs kontinuitetskontrollen utifrån kärnverksamheten och sådana processer som kan påverka kundernas hälsa och välmående. Det är inte ändamålsenligt att tillämpa kontinuitetskontrollen på alla nivåer, men också under den kommande rapportperioden ska man satsa på avtal och använda dem för att säkerställa att kontinuitetskontrollen beaktas. Världen förändras och digitaliseras kontinuerligt, vilket gör att kontinuitetskontrollen hela tiden är som sagt ”på tapeten”.

6.5 Dataskyddet blir ännu viktigare

Dataskyddet får en större betydelse i och med att världen kontinuerligt digitaliseras och nya nätverk skapas. Med digitalisering ökar också behovet av att utnyttja personuppgifter på en bredare skala. Informationsteknologi och digitalisering är ett centralt sätt att påverka hur man behandlar personuppgifter samt hur varje individ och organisation borde förhålla sig till det i sin egen verksamhet. Vi är nästan varje dag tvungna att fatta beslut om var vi ger eller inte ger uppgifter om oss själva. I dagens läge kan personuppgifter användas som betalningsmedel. Därför ska de hanteras lika varsamt som pengar. Personuppgifter används som betalningsmedel på webben. Olika aktörer säljer och köper dem.

Lagstiftningen behövs för att trygga individernas rättigheter och friheter. När man behandlar personuppgifter och planerar nya funktioner ska man alltid se till att inte äventyra individernas rättigheter, friheter och rättsskydd. På så sätt skapar man även tillit mellan kommunen och kommuninvånarna. Kommuninvånarna ska kunna lita på att deras personuppgifter behandlas på ett lagenligt och datasäkert sätt. Tillgång till personuppgifter ges enbart personer som behöver dem för att genomföra sina arbetsuppgifter.

Det är nödvändigt att ledningen starkt förbinder sig till att utveckla och förbättra behandlingen av personuppgifter. Resursfördelningen kommer att ha en stor roll. I en värld som ständigt förändras och digitaliseras ska till exempel utbildningar som riktas till hela personalen kontinuerligt utvecklas.

I Sibbo kommun har man fäst mer och mer uppmärksamhet vid behandlingen och förvaltningen av personuppgifter. Databokslutet redogör för nuläget av personuppgiftsbehandlingen och utgör en bra grund för utarbetningen av en ännu bättre behandling av personuppgifter i Sibbo.

Kunderna är alltmer medvetna om sina rättigheter när det gäller behandlingen av deras uppgifter. Kommunen har åtagit sig att se till att vi fortsätter att svara på förfrågningar om information och frågor om kundernas dataskydd så snabbt som möjligt och med högsta möjliga kvalitet.