Databokslut 2020

Sibbo kommun

31.5.2021

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 förtroende 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.

Efter 2018 har man börjat satsa betydligt mer på utveckling av datasäkerhet och dataskydd. Under de gångna tre åren han man bland annat utarbetat kartläggningar av personuppgiftsmaterial, utarbetat och uppdaterat anvisningar för datasäkerhet och dataskydd samt ordnat flera dataskyddsutbildningar för personalen. Genom att utnyttja digitalisering och data på ett säkert sätt har man som mål att bygga kundorienterade, pålitliga och kostnadseffektiva tjänster för kommuninvånarna. Allt detta förutsätter att man tar hand om dataskydd och datasäkerhet tillräckligt bra. Principerna för datasäkerhet och dataskydd ska alltså konkretiseras och de ska bli en del av organisationens verksamhet.

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 systemen säkerhetskopieras regelbundet.

Användarrättigheterna i 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. För tillfället hanteras användarrättigheterna inte centraliserat i kommunen. Målet är att IT-tjänster hanterar användarrättigheterna centraliserat. En teknisk plattform för hantering av användarrättigheterna anskaffades 2020 och den tas i bruk under våren 2021. I samband med projektet 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 för hantering av datasäkerhetsincidenter har utarbetats. 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 Datasäkerhetsteamet behandlar dem enligt en bestämd process. På detta sätt kan åtgärderna planeras, koordineras och dokumenteras på ett enhetligt och kompetent sätt.

En del av kommunens anställda började på våren arbeta på distans 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 har publicerat 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.

Cyberbrottsligheten har tagit vara på chanserna som coronaepidemin möjliggör. Cyberbrottslingarna har redan utnyttjat ändringarna i organisationernas verksamhetsmodeller och börjat sprida skadegörande program och samla in konfidentiella uppgifter med hjälp av nätfiske. Som resultat kan företagen stå inför informationssäkerhetsincidenter som måste rapporteras till dataskydds- eller andra myndigheter och som kan innebära stor förödelse för verksamheten. Därför är det viktigt att det i kommunen har utarbetats anvisningar och instruktioner för eventuella cybersäkerhetsincidenter. Kommunen utvecklar detta arbete kontinuerligt.

Den mest betydande hotbilden i cybervärlden var också år 2020 nätfiske (phishing) riktat till e-postkonton med syfte att få kontroll av kommunanställdas 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 2020 betydligt högre än året innan. Fenomenet framkommer även på nationell nivå, bland annat i varningar som Cybersäkerhetscentret publicerar. Nätfiske på olika nivåer riktat till e-postkonton kan uppskattas ha varit det största enskilda hotet mot kommunen år 2020.

Också antalet så kallade bluffsamtal ökade år 2020. 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.

Nätfiskekampanjer får hela tiden nya former och nätfisket görs smartare, vilket också gör det svårare att försvara sig mot det. Personalens medvetenhet om nätfiske och riskerna förknippade med det ökades år 2020 med hjälp av utbildningar och anvisningar, och information om fenomenet publicerades upprepade gånger på kommunens Intranät. Kommunen tog 15.4.2020 i bruk ett multifaktorautentiseringssystem (MFA) med vilket det är möjligt att avsevärt minska sannolikheten för lyckat nätfiske.

Beträffande riskerna har kommunen uppskattat att slutanvändarna utgör den största risken. Personuppgiftsincidenter beror oftare på mänskliga fel än på fel som görs av datorer. Med andra ord utnyttjar förbrytaren oftast mänsklig sårbarhet. Incidenter kan också bero på ett mänskligt fel som uppstår antingen i processen eller som ett fel som en enskild anställd gör när hen utför sina arbetsuppgifter. Vid utveckling av datasäkerhet bör 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. Datasäkerhetsteamet gör även vid behov besök i arbetsenheterna.

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 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”.

Datasäkerhetsteamet har år 2020 upprättat eller förnyat följande dokument som kommunen använder:

Anvisningar:

- Tietoturva etätyössä / Datasäkerhet i distansjobb
- Turvallisuusopas uusi normaali COVID19 jälkeen / Säkerhetsopus Livet efter COVID19
- Tunnista kalasteluansa (på finska)
- Selaustietojen poisto (på finska)
- Conditional Access ja MFA (på finska)
- Tiedossa olevat ongelmat ja ratkaisut (MFA) (på finska)
- Miten otan O365 salasanapalvelun käyttööni / Hur jag tar O365 lösenordtjänsten ibruk
- Miten vaihdan salasanan itse / Hur byter jag själv mitt lösenord
- Sopimukset henkilötiedot ja EUn tietosuoja-asetus (på finska)
- Discord (på finska)
- Outlook Appin sähköpostin allekirjoituksen määrittäminen (Android) (på finska)
- Tietoturva Perusteet Wistec (på finska)

Blankett:

- Sekretess- och datasekretessförbindelse för tredje parter

På grund av covid-19-pandemin har Datasäkerhetsteamet publicerat ännu fler meddelanden om dataskyddet och datasäkerheten i Intra. Även Datasäkerhetsteamets meddelanden till fullmäktigeledamöterna har varit fler än förr. Datasäkerhetsteamet har år 2020 delat ut anvisningar om bland annat följande:

- Säker e-post och tjänsten Avauslinkki (uppdatering när Avauslinkki togs i bruk)
- Flera varningar om nätfiskemeddelanden till e-posten
- Coronablinkern till din arbetstelefon
- Justering i anvisningen angående rättigheter att kontrollera kameraövervakningens inspelningsband
- Windows 10: Datasäkerhetsuppdatering
- Mötesinbjudan där det finns en Teams-länk
- Delta i skolning via Zoom
- Datasäkerhets- och dataskyddspåminnelse
- Signal snabbmeddelandetjänst
- Installering av WhatsApp i mobilapparater som förvaltas av Sibbo kommun
- Sibborelaterad bakgrundsbild i Teams
- Teams i kundarbete och i intern användning
- Hälsingar från datasäkerhetsteamet under rådande undantagstillstånd
- Säker utskrift
- Sparar du dokumenten på rätt ställe?

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. Det har konstaterats att rapporteringen för tillfället är både svår och arbetsdryg. Under den kommande rapporteringsperioden ska vi göra ändringar i nätutbildningarnas process. I fortsättningen är utbildningen om datasäkerhet och dataskydd samt att datasäkerhetsförbindelsen undertecknas i samband med introduktion till arbetet en förutsättning. Användarnamnet låses om den anställda eller den förtroendevalda inte avlägger utbildningen. Ett meddelande om ärendet publiceras i Intra i god tid innan användarnamnen låses. Utöver datumet när användarnamnen kommer att låsas innehåller meddelandet en uppmaning om att anställda ska avlägga utbildningen och godkänna datasäkerhetsförbindelsen.

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 TAISTO-övningar

I november år 2019 deltog Sibbo kommun i den riksomfattande övningen TAISTO19. Under år 2020 har man kartlagt utmaningarna upptäckta under övningens gång och försökt hitta lösningar för dem. När anmälningen till TAISTO20 var aktuell beslutade kommunens ledningsgrupp att Sibbo kommun inte deltar i Taisto-övningen år 2020. Årets ämne var hur informationsläckor ska behandlas. I stället för att delta i övningen beslutade man att säkerställa att utvecklingsåtgärder som identifierades på grund av den föregående övningen kan vidtas. I stället för att öva ville man använda tid till att behandla en aktuell, äkta informationsläcka som hade tagit plats i kommunen.

Deltagarna i den här tillställningen som kommunen själv ordnade representerade kommunens ledning, datasäkerhet, dataskydd, IT-tjänster och kommunikationsavdelning. Att behandla en incident som de facto hade hänt i Sibbo upplevdes som nyttigt. Iakttagelserna har antecknats som utvecklingsobjekt och de har fått en tidtabell.

2.7 Av vem erhålls personuppgifterna och till vem överförs dem?

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.

2.8 Webbtjänster och andra ICT-tjänster

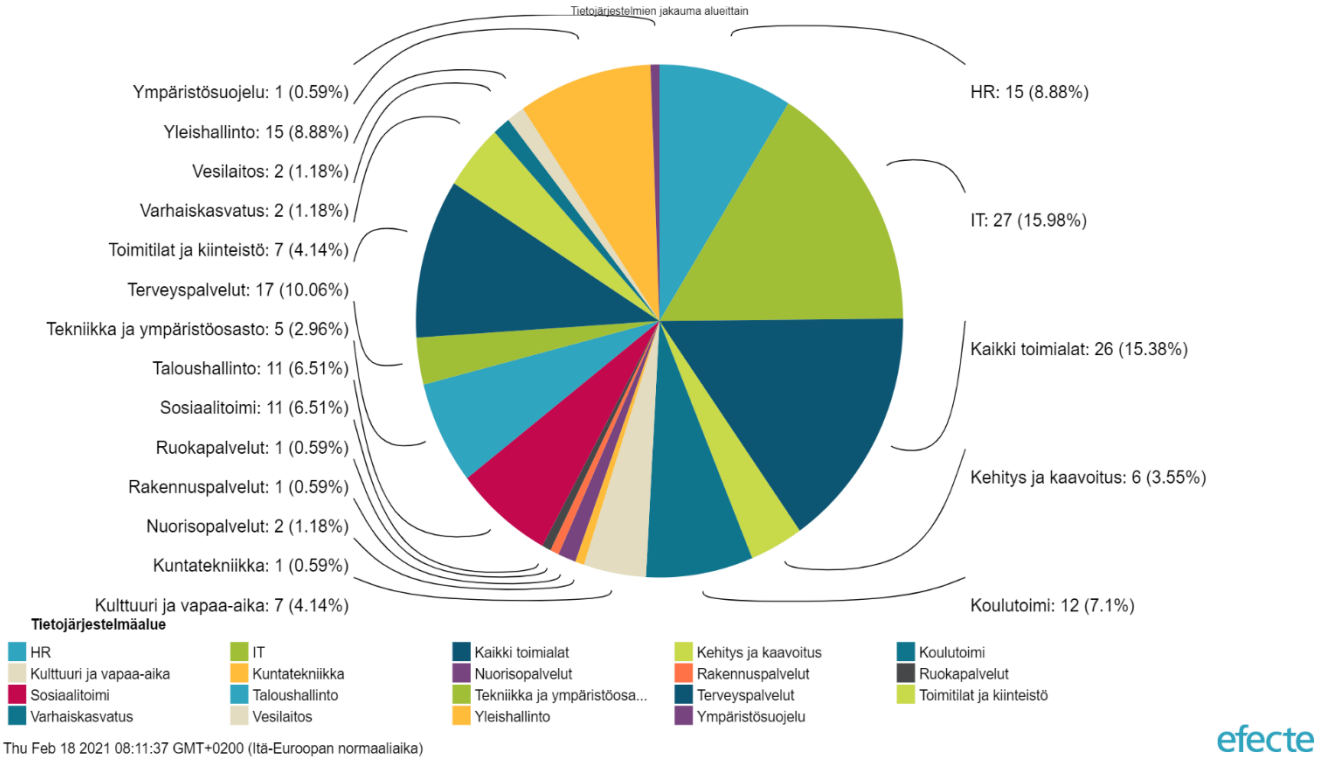
IT-enheten producerar infratjänster, kommunens gemensamma tjänster samt tjänster inom separata verksamhetsområden och/eller resultatenheter. Dessa tjänster är nödvändiga för kommunens verksamhet. Infratjänsterna består av följande helheter: tjänster för slutanvändare, datakommunikationstjänster, server-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



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.

2.9 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 alla upphandlingar använder man i första hand kommunens egna avtalsmodeller och allmänna, vid tidpunkten gällande krav som lämpar sig för 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.

Dataskyddsförordningen förutsätter att parterna ingår avtal om behandling av personuppgifter respektive upprättar någon annan handling med rättslig verkan som personuppgiftsbiträdet förbinder sig till. Därför ska alla avtal i vilka kommunen har lagt ut behandling av personuppgifter till en extern tjänsteleverantör uppdateras så att de uppfyller förordningens krav. Uppdatering av avtal är en av de viktigaste punkterna i EU:s dataskyddsförordning. Val av strategi gjordes utifrån riskhanteringen: de mest värdefulla avtalen uppdaterades först. Även avtal i vilka det behandlas information av hög riskklass prioriteras. I Databokslutet 2019 var uppdatering av avtalen fortfarande ett identifierat utvecklingsobjekt. Arbetet med att säkerställa att det i kommunen inte finns ouppdaterade avtal, t.ex. på grund av det att avtalet inte fanns i ärendehanteringssystemet, fortsatte också under år 2020. Därtill har man förberett en ny anvisning för avtalshanteringen, och den förväntas bli färdig i början av 2021.

2.10 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 anvisningar för dokumentförvaltning och arkivering.

Kommunen har arkiveringsskyldighet och den följer vissa lagenliga bestämmelser om informationsutbyte, vilket gör att det i kommunen fortfarande behandlas mycket information i pappersform. Kommunen övergår till elektronisk behandling av klientuppgifter i takt med att digitala möjligheter utvecklas och kan godkännas med tanke på utförande av lagstadgade uppgifter. De ska också passa in i kommunens helhetsarkitektur. Den största förändringen i kommunen är att man förnyar informationshanteringspraxisen och bryter 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 organisationens många avdelningar orsakar problem och behovet av anvisningar är skriande. Många avdelningar har dock börjat visa större intresse för arkiveringsfrågorna och strävar efter att tillämpa anvisningarna och förbättra sin praxis. Att tillämpa aktuella och fungerande praxis inom dokumenthantering och arkivering som en systematisk del av avdelningarnas vardag är ett långsiktigt mål.

Dokumentförvaltningen samarbetar kontinuerligt med IT-avdelningen för att uppnå informationshanteringens övergripande mål. Arkiveringsgruppen fungerar som ett samarbetsnät för avdelningarnas arkivärenden. Gruppen sammanträder vid behov.

Kommunens förvaltning flyttade till nya lokaler i början av 2020, vilket förutsatte nya lösningar även för arkivmaterialen. I samband med flyttningen har man förstört en stor del av materialet i närarkiven. Materialmängden är dock stor, vilket gör att arbetet med att gå igenom och förstöra dokument fortsätter. En del av det gallrade närarkivmaterialet rengjordes och flyttades till arkivlokaler i 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.

Målet är att Sibbo kommun tar i bruk en informationsstyrningsplan (ISP) som beskriver processernas nuvarande tillstånd och uppfyller SÄHKE2-kraven i början av år 2021. 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.

I workshopar som ordnades 2020 har det utarbetats processbeskrivningar i samarbete med substanskunniga. Projektgruppen har lett arbetet och gett handledning och råd. I samband med processbeskrivningarna har man också identifierat utvecklingsbehoven i anslutning till processerna. Informationsstyrningsplanen ska hela tiden hållas uppdaterad. Med andra ord ska avdelningarna meddela dokumenthanteringen om uppdateringsbehov. I och med att informationsstyrningsplanen togs i bruk är Sibbo kommuns arkivbildningsplaner (ABP), som i flera delar redan var föråldrade eller ofullständiga, inte längre i kraft.

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:

- 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 (artikel 5). För att uppfylla informationsplikten använder man fortfarande dataskyddsbeskrivningar. Godkända och aktuella dataskyddsbeskrivningar finns på kommunens webbplats (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 yrkan om rättelse av registeruppgift, som baserar sig på de registrerades rättigheter (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 år 2020 kan beskrivas med följande nyckeltal:

Grundläggande datateknik och telefoner:

- Datasystem 160 st.
- Datorer, inklusive elevdatorer, 4 028 st. (+13 st. jämfört med föregående år)
- Multifunktionsapparater 91 st. (–11 st. jämfört med föregående år)
- Telefon- och dataabonnemang 1 149 st. (antalet vanliga telefonabonnemang år 2019 var 891 st.)
- Antal ICT-servicebegäranden: Antalet stödbegäranden totalt 8 159 st. (+2 489 st. jämfört med föregående år). Av dessa var 3 968 st. stödbegäranden (+1 599 st. i jämförelse) och 4 191 st. beställningar (+890 st. i jämförelse)

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

Begäran om insyn: 6 st.
Yrkan om rättelse: 0 st.
Begäran om radering av uppgifter: 0 st.
Begäran om logguppgifter (användningen eller utlämnande): 0 st.

Informationssäkerhetsincidenter:

Anmälan av personuppgiftsincidenter 22 st.
Allvarliga informationssäkerhetsincidenter: 0 st.
Framkomna bekräftade eller misstänkta datasekretessförbrytelser: 0 st.

Utförda utbildningar:

Nätutbildning för hela personalen, genomfört av cirka 90–95 % av anställda
Utbildning för förtroendevalda, genomfört av 96 % av förtroendevalda
Tilläggsutbildning för chefer, genomfört av 90 % av cheferna
Dataskyddsutbildningar för personalen: 3 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 verksamheten överensstämmer med förordningens krav på flera delområden. Det finns dock även saker som ska utvecklas.

6.1 Rekonstruktion av datasäkerhets- och dataskyddsgruppen

Sibbo kommun har en dataskyddsansvarig som arbetar på heltid och en datasäkerhetsansvarig som arbetar på deltid. Tillsammans bildar de kommunens Datasäkerhetsteam. Datasäkerhets- och dataskyddsgruppen sammanträdde 8 gånger under år 2018, men på grund av personaländringarna hade gruppen inga möten år 2019. Det var meningen att grunda en ny grupp under år 2020, men kommundirektören inrättade ingen datasäkerhets- och dataskyddsgrupp för kommunen under det gångna året.
Kommundirektören tillsätter 2021 en grupp vars uppgift är att följa med hur dataskyddet genomförs och att ge utvecklingsförslag samt erbjuda stöd till dataskyddsansvariga och systemadministratörer inom olika verksamhetsområden. Man ber att verksamhetsområdena och nyckelenheterna tillsätter sina representanter i gruppen. Målet är att gruppen ska bestå av experter i flera olika branscher: dataskyddet, datasäkerhet, riskhantering, ICT och juridik. Gruppen ska med sex månaders mellanrum rapportera till kommunens ledningsgrupp om hur datasäkerheten och dataskyddet genomförs.

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.

I det första skedet borde informationshanteringsmodellen ha blivit färdig i början av 2021. På grund av den arbetsbörda som coronapandemin orsakat har en del av arbetet blivit ogjort. Informationshanteringen i Sibbo kommun utvecklas under de kommande åren bland annat inom följande delområden:
- insamling av logguppgifter
- ärendehantering
- ärenderegister och kraven på genomförande av informationssäkerheten
- utveckling av risk- och konsekvensbedömningar gällande datasäkerhets- och dataskyddsärenden
- betoning av dataskydds- och datasäkerhetsfrågor som ett obligatoriskt krav vid systemanskaffningar

Mängden information i digital form växer i accelererande takt. Digital information produceras i kommunens verksamhet, bl.a. vid olika tjänster, transport eller till exempel byggnader. Mängden information växer, vilket möjliggör att utvecklingen av helt nya tjänster. Samtidigt ställs också ytterligare krav för informationshanteringen och databehandlingen.

Den nya lagstiftningen som ålägger kommunerna t.ex. angående öppna data är under beredning, och den kommer att vara utmanande med tanke på både kommunens ekonomi och resursfördelningen.

Åtgärder som rekommenderas i informationshanteringslagen är problematiska med tanke på datasäkerheten, för de grundar sig på de redan föråldrade Vahti-anvisningarna för riskhantering, vilket gör förpliktelserna delvis otydliga. Kraven förutsätter även riksomfattande tjänster som inte har blivit färdiga enligt tidtabellen. För denna del är situationen med andra ord utmanande för alla finska kommuner.

Genom att utnyttja digitalisering och data på ett säkert sätt har man som mål att bygga kundorienterade, pålitliga och kostnadseffektiva tjänster för kommuninvånarna. Allt detta förutsätter att man tar hand om dataskydd och datasäkerhet tillräckligt bra. Principerna för datasäkerhet och dataskydd ska alltså konkretiseras och de ska bli en del av organisationens verksamhet.

Under år 2021 kommer kommunen att kartlägga olika dataloggningssystem (SIEM) på marknaden. Efter kartläggningen ska kommunens loggningspolicy definiera uppgifterna som ska överföras till det centraliserade dataloggningssystemet. Kommunen följer Informationhanteringsnämndens rekommendationer om insamling av logguppgifter.

Angående användarförvaltningen har kommunen år 2020 anskaffat Efectes IGA-system med vilket kommunen har färdighet att inom informationshanteringslagens gränser vidta användarförvaltningsåtgärder under år 2021. Användarnamn hålls aktuella när deras giltighet kopplas till de anställdas arbetsavtal. Användarrättigheterna ges enligt respektive anställdas uppgifter i IGA-systemet.

Genom att uppdatera och kryptera anslutningarna har man satsat på dataöverföringen. Kommunens ICT-avdelning har år 2020 låtit göra en auditering av datasäkerheten enligt standarden ISO-27001. Utvecklingsåtgärder vidtas på grund av auditeringen redan 2021. På en allmän nivå kan man konstatera att det på grund av auditeringen rekommenderades att Sibbo utvecklar strategier och riktlinjer angående datasäkerhet och säkerställer tillräckliga personalresurser för att utveckla ICT och datasäkerhet.

Suomi.fi-identifieringen blev i fjol betydligt vanligare i olika myndighetssystem. I Sibbo har man utrett olika alternativ till att identifiera personalen så att de anställda inte behöver använda personliga identifierare i sitt arbete. Kommunen ska beställa organisationskort av Myndigheten för digitalisering och befolkningsdata. Med korten kan anställda med stark autentisering identifiera sig i system som använder suomi.fi-identifieringen. 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.

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.

Dataläckage förekommer kontinuerligt. Den incident som väckte mest uppmärksamhet 2020 var säkert Vastaamo. Det har rapporterats identitetsstölder även i flera kommuner. De får bara oftast inte så mycket publicitet. Att skydda de anställdas elektroniska identiteter är nuförtiden lika viktigt som att skydda deras personliga identiteter.

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.