VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Rekommendation om tekniska gränssnitt och elektroniska förbindelser

Nämnder

Finansministeriets publikationer – 2021:38

Finansministeriets publikationer 2021:38

Rekommendation om tekniska gränssnitt och elektroniska förbindelser

Finansministeriet Helsingfors 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Finansministeriet

ISBN pdf: 978-952-367-724-1
ISSN pdf: 1797-9714

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2021

Presentationsblad

6.7.2021

Rekommendation om tekniska gränssnitt och elektroniska förbindelser

Finansministeriets publikationer 2021:38		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	svenska	**Sidantal**	20

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen) finns bestämmelser om hur informationsöverföringen via tekniska gränssnitt och elektroniska förbindelser ska ske. Med tekniskt gränssnitt avses en kommunikationsmetod för elektroniskt informationsutbyte mellan två eller flera informationssystem.

Denna rekommendation innehåller preciseringar som gäller elektronisk överföring enligt informationshanteringslagen. Rekommendationen är inte bindande, utan redogör för hur myndigheterna kan genomföra elektronisk överföring på det sätt som krävs enligt informationshanteringslagen.

Informationshanteringsnämnden godkände rekommendationen den 31 augusti 2020.

Nyckelord	informationshanteringsnämnden, informationshanteringslagen, elektronisk förbindelse, nämnder, rekommendationer, gränssnitt, e-förvaltning, myndigheter

ISBN PDF	978-952-367-724-1	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-724-1		

Kuvailulehti

6.7.2021

Suositus teknisistä rajapinnoista ja katseluyhteyksistä

Valtiovarainministeriön julkaisuja 2021:38		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	ruotsi	**Sivumäärä**	20

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jatkossa tiedonhallintalaki) säädetään teknisten rajapintojen ja katseluyhteyksien kautta tapahtuvien tietojen luovutusten toteutustavoista. Teknisellä rajapinnalla tarkoitetaan sähköisen tiedonvaihdon mahdollistavaa tiedonsiirtoratkaisua kahden tai useamman tietojärjestelmän välillä.

Tämä suositus sisältää tarkennuksia tiedonhallintalaissa säädettyjen sähköisten luovutustapojen toteuttamiseen. Suositus ei ole sitova, vaan siinä esitetään, miten viranomaiset voivat toteuttaa sähköiset luovutukset tiedonhallintalain edellyttämällä tavalla.

Tiedonhallintalautakunta hyväksyi suosituksen 31.8.2020.

Asiasanat	tiedonhallintalautakunta, tiedonhallintalaki, katseluyhteys, lautakunnat, suositukset, rajapinnat (tietokoneohjelmat), sähköinen hallinto, viranomaiset		
ISBN PDF	978-952-367-724-1	**ISSN PDF**	1797-9714
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-724-1		

Description sheet

6 July 2021

Recommendation concerning technical interfaces and viewing access

Publications of the Ministry of Finance 2021:38		**Subject**	Board
Publisher	Ministry of Finance		
Group Author	Information Management Board		
Language	Swedish	**Pages**	20

Abstract

The Act on Information Management in Public Administration (906/2019), also known as the Information Management Act, includes provisions on methods of disclosing information via technical interfaces and viewing access arrangements. A technical interface means a data transfer solution enabling electronic data transfer between two or more information systems.

This recommendation sets out further details concerning implementation of the electronic disclosure methods referred to in the Information Management Act. The recommendation is not binding but sets out how public authorities can implement electronic disclosure in the manner required by the Information Management Act.

This recommendation was approved by the Information Management Board on 31 August 2020.

Keywords Information Management Board, Information Management Act, viewing access, boards, recommendations, interfaces (computer programs), e-government, public authorities

ISBN PDF	978-952-367-724-1	**ISSN PDF**	1797-9714
URN address	http://urn.fi/URN:ISBN:978-952-367-724-1		

Innehåll

1 Inledning

I lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen) finns bestämmelser om hur överlåtelsen av information via tekniska gränssnitt och elektroniska förbindelser. Med tekniskt gränssnitt avses en kommunikationsmetod för elektroniskt informationsutbyte mellan två eller flera informationssystem. Bestämmelserna i informationshanteringslagen berättigar inte till att erhålla information, utan innehåller information om hur den elektroniska överlåtelsen ska ske och med vilka villkor i de situationer där överlåtelsen sker med hjälp av tekniska gränssnitt eller elektroniska förbindelser. Tekniska gränssnitt och elektroniska förbindelser kan ha delvis överlappande funktioner och det är inte alltid ändamålsenligt att genomföra båda för samma användningsändamål.

Vid användningen av tekniska gränssnitt och elektroniska förbindelser ska man se till att de uppgifter som överlämnas är uppdaterade med tanke på sitt användningsändamål. Enligt 20.1 § i informationshanteringslagen ska en myndighet sträva efter att utnyttja en annan myndighets informationsmaterial, om den första myndigheten har rätt att via ett tekniskt gränssnitt eller en elektronisk förbindelse få den behövliga informationen från den andra myndigheten. Vid utnyttjandet av informationen ska parters och andra förvaltningskunders rättssäkerhet tillgodoses.

Den här rekommendationen innehåller preciseringar för genomförandet av de elektroniska överföringssätt som stadgas i informationshanteringslagen. **Rekommendationen är inte bindande utan den presenterar hur myndigheterna kan genomföra elektroniska överföringar på det sätt som informationshanteringslagen förutsätter.**

Regleringen av tekniska gränssnitt och elektroniska förbindelser ersätter tidigare bestämmelser om tekniska användningsförbindelse. Informationshanteringsnämnden anser det vara nödvändigt att man under övergångstiden utvärderar om de tidigare genomföra förfaranden för elektronisk informationsföring de facto varit tekniska användningsanslutningar. Till exempel är inlämnande av uppgifter till en myndighet med hjälp av en blankett i en digital tjänst inte överföring av uppgifter via ett tekniskt gränssnitt eller en elektronisk förbindelse, utan inlämnande av uppgifter med hjälp av den mottagande myndighetens elektroniska dataöverföringsmetod. Bestämmelser om elektroniska dataöverföringsmetoder finns i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) samt i lagen om tillhandahållande av digitala tjänster (306/2019).

2 Överlåtelse av uppgifter via tekniska gränssnitt

Bestämmelserna på användningen av tekniska gränssnitt tillämpas i situationer där informationsutbytet sker automatiskt via informationssystem. De nämnda bestämmelserna tillämpas inte om uppgifterna sparas i ett informationssystem till exempel då användaren använder en elektronisk blankett eller en digital tjänst. Då sker sparandet av uppgifterna eller överföringen genom att använda en elektronisk informationsöverföringsmetod.

2.1 Överlämnande av uppgifter mellan olika informationssystem

Enligt 22.1 § i informationshanteringslagen ska myndigheterna genomföra regelbundet återkommande och standardiserad elektronisk överföring av information mellan informationssystem via tekniska gränssnitt, om den mottagande myndigheten enligt lag har rätt till informationen. Då det regelbundet sker informationsöverföring i elektroniskt format mellan myndigheterna ska överföringen ske via tekniska gränssnitt. I informationshanteringslagen finns inga närmare bestämmelser om regelbundenheten så en regelbunden överföring av uppgifter kan ske exempelvis varje dag, varje vecka, en gång per verksamhetsperiod eller rent av en gång i året.

Informationsöverföringen som sker via tekniska gränssnitt förpliktigas om överföringen av information har standardiserat innehåll, till exempel om den överförda informationens struktur inte på ett väsentligt sätt förändras mellan överföringarna. Överföringen av information kan inte utföras med hjälp av de tekniska gränssnitten om överföringen av information är kopplad till myndighetens möjlighet till övervägande om vilka uppgifter som är nödvändiga med tanke på myndighetens delfåenderätt och informationens användningsbehov. När den mottagande myndighetens rätt att få information begränsas till endast nödvändiga uppgifter ska man särskilt reda ut om givandet av uppgifterna är kopplat till behovsprövning och i sådana fall är det informationsinnehåll som överlämnas inte standardformat. Därmed kan inte vilken information som helst överföras automatiskt via informationssystemen med hjälp av de tekniska gränssnitten.

Strukturerna för de tekniska gränssnitten fastställs av den överlåtande myndigheten som även har befogenheter att besluta om överlåtandet av uppgifterna. Den myndighet som

överlåter uppgifterna definierar därmed i praktiken de situationer där gränssnittet kan öppnas för en annan myndighet med beaktande av vad som stadgas i lag om möjligheten att överlåta information och om skyldigheten att överlåta den.

Information kan överföras mellan myndigheternas informationssystem med hjälp av tekniska gränssnitt även i situationer där överföringen av information inte är regelbunden om den information som överförs har standardinnehåll. Men då kan det hittas mer ekonomiskt och tekniskt ändamålsenliga metoder för att utföra enskilda dataöverföringar. I de här situationerna kan överlämnandet av uppgifterna vara mer effektivt med en digital tjänst såsom säker e-post eller annan elektronisk informationsöverföringsmetod.

Den **myndighet** vars dokument eller information det tekniska gränssnittet når beslutar om överlämnandet av uppgifterna, **inte** den aktör som ansvarar för informationssystemets tekniska underhåll såsom **servicecentret**. Vid beslut om öppnandet av det tekniska gränssnittet kan den myndighet som överlämnar uppgifterna inte ställa sådana villkor för överlämnandet som bestäms i informationshanteringslagen eller en annan lag, och villkoren kan inte stå i strid med lagen. Den myndighet som överlämnar informationen kan ställa upp villkor på överföringen till den del som de preciserar informationssäkerhetskraven i informationshanteringslagens 4 kapitel. Vid utarbetandet av villkoren är det rekommenderat att utnyttja informationssäkerhetsrekommendationerna som informationshanteringsnämnden givit. Av beslutet om att öppna det tekniska gränssnittet ska det framgå för vilket ändamål uppgifterna överlämnas och på vilken lagstadgad rätt att få information överföringen sker.

2.2 Undantag i överlåtelse av information mellan informationssystem

Skyldigheten att använda tekniska gränssnitt enligt informationshanteringslagen inkluderar en del undantag. Regelbundet upprepad överföring av information av standardformat kan genomföras utan användning av tekniska gränssnitt om det inte är tekniskt eller ekonomiskt ändamålsenligt att genomföra eller använda sådana. Undantag kan komma på fråga i situationer där de informationssystem som används är i slutet av sin livscykel då det inte av tekniska eller ekonomiska orsaker är ändamålsenligt att genomföra gränssnitten i det gamla informationssystemet. Myndigheterna ska dock i dessa fall utvärdera grunderna för varför överföringen av informationen inte kan genomföras enligt skyldigheten enligt informationshanteringslagen. Utvärderingen ska inkluderas som en del av informationshanteringens konsekvensbedömning enligt 5 § i informationshanteringslagen om det tekniska gränssnittet inte genomförs i samband med en ändring av informationshanteringen eller ibruktagandet av ett nytt informationssystem.

2.3 Förutsättningar för överlåtelse av information via informationssystem

Den myndighet som överlämnar informationen ska utreda den mottagande myndighetens rätt att få information, de uppgifter som överförs i standardformat samt den tidsbundna upprepningen av den regelbundna informationsöverföringen. Utifrån utredningarna fastställer den överlämnande myndigheten informationsstrukturen för gränssnittet per mottagare, ifall de olika myndigheternas delfående avviker från varandra. Om överlämnandet av uppgifterna förutsätter utvärdering från fall till fall samt om de uppgifter som överlåts avviker från fall till fall rekommenderas det inte att uppgifterna överförs via tekniska gränssnitt eftersom utvärderingen inte kan automatiseras. Om användningsbehovet däremot varierar utifrån de olika uppgifterna och om datainnehållet är av standardinnehåll kan omfattningen och mängden information som överförs variera även då samma tekniska gränssnitt används.

Användarrättigheterna definieras i det system som begär informationen. Att användarrättigheterna definieras i det överlämnande innebär främst definitionen av användarrättigheten för det informationssystem som får uppgifterna. Utöver användarrättigheterna definieras de uppgifter som behövs för att identifiera informationssystemet som får uppgifter. Användarens arbetsuppgifter samt grunden för delfåendet av de överförda uppgifterna och användningsändamålet inverkar på definitionen av användarrättigheterna. Den myndighet som överlämnar information kan ställa upp särskilda men lagbaserade villkor på användarrättigheterna i informationssystemet hos den mottagande myndigheten. I beviljandet av användarrättigheter ska kraven som beskrivs i 16 § i informationshanteringslagen beaktas.

Behovet av att överlämna sekretessbelagda uppgifter eller personuppgifter eller säkerställandet av nödvändigheten från fall till fall kan genomföras till exempel så att det informationsbegärande systemet kontrollerar användarens verksamhet då denne söker uppgifter i ett annat informationssystem via ett gränssnitt i realtid. Följande rekommenderas som kontroller:

- Det informationssystem som begär uppgifterna informerar användaren om för vilket ändamål informationen kan användas och
- begär användaren bland på förhand fastställda användningsändamål specificera det för vilket uppgifterna begärs, om uppgifterna kan användas för flera ändamål.
- I processtyrda informationssystem är utredningen av användningsändamålet inte nödvändigt eftersom gränssnittet öppnas till det andra

informationssystemet endast för vissa enskilda användningsändamål och då meddelas ändamålet som en del av informationen till användaren.

- Grunden för rätten att få information inkluderas som en del i överföringsloggarna både för det överlämnande och det mottagande informationssystemet.

Om överlämnandet av information sker automatiskt mellan myndigheternas informationssystem regelbundet, såsom i postbaserade eller andra filbaserade informationsöverföringar kan lagens krav uppfyllas exempelvis genom att i överföringsloggen registrera information om vilka uppgifter som överlämnats och för vilket ändamål. I de här fallen ska man vid det tekniska genomförandet av överföringen fästa uppmärksamhet vid att de uppgifter som överlämnas är nödvändiga eller oumbärliga från fall till fall. Med tekniska kontroller ska man säkerställa att den myndighet som får överföringen alltjämt har ett fortsatt behov av att få uppgifter om kunden eller en annan part av en annan myndighet.

Därför räcker det inte vid användningen av tekniska gränssnitt med att uppgifterna regelbundet levereras automatiskt från det överförande informationssystemet. I den mottagande myndighetens informationssystem ska man för varje informationsöverföring göra en teknisk begäran om information till det överlämnande informationssystemet om ärendebehandlingen baserar sig på att kundrelationen och behovet av att få information är tidsbunden. Utvärderingen från fall till fall kan ske även så att det informationssystem som överlåter uppgifterna identifierar ändringarna i kundens uppgifter och förmedlar dem automatiskt till de mottagande systemen om överlåtelsen av uppgifterna baserar sig på ett kontinuerligt behov av information till exempel vid körningar av informationsmaterialuppdateringar.

2.4 Kompatibilitet och genomföring av informationsöverföringen

Kraven på interoperabilitet för de tekniska gränssnittens del förutsätter att man beaktar och säkerställer interoperabiliteten både för de tekniska genomföringarna (gränssnittet och överföringsförbindelsen), den semantiska genomföringen (ordlistorna och kodlistorna) samt för informationsmodelleringen (metadata och struktur). De ordlistor som används borde basera sig på de lagstadgade begreppen och de ska inte omdefinieras med en annan betydelse eller innebörd. Definitionen av ordlistorna är beroende av att man enligt 2.3 § i grundlagen ska följa lagen i all offentlig verksamhet. Begreppen som bestäms i lag binder deras användning i myndigheternas verksamhet. För att främja interoperabiliteten rekommenderas att man i beskrivningen använder gemensamma ordlistor, informationsmodeller och kodlistor.

I lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016, stödtjänstlagen) finns bestämmelser om informationsförmedlingskanalen, eller servicekanalen, med hjälp av vilken användarorganisationerna kan överföra och lämna ut uppgifter som ingår i deras datalager och tillhandahålla elektroniska tjänster. Enligt 5.1 § i stödtjänstlagen är statliga förvaltningsmyndigheter, ämbetsverk, inrättningar och affärsverk, kommunala myndigheter, när de sköter sina lagstadgade uppgifter, domstolar och andra rättskipningsorgan skyldiga att använda servicekanalen när stödtjänsten är tillgänglig och det serviceavtal för en tjänst som anskaffats självständigt och som motsvarar stödtjänsten i fråga har löpt ut, om inte myndigheten av tekniska eller funktionella skäl eller av skäl som hänför sig till kostnadseffektiviteten eller informationssäkerheten nödvändigtvis måste använda andra tjänster i sin verksamhet eller i en del av den.

Varje organisation som har anslutit sig till servicekanalen hanterar uppgifterna i sina system och ansvarar för att de uppgifter som andra behöver är tillgängliga och finns beskrivna i katalogen över anslutningarna (anslutningskatalogen). Dessutom ska organisationen själv beakta eventuella begränsningar som gäller delningen av information.

Statens, kommunernas och samkommunernas informationshanteringsenheter ska använda servicekanalen med hjälp av tekniska gränssnitt för att överföra informationen, om det inte finns en lagstadgad grund att avvika från bestämmelserna till exempel vad gäller användningen filöverföringstyper. Sådana här grunder för avvikande ska antecknas i informationshanteringens ändringskonsekvensbedömning som enligt 5.3 § i informationshanteringslagen då ändringen av informationshanteringen leder till väsentliga ändringar i informationshanteringsenhetens informationshanteringsmodell.

3 Elektronisk förbindelse

3.1 Förutsättning för öppnandet av en elektronisk förbindelse

Myndigheten kan öppna en elektronisk förbindelse åt en annan myndighet till datalagrets sådana uppgifter som myndigheten som får den elektroniska förbindelsen har rätt att få information om.

Myndigheten som överlämnar uppgifter ska gå igenom rätten att få information med den mottagande myndigheten. Utifrån rätten att få information definieras den elektroniska förbindelsens vy som baserar sig på respektive myndighets rätt att få information och som därmed kan vara olik för olika myndigheter.

Användarrättigheterna till den elektroniska förbindelsen beviljas till den mottagande myndigheten utifrån rätten och behovet att få information. Den myndighet som beviljas användarrättigheterna ansvarar för att användarrättigheterna och deras användarnamn eller uppgifter som skaffas med hjälp av dem inte överlämnas till oberättigade personer och att användarrättigheterna endast används för det ändamål de beviljats för.

Dessutom ska myndigheten anmäla ändringar i användarnas tjänster till den myndighet som beviljat användarrättigheterna till den delar som de inverkar på hanteringen av användarrättigheterna såsom ändring, frysning eller radering av rättigheterna. Den myndighet som beviljat användarrättigheten ansvarar för att säkerställa att användarrättigheterna är aktuella och att tillträdet som användarrättigheten beviljar verkställs.

I beviljandet av användarrättigheter ska kraven som beskrivs i 16 § i informationshanteringslagen beaktas.

3.2 Genomföring av elektronisk förbindelse

Den myndighet som erbjuder den elektroniska förbindelsen ska skapa systemet så att det stöder begränsningen av den elektroniska förbindelsen endast till de behov eller nödvändiga uppgifter som rätten till information definierar.

Den myndighet som erbjuder den elektroniska förbindelsen kan genomföra den genom att utvärdera och dokumentera de uppgifter som behövs eller är nödvändiga för att sköta

de uppgifter som myndigheten som får den elektroniska förbindelsen sköter. Den myndighet som erbjuder den elektroniska förbindelsen kan genomföra systemet tekniskt så att den elektroniska förbindelsen begränsas per myndighet eller användare enligt de uppgifter som behövs eller är nödvändiga.

Den myndighet som erbjuder den elektroniska förbindelsen ska genomföra den så att uppgifterna endast kan hämtas som enskilda sökningar. Då ska sökkriterierna vara sådana att man utifrån dem inte kan söka en stor mängd uppgifter om flera personer utan att sökningen i regel begränsas till uppgifterna om en eller ett fåtal personer som uppfyller kriterierna.

Kravet kan även främjas genom att datatekniskt genomföra den elektroniska förbindelsen så att användaren vid sökningen av informationen matar in eller väljer grunden för varför uppgifterna söks i en meny. Motiveringen och användarens uppgifter samlas i logguppgifterna som samlas in med hjälp av den elektroniska förbindelsen och i efterhand kan man verifiera syftet för och den lagenliga rättsgrunden för behandlingen av varje elektronisk förbindelse. Detta förfarande tvingar användaren att innan varje sökning utvärdera om sökningen är nödvändigt för skötseln av tjänste- eller arbetsuppgifterna. Med detta strävar man även efter att förhindra att sökningar inte kan göras automatiskt till med en sökrobot.

Den myndighet som erbjuder en elektronisk förbindelse ska genomföra den elektroniska förbindelsen till datalagret så att det informationssystem som möjliggör den elektroniska förbindelsen automatiskt identifierar avvikandeinformationssökningar. Dessutom rekommenderas att informationssystemet strävar efter att förhindra att informationssökningarna fortsätter tills avvikelsen har utretts. Dessutom borde det finnas en på förhand definierad process som snabbt kan utreda orsakerna till ovanliga informationssökningar. Det rekommenderas att sådana här avvikelser styrs till exempel till systemets huvudanvändare eller dataskyddsansvarig för vidare utredningar. Tjänstemännen som är arbetsgivare hos den myndighet som tar emot uppgifterna ska utreda grunderna för de sökningar som den som sökt uppgifterna har samt att ge en utredning om detta till den myndighet som överlämnas uppgifterna.

Med avvikande informationssökningar avses exempelvis följande:

1. Användaren söker sådan information som hen antagligen inte är berättigad till eller så gör hen en ovanligt stor mängd sökningar inom en kort tid. Risken kan hanteras genom att utarbeta olika larm för att identifiera avvikande beteende. Larmet ger en varning till exempel i situationer där sökningarna tydligt riktas till datainnehåll utanför användarens uppgifter eller geografiska läge eller om sökningarna infaller en tidpunkt som avviker från det normala.

2. En del enskilda uppgifter eller en enskild persons information söks mer än normalt.
3. Användaren matar in sökord eller specialtecken i sökfältet som avviker från det normala eller användarens verksamhet tyder på en verksamhet som klart skiljer sig från det normala och vars ändamål är att bryta systemets skydd. Denna risk kan hanteras genom att innan ibruktagandet utföra en ändamålsenlig datasäkerhetstestning för systemet där man beaktar t.ex. behovet att skydda systemet mot databasattacker. Dessutom ska man förhindra inmatningen av sådana sökord eller -tecken som antagligen inte behöver användas.

Om något av de inställda larmen alarmerar kan systemet till exempel meddela användaren om detta, stänga användarens användarrättigheter, avsluta användarens elektroniska förbindelse och berätta vart hen kan ta kontakt för att återaktivera användarnamnet. Dessutom ska larmhändelsen vara en inledning för den planerade utredningsprocessen för datasäkerhetsavvikelser.

Den automatiska identifieringen av avvikande informationssökningar kan genomföras på olika sätt och med flera tekniker. För genomförandet finns det både lösningar med öppen källkod och kommersiella lösningar. Som enklast kan man i genomförandet använda system vars funktioner möjliggör observation av en avvikande verksamhet och ett larm om detta exempelvis med hjälp av inställda regler för analysering av loggar. Regelbaserade system identifierar dock endast **på förhand definierade** avvikande funktioner. Därmed förutsätts en ständig utvärdering och utveckling av reglernas funktioner. Identifikationen av avvikande verksamheter kan vidare förbättras t.ex. genom att utnyttja maskininlärning eller annan avancerad analys som kompletterar reglerna.

4 Tillämpning av allmänna datasäkerhetsåtgärdskrav på tekniska gränssnitt och elektroniska förbindelser

4.1 Riskbaserad planering

Myndigheten ska bedöma riskerna med genomförandet av de tekniska gränssnitten och de elektroniska förbindelserna samt planera åtgärder för att hantera riskerna så att de elektroniska informationsöverföringsmetoderna kan genomföras och användas på ett säkert sätt. I riskbedömningen och -hanteringen ska man beakta minimikraven på informationssäkerheten som fastställs i informationshanteringslagens kapitel 4. Myndigheter som upprätthåller basregister, förmedlar hälsouppgifter eller överlämnar mer information än vanligt via tekniska gränssnitt bör utarbeta en omfattande riskbedömning. Riskbedömningen rekommenderas att utföras i samarbete mellan de aktörer som överlåter och mottar information samt även i samarbete med andra myndigheter som utför samma eller liknande uppgifter. Detta möjliggör delning av risker och god praxis mellan aktörerna.

I riskbedömningen av genomförandet och användningen av de tekniska gränssnitten och de elektroniska förbindelserna identifieras de väsentliga riskerna som kan påverka på hållbarheten och tillgängligheten hos gränssnitten eller förbindelserna eller på datasäkerheten hos det material som behandlas. Risker kan orsakas bland annat av skydd mot anfallsmetoder, nyckelhantering, brister i kvaliteten på den information som sänds eller i automatiseringen av informationsöverföringen eller andra säkerhetsproblem i informationsöverföringsmetoderna.

Dessutom kan risker orsakas av brister i den mottagande myndighetens informationshanteringsmiljö, okunskap om användningen av elektroniska informationsöverföringsmetoder eller källsystemet eller i behandlingen av den information som tas emot.

Dessa risker kan man sträva efter att hantera genom att säkerställa den mottagande myndighetens och systemanvändarnas datasäkerhetskunskap om systemets särdrag och om de uppgifter som behandlas. Därmed ska den myndighet som överlämnar uppgifterna ska anvisa och vid behov säkerställa kunnandet exempel genom utbildningar:

- Hur ska det elektroniska informationsöverföringssystemet och informationssystemet användas för att användaren ska undvika riskfyllda och datasäkerhetsäventyrande användningssätt?
- Hur ska uppgifterna i systemet behandlas så att deras konfidentialitet, integritet och tillgänglighet äventyras?

En dokumentering av användargrunderna ökar dataskyddet: till exempel dokumenterad information om på vilket sätt databegärandena behandlas, vem de ska hänvisas till och hur länge information kan begäras utan separata kostnader.

Utöver handledning och utbildning kan man hantera risker som beror på användarnas slarv och brådska genom att påminna användarna alltid i samband med inloggning.

Riskerna som gäller den mottagande myndighetens informationshanteringsmiljö kan hanteras exempelvis genom att man förutsätter tekniska åtgärder som behövs, utredningar eller datasäkerhetsauditeringar av tredje parter för att säkerställa informationssäkerhetskraven som behandlingen av uppgifterna kräver.

4.2 Minimering av de uppgifter som överlämnas

Myndigheten som överlämnar uppgifter ska se till att de minimeras innan överlåtandet. Detta innebär att myndigheten endast överlåter de uppgifter som den mottagande myndigheten motiverat behöver för att sköta sina uppgifter. Den myndighet som överlämnar informationen ska säkerställa att man inte med de överförda uppgifterna överför sådan information som den mottagande myndigheten inte har bett om, som den inte behöver eller som den inte har åtkomsträtt till. Denna risk kan gälla särskilt metadata som finns i de överförda informationsmaterialen och vars uppgifter den överlämnande myndigheten bör kartlägga och säkerställa att det inte finns sådana uppgifter som inte bör överlämnas. Till minimeringen av uppgifterna hör även raderingen av onödiga individuella identifikatorer från de överförda uppgifterna då överföringen av dem inte är separat motiverat.

Om en myndighet har rätt att från en annan myndighets informationslager via ett tekniskt gränssnitt eller en elektronisk förbindelse få tillförlitlig och uppdaterad information för skötseln av sina uppgifter, får den inte enligt 20.2 § i informationshanteringslagen kräva att dess kunder visar upp eller lämnar in intyg eller utdrag, om det inte är nödvändigt för utredning av ärendet. Tillförlitlig och uppdaterad innebär att den myndighet som överlåter uppgifterna har säkerställt att materialet är uppdaterat och att uppgifternas ursprunglighet och integritet har säkerställts i de processer som gäller informationsskötseln av materialet. Till informationsmaterialets tillförlitlighet hör även att förvaltningens kund ska

ha möjlighet att bekanta sig med uppgifterna i den myndighets datalager därifrån uppgifterna överförs till en annan myndighet.

Redan i planeringsskedet ska man beakta eventuell praxis för överföring av uppgifter. I systemöverföringarna kan det gå (rentav okrypterad) information som det inte är tillåtet att överlåta antingen enligt lag eller på grund av dataskyddsbestämmelser. Ett exempel är personbeteckningen som tidigare i hög utsträckning använts som identifikation i systemen. Det är onödigt att överföra identifikationsuppgifter med data även om uppgifterna används för sökningen. Då överförs endast den data som söktes. Samtidigt ska man då man gör utskrifter åt slutkunden granska att det inte på verifikatet eller myndighetens utskrift i onödan sparas andra specialskyddade uppgifter om kunden eller den begärda informationen.

4.3 Feltåligheten och användbarheten hos gränssnitten och de elektroniska förbindelserna

Dessutom ska myndigheten säkerställa feltåligheten hos systemets tekniska gränssnitt och elektroniska förbindelser och deras funktionella användbarhet genom tillräcklig regelbunden testning. Feltåligheten ska dimensioneras utifrån hur kritiskt systemet är för funktionen och hur länge verksamheten kan fortsättas även om systemet inte finns tillgängligt.

I utvärderingen av feltåligheten ska man även beakta att systemens användbarhetskrav förändras under olika tidpunkter. Systemet kan vara kritiskt endast till exempel vid månadsskiftet eller under en viss tid på året. I utvärderingen av kritiskheten ska man dessutom beakta de lagstadgade uppgifterna samt beroendet av andra system (inom den egna organisationen samt mellan myndigheterna).

Nivån på feltåligheten och den funktionella användbarheten ska fastställas innan de tekniska gränssnitten och den elektroniska förbindelsen genomförs. De tekniska gränssnitten och elektroniska förbindelserna ska genomföras utifrån de fastställda kraven genom att följa god praxis och anvisningarna för säker applikationsutveckling. Även feltåligheten hos systemets tekniska gränssnitt och elektroniska förbindelser och deras funktionella användbarhet ska säkerställas genom tillräcklig regelbunden testning. Det rekommenderas att ett dokument upprätthålls över den regelbundna testningens resultat där det framgår med hurdana kriterier feltåligheten och den funktionella användbarheten har säkerställts. Det rekommenderas att dokumentet ges för kännedom till de instanser för vars verksamhet gränssnittet eller den elektroniska förbindelsen är väsentlig. Testningen utförs enligt de krav som definierats om testningens regelbundenhet dimensioneras på så vis att den kan säkerställa den feltålighet och funktionella användbarhet som förutsätts.

4.4 Informationssäkerhetsåtgärder för dataöverföringen

Myndigheten ska genomföra informationsöverföringen som sker via tekniska gränssnitt och elektroniska förbindelser krypterat i informationsnätet eller genom att använda en annan krypterad inforationsöverföringsanslutning eller -metod ifall uppgifterna är sekretessbelagda. I överföringen av information i informationsnätet ska man beakta informationens integritet, konfidentialitet och tillgänglighet. För att uppnå detta ska man genomföra tillräckliga tekniska och administrativa skyddsmetoder. Vid överföring av sekretessbelagd information via ett offentligt nät ska informationsmaterialet eller dataförbindelsen skyddas med en tillräckligt säker kryptering såsom säker post eller genom att använda Transport- och kommunikationsverkets godkända krypteringslösningar för att skydda trafiken mellan den elektroniska tjänsten och slutanvändaren (de krypteringslösnigar som godkänts av Transport- och kommunikationsverket Traficoms NCSA-funktion (på finska)).

Praktiska sätt att genomföra en säker kryptering är till exempel:

- VPN-lösningar mellan användarens enhet och myndighetens informationssystem,
- TLS-kryptering av trafiken mellan e-tjänsten och slutanvändaren,
- IPSec-kryptering av nätet mellan organisationerna samt
- lösningar för säker e-post och filkryptering för slutanvändarna.

Informationsöverföringen ska ordnas så att mottagaren säkerställs eller identifieras på ett tillräckligt datasäkert sätt innan mottagaren kan behandla de överförda sekretessbelagda uppgifterna. I identifikationen av användare kan man använda till exempel personliga användarnamn och lösenord. Vid överföring av sekretessbelagt informationsmaterial identifieras och verifieras användarna med känd och säker teknik. Sådana här tekniker är exempelvis engångsinloggning och verifikation med flera kriterier. Identifikationsmetoden och -styrkan ska utvärderas från fall till fall för varje tjänst samt utifrån uppgifterna som behandlas i den om riskerna för att dessa avslöjas.

Källsystemet samt det informationsmaterial som överförs via tekniska gränssnitt och elektroniska förbindelser är skyddade från tekniska och fysiska skador. Detta kan genomföras till exempel genom att förhindra olovlig fysisk tillgång till de maskiner som behandlar informationsmaterialet med passagekontroll. I de lokaler där informationsmaterial som överförs behandlas ska man säkerställa tillräckliga kontroller av brand-, vatten- och elsäkerhet.

4.5 Administration av användarrättigheter och insamling av logguppgifter

Den myndighet som ansvarar för informationssystemet ska definiera informationssystemets användarrättigheter även för de tekniska gränssnittens och de elektroniska förbindelsernas del. Användarrättigheterna ska definieras utifrån användarens användningsbehov för sina uppgifter och de ska hållas uppdaterade.

Med hjälp av ändamålsenlig åtkomstkontroll och hantering av användare möjliggörs en lovlig användning av informationen och olovlig användning förhindras. Endast befullmäktigade användare och system beviljas åtkomst- och användarrättigheter och i hanteringen av dessa ska man följa principen för minsta rättigheter. Det innebär att användarna endast ges sådana användarrättigheter och -fullmakter för datasystemen som behövs för att uträtta arbetet. Hanteringen och användningen av användarkontona följs upp och övervakas för att iaktta avvikelser och hot samt för att reagera på dessa. Befintliga användarbefogenheter ska utvärderas regelbundet med tanke på om de är nödvändiga och uppdaterade. Användarbefogenheterna ska efter dessa utvärderingar uppdateras till att motsvara nulägets användarfullmaktsbehov.

Användningsändamålet för logguppgifterna är att följa upp hur uppgifterna i informationssystemet används och överlämnas samt att utreda tekniska fel i informationssystemet. Eftersom man överlämnar information via tekniska gränssnitt och elektroniska förbindelser ska överlåtelseloggar föras om användningen av dessa. Som minsta information rekommenderas att syftet med överföringen, mottagaren av överföringen (antingen myndigheten eller användaren), de informationshelheter som överförs och överföringstidpunkten samlas in.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

FINANSMINISTERIET
Snellmansgatan 1 A
PB 28, 00023 STATSRÅDET
Telefon 0295 160 01
finansministeriet.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-724-1 (pdf)

Juli 2021