Regeringens proposition till riksdagen med förslag till lag om ändring av lagen om sekundär användning av personuppgifter inom social- och hälsovården

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att kraven på informationssäkra driftmiljöer i lagen om sekundär användning av personuppgifter inom social- och hälsovården ändras så att kraven möjliggör utlämnande av i lagen avsedda uppgifter till andra informationssäkra driftmiljöer än sådana som är belägna i Finland. Syftet med ändringen är att möjliggöra användning av finländska register-uppgifter inom internationellt forskningssamarbete samtidigt som man säkerställer en hög nivå av informationssäkerhet och dataskydd.

Den föreslagna lagen avses träda i kraft den 1 december 2023.

_____

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Regeringsprogrammet 2019 för statsminister Sanna Marins regering har bland annat som mål att främja flexibel och omfattande användning av social- och hälsovårdsdata, dock så att en hög nivå av dataskydd säkerställs för de registrerade.

Lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019, nedan *lagen om sekundär användning*) trädde i kraft den 1 maj 2019. Syftet med lagen om sekundär användning är att skapa förutsättningar för att de kunduppgifter på personnivå som uppkommer i samband med serviceverksamheten inom social- och hälsovården samt andra personuppgifter som gäller hälsa och välfärd ska kunna användas för statistikföring, forskning, utvecklings- och innovationsverksamhet, undervisning, informationsledning, myndighetsstyrning och myndighetstillsyn samt för myndigheternas planerings- och utredningsuppgifter. Lagen ger möjligheter att i större utsträckning än nu utnyttja kund- och patientuppgifter inom social- och hälsovården för andra ändamål än det ursprungliga.

I lagen om sekundär användning fastställs krav för en informationssäker driftmiljö, med vilket enligt 3 § 11 punkten i lagen avses en teknisk, organisatorisk och fysisk driftmiljö för behandling av uppgifter där informationssäkerheten har säkerställts genom lämpliga administrativa och tekniska åtgärder. Personuppgifter får lämnas ut till informationssäkra driftmiljöer med stöd av ett dataanvändningstillstånd enligt 3 § 8 punkten i lagen om sekundär användning.

I 60 § 1 mom. i lagen om sekundär användning föreskrivs om en övergångstid enligt vilken bestämmelserna om kraven på informationssäkra driftmiljöer i 20 § 3 mom. och 21–34 § tillämpas från och med den 1 maj 2022. Efter övergångstiden kan i lagen om sekundär användning avsedda personuppgifter utlämnas för behandling med stöd av ett dataanvändningstillstånd endast i Tillståndsmyndigheten för användning av social- och hälsovårdsdatas (nedan *Tillståndsmyndigheten*) informationssäkra driftmiljö (driftmiljön Kapseli[1]) eller i en reviderad informationssäker driftmiljö enligt lagen om sekundär användning. Aggregerade statistiska uppgifter kan utlämnas fritt på basis av en begäran om information.

Kravet på behandling av personuppgifter i en informationssäker driftmiljö enligt lagen om sekundär användning kan vara utmanande särskilt för det internationella forskningssamfundet, där man vill använda social- och hälsovårdsuppgifter från Finland som en del av det datamaterial som samlas in från andra länder. Den medicinska forskningen är internationell till sin natur och bedrivs mycket ofta inom internationella konsortier. I lagen om sekundär användning förutsätts det att datamaterial som fås från Finland lämnas ut endast till en reviderad informationssäker driftmiljö i enlighet med lagens krav. Lagen om sekundär användning tar inte ställning till var driftmiljön geografiskt är belägen, men Tillståndsmyndighetens gällande föreskrift begränsar driftmiljön till EU-/EES-området.[2] En del av kraven gällande informationssäkra driftmiljöer i

[1] Se https://findata.fi/sv/kapseli/
[2] Se https://findata.fi/sv/tjanster-och-anvisningar/foreskrifter/

lagen om sekundär användning kan endast tillgodoses genom iakttagande av den nationella lagstiftningen och de nationella myndigheternas föreskrifter.[3] Informationssäkerheten i driftmiljön ska påvisas genom ett intyg från ett bedömningsorgan för informationssäkerhet som godkänts av Transport- och kommunikationsverket (nedan *Traficom*). I praktiken görs bedömningar gällande informationssäkerhet av bedömningsorgan som Traficoms Cybersäkerhetscenter godkänt separat.

Även om en informationssäker driftmiljö enligt Tillståndsmyndighetens föreskrift kan finnas inom EU-/EES-området, befinner sig i praktiken alla driftmiljöer enligt lagen om sekundär användning för närvarande i Finland. Utländska aktörer har ingen täckande information om revideringsskyldigheten enligt lagen om sekundär användning och ingen utländsk aktör har börjat revidera sina egna system på basis av lagen om sekundär användning. En övergång av forskning i någon större utsträckning till Tillståndsmyndighetens eller andra finländska aktörers driftmiljöer anses inte vara ett sannolikt alternativ. Till följd av detta är det möjligt att utnyttjandet av finländska data inom internationellt forskningssamarbete och således finländska forskares möjligheter att delta i forskningssamarbete försvåras.

1.2 Beredning

Regeringens proposition har beretts som tjänsteuppdrag vid social- och hälsovårdsministeriet. Beredningen av regeringens proposition har stötts av arbetsgruppen för internationellt utlämnande av uppgifter (VN/16772/2021). Arbetsgruppen hade som målsättning att utreda och bedöma på internationella utlämnanden tillämpliga bestämmelser om informationssäkerhet i lagen om sekundär användning i samarbete med sakkunniga inom informationssäkerhet och dataskydd, de myndigheter som styr och övervakar lagen om sekundär användning samt andra centrala intressegrupper inom området.

Till stöd för beredningen av propositionen beställde social- och hälsovårdsministeriet en utredning om internationella standarder och förfaranden på basis av vilka det vore möjligt att uppfylla i Tillståndsmyndighetens föreskrift fastställda krav på informationssäkra driftmiljöer.

Social- och hälsovårdsministeriet ordnade en remissrunda om utkastet till regeringens proposition 10.6.2022–29.7.2022. Kompletteras på basis av remissrundan.

Beredningsunderlaget till regeringens proposition finns i den offentliga tjänsten på adressen https://stm.fi/sv/projekt-och-lagberedning med identifieringskoden STM154:00/2021.

2 Nuläge och bedömning av nuläget

2.1 Allmänt

Syftet med lagen om sekundär användning är att möjliggöra en effektiv och informationssäker behandling av personuppgifter som har registrerats i social- och hälsovårdsverksamhet och för styrnings-, tillsyns-, forsknings- och statistikändamål inom social- och hälsovården samt en samkörning av dessa personuppgifter med Folkpensionsanstaltens, Befolkningsregistercentralens, Statistikcentralens och Pensionsskyddscentralens personuppgifter. Ett primärt mål för lagen om sekundär användning är att i all sekundär behandling av personuppgifter inom social-

[3] Det bör dock beaktas att nationella uppsättningar av kriterier, såsom Vahti och Katakri, grundar sig på allmänna informationssäkerhetsprinciper och delvis på internationella standarder, såsom ISO/IEC 27001.

och hälsovården skydda personuppgifterna så att allmänhetens förtroende för sekundär användning av deras personuppgifter kan stärkas. Lagen om sekundär användning möjliggör bättre informationssäkerhet än tidigare vid sekundär behandling av känsliga personuppgifter inom social- och hälsovården.

En informationssäker driftmiljö är en av de viktigaste skyddsåtgärderna i lagen om sekundär användning, genom vilka man säkerställer behandlingen av känsliga personuppgifter i en trygg miljö och tryggar skyddet av personens personuppgifter. Övriga centrala skyddsåtgärder beskrivs på sidan 32 i regeringens proposition om ändring av 60 § i lagen om sekundär användning (RP 96/2021 rd). Med en informationssäker driftmiljö kan man förebygga missbruk och verkställa cybersäkerhet vid användning av personuppgifter för sekundära ändamål. I Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan *dataskyddsförordningen*) förutsätts tillräckliga skyddsåtgärder när man behandlar känsliga och särskilda kategorier av personuppgifter.

I 60 § i lagen om sekundär användning fastställdes en övergångstid varefter personuppgifter endast kan utlämnas för behandling i en informationssäker driftmiljö. I samband med beredningen av lagen om sekundär användning uppskattades det ta omkring två år att skapa informationssäkra driftmiljöer efter det att lagen godkänts och övergångstiden föreslogs då löpa ut den 1 maj 2021. Övergångstiden förlängdes med ett år genom en lag om ändring av lagen om sekundär användning av personuppgifter inom social- och hälsovården (793/2021), enligt vilken övergångstiden löpte ut den 1 maj 2022.

I samband med beredningen av regeringens proposition om ändring av 60 § i lagen om sekundär användning (RP 96/2021 rd) hade man konstaterat att i informationssystemen som är avsedda för forskare inte genomförts alla dataskydds- och säkerhetskrav som förutsätts i lagen om sekundär användning och att ingen aktör, bortsett från Tillståndsmyndigheten, fram till den 1 maj 2021 hade en sådan informationssäker driftmiljö som förutsätts i 20 § i lagen om sekundär användning och till vilken datamaterial får lämnas ut för att behandlas av tillståndshavaren. Genom att förlänga övergångstiden ville man trygga forskningen inom hälso- och sjukvården och ge mer tid till aktörerna att revidera informationssäkra driftmiljöer som passar deras behov.

Lagen om sekundär användning möjliggör inrättande av flera informationssäkra driftmiljöer, så länge de uppfyller informationssäkerhetskraven i lagen om sekundär användning. Flera informationssäkra driftmiljöer behövs för att forskarna ska kunna välja den lämpligaste driftmiljön för sin forskning och olika driftmiljöer kan specialisera sig på behandlingen av visst material. Till exempel universitetssjukhusen kan för sin forskning behöva datamaterial, för vars behandling det behövs specialkunnande och specialutrustning. Som exempel kan nämnas hälso- och sjukvårdens bilddiagnostiska material (till exempel röntgenbilder, ultraljudsbilder och EKG), som omfattas av tillämpningsområdet för lagen om sekundär användning. Behandlingen av bilddiagnostiskt material kräver utrustning och programvara som endast finns hos aktörer inom hälso- och sjukvården. Behandlingen av bilddiagnostiskt material förutsätter också nästan alltid att behandlingen görs av eller i den deltar en läkare som specialiserat sig på området i fråga.

Vid tidpunkten för färdigställande av denna regeringsproposition har det förutom Tillståndsmyndighetens informationssäkra driftmiljö reviderats sex andra; samkommunen Helsingfors och Nylands sjukvårdsdistrikts HUS Academic, Istekki Oy:s T3 Tutkijan työtila, ESiOR Oy:s SPESiOR, Helsingfors universitets FinnGen Sandbox, CSC Tieteen tietotekniikan keskus Oy:s SD Desktop och Statistikcentralens driftmiljö Fiona. Driftmiljöerna registreras i det register

över driftmiljöer som förs av Tillstånds- och tillsynsverket för social- och hälsovården (nedan *Valvira*).[4]

Den nuvarande regleringen möjliggör användning av finländska registeruppgifter inom internationellt forskningssamarbete, om forskarna vid behandlingen av uppgifterna använder driftmiljöer som reviderats enligt lagen om sekundär användning. Det är möjligt för forskare att genom distansuppkoppling få tillträde till antingen Tillståndsmyndighetens eller en annan finländska aktörs reviderade driftmiljö och att där behandla finländska registeruppgifter. För att forskaren flexibelt ska kunna kombinera och analysera registeruppgifter i förhållande till andra uppgifter som behandlas inom forskningen, ska forskaren eller forskningsgruppen överföra datamaterialet i sin helhet till den finländska driftmiljön. Det är möjligt att överföra allt datamaterial som behandlas inom forskningen till en driftmiljö enligt lagen om sekundär användning och behandla den där inom ramen för nuvarande reglering. Användningen finländska registeruppgifter i internationellt forskningssamarbete skulle främjas av att driftmiljöer som forskare använder revideras av bedömningsorgan för informationssäkerhet i enlighet med kraven i lagen om sekundär användning och Tillståndsmyndighetens föreskrift inom EU- och EES-området. Utländska aktörer har dock inte hittills börjat revidera sina driftmiljöer i överensstämmelse med lagen om sekundär användning.

Användningen av finländska registeruppgifter i det internationella forskningssamarbetet kunde främjas genom att kraven på informationssäkra driftmiljöer i lagen om sekundär användning ändras så att de uppgifter som avses i lagen om sekundär användning kan lämnas ut också till driftmiljöer som befinner sig utanför Finland.

2.2 Standard, certifiering och ackreditering

Genom certifieringar och revideringar övervakas uppfyllandet av kraven och skapas förtroende. Genom standardisering kan man utveckla verksamhetens kvalitet, säkerhet och transparens. I central ställning med tanke på standardiseringens genomslag är det faktum att standarderna är internationella, att standardiseringsprocessen är öppen, snabb, förutsägbar och flexibel samt föremålet för standardiseringen. Standardiseringens genomslag kan effektiviseras genom certifiering, som berättar att de krav som fastställts i standarden uppfylls. Också tillgängligheten påverkar omfattningen av användningen av standarden och dess genomslag. Vid fastställandet av revideringarnas kvalitet är också ackrediteringen, det vill säga konstaterandet av att de instanser som gör revideringar är kompetenta, viktig.[5]

Informationssäkerheten standardiseras inom många olika branscher på såväl europeisk som internationell nivå. Med officiell standardisering avses internationella, europeiska och nationella standardiseringsorganisationer, vars medlemskap är landsspecifikt. De officiella standardiseringsorganisationerna, såsom det internationella standardiseringsorganet ISO (International Organization for Standardization) är etablerade och välkända. Som exempel på standarder kan nämnas ISO/IEC 27001 och CSA STAR. Den internationella kravstandarden som gäller informationssäkerhet är ISO/IEC 27001 för ledningssystem för informationssäkerhet som är en av de

[4] https://www.valvira.fi/web/sv/halso-och-sjukvard/informationssystem-inom-social-och-halsovarden/informationssakra-driftsmiljoer-i-enlighet-med-lagen-om-sekundar-anvandning-av-personuppgifter-inom-social-och-halsovarden/register-over-sekundara-driftsmiljoer

[5] Traficom: Redogörelsen Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin 2019, s. 3 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf.

internationellt mest kända och använda standarderna för hantering av en organisations informationssäkerhet. CSA STAR är en internationellt erkänd certifiering som utvecklats för leverantörer av molntjänster och som grundar sig på Cloud Controls Matrix som utvecklats av den icke-vinstdrivande amerikanska organisationen Cloud Security Alliance.[6]

Certifiering är enligt definitionen bedömning av överensstämmelse. Tillämpningar som bevisligen uppfyller kraven på överensstämmelse kan beviljas godkännande eller ett certifikat, som beviljas av en oberoende tredje part. Certifikat kan till exempel beviljas it-tjänstehanteringssystem, leverantörer av molntjänster och tekniska lösningar. Bakom certifieringen finns ofta kundens krav. Certifikatet är i vissa situationer också en konkurrensfaktor, med hjälp av vilken man kan skilja sig från konkurrenterna som ett mer riskfritt alternativ.[7]

Certifieringsorganet bedömer om det system som ska certifieras uppfyller certifieringskraven. På basis av bedömningen utfärdar certifieringsorganet ett intyg där det konstateras att ledningssystemet, produkten, processen eller personen uppfyller vissa krav. Certifieringen gäller en viss tid, varefter man kan göra en ny certifiering.[8]

Ackreditering betyder konstaterande av kompetens på ett opartiskt och oberoende sätt. Ackrediterade certifieringsorgan är opartiska och av objektet för certifieringen oberoende aktörer för en tredje part som ska ha en i internationella standarder fastställd kompetens och övriga förutsättningar för sin verksamhet.[9] I varje EU-land finns det ett nationellt ackrediteringsorgan enligt EU-lagstiftningen och i Finland är det FINAS (Finnish Accreditation Service) som är ackrediteringsorgan.

Ackrediteringen ger kunderna en uppfattning om att verksamheten är kompetent, trovärdig och tillförlitlig samt gör tolkningen av kraven enhetligare och ökar interoperabiliteten. Dessutom främjar ackrediteringen funktionen för EU:s inre marknad genom att det säkerställs att man internationellt kan lita på kvaliteten på de tjänster som en ackrediterad aktör producerar och på aktörens tolkning av standarden. Av dessa orsaker bör endast ackrediterade aktörer användas vid certifieringar.[10]

ISO 27001–standarden

Internationella standardiseringsorganisationens standard ISO/IEC 27001 för ledningssystem för informationssäkerhet är en internationell officiell kravstandard som gäller ledningssystemet för informationssäkerhet. Centralt i ISO 27001–standarden är att ledningen engagerar sig för informationssäkerhet, kontinuerlig förbättring och ett riskbaserat val av metoder för hantering av informationssäkerheten. Standarden har utarbetats så att till hanteringssystemet också kan fogas andra metoder för hantering av informationssäkerheten (kontroller) än de som följer av ISO 27001–standarden.

---

[6] Traficom: Redogörelsen Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 7–8.
[7] Traficom: Redogörelsen Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 13.
[8] Se https://www.finas.fi/sites/sv/ackreditering/Sidor/default.aspx
[9] Se https://www.finas.fi/sites/sv/ackreditering/Ackrediteringsaktivitet/Sidor/Certifieringsorgan.aspx
[10] Traficom: Redogörelsen Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 14.

ISO 27001–standarden är en internationellt allmänt tillämpad etablerad standard som anses vara tillförlitlig. Det finns över 40 000 certifierade organisationer och i Finland finns det omkring 100 gällande ISO 27001-certifieringar. Ackrediterade ISO 27001-certifieringsorgan finns i så gott som alla länder. Certifieringsorganen kan också certifiera andra ledningssystem för informationssäkerhet än sådana som är belägna i deras etableringsland.[11]

CSA STAR-standarden

Cloud Security Alliances (CSA) Security, Trust, Assurance and Risk Registry (STAR)-standard har riktats särskilt till leverantörer av molntjänster som ett redskap för att påvisa att de tjänster de erbjuder stämmer överens med kraven. Vid certifieringen utnyttjas kraven i standarden ISO/IEC 27001 för ledningssystem för informationssäkerhet tillsammans med CSA:s metod Cloud Controls Matrix (CCM). CSA STAR-standarden håller på att bli allmännare, men är dock inte väldigt vanlig hos små aktörer.

STAR-certifieringen grundar sig på IEC 27001-standarden och uppnåendet av de kriterier som läggs fram i matrisen för kontroll av molntjänsten, dvs. CCM, som kan anses vara tilläggskontroller enligt IEC 27001–standarden. Således gäller inget certifikat som gäller CCM-bedömning utan ett anslutande ISO 27001-certifikat vars tillämpningsområde är minst lika stort som STAR-certifieringens.[12]

2.3 Krav på informationssäkra driftmiljöer i lagen om sekundär användning

I 18 § i lagen om sekundär användning ställs allmänna informationssäkerhetskrav för sekundär användning. En tillräcklig informationssäkerhet för behandlingen ska säkerställas genom riskhantering, åtkomsthantering, aktiv övervakning och genom iakttagande av föreskrifter och anvisningar från den myndighet som svarar för förverkligandet och övervakningen av informationssäkerhet och dataskydd. Särskild uppmärksamhet ska fästas vid att användningsbegränsningar och sekretessplikten iakttas.

I 20–30 § i lagen om sekundär användning ställs krav på en informationssäker driftmiljö. Enligt 20 § 1 mom. i lagen om sekundär användning ska Tillståndsmyndigheten ensam eller tillsammans med andra myndigheter förvalta en informationssäker driftmiljö som gör det möjligt att garantera en informationssäker, tillståndsenlig behandling av uppgifter som Tillståndsmyndigheten eller någon annan myndighet som avses i den lagen lämnat ut med stöd av den lagen.

En informationssäker driftmiljö inbegriper bland annat terminalutrustning, servrar, arbetsstationer, operativsystem och systemprogramvara samt lednings- och informationssäkerhetspraxis, som inte är en del av informationssystemet eller informationssystemtjänsten. I en informationssäker driftmiljö ingår också administreringen av informationssäkerhetsprocesserna och ledningssystem inklusive säkerhet för personal, utrustning, telekommunikation, drift och programvara samt fysisk säkerhet (RP 159/2017 rd, s. 96).

Enligt 20 § i lagen om sekundär användning lämnas personuppgifter i första hand ut till Tillståndsmyndighetens informationssäkra driftmiljö. Om ansökan om dataanvändningstillstånd innehåller en begäran om att datamaterial ska lämnas ut för behandling i en annan miljö än Tillståndsmyndighetens driftmiljö, ska det enligt 20 § 3 mom. i lagen om sekundär användning i ansökan särskilt motiveras varför detta är nödvändigt. Tillståndsmyndigheten eller någon annan

[11] Nixu Certification AB:s redogörelse, april 2022.
[12] Nixu Certification AB:s redogörelse, april 2022.

myndighet som avses i lagen om sekundär användning får då lämna ut uppgifter till sökanden endast om driftmiljön uppfyller villkoren i den lagens 20 § 2 mom. och i 21–29 §.

Enligt 21 § 1 mom. i lagen om sekundär användning ska användarna i en informationssäker driftmiljö identifieras på ett tillförlitligt sätt och verifieras. I 22 § i lagen om sekundär användning föreskrivs om åtkomsträttigheter för användare i informationssäkra driftmiljöer och enligt 22 § 3 mom. meddelar Tillståndsmyndigheten föreskrifter om de grunder enligt vilka tjänsteleverantören ska specificera tillståndshavarens åtkomsträttigheter till kunduppgifterna.

Enligt 23 § 1 mom. i lagen om sekundär användning ska en informationssäker driftmiljö skyddas i enlighet med statliga myndigheters skyldigheter i fråga om informationssäkerhet enligt vad som föreskrivs i 36 § i offentlighetslagen och i den statsrådsförordning som utfärdats med stöd av 1 mom. i den paragrafen. Bestämmelser om informationssäkerhet i fråga om informationsmaterial och informationssystem finns för närvarande i 4 kap. i lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan *informationshanteringslagen*). I 18 § i informationshanteringslagen föreskrivs om handlingar som ska säkerhetsklassificeras inom statsförvaltningen. Närmare bestämmelser om säkerhetsklassificering, anteckningar i säkerhetsklassificerade handlingar och informationssäkerhetsåtgärder som anknyter till behandlingen av säkerhetsklassificerade handlingar finns i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019).

Enligt 24 § 1 mom. i lagen om sekundär användning ska informationssäkra driftmiljöer uppfylla kraven på informationssäkerhet och interoperabel informationsöverföring som bygger på myndigheternas föreskrifter, rekommendationer och de standarder som enligt dessa lämpar sig för en informationssäker driftmiljö. Enligt 24 § 2 mom. i lagen om sekundär användning meddelar Tillståndsmyndigheten närmare föreskrifter om de krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. Kraven ska förutsätta informationssäkerhet på motsvarande nivå som i Tillståndsmyndighetens egen driftmiljö.

Informationssäkra driftmiljöer ska revideras av bedömningsorgan enligt lagen om bedömningsorgan för informationssäkerhet (1405/2011) i enlighet med bestämmelserna om informationssäkerhet i lagen om sekundär användning. Informationssäkerheten i driftmiljön ska enligt 25 § i lagen om sekundär användning påvisas genom ett i 26 § avsett intyg från ett bedömningsorgan för informationssäkerhet. Tillståndsmyndigheten får meddela närmare föreskrifter om de förfaranden som ska iakttas vid påvisande av informationssäkerhet.

I 26 § i lagen om sekundär användning ställs krav på bedömningen av informationssäkerheten i driftmiljöer. Enligt 26 § 1 mom. i lagen om sekundär användning bedömer ett bedömningsorgan för informationssäkerhet i enlighet med den lagen och lagen om bedömningsorgan för informationssäkerhet, på ansökan av tjänsteleverantören, om driftmiljön uppfyller kraven på informationssäkerhet. Som bedömningskriterier ska användas föreskrifter om kraven på en säker driftmiljö från Tillståndsmyndigheten.

Om driftmiljön uppfyller informationssäkerhetskraven enligt lagen om sekundär användning, ska bedömningsorganet för informationssäkerhet enligt 26 § 2 mom. i den lagen ge tjänsteleverantören ett intyg över sin bedömning och en anknytande kontrollrapport. Om bedömningen eller en förnyad bedömning gäller endast en del av driftmiljön, ska det i bedömningsorganets intyg tydligt antecknas vilken del av driftmiljön som har bedömts.

Enligt 26 § 3 mom. i lagen om sekundär användning är bedömningsorganets intyg i kraft högst fem år. Bedömningsorganet för informationssäkerhet kan av tjänsteleverantören kräva alla de uppgifter som förutsätts för bedömningen och för uppgörandet och upprätthållandet av intyget.

På utfärdande av intyget tillämpas i övrigt 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet.

I 27 § i lagen om sekundär användning föreskrivs om de förutsättningar under vilka ett bedömningsorgan kan återkalla ett intyg som det beviljat. Enligt 28 § i lagen om sekundär användning ska bedömningsorgan för informationssäkerhet underrätta Tillstånds- och tillsynsverket för social- och hälsovården om alla intyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats samt om de uppmaningar och begränsningar som avses i 27 §. Dessutom ska bedömningsorgan för informationssäkerhet på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

Enligt 29 § 1 mom. i lagen om sekundär användning ska tjänsteleverantören ge akt på ändringar i den lagen och justera driftmiljön i enlighet med ändringarna. Väsentliga förändringar i driftmiljön ska anmälas till bedömningsorganet för informationssäkerhet. Bedömningsorganets intyg ska förnyas, om betydande förändringar görs i driftmiljön eller om minimikraven på driftmiljön har ändrats på ett sätt som förutsätter en förnyad bedömning.

I 30 § i lagen om sekundär användning föreskrivs det att Tillstånds- och tillsynsverket för social- och hälsovården ska övervaka och främja att informationssäkra driftmiljöer uppfyller kraven på dataskydd och informationssäkerhet. Tillstånds- och tillsynsverket för social- och hälsovården för ett offentligt register över driftmiljöer som uppfyller kraven och som anmälts till verket. Tillstånds- och tillsynsverket för social- och hälsovården har rätt att utföra inspektioner som krävs för tillsynen.

I 52 § i lagen om sekundär användning föreskrivs det om publicering av resultat baserade på uppgifter utlämnade med stöd av ett dataanvändningstillstånd. När uppgifter lämnats ut med stöd av ett dataanvändningstillstånd för behandling i en informationssäker driftmiljö och någon vill publicera resultatet utifrån uppgifterna ska Tillståndsmyndigheten försäkra sig om att de uppgifter som publiceras är anonymiserade. Myndigheten kan emellertid av grundad anledning i tillståndsbeslutet bevilja tillståndshavaren rätt att själv anonymisera de uppgifter som ska publiceras, förutsatt att uppgifterna ges in till myndigheten i efterhand. Tillståndsmyndigheten producerar anonymiserade resultat och överlämnar dem till tillståndshavaren som får publicera dem fritt enligt sin begäran och de bifogade förslagen oberoende av om dataanvändningstillståndet beviljats av en enskild personuppgiftsansvarig eller Tillståndsmyndigheten.

2.4 Krav på informationssäkra driftmiljöer i Tillståndsmyndighetens föreskrift

Enligt 24 § 2 mom. i lagen om sekundär användning meddelar Tillståndsmyndigheten närmare föreskrifter om de krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. Den första föreskriften om informationssäkra driftmiljöer publicerades den 5 oktober 2020. Tillståndsmyndigheten publicerade en uppdaterad version av föreskriften den 19 januari 2022.[13]

Föreskriften tillämpas på alla de ändamål som föreskrivs i lagen om sekundär användning, för vilka det behövs dataanvändningstillstånd. Sådana ändamål är vetenskaplig forskning, statistikföring, undervisning samt myndighetens planerings- och utredningsuppgifter. När det gäller undervisning gäller föreskriften utarbetande av undervisningsmateriel, inte undervisningen i sig.

[13] https://findata.fi/sv/tjanster-och-anvisningar/foreskrifter/

Fullgörande av kraven enligt föreskriften är från och med den 1 maj 2022 en förutsättning för att uppgifter får lämnas ut för att behandlas av tillståndshavaren för sekundära ändamål i någon annan driftmiljö än Tillståndsmyndighetens informationssäkra driftmiljö i enlighet med 20 § 3 mom. i lagen om sekundär användning.

Om ansökan om dataanvändningstillstånd innehåller en begäran om att datamaterial ska lämnas ut för behandling i en annan driftmiljö än Tillståndsmyndighetens informationssäkra driftmiljö, ska det enligt 20 § 3 mom. i lagen om sekundär användning i ansökan särskilt motiveras varför detta är nödvändigt. Tillståndsmyndigheten eller någon annan myndighet som avses i lagen om sekundär användning får då lämna ut uppgifter till sökanden endast om driftmiljön uppfyller villkoren i 20 § 2 mom. och i 21–29 §. Om en enskild personuppgiftsansvarig som avses i 44 § 3 mom. i lagen om sekundär användning har fattat ett beslut om dataanvändningstillstånd i fråga om uppgifter i dess egna register, ska den personuppgiftsansvarige alltid lämna ut datamaterialet för behandling av tillståndshavaren i en sådan informationssäker driftmiljö som avses i 20 § i lagen om sekundär användning.

Uppfyllandet av kraven enligt föreskriften påvisas med ett intyg som utfärdats av ett

bedömningsorgan för informationssäkerhet enligt 26 § i lagen om sekundär användning Intyget beviljas på basis av observationerna i kontrollrapporten. För att intyget ska kunna beviljas får kontrollrapporten inte innehålla några observationer som klassificeras som allvarliga avvikelser enligt föreskriften.

Klassificeringen av avvikelser sker som en del av den bedömning som bedömningsorganet för informationssäkerhet gör så att avvikelserna klassificeras på basis av allvarliga avvikelser, avvikelser på medelnivå och lindriga avvikelser. Om det i kontrollrapporten konstateras en eller flera observationer som enligt

denna föreskrift klassificeras som en avvikelse på medelnivå, ska kontrollrapporten även innehålla en reparationsplan som godkänts av bedömningsorganet och i vilken också fastställs en tidsfrist för slutförandet av den nya bedömningen i enlighet med reparationsplanen. Den nya bedömningen ska göras med godkänt resultat senast 6 månader efter det att kontrollrapporten har färdigställts. Andra än allvarliga avvikelser bedöms inte tillsammans utgöra en avvikelse som klassificeras som allvarlig.

Det bedömningsorgan för informationssäkerhet som gör bedömningen och beviljar intyget bedömer om tjänsteleverantörens gällande intyg som gäller en informationssäker driftmiljö och hänger samman med informationssäkerheten lämpar sig för påvisande av överensstämmelse med de krav som anges i föreskriften. De delar av föremålet för bedömning som inte omfattas av ett befintligt intyg ska bedömas separat. Bedömningsorganet kontrollerar giltighetstiden för tjänsteleverantörens gällande intyg och fastställer vid behov en begränsning för giltighetstiden för det intyg som beviljas på basis av denna föreskrift.

I informationssäkerhetskraven hänvisas bland annat till verktyget för informationssäkerhetsauditering för myndigheter (Katakri[14]) och till säkerhetskriterierna för molntjänster (PiTuKri[15]). Bedömningsorganet har en möjlighet att basera sin bedömning på kraven enligt PiTuKri i stället för Katakri i fråga om objekt där det i fråga om det objekt som ska bedömas är ändamålsenligt. I informationssäkerhetskraven hänvisas dessutom till dataskyddsförordningen och till Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. I kraven nämns dessutom ISO/IEC 27001-standarden.

En informationssäker driftmiljö ska ha en namngiven tjänsteleverantör som ansvarar för att den informationssäkra driftmiljön och de parter som deltar i produktionen av den iakttar de krav som fastställts i föreskriften. Tjänsteleverantören kan anlita underleverantörer till exempel för att producera informationstekniska tjänster, men tjänsteleverantören ansvarar alltid för att en

informationssäker driftmiljö överensstämmer med kraven. I praktiken måste det finnas ett bindande avtalsförhållande mellan tjänsteleverantören och underleverantören.

Tjänsteleverantören ska också identifiera en eventuell kumulativ effekt av personuppgifterna och beakta detta i skyddet av den driftmiljö som tjänsteleverantören tillhandahåller. Kumulativa effekter kan uppstå till exempel i situationer där avsikten är att lagra flera personuppgiftsmaterial i driftmiljön och/eller materialets storlek blir stor. Valvira för ett offentligt register över driftmiljöer som uppfyller kraven och anmälts till verket.

I tillståndsmyndighetens föreskrift fastställs tekniska krav för identifiering, hantering av användare och åtkomsträttigheter, skydd av miljön, loggning, hantering och övervakning av miljön och avlägsnande av material från driftmiljön samt krav på aktörens tillförlitlighet, dataskydd, lokaler och personal.

3 Målsättning

Syftet med regeringens proposition är att möjliggöra användning av finländska registeruppgifter inom internationellt forskningssamarbete samtidigt som man säkerställer en hög nivå av informationssäkerhet och dataskydd. I denna proposition föreslås det att kraven på informationssäkra driftmiljöer i lagen om sekundär användning av personuppgifter inom social- och hälsovården ändras så att kraven möjliggör utlämnande av i lagen avsedda uppgifter till andra informationssäkra driftmiljöer än sådana som är belägna i Finland.

[14] Katakri är ett auditeringsverktyg som myndigheterna kan använda när de bedömer den berörda organisationens förmåga att skydda myndighetens sekretessbelagda information. Katakri kan användas som auditeringsverktyg när man bedömer företagets säkerhetsarrangemang i samband med säkerhetsutredningen av företag och säkerheten i myndigheternas informationssystem. Det kan också användas som hjälp i företags, sammanslutningars och myndigheters säkerhetsarbete i övrigt och i dess utveckling. Se https://um.fi/katakri-verktyg-for-informationssakerhetsauditering-for-myndigheter.

[15] Syftet med säkerhetskriterierna för molntjänster (PiTuKri) är att förbättra säkerheten för sekretessbelagd myndighetsinformation som behandlas i molntjänster. Kriterierna är ett bedömningsverktyg som hjälper avgöra hur säker en molntjänst är. Kriterierna har utarbetats med tanke på Finlands nationella behov. Se https://www.kyberturvallisuuskeskus.fi/sv/publikationer/sakerhetskriterier-molntjanster-pitukri.

De informationssäkra driftmiljöerna ska för att säkerställa en hög nivå av dataskydd och informationssäkerhet uppfylla de krav på informationssäkerhet som uppställs i lagen om sekundär användning och Tillståndsmyndighetens föreskrift. Säkerställandet av en hög nivå av dataskydd och informationssäkerhet är särskilt viktigt när man behandlar känsliga uppgifter och uppgifter som hör till särskilda kategorier av personuppgifter.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

I regeringens proposition föreslås det att kraven på informationssäkra driftmiljöer i lagen om sekundär användning ska ändras så att de krav som lagen och Tillståndsmyndighetens föreskrift fastställt ska kunna uppfyllas också genom iakttagande av internationella standarder och förfaranden som fastställts i Tillståndsmyndighetens föreskrift. Dessutom kan bedömningarna av informationssäkra driftmiljöers överensstämmelse med kraven utöver av bedömningsorgan för informationssäkerhet som godkänts av Traficom genomföras av ackrediterade certifieringsorgan. Det ackrediterade certifieringsorganet levererar intyget över att den informationssäkra driftmiljön stämmer överens med kraven till Valvira, som fogar uppgiften om driftmiljön till det register över driftmiljöer som Valvira för.

I lagen om sekundär användning ska föreskrivas om kraven på informationssäkra driftmiljöer endast på allmän nivå och de närmare bestämmelserna om kraven ska utfärdas av Tillståndsmyndigheten i enlighet med 24 § i lagen om sekundär användning. Tillståndsmyndighetens föreskrift ska utvecklas så att de krav som fastställs i den utöver genom att iaktta nationella krav också ska kunna uppfyllas genom iakttagande av internationella standarder och förfaranden, Tillståndsmyndigheten ska kunna uppdatera kraven på informationssäkra driftmiljöer på ett smidigt sätt, så att de möjliggör beaktande av de senaste standarderna och förfarandena vid bedömningen av driftmiljöerna.

Tillståndsmyndigheten ska i sin föreskrift kunna fastställa de ackrediterade certifieringsorgan som anses ha tillräckliga förutsättningar att bedöma informationssäkra driftmiljöers överensstämmelse med kraven på basis av de krav som fastställt i lagen om sekundär användning och Tillståndsmyndighetens föreskrift,

I Tillståndsmyndighetens föreskrift ska listas de tillämpliga internationella standarder och förfaranden som kan räknas till godo för uppfyllande av de krav som fastställts i föreskriften. Dessutom ska i föreskriften beskrivas vilka krav som inte kan uppfyllas genom iakttagande av internationella standarder och förfaranden och vilkas uppfyllande således bör bedömas separat, På basis av kombinationen av de internationella standarderna och tilläggsbedömningarna kan man bedöma om den informationssäkra driftmiljön uppfyller de krav som fastställts i lagen om sekundär användning och Tillståndsmyndighetens föreskrift.

De föreslagna ändringarna är motiverade, eftersom kombinationen av internationella standarder och tilläggsbedömningar kan säkerställa en hög nivå av dataskydd och informationssäkerhet som förutsätts för utlämnande av uppgifter till en informationssäker driftmiljö. Tillståndsmyndigheten och andra i lagen om sekundär användning avsedda myndigheter ska kunna lämna ut datamaterial på basis av en begäran om information såväl till driftmiljöer som revideras av bedömningsorgan för informationssäkerhet som till driftmiljöer som revideras av ackrediterade certifieringsorgan och som antecknats i Valviras register över driftmiljöer.

4.2 De huvudsakliga konsekvenserna

4.2.1 Ekonomiska konsekvenser

Förslaget kan ha ekonomiska konsekvenser för företag och andra aktörer, såsom forskningssamfund, som reviderar en informationssäker driftmiljö i enlighet med lagen om sekundär användning eller behandlar personuppgifter i driftmiljön. Öppnandet av flera informationssäkra driftmiljöer ökar konkurrensen och möjliggör specialisering av driftmiljöerna på behandling av vissa slags uppgifter, Dessutom kan öppnandet av flera driftmiljöer minska de avgifter som tas ut av användarna för behandlingen av uppgifter i driftmiljön.

Redan i nuvarande reglering förutsätts användning av informationssäkra driftmiljöer när de uppgifter som lämnas ut är personuppgifter. Förslaget gör det endast möjligt att uppfylla kraven på informationssäkra driftmiljöer med internationella standarder och förfaranden och dessutom ska det vara möjligt att påvisa överensstämmelse med kraven genom en bedömning som utförs av ett ackrediterat certifieringsorgan.

Uppfyllandet av informationssäkerhetskraven ökar företags och andra aktörers kostnader, om de verkställer en driftmiljö enligt lagen om sekundär användning och Tillståndsmyndighetens föreskrift. Å andra sidan är avsikten med förslaget att det för uppfyllande av kraven ska vara möjligt att använda internationella standarder och förfaranden i allmänt bruk, vilkas ibruktagande inte medför oskäliga kostnader för företagen eller andra aktörer. Det kan också beaktas att aktörer som behandlar personuppgifter ska verkställa lämpliga informationssäkerhetsåtgärder i sin verksamhet redan med stöd av EU:s dataskyddslagstiftning och den nationella reglering som gäller dem.

Anskaffande av certifikat genom vilka man påvisar iakttagande av en internationell standard kan vara enklare för större aktörer än för medelstora och små aktörer, Kostnaderna för certifiering kan vara stora framför allt för mindre aktörer.[16] Redan de nuvarande bestämmelserna orsakar vissa kostnader för aktörerna om de vill revidera en informationssäker driftmiljö i enlighet med lagen om sekundär användning. Iakttagandet av internationella standarder kan medföra konkurrensfördelar för en aktör och ett rykte som tillförlitlig aktör vars dataskydds- och informationssäkerhetsärenden är i sin ordning.

Det ska fortfarande vara möjligt för finländska aktörer att påvisa informationssäkra driftmiljöers överensstämmelse med kraven med ett intyg som utfärdats av ett bedömningsorgan för informationssäkerhet. Å andra sidan ska aktören också kunna besluta använda internationella standarder och certifieringar, och överensstämmelsen med kraven ska också kunna påvisas med ett intyg som utfärdats av ett ackrediterat certifieringsorgan. Förslaget ökar flexibiliteten när det gäller påvisande av informationssäkra driftmiljöers överensstämmelse med kraven.

4.2.2 Konsekvenser för myndigheterna

Förslaget påverkar Tillståndsmyndighetens, i 6 § i lagen om sekundär användning avsedda myndigheters samt Valviras verksamhet.

[16]Förbättring av datasäkerheten och dataskyddet i samhällets kritiska områden: Arbetsgruppens slutrapport 2021, s. 55.

Tillståndsmyndighetens och i 6 § i lagen om sekundär användning avsedda myndigheters verksamhet påverkar förslaget så att de kan begäras lämna ut i lagen om sekundär användning avsedda uppgifter till informationssäkra driftmiljöer annanstans än i Finland. Myndigheterna ska då kontrollera att den som begär ett dataanvändningstillstånd har tillgång till en informationssäker driftmiljö enligt lagen om sekundär användning som fogats till det register över driftmiljöer som förs av Valvira.

Genomförandet av förslaget förutsätter att Tillståndsmyndighetens föreskrift revideras och utredningsarbete i anslutning till detta i fråga om motsvarigheten mellan internationella standarder och de krav som fastställs i föreskriften. Över motsvarigheten mellan internationella standarder och förfaranden och de krav som fastställts i föreskriften bör det utarbetas en motsvarighetstabell med hjälp av vilken man kan fastställa vilka av föreskriftens krav kan uppfyllas genom iakttagande av internationella standarder eller förfaranden. Dessutom bör i utredningsarbetet bedömas till vilka delar de krav som uppställs i Tillståndsmyndighetens föreskrift inte kan uppfyllas med internationella standarder och hur många krav som bör bedömas genom en tilläggsbedömning. För närvarande är den direkta motsvarigheten mellan Tillståndsmyndighetens föreskrift och internationella standarder liten och motsvarigheten borde ökas genom att ändra föreskriften mer i enlighet med de internationella standarderna, så att den föreslagna lösningen kunde genomföras.[17]

Arbetet för att förnya och utreda Tillståndsmyndighetens föreskrift, inklusive utarbetandet av en motsvarighetstabell, kan bedömas kräva resurser uppgående till cirka 640 timmar och den uppskattade kostnaden till cirka 150 000 euro.[18]

Förslaget kommer att påverka Valviras verksamhet så att också andra informationssäkra driftmiljöer än sådana som bedömts av bedömningsorgan för informationssäkerhet kan godkännas till registret över driftmiljöer på basis av ett intyg av ett ackrediterat certifieringsorgan. Dessutom ska Valvira utöver intygen ta emot kontrollrapporter över bedömningarna.

Förslaget försvårar den uppgift som givits Valvira i den nuvarande lagstiftningen att övervaka och främja att informationssäkra driftmiljöer uppfyller kraven på dataskydd och informationssäkerhet. Det är sannolikt att Valvira inte i praktiken har möjlighet att övervaka överensstämmelsen med kraven för andra informationssäkra driftmiljöer än sådana som är belägna i Finland. Dessutom kan de kontroller som hör till övervakningen inte genomföras utanför Finland.

Av denna anledning ges certifieringsorganen i förslaget i uppgift att övervaka och främja att de informationssäkra driftmiljöer som de bedömt uppfyller kraven på dataskydd och informationssäkerhet. Valvira kunde utfärda närmare föreskrifter om övervakningen av informationssäkra driftmiljöer.

De föreslagna ändringarna hänger samman med Valviras nuvarande uppgifter och orsakar således inte Valvira några betydande ytterligare uppgifter eller kostnader.

[17] Nixu Certification AB:s uppskattning, april 2022.
[18] Nixu Certification AB:s uppskattning, april 2022.

4.2.3 Övriga samhälleliga konsekvenser

4.2.3.1 Konsekvenser för medborgarnas ställning och verksamhet i samhället

Förslaget har konsekvenser för skyddet för personers privatliv och deras personuppgifter. I regeringens proposition om lagen om sekundär användning (RP 159/2017 rd) bedömdes konsekvenserna av sekundär användning för medborgarnas ställning. Syftet med lagen om sekundär användning är att förbättra skyddet för de registrerades personuppgifter genom att fastställa krav på informationssäkerhet för behandling av personuppgifter i sekundärt syfte. Personuppgifter kan endast behandlas i en informationssäker driftmiljö där informationssäkerheten har säkerställts genom ändamålsenliga administrativa och tekniska åtgärder och med ändamålsenliga standarder för informationssystemen.

I förslaget ändras inte denna grundprincip, utan personuppgifter ska fortfarande kunna lämnas ut endast till driftmiljöer som uppfyller kraven i lagen om sekundär användning och Tillståndsmyndighetens föreskrift, Endast de metoder med vilka överensstämmelsen med kraven kan påvisas ändras och blir mer mångsidiga, Utgångspunkten är att en överensstämmelse med kraven som påvisats med internationella standarder och metoder ska garantera en minst lika god informationssäkerhetsnivå som nuvarande nationella krav.

4.2.3.2 Konsekvenser för forsknings- och utvecklingsverksamheten

Förslaget kunde ha konsekvenser för forsknings- och utvecklingsverksamheten. Också den nuvarande lagen om sekundär användning möjliggör internationellt forskningssamarbete via en distansanslutning, men den föreslagna lösningen kan öka förutsättningarna för internationellt forskningssamarbete genom att underlätta inrättandet av informationssäkra driftmiljöer också utanför Finland. Förslaget kunde också främja användningen av finländska registerdata inom det internationella forskningssamarbetet och förbättra finländska forskares möjligheter att delta i forskningssamarbetet.

4.2.3.3 Konsekvenser för social- och hälsovården

Förslaget har inga direkta konsekvenser för människors hälsa och välfärd. Förslaget kan dock på längre sikt medföra fördelar vid vården av finländska social- och hälsovårdsklienter, eftersom det internationella forskningssamarbete med finländska registeruppgifter som förslaget möjliggör kunde möjliggöra utvecklande av nya vårdformer och vårdmetoder för finländska patienters behov. Inom den nuvarande regleringen finns det risk för att de nyaste forskningsresultaten och vårdformerna inte utvecklas i enlighet med finländska behov och det är svårt för finländska forskare att bedriva forskning som en del av det internationella forskningssamarbetet.

4.2.3.4 Konsekvenser för informationssamhället

Förslaget har konsekvenser för skyddet för personuppgifter och informationssäkerheten. I regeringens proposition om lagen om sekundär användning (RP 159/2017 rd) bedömdes lagens konsekvenser för skyddet för personuppgifter. Förslaget ändrar inte på de grunder eller syften för behandling av personuppgifter som fastställs i lagen om sekundär användning eller andra förutsättningar för behandling av personuppgifter, men det möjliggör inrättande av fler informationssäkra driftmiljöer än tidigare och utlämnande av uppgifter också till informationssäkra driftmiljöer utanför Finland, Riskerna för skyddet för personuppgifter kunde öka, eftersom finländska myndigheter inte har möjligheten att övervaka alla informationssäkra driftmiljöer och bedömningen och övervakningen av informationssäkerheten hos utländska driftmiljöer vilar på ackrediterade certifieringsorgans ansvar.

Således är det nödvändigt att i denna proposition bedöma de planerade ändringarnas konsekvenser för skyddet för personuppgifter. Behandlingen av personuppgifter som avses i lagen om sekundär användning grundar sig på artikel 6.1 e i dataskyddsförordningen och i fråga om särskilda kategorier av personuppgifter grundar sig behandlingen beroende på användningsändamål på artikel 9.2 g, h eller j i förordningen. I lagen om sekundär användning har man noggrant definierat de användningsändamål för vilka uppgifter får behandlas i sekundärt syfte. Tillståndsmyndigheten eller någon annan i lagen om sekundär användning avsedd myndighet kontrollerar i samband med mottagandet av ansökan om dataanvändningstillstånd att den uppfyller kraven i lagen om sekundär användning och dataskyddslagstiftningen. Förslaget ändrar inte på dessa krav, utan behandlingen av personuppgifter grundar sig fortfarande på i lagen om sekundär användning fastställda användningsändamål och i den lagen avsett dataanvändningstillstånd som beviljas av en myndighet.

I lagen om sekundär användning avsedda personuppgifter är känsliga uppgifter och uppgifter som hör till särskilda kategorier av personuppgifter, varför det i dataskyddslagstiftningen fastställts särskilda krav på skyddet för dem. I lagen om sekundär användning har man fastställt att social- och hälsovårdsuppgifter är särskilt känsliga, varför personuppgifter kan utlämnas endast till driftmiljöer som uppfyller kraven i lagen om sekundär användning. Lagen om sekundär användning innehåller också andra skyddsåtgärder genom vilka personuppgifter skyddas och dessa skyddsåtgärder har beskrivits på sidan 32 regeringens proposition om ändring av lagen om sekundär användning (RP 96/2021 rd).

I lagen om sekundär användning föreskrivs om lämpliga och särskilda skyddsåtgärder för tryggande av de registrerades rättigheter och friheter. I detta förslag ändras inte i lagen om sekundär användning föreskrivna skyddsåtgärder för behandling av personuppgifter. Behandlingen av personuppgifter skyddas fortfarande genom användning av en informationssäker driftmiljö. För alla informationssäkra driftmiljöer gäller samma krav som fastställts i lagen om sekundär användning och Tillståndsmyndighetens föreskrift, oberoende av var de är belägna. Endast sättet för påvisande av överensstämmelse med kraven ändras så att överensstämmelsen utöver genom en revidering av ett bedömningsorgan för informationssäkerhet också ska kunna påvisas på basis av ett intyg som utfärdats av ett ackrediterat certifieringsorgan och genom iakttagande av internationella standarder eller förfaranden.

I förslaget möjliggörs utlämnande av uppgifter till en driftmiljö som befinner sig utanför Finland smidigare än tidigare. Också den nuvarande lagen om sekundär användning möjliggör inrättande av en driftmiljö utanför Finland och enligt Tillståndsmyndighetens föreskrift ska driftmiljön finnas inom EU/EES-området. I förslaget begränsas inte placeringsorten för informationssäkra driftmiljöer. Således är det möjligt att inrätta en driftmiljö också utanför EU:s område. Bestämmelser om överföring av personuppgifter till tredjeländer finns i kapitel V i dataskyddsförordningen. Om personuppgifter ska överföras till tredjeländer ska överföringen uppfylla de krav som fastställs i kapitel V i dataskyddsförordningen.

Åtgärder för behandling av personuppgifter behövs för att internationellt forskningssamarbete med finländska registeruppgifter ska vara möjligt och uppgifter kunna överföras till andra driftmiljöer än sådana som är belägna i Finland. Behandlingsåtgärdernas proportionalitet motiveras av att personuppgifter i lagen om sekundär användning skyddas på flera olika sätt och att det fortfarande endast är möjligt att behandla personuppgifter i reviderade informationssäkra driftmiljöer.

I och med ändringen kan riskerna för de registrerades rättigheter och friheter öka. Dessa risker föranleds särskilt av att de nationella myndigheternas möjligheter att övervaka driftmiljöer annanstans än i Finland är små. Bedömningar av överensstämmelsen med kraven kunde utföras

av ackrediterade certifieringsorgan, vilkas verksamhet regleras av EU-lagstiftningen och varje lands nationella lagstiftning. Särskild uppmärksamhet bör också ägnas åt säkerställande av anonymiseringen av uppgifter som ska publiceras, eftersom Tillståndsmyndighetens möjligheter att säkerställa anonymiseringen av uppgifter som ska publiceras inom internationellt forskningssamarbete är mycket begränsade och således föreslås det i propositionen att Tillståndsmyndigheten ska kunna meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

Lagen om sekundärt användning och Tillståndsmyndighetens föreskrift innehåller skydds- och säkerhetsåtgärder och mekanismer genom vilka skyddet för personuppgifter säkerställs. Informationssäkerheten för driftmiljöer som är belägna annanstans än i Finland ska verifieras med ett intyg som utfärdats av ett ackrediterat certifieringsorgan, med vilket påvisas att lagen om sekundär användning och Tillståndsmyndighetens föreskrift iakttas. De villkor som uppställts i lagstiftningen och i Tillståndsmyndighetens föreskrift ska säkerställa att dataskyddet och informationssäkerheten för personuppgifter tillgodoses och att registrerades och andra berördas rättigheter och legitima intresse beaktas vid behandlingen av personuppgifter.

I denna regeringsproposition kan riskerna för behandlingen av personuppgifter endast bedömas på allmän nivå. I enlighet med dataskyddsförordningen ska de personuppgiftsansvariga före behandlingen genomföra en konsekvensbedömning avseende dataskydd som avses i artikel 35 i dataskyddsförordningen, om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

Alternativ 1: De krav som uppställts i lagen om sekundär användning kvarstår.

Ett alternativ till den föreslagna lösningen hade varit att hålla kvar kraven på informationssäkra driftmiljöer i lagen om sekundär användning i sin tidigare form. I det fallet skulle det vara möjligt att bedriva internationellt forskningssamarbete med finländska registeruppgifter så att forskaren ansluter sig till den finländska driftmiljön med en distansanslutning och behandlar de uppgifter som begärts med stöd av lagen om sekundär användning i denna driftmiljö. Analyseringen av uppgifter och kombinationen av dem med andra uppgifter som insamlats genom forskning är möjligt, om forskaren överför hela forskningsmaterialet till en finländsk driftmiljö.

Det internationella forskningssamarbetet främjas av att utländska aktörer börjar revidera sina driftmiljöer i överensstämmelse med lagen om sekundär användning inom EU- och EES-området. Hittills har utländska aktörer inte inlett revideringar enligt lagen om sekundär användning.

Alternativ 2: Gemensamma europeiska lösningar

Inom Europeiska unionen pågår för närvarande projekt som syftar till att underlätta dataanvändning för olika mål som gagnar det gemensamma intresset, såsom vetenskaplig forskning. Syftet med den datastrategi som Europeiska kommissionen publicerade år 2020 är att utvidga användningen av data, inklusive hälsodata, inom Europeiska unionen. I datastrategin föreslås det att det ska inrättas ett europeiskt hälsodataområde (European Health Data Space, EHDS) som en del av den europeiska datapolitiken.

I EU finns det för närvarande ingen gemensam praxis för sekundär användning av hälsouppgifter. Enligt artikel 9.4 i dataskyddsförordningen får medlemsstaterna behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Detta har lett till att praxis inom EU är splittrad.

I EU finns det för närvarande ingen lagstiftning eller allmänt antagen praxis som kunde användas för bedömning av informationssäkra driftmiljöers informationssäkerhet. Inom EU pågår ett flertal projekt särskilt för verifiering av molntjänsters säkerhet. Sådana är till exempel bedömning och korsgodkännande av kriterierna för EUSEC:s molntjänster.[19] EU:s cybersäkerhetsbyrå (Enisa)[20] har publicerat ett förslag till kriterier för molntjänsters cybersäkerhet (EUCS).[21] EUCS erbjuder när det färdigställs gemensamma kriterier för molntjänster i Europeiska unionen. Enisa har också offentliggjort en promemoria om informationssäkerheten för hälsovårdens molntjänster.[22]

Europeiska kommissionen publicerade ett förslag om inrättande av ett europeiskt hälsodataområde (EHDS) i maj 2022. Inrättandet av ett europeiskt hälsodataområde är ett av Europeiska kommissionens politiska tyngdpunktsområden åren 2019–2025. Syftet med EHDS är att förbättra utbytet av och tillgången till olika hälsovårdsuppgifter (bland annat elektroniska patientjournaler, genomdata och patientregisteruppgifter) och stödja tillhandahållandet av hälso- och sjukvård (primär användning av uppgifter) samt forskningen inom hälso- och sjukvårdsområdet och utarbetandet av hälso- och sjukvårdspolitik (sekundär användning).

Det allmänna målet för EHDS-lagstiftningsförslaget är att förbättra unionsmedborgarnas möjligheter att kontrollera sina egna hälsouppgifter. Syftet med förslaget är att skapa en rättslig ram som omfattar tillförlitliga förvaltningsmekanismer och en trygg miljö för behandling av uppgifter på EU- och medlemsstatsnivå med hjälp av vilken forskare, beslutsfattare och lagstiftningsmyndigheter på EU- och medlemsstatsnivå kan ta emot och behandla hälsouppgifter för att främja en bättre diagnostisering, vård och välfärd för enskilda samt för att skapa bättre, kunskapsbaserade verksamhetsprinciper.

EHDS-lagstiftningsförslaget gäller också sekundär användning av hälsouppgifter och i det regleras de mekanismer genom vilka det är möjligt att förmedla hälsouppgifter i EU:s medlemsstater med hjälp av gemensam praxis. Förslaget innehåller bestämmelser om informationssäkra miljöer för behandling av uppgifter, i vilka det är möjligt att behandla hälsouppgifter som förmedlas med stöd av förslaget i personifierad form. EHDS kommer när det införs att skapa bestämmelser med vilka man möjliggör ett europeiskt och eventuellt också internationellt forskningssamarbete med hälsouppgifter. Finland har en möjlighet att påverka sättet för genomförande av den kommande EHDS-författningen så att genom den främjas internationellt forskningssamarbete med finländska registeruppgifter. Ett alternativ till den föreslagna lösningen är följaktligen att invänta gemensamma europeiska lösningar och påverka dem. Behandlingen av förslaget och införande av miljöer för behandling av uppgifter enligt författningen kommer dock att ta tid.

[19] Se https://www.sec-cert.eu/
[20] Se https://www.enisa.europa.eu/
[21] Se Candidate scheme European Cybersecurity Certification Scheme for Cloud Services
[22] Se https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

5.2 Lagstiftning och andra handlingsmodeller i utlandet

Lagstiftningen och andra handlingsmodeller i utlandet utvärderades i regeringspropositionen om lagen om sekundär användning (RP 159/2017 rd) på sidorna 34–60 och i regeringens proposition om ändring av 60 § i lagen om sekundär användning (RP 96/2021 rd) på sidan 22.

Det har inte stiftats lagstiftning om informationssäkra driftmiljöer som motsvarar lagen om sekundär användning i andra länder och Finland är ett föregångarland i detta hänseende. I stycket ovan togs det upp att Europeiska kommissionen offentliggjort ett förslag till ett europeiskt hälsodataområde, i vilket också ingår bestämmelser om informationssäkra behandlingsmiljöer.

Joint Action-projektet Tehdas (Towards the European Health Data Space) som samordnas av Jubileumsfonden för Finlands självständighet Sitra har i sin rapport utrett regleringen av sekundär användning av hälsouppgifter i Europa.[23]

I rapporten konstateras att informationssystemen för förvaltning och hälsouppgifter i Europa skiljer sig från varandra och att det i EU:s medlemsstater finns nationella förvaltningsmodeller för hälsouppgifter som är allt från decentraliserade till federala system. Enligt rapporten utgör bristen på en gemensamt överenskommen definition på sekundär användning ett hinder för gränsöverskridande datadelning. Sekundär användning har inte någon rättslig grund i alla medlemsstater och det finns ingen tydlig gränsdragning mellan primär och sekundär användning.

Dessutom kan skillnader i tolkningen av dataskyddsförordningen mellan olika länder och nationella tilläggsbestämmelser försvåra sekundär användning av hälsouppgifter över medlemsstaternas gränser. Överlappande lagstiftning inom EU och på nationell nivå har lett till skillnader i tolkningen och tillämpningen av datadelning på olika håll i Europa

De nationella dataskyddsmyndigheternas och Europeiska dataskyddsstyrelsen EDPB:s anvisningar och tolkningspraxis gällande dataskyddsförordningen preciseras kontinuerligt. För närvarande tillämpas olika regler i olika länder, vilket kan försena och försvåra gränsöverskridande forskning och datadelning, eftersom bestämmelserna om samtycke och delning av hälsouppgifter är oklara. Också tillämpningen av olika interoperabilitetsstandarder i Europa leder till att det är svårt att jämföra och dela uppgifter och forskningsresultat.

I Tehdas-rapporten föreslås som en lösning på problemet en informationssäker driftmiljö. Kommissionen kunde ge anvisningar om kraven och definitionerna på informationssäkra driftmiljöer. Medlemsstaterna kunde godkänna en princip för ömsesidigt erkännande av gränsöverskridande informationssäkra driftmiljöers verksamhet och funktioner.

Europeiska kommissionen har antagit en promemoria om bedömning av medlemsstaternas bestämmelser om hälsouppgifter i ljuset av dataskyddsförordningen.[24] Enligt promemorian finns det i alla medlemsstater en mekanism med hjälp av vilken forskarna kan behandla hälsouppgifter som ursprungligen samlats in i ett annat syfte. I godkännandet av sekundär användning deltar i allmänhet en forskningsetisk kommitté av något slag eller i vissa fall meddelas godkännandet av behandlingen av uppgifter av en central myndighet. Ofta deltar den nationella dataskyddsmyndigheten i godkännandeprocessen. Den mekanism som ska iakttas fastställs ofta på grundval av forskningens karaktär, uppgifter eller vem som genomför forskningen. För iakttagande

[23] TEHDAS Joint Action Report on secondary use of health data through European case studies.
[24] Assessment of the EU Member States' rules on health data in the light of GDPR, se https://ec.europa.eu/newsroom/sante/items/702120/en.

av dataskyddsförordningen används allmänt såväl anonymiserings- som pseudonymiseringsverktyg, beroende på karaktären av begäran om information.

6 Remissvar

Kompletteras på basis av remissvaren.

7 Specialmotivering

3 §. *Definitioner*.

Det föreslås att till 3 § 21 punkten i lagen om sekundär användning av personuppgifter inom social- och hälsovården fogas en ny definition på certifieringsorgan. Med certifieringsorgan ska avses ett bedömningsorgan som ackrediterats enligt enhetliga internationella och europeiska bedömningsgrunder och som godkänts av ett nationellt ackrediteringsorgan enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

Ett certifieringsorgan ska vara ackrediterat enligt enhetliga internationella och europeiska bedömningsgrunder, såsom till exempel ISO/IEC 17021-standarden och den ISO/IEC 27006-standard som kompletterar den. Ackrediteringen görs av ett ackrediteringsorgan som godkänner certifieringsorganet enligt internationella och europeiska bedömningsgrunder. Med ackrediteringsorgan avses i detta sammanhang ett nationellt ackrediteringsorgan som utsetts enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter.

I propositionen föreslås att Tillståndsmyndigheten ska få meddela närmare föreskrifter om certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet.

21 §. *Identifiering av användare i informationssäkra driftmiljöer.*

Det föreslås att lagens 21 § 2 mom. enligt vilket närmare bestämmelser om de tekniska identifierings- och verifieringsmedlen får utfärdas genom förordning av social- och hälsovårdsministeriet ska upphävas. Bestämmelser om de tekniska identifierings- och verifieringsmedlen finns bland annat i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG samt i lagen om stark autentisering och betrodda tjänster (617/2009).

23 §. *Skydd för informationssäkra driftmiljöer*.

Det föreslås att lagens 23 § 1 mom. ändras så att i det hänvisas till de informationssäkerhetskrav som föreskrivs i 4 kap. i informationshanteringslagen (906/2019) och till Tillståndsmyndighetens föreskrift. Den tidigare hänvisningen till 36 § i offentlighetslagen är föråldrad. Statliga myndigheters nuvarande skyldigheter i fråga om informationssäkerhet finns i informationshanteringslagen. I och med informationshanteringslagen upphävdes den förordning om informationssäkerheten inom statsförvaltningen (681/2010) som utfärdats med stöd av offentlighetslagen.

Informationshanteringslagens bestämmelser kan endast förplikta i Finland belägna driftmiljöers tjänsteleverantörer. Av denna anledning föreslås det att till 23 § 1 mom. i lagen om sekundär användning ska fogas en bestämmelse om att en informationssäker driftmiljö ska skyddas med iakttagande av vad som förutsätts i Tillståndsmyndighetens föreskrift. I Tillståndsmyndighetens

föreskrift ska fastställas krav som motsvarar informationshanteringslagens förutsättningar för skydd av driftmiljöer.

25 §. *Påvisande av informationssäkerhet i en informationssäker driftmiljö*.

Det föreslås att 25 § 1 mom. ändras så att informationssäkerheten i driftmiljön utöver genom ett intyg från ett bedömningsorgan för informationssäkerhet ska kunna påvisas genom ett intyg från ett certifieringsorgan.

Det föreslås att 25 § 2 mom. ändras så att Tillståndsmyndigheten ska få meddela närmare föreskrifter om de förfaranden som ska iakttas vid påvisande av informationssäkerhet samt om de certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet.

26 §. *Bedömning av informationssäkerhet*.

I propositionen föreslås det att 26 § 1 mom. ändras så att utöver ett bedömningsorgan för informationssäkerhet också ett certifieringsorgan på ansökan av en tjänsteleverantör ska kunna bedöma, om driftmiljön uppfyller kraven på informationssäkerhet.

Det föreslås att 26 § 2 mom. ändras så att också certifieringsorganet ska kunna ge tjänsteleverantören ett intyg över sin bedömning och en anknytande kontrollrapport, om driftmiljön uppfyller informationssäkerhetskraven enligt lagen om sekundär användning. Om bedömningen eller en förnyad bedömning endast gäller en del av driftmiljön, ska det i certifieringsorganets intyg tydligt antecknas vilken del av driftmiljön som har bedömts.

Det föreslås att 26 § 2 mom. ändras så att såväl bedömningsorganets som certifieringsorganets intyg ska vara i kraft högst tre år. En förkortning av intygets giltighetstid från fem till tre år är motiverad, eftersom informationssäkerhetsmiljön och kraven på informationssäkerhet hinner förändras betydligt på fem år och tre år är etablerad praxis för de flesta intyg inom branschen. Till exempel ISO 27001- och CSA Star-certifieringen är i kraft tre år och uppföljningsrevideringar görs årligen.

Dessutom föreslås det att 26 § 2 mom. i lagen ska ändras så att också certifieringsorganet ska kunna kräva alla de uppgifter som förutsätts för bedömningen och för uppgörandet och upprätthållandet av intyget av tjänsteleverantören. Dock ska 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet i övrigt endast tillämpas på bedömningsorgans utfärdande av intyg. På certifieringsorgans utfärdande av intyg tillämpas i övrigt Tillståndsmyndighetens föreskrift.

27 §. *Återkallande av bedömningsorganets och certifieringsorganets intyg*.

Det föreslås att 27 § ändras så att också certifieringsorganet ska uppmana tjänsteleverantören att avhjälpa bristerna, om certifieringsorganet konstaterar att en driftmiljö inte har uppfyllt eller inte längre uppfyller kraven i lagen om sekundär användning eller att ett intyg av någon annan orsak inte borde ha beviljats. Certifieringsorganet får också återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tjänsteleverantören avhjälper bristerna inom den tid som organet satt ut.

28 §. *Anmälningsskyldighet för bedömningsorgan för informationssäkerhet och certifieringsorgan*.

Det föreslås att lagens 28 § ska ändras så att också certifieringsorgan ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om alla intyg som har utfärdats, ändrats eller

kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats och om de kontrollrapporter som avses i 26 § samt om de uppmaningar och begränsningar som avses i 27 §. Dessutom ska certifieringsorgan på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

29 §. *Uppföljning efter ibruktagande av informationssäker driftmiljö*.

Det föreslås att 28 § 1 mom. ska ändras så att väsentliga förändringar i driftmiljön ska anmälas antingen till bedömningsorganet för informationssäkerhet eller certifieringsorganet, beroende på vilken organisation som bedömt driftmiljön. Också certifieringsorganets intyg ska förnyas, om betydande förändringar görs i driftmiljön eller om minimikraven på driftmiljön har ändrats på ett sätt som förutsätter en förnyad bedömning.

I enlighet med 29 § 2 mom. ska tjänsteleverantören bevara uppgifterna om överensstämmelse med kraven och övriga uppgifter som tillsynen kräver i minst fem år efter det att den informationssäkra driftmiljön inte längre används för produktion.

30 §. *Övervakning och inspektioner av informationssystem*.

Det föreslås att lagens 30 § 1 mom. ändras så att certifieringsorganen ska övervaka och främja att de driftmiljöer som de bedömt som informationssäkra uppfyller kraven på dataskydd och informationssäkerhet.

Det föreslås att till lagens 30 § fogas ett nytt fem mom. enligt vilket Tillstånds- och tillsynsverket för social- och hälsovården ska kunna meddela närmare föreskrifter om övervakningen av informationssäkra driftmiljöer. Övervakningen av informationssäkra driftmiljöers överensstämmelse med kraven har i lagen om sekundär användning getts Valvira i uppgift. Den nationella myndighetens möjligheter att övervaka andra driftmiljöer än sådana som är belägna i Finland är dock i praktiken begränsade. Av denna anledning ska det vara möjligt för Valvira att meddela närmare föreskrifter om övervakningen av informationssäkra driftmiljöer. I föreskriften kan det bestämmas närmare till exempel om hur övervakningen av andra driftmiljöer än sådana som är belägna i Finland ska genomföras.

52 §. *Publicering av resultat baserade på uppgifter utlämnade med stöd av ett dataanvändningstillstånd*.

Det föreslås att 52 § i lagen om sekundär användning ska ändras så att till paragrafen fogas ett nytt 3 mom., enligt vilket Tillståndsmyndigheten kan meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

I lagen om sekundär användning har man fastställt som Tillståndsmyndighetens uppgift att försäkra sig om att de uppgifter som publiceras är anonymiserade. Tillståndsmyndigheten kan av grundad anledning i tillståndsbeslutet bevilja tillståndshavaren rätt att själv anonymisera de uppgifter som ska publiceras, förutsatt att uppgifterna ges in till myndigheten i efterhand.

Enligt förslaget ska Tillståndsmyndigheten kunna meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras. I föreskriften kan man närmare fastställa hur tillståndshavaren ska säkerställa anonymiseringen av de uppgifter som publiceras.

8 Bestämmelser på lägre nivå än lag

Enligt 24 § 2 mom. i lagen om sekundär användning meddelar Tillståndsmyndigheten närmare föreskrifter om de krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. I propositionen föreslås det att 25 § 2 mom. i lagen om sekundär användning ändras så att Tillståndsmyndigheten utöver om de förfaranden som ska iakttas vid påvisande av informationssäkerhet ska få meddela närmare föreskrifter om de certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet. Dessutom föreslås det att 52 § i lagen om sekundär användning ska ändras så att till paragrafen fogas ett nytt 3 mom., enligt vilket Tillståndsmyndigheten kan meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

För genomförande av den lösning som föreslås i propositionen bör Tillståndsmyndighetens föreskrift om informationssäkra driftmiljöer ändras så att de krav som fastställs i den också kan uppfyllas genom iakttagande av internationella standarder och förfaranden och bedömningen av överensstämmelsen med kraven utföras av ett ackrediterat certifieringsorgan.

På sidan 182 i regeringens proposition om lagen om sekundär användning (RP 159/2017 rd) behandlas Tillståndsmyndighetens bemyndiganden att meddela föreskrifter. Tillståndsmyndighetens bemyndigande att meddela föreskrifter om kraven på informationssäkra driftmiljöer motiveras med att bemyndigandena att meddela föreskrifter huvudsakligen gäller tekniska detaljer, som det faller sig naturligt att sköts av Tillståndsmyndigheten. Dessutom är det enligt regeringens proposition nödvändigt att tekniska och närmare föreskrifter utfärdas, eftersom den tekniska utvecklingen går så snabbt framåt och de förutsätter specialsakkunskap om informationssäkra driftmiljöer.

I propositionen föreslås det att Valvira ska ges rätt att meddela närmare föreskrifter om övervakningen av informationssäkra driftmiljöer. Ändringen motiveras med att den nationella myndighetens möjligheter att övervaka driftmiljöer annanstans än i Finland är begränsade och att det därför ska vara certifieringsorganens uppgift att övervaka och främja att de informationssäkra driftmiljöer som de bedömt uppfyller kraven på informationssäkerhet. Valvira ska kunna meddela närmare föreskrifter om hur certifieringsorganens övervakningsuppgifter ska genomföras.

9 Ikraftträdande

Det föreslås att lagen ska träda i kraft den 1 december 2023. Förslagets ikraftträdande förutsätter att Tillståndsmyndighetens föreskrifter ändras och genomförandet av dessa ändringar beräknas ta ungefär ett år i anspråk.

10 Verkställighet och uppföljning

Social- och hälsovårdsutskottet har i sitt betänkande om regeringens proposition om lagen om sekundär användning (RP 159/2017 rd) konstaterat att statsrådet noga måste följa upp och ta ställning till hur regelverket har verkställts och fungerar. Detta är viktigt för att lagstiftningen ska tillgodose de behov som kommer med den tekniska utvecklingen, för att den sekundära användningen av personuppgifter ska fungera smidigt, för att informationssäkerheten för behandling av känsliga social- och hälsovårdsuppgifter ska ligga på hög nivå och för att den sekundära användningen av personuppgifter ska vara till nytta för social- och hälsovårdssystemet. Utskottet fann det viktigt att statsrådet noga följer upp och utvärderar hur det föreslagna systemet och den anknytande lagstiftningen fungerar i sin helhet också när verksamheten har kommit

i gång. Detta är enligt utskottet av relevans för att man ska kunna nyttiggöra den tekniska utvecklingen på behörigt sätt för att skydda personuppgifter. I förekommande fall måste lagarna ändras.

Enligt regeringens uppfattning bör verkställigheten av lagen om sekundär användning alltjämt följas upp tillsammans med de myndigheter som utövar tillsyn och den expertgrupp på hög nivå som nämns i 8 § 4 mom. i lagen om sekundär användning så att det säkerställs att den tekniska utvecklingen utnyttjas på lämpligt sätt i verksamheten för att trygga skyddet av personuppgifter.

För genomförande av den lösning som föreslås i propositionen bör man vidta och följa upp behövliga åtgärder för ändring av Tillståndsmyndighetens föreskrift. I dessa åtgärder ska det ingå utarbetandet av en motsvarighetstabell mellan de krav som fastställs i Tillståndsmyndighetens föreskrift och de krav som fastställs i internationella standarder och förfaranden. Dessutom förutsätter genomförandet av propositionen samarbete mellan Tillståndsmyndigheten och Valvira, så att godkännandet av informationssäkra driftmiljöer på basis av de uppdaterade kraven sker smidigt. Den expertgrupp på hög nivå som nämns i 8 § 4 mom. i lagen om sekundär användning kan utarbeta genomförande- och uppföljningsplanen.

11 Förhållande till andra propositioner

11.1 Samband med andra propositioner

Propositionen har inget samband med regeringens propositioner som för närvarande överlåtits till riksdagen eller som är under beredning.

11.2 Förhållande till budgetpropositionen

Propositionen påverkar Tillståndsmyndighetens budget. För genomförande av den lösning som föreslås i propositionen bör Tillståndsmyndigheten uppdatera sin föreskrift om informationssäkra driftmiljöer. Detta bedömnings- och reformarbete förutsätter resurser.

12 Förhållande till grundlagen samt lagstiftningsordning

Skydd för privatlivet

I regeringens proposition om lagen om sekundär användning (RP 159/2017 rd) bedömdes särskilt propositionens förhållande till skyddet för privatlivet och offentlighetsprincipen och till utövandet av offentlig makt.

I regeringens proposition om ändring av lagen om sekundär användning (RP 96/2021 rd) behandlades propositionens förhållande till skyddet för privatlivet och grundlagsutskottets utlåtandepraxis i samband med rätten att få uppgifter och behandlingen av känsliga uppgifter, Nedan beskrivs i korthet grundlagsutskottets praxis i anslutning till propositionen.

Enligt 10 § 1 mom. i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Bestämmelsen hänvisar till behovet att trygga skyddet för individens privatliv vid behandlingen av personuppgifter, det vill säga skyddet för personuppgifter ingår delvis i skyddet för privatlivet. Närmare bestämmelser om skyddet för personuppgifter får utfärdas genom lag, men samtidigt ska man trygga dataskyddet på ett sådant sätt som kan anses vara godtagbart med tanke på systemet för grundläggande fri- och rättigheter i sin helhet.

Riksdagens grundlagsutskott har i sitt utlåtande (GrUU 8/1995 rd, GrUU 26/1996 rd samt GrUU 7, 28 och 29/1997 rd) tagit ställning till skyldigheten att föreskriva om behandling av personuppgifter genom lag i 8 § 1 mom. i regeringsformen (nuvarande 10 § 1 mom. i grundlagen). Utskottet har konstaterat att det är viktigt med tanke på bestämmelsen om grundläggande fri- och rättigheter gällande skyddet för personuppgifter att reglera åtminstone registreringens syfte, innehållet i de registrerade personuppgifterna och tillåtna användningsändamål, vilket inbegriper uppgifternas överlåtbarhet och bevaringstiden för uppgifterna i personregistren, samt den registrerades rättsskydd. Regleringen av dessa faktorer på lagnivå ska dessutom vara omfattande och detaljerad. I sina senare utlåtanden (GrUU 12/2002 rd, 14/2002 rd, 51/2002 rd och 11/2008 rd) har utskottet reviderat sin åsikt och konstaterat att kravet på bestämmelser i lag också gäller möjligheten att lämna ut personuppgifter via en teknisk anslutning.

Lagstiftning som gäller behandlingen av personuppgifter ska vara heltäckande, exakt och noga avgränsad. Grundlagsutskottet har dessutom i flera utlåtanden noterat vad och vem rätten att få uppgifter gäller och hur rätten är kopplad till nödvändighetskriteriet. Myndigheternas rätt att få och möjlighet att lämna ut uppgifter har enligt utskottet kunnat gälla ”behövliga uppgifter” för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att "informationen är nödvändig" för ett visst syfte (till exempel GrUU 10/2014 rd, s. 6/II samt GrUU 17/2016 rd, GrUU 48/2018 rd, s. 2–3 och GrUU 38/2016 rd, s. 2). Dessutom ska om möjligheten att kombinera registeruppgifter föreskrivas i lag (GrUU 17/2007 rd och GrUU 30/2005 rd).

Enligt grundlagsutskottet är det i regel tillräckligt med tanke på 10 § 1 mom. i grundlagen att bestämmelserna uppfyller kraven enligt EU:s allmänna dataskyddsförordning. Enligt utskottet bör skyddet för personuppgifter i första hand tillgodoses med stöd av EU:s allmänna dataskyddsförordning och den nationella allmänna lagstiftningen. Lagstiftaren bör således vara restriktiv när det gäller att införa nationell speciallagstiftning. Sådan lagstiftning bör vara avgränsad till nödvändiga bestämmelser inom ramen för det nationella handlingsutrymme som dataskyddsförordningen medger (se GrUU 14/2018 rd, s. 4–5).

Grundlagsutskottet ser det dock som klart att behovet av speciallagstiftning i enlighet med det riskbaserade synsätt som också krävs i dataskyddsförordningen måste bedömas utifrån de hot och risker som behandlingen av personuppgifter orsakar. Ju större risk fysiska personers rättigheter och friheter utsätts för på grund av behandlingen, desto mer motiverat är det med mer detaljerade bestämmelser. Denna omständighet är av särskild betydelse när det gäller behandling av känsliga uppgifter (se GrUU 14/2018 rd, s. 5).

Grundlagsutskottet har lyft fram riskerna med behandlingen av känsliga uppgifter. Utskottet anser att omfattande databaser med känsliga uppgifter medför allvarliga risker för informationssäkerheten och missbruk av uppgifter. Riskerna kan i sista hand utgöra ett hot mot personers identitet (se GrUU 13/2016 rd, s. 4, GrUU 14/2009 rd, s. 3/I). Också enligt skäl 51 i ingressen till den allmänna dataskyddsförordningen bör i artikel 9 i förordningen avsedda särskilda personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Utskottet har därför särskilt påpekat att det bör finnas exakta och noga avgränsade bestämmelser om att det är tillåtet att behandla känsliga uppgifter bara om det är absolut nödvändigt, och bestämmelserna om behandling av känsliga uppgifter måste vara detaljerade och omfattande, inom de ramar som dataskyddsförordningen tillåter (GrUU 65/2018 rd, s. 45 och GrUU 15/2018 rd, s. 40). Utskottet betonade dock i samband med bedömningen av dataskyddslagen att i fråga om behovet av reglering bör också

det riskbaserade synsättet i förordningen vägas in och framhöll att även lagstiftningen om behandling av känsliga personuppgifter bör vara så tydlig och begriplig som möjligt (GrUU 14/2018 rd, s. 6).

Grundlagsutskottet har betonat att informationssäkerheten fungerar och förhindrar missbruk och finns tillgänglig genast när registret börjar användas. Utskottet anser att det i och för sig är nödvändigt, men inte tillräckligt, att i efterhand och effektivt övervaka, exempelvis med hjälp av logguppgifter, att behandlingen är nödvändig och laglig. Utskottet har betonat att skyddet för uppgifter från obehörig användning inte uteslutande kan baseras på det tjänsteansvar som gäller för den personuppgiftsansvarige eller den som behandlar uppgifterna eller på något annat påföljdssystem (GrUU 65/2018 rd, s. 47, GrUU 51/2018 rd, s. 5, GrUU 52/2018 rd, s. 4).

Den lösning som föreslås i denna regeringsproposition är av betydelse med avseende på skyddet för privatlivet och skyddet för personuppgifter som tryggas i 10 § 1 mom. i grundlagen. De föreslagna regleringen har också betydelse med avseende på EU:s stadga om de grundläggande rättigheterna. I artikel 7 i EU:s stadga om de grundläggande rättigheterna tryggas skyddet för privatlivet och i artikel 8 var och ens rätt till skydd av sina personuppgifter. Förslaget möjliggör utlämnande av i lagen om sekundär användning avsedda personuppgifter till en informationssäker driftmiljö annanstans än i Finland. Den föreslagna lösningen kunde öka riskerna för de registrerade jämfört med nuläget, där de informationssäkra driftmiljöerna revideras av bedömningsorgan för informationssäkerhet som godkänts av Traficoms Cybersäkerhetscenter. Avsikten är dock inte att genom förslaget ändra den nivå av informationssäkerhet som i lagen om sekundär användning förutsätts av informationssäkra driftmiljöer, utan en hög nivå av dataskydd och informationssäkerhet säkerställs genom de krav på informationssäkerhet som förutsätts i lagen om sekundär användning och Tillståndsmyndighetens föreskrift.

Alla informationssäkra driftmiljöer ska fortfarande uppfylla samma krav oberoende av deras geografiska läge och av om bedömningen av överensstämmelsen med kraven görs av ett bedömningsorgan för informationssäkerhet eller ett ackrediterat certifieringsorgan. Avsikten är att med internationella standarder och förfaranden säkerställa en lika hög informationssäkerhetsnivå som med nationella bedömningskriterier,

Med tanke på skyddet för personuppgifter bör man också beakta att en informationssäker driftmiljö inte är den enda metoden i lagen om sekundär användning att säkerställa dataskyddet och informationssäkerheten för personuppgifter, utan i lagen ingår flera mekanismer som skyddar personuppgifter. Dessutom gäller i lagen om sekundär användning fortfarande principen enligt vilken de uppgifter som avses i lagen i första hand alltid utlämnas till Tillståndsmyndighetens informationssäkra driftmiljö.

I regeringens proposition om ändring av lagen om sekundär användning (RP 96/2021 rd) beskrivs lagens arrangemang gällande dataskydd och informationssäkerhet, som skyddar personuppgifter som behandlas i sekundärt syfte. Lagen om sekundär användning innehåller så noggrant avgränsat som möjligt de användningsändamål till vilka uppgifter får utlämnas samt de grunder på vilka beslutet om utlämnande ska avgöras. I lagen om sekundär användning ingår betydande tekniska och andra säkerhetsgarantier med hjälp av vilka man kan försäkra sig om att mottagaren behandlar personuppgifterna på ett sätt som tryggar den registrerades skydd för privatlivet. Sådana är till exempel tjänsten för insamling, samkörning och förbehandling av uppgifter, tjänsten för administrering av identifierare, systemet för hantering av begäranden om information och den informationssäkra drifttjänsten.

Den registrerades rättigheter och friheter skyddas bland annat så att personuppgifter endast kan behandlas på basis av ett dataanvändningstillstånd som beviljats av en myndighet och för tillståndshavaren gäller tystnadsplikt. I sekretessparagrafen i lagen om sekundär användning är det fråga om utvidgande av sekretessbestämmelserna till att också gälla annat än myndighetsverksamhet, Dessutom förbjuds i paragrafen i regel användning av uppgifter vid beslutsfattande som gäller en enskild person. Syftet med tystnadsplikten är samtidigt att trygga individers skydd för personuppgifter som en grundläggande fri- och rättighet.

Personuppgifterna ska anonymiseras eller pseudonymiseras alltid när det är möjligt med tanke på ändamålet. Tillståndsmyndigheten och andra myndigheter som beviljar dataanvändningstillstånd enligt lagen om sekundär användning samt Valvira ska för sin egen del följa med och övervaka att villkoren i de tillstånd som de beviljat iakttas. Om Tillståndsmyndigheten eller en myndighet som beviljar dataanvändningstillstånd i enlighet med lagen om sekundär användning har grundad anledning att misstänka att den som behandlar uppgifter med stöd av ett dataanvändningstillstånd från myndigheten inte behandlar personuppgifter i enlighet med lag, ska myndigheten enligt 56 § i lagen om sekundär användning underrätta dataombudsmannen om saken snarast möjligt.

Lagen om sekundär användning och Tillståndsmyndighetens föreskrift bildar tillsammans en helhet som tryggar skyddet för personuppgifter som också kompletteras av annan tillämplig nationell och europeisk lagstiftning. Syftet har varit att genom lagen om sekundär användning till de delar som hör till dess område verkställa EU:s allmänna dataskyddsförordning och också beakta övrig unionslagstiftning som gäller området. Genom lagen om sekundär användning utfärdas bestämmelser som kompletterar dataskyddsförordningen inom ramen för det nationella handlingsutrymmet.

I förslaget föreslås bestämmelser som kompletterar dataskyddsförordningen inom ramen för det nationella handlingsutrymmet. Det nationella handlingsutrymmet grundar sig på artikel 6.1 e i dataskyddsförordningen samt, när det gäller särskilda kategorier av personuppgifter, på artikel 9.2 g, h och j i förordningen. Enligt artikel 6.3 i dataskyddsförordningen kan medlemsstatens lagstiftning innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen. Sådana särskilda bestämmelser kan bl.a. omfatta de allmänna villkor som ska gälla lagenligheten för den personuppgiftsansvariges behandling av uppgifter, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling. Enligt artikel 9.4 i dataskyddsförordningen får medlemsstaterna dessutom behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

De bestämmelser som föreslås i propositionen utgör sådana skyddsåtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen som förutsätts i dataskyddsförordningen. De föreslagna bestämmelserna ingår således i det nationella handlingsutrymme som ges medlemsstaterna i dataskyddsförordningen.

På basis av det ovan anförda tryggar de föreslagna bestämmelserna kraven på skydd för privatlivet samt skydd för personuppgifter på det sätt som grundlagen och dataskyddsförordningen förutsätter.

Utövning av offentlig makt

I 124 § i grundlagen föreskrivs om överföring av förvaltningsuppgifter på andra än myndigheter. Enligt paragrafen kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning.

Enligt motiveringen till 124 § i grundlagen och grundlagsutskottets tolkningspraxis hänvisar ”offentlig förvaltningsuppgift” till en större helhet än ”utövning av offentlig makt”. En offentlig förvaltningsuppgift kan också vara en serviceuppgift som inte nödvändigtvis innebär utövning av offentlig makt, eller andelen utövning av offentlig makt kan åtminstone vara obetydlig.

Enligt 124 § i grundlagen kan dessutom en uppgift med betydande offentlig makt endast skötas av en myndighet. Sådan betydande offentlig makt kan bland annat ingå i prövningen av dataanvändningstillstånd och andra beslut om utlämnande av uppgifter med stöd av denna lag. Skötseln av en offentlig förvaltningsuppgift är med stöd av paragrafen i regel en myndighetsuppgift och kan endast i begränsad omfattning anförtros andra än myndigheter.

Av grundlagsutskottets tolkningspraxis framgår att ett arrangemang enligt 124 § i grundlagen, det vill säga att anförtro en förvaltningsuppgift åt andra än myndigheter, i synnerhet i situationer som väsentligt inverkar på den rättsliga ställningen för enskilda endast kan vara sådant som kompletterar och bistår myndigheternas verksamhet. Grundlagsutskottet har i sin praxis bland annat utvärderat rättshjälps- och intressebevakningstjänster (GrUU 16/2016 rd), uppehållstillståndsuppgifter (GrUU 64/2014 rd), utläggning av förfarandet för utfärdande av pass (GrUU 6/2013 rd), anförtroendet av verksamheten i myndigheternas säkerhetsnät åt statliga bolag (GrUU 8/2014 rd) och anförtroendet av den tekniska bedömningen av järnvägstrafikens överensstämmelse och inspektionsuppgifter åt enskilda juridiska personer (GrUU 16/2002 rd). Det har varit fråga om en verksamhetshelhet som skapar förutsättningar för myndighetsverksamheten, är av teknisk karaktär eller osjälvständig.

Grundlagsutskottet har i sin praxis delat in bedömningen enligt 124 § i tre delar. Indelningen grundar sig på förarbetena till grundlagen. Utskottet har förutsatt att det är inte fråga om överföring av betydande offentlig makt, att uppgiftsöverföringen är ändamålsenlig bland annat med tanke på förvaltningens effektivitet och övriga interna behov inom förvaltningen liksom också enskilda personers och samfunds behov, och att de grundläggande fri- och rättigheterna, rättsskyddet och övriga krav på god förvaltning tillgodoses i samband med överföringen.

I regeringens proposition om ändring av lagen om sekundär användning (RP 96/2021 rd) behandlas utövning av offentlig makt och inrättande av informationssäkra driftmiljöer i förhållande till 124 § i grundlagen. En informationssäker driftmiljö som avses i 20 § i lagen om sekundär användning kan också inrättas av någon annan än en myndighet, även av en civilrättslig juridisk person. Inom driftmiljön behandlas personuppgifter.

Tillståndsmyndighetens informationssäkra driftmiljö är alltid den plats dit personuppgifter utlämnas i första hand. Tillståndsmyndighetens driftmiljö ska inte i sig begränsa verkställandet av ett användningsändamål som stämmer överens med grundlagen. Därför är det ändamålsenligt att uppgifter också kan behandlas i andra driftmiljöer än Tillståndsmyndighetens. Dessutom har det inom ramen för nuvarande lagstiftning även varit möjligt att behandla känsliga personuppgifter i andra driftmiljöer än myndighetens driftmiljö. För dem som behandlat uppgifter har naturligtvis gällt tystnadsplikt.

Även om uppgifter kan överföras till andra informationssäkra driftmiljöer än sådana som är belägna i Finland, är det inte tillåtet att i dessa situationer äventyra den registrerades grundläggande rättigheter. För en informationssäker driftmiljös informationssäkerhet uppställs för skyddande av personuppgifter i 21–29 § i lagen angivna minimikrav som ska uppfyllas. Ett bedömningsorgan för informationssäkerhet eller ett ackrediterat certifieringsorgan genomför en revidering av systemen genom vilken säkerställs att minimikraven uppfylls. Det ackrediterade certifieringsorganet övervakar de system som det bedömt. Tillståndshavaren har dessutom tystnadsplikt. Tillståndsmyndigheten övervakar under de förutsättningar som anges i lagen om sekundär användning att personuppgifterna behandlas i enlighet med lagen och tillståndsvillkoren. På så sätt kan man tillse att personuppgifterna behandlas på lämpligt sätt.

I 10 § i grundlagen förutsätts inte att personuppgifterna ska behandlas av en myndighet. I praktiken behandlar privata aktörer personuppgifter inbegripet känsliga personuppgifter, i betydande utsträckning. Tekniska uppgifter i samband med behandling av personuppgifter sköts också av civilrättsliga juridiska personer till exempel med stöd av avtal.

Normgivningsbemyndiganden

Enligt 80 § 1 mom. i grundlagen kan statsrådet och ministerierna utfärda förordningar med stöd av ett bemyndigande i grundlagen eller i någon annan lag. Genom lag ska dock utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter samt om frågor som enligt grundlagen i övrigt hör till området för lag. Enligt 80 § 2 mom. i grundlagen kan även andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett bemyndigande ska vara exakt avgränsat. Av grundlagen följer också att de frågor som bemyndigandet gäller måste vara exakt avgränsade i lag. I fråga om bemyndiganden i lag har grundlagsutskottet i sin utlåtandepraxis krävt exakta och noggrant avgränsade regler (GrUU 19/2002 rd, s. 5, GrUU 1/2004 rd, s. 2 och GrUU 17/2010 rd, s. 2).

I propositionen föreslås bemyndiganden att utfärda föreskrifter för Tillståndsmyndigheten och Valvira. Det föreslås att 25 § 2 mom. i lagen om sekundär användning ändras så att Tillståndsmyndigheten ska få meddela närmare föreskrifter om de certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet. Dessutom föreslås det att 52 § i lagen ändras så att till paragrafen fogas ett nytt 3 mom., enligt vilket Tillståndsmyndigheten ska kunna meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

Ovannämnda normgivningsbemyndiganden som föreslås för Tillståndsmyndigheten gäller huvudsakligen tekniska detaljer, som det är naturligt att Tillståndsmyndigheten sköter. Det är nödvändigt att utfärda närmare bestämmelser om certifieringsorgan eftersom Tillståndsmyndigheten i sin föreskrift om informationssäkra driftmiljöer ska fastställa de internationella standarder och förfaranden på basis av vilka man kan påvisa att de krav som fastställts i lagen om sekundär användning och Tillståndsmyndighetens föreskrift uppfylls. Dessa standarder och förfaranden avgör också vilka ackrediterade certifieringsorgan som kan bedöma om driftmiljön stämmer överens med kraven. Närmare bestämmelser om säkerställande av anonymisering behövs för att Tillståndsmyndigheten på ett effektivt sätt också ska kunna säkerställa anonymiseringen av publikationer från aktörer utanför Finland.

Det föreslås att till lagens 30 § fogas ett nytt fem mom. enligt vilket Tillstånds- och tillsynsverket för social- och hälsovården ska kunna meddela närmare föreskrifter om övervakningen av

informationssäkra driftmiljöer. I föreskriften kan det bestämmas närmare till exempel om hur övervakningen av andra driftmiljöer än sådana som är belägna i Finland ska genomföras.

De föreslagna bestämmelserna om bemyndigande har i huvudsak avgränsats till att enbart gälla detaljer av teknisk karaktär. Grunderna för individens rättsliga ställning fastställs på basis av lagens bestämmelser. Förslagets normgivningsbemyndigande kan på ovannämnda grunder inte anses stå i strid med 80 § i grundlagen.

På ovan beskrivna grunder anser regeringen att propositionen står i samklang med grundlagen, varför den föreslagna lagen kan behandlas i vanlig lagstiftningsordning. Regeringen anser det dock önskvärt att grundlagsutskottet lämnar utlåtande i ärendet.

Kläm

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

Lag

om ändring av lagen om sekundär användning av personuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

upphävs i lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019) 21 § 2 mom.,

ändras 3 § 20 punkten, 23 § 1 mom., 25–28 §, 29 § 1 mom. och 30 § 1 mom. samt

fogas till 3 § en ny 21 punkt, till 30 § ett nytt 5 mom. och till 52 § ett nytt 3 mom. som följer:

3 §

Definitioner

I denna lag avses med

— —

20) bedömningsorgan för informationssäkerhet sådana företag, sammanslutningar och myndigheter som Transport- och kommunikationsverket med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011) har godkänt att utföra bedömningar av om informationssystem överensstämmer med kraven i fråga om informationssäkerhet,

21) *certifieringsorgan* ett bedömningsorgan som ackrediterats enligt enhetliga internationella och europeiska bedömningsgrunder och som godkänts av ett nationellt ackrediteringsorgan enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

23 §

Skydd för informationssäkra driftmiljöer

En informationssäker driftmiljö ska skyddas i enlighet med statliga myndigheters skyldigheter i fråga om informationssäkerhet enligt vad som föreskrivs i 4 kap. i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och vad som förutsätts i Tillståndsmyndighetens föreskrift.

— —

25 §

Påvisande av informationssäkerhet i en informationssäker driftmiljö

Informationssäkerheten i driftmiljön ska påvisas genom ett i 26 § avsett intyg från ett bedömningsorgan för informationssäkerhet eller ett certifieringsorgan.

Tillståndsmyndigheten får meddela närmare föreskrifter om de förfaranden som ska iakttas vid påvisande av informationssäkerhet samt om de certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet.

26 §

Bedömning av informationssäkerhet

Ett bedömningsorgan för informationssäkerhet bedömer i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet, på ansökan av tjänsteleverantören, om driftmiljön uppfyller kraven på informationssäkerhet. Ett certifieringsorgan bedömer i enlighet med denna lag, på ansökan av tjänsteleverantören, om driftmiljön uppfyller kraven på informationssäkerhet. Som bedömningskriterier ska användas föreskrifter om kraven på en säker driftmiljö från Tillståndsmyndigheten.

Om driftmiljön uppfyller informationssäkerhetskraven enligt denna lag, ska bedömningsorganet för informationssäkerhet eller certifieringsorganet ge tjänsteleverantören ett intyg över sin bedömning och en anknytande kontrollrapport. Om bedömningen eller en förnyad bedömning gäller endast en del av driftmiljön, ska det i bedömningsorganets eller certifieringsorganets intyg tydligt antecknas vilken del av driftmiljön som har bedömts.

Bedömningsorganets eller certifieringsorganets intyg är i kraft högst tre år. Bedömningsorganet för informationssäkerhet eller certifieringsorganet kan av tjänsteleverantören kräva alla de uppgifter som förutsätts för bedömningen och för uppgörandet och upprätthållandet av intyget. På bedömningsorgans utfärdande av intyg tillämpas i övrigt 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet.

27 §

Återkallande av bedömningsorganets och certifieringsorganets intyg

Om ett bedömningsorgan för informationssäkerhet eller ett certifieringsorgan konstaterar att en driftmiljö inte har uppfyllt eller inte längre uppfyller kraven i denna lag eller att ett intyg av någon annan orsak inte borde ha beviljats, ska organet uppmana tjänsteleverantören att avhjälpa bristerna. Bedömningsorganet eller certifieringsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tjänsteleverantören avhjälper bristerna inom den tid som organet satt ut. När tidsfristens längd bestäms ska det beaktas att en skälig tid behövs för att korrigera driftmiljön.

28 §

Anmälningsskyldighet för bedömningsorgan för informationssäkerhet och certifieringsorgan

Bedömningsorgan för informationssäkerhet och certifieringsorgan ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om alla intyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats och om de kontrollrapporter som avses i 26 § samt om de uppmaningar och begränsningar som avses i

27 §. Dessutom ska bedömningsorgan för informationssäkerhet och certifieringsorgan på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

29 §

Uppföljning efter ibruktagande av informationssäker driftmiljö

Tjänsteleverantören ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera erfarenheterna av en informationssäker driftmiljö under den tid den används för produktion. Tjänsteleverantören ska ge akt på ändringar i denna lag och i Tillståndsmyndighetens föreskrift och justera driftmiljön i enlighet med ändringarna. Väsentliga förändringar i driftmiljön ska anmälas till bedömningsorganet för informationssäkerhet eller certifieringsorganet. Bedömningsorganets eller certifieringsorganets intyg ska förnyas, om betydande förändringar görs i driftmiljön eller om minimikraven på driftmiljön har ändrats på ett sätt som förutsätter en förnyad bedömning.

— —

30 §

Övervakning och inspektioner av informationssystem

Tillstånds- och tillsynsverket för social- och hälsovården ska övervaka och främja att informationssäkra driftmiljöer uppfyller kraven på dataskydd och informationssäkerhet. Certifieringsorganen ska övervaka och främja att de driftmiljöer som de bedömt som informationssäkra uppfyller kraven på dataskydd och informationssäkerhet. Tillstånds- och tillsynsverket för social- och hälsovården för ett offentligt register över driftmiljöer som uppfyller kraven och som anmälts till verket.

— —

Tillstånds- och tillsynsverket för social- och hälsovården kan meddela närmare föreskrifter om övervakningen av informationssäkra driftmiljöer.

52 §

Publicering av resultat baserade på uppgifter utlämnade med stöd av ett dataanvändningstillstånd

— —

Tillståndsmyndigheten kan meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

———

Denna lag träder i kraft den 2022 .

———

Helsingfors den 2022

Statsminister

Sanna Marin

Familje- och omsorgsminister Aki Lindén