FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 30 augusti 2021

784/2021

Lag
om elektronisk behandling av kunduppgifter inom social- och hälsovården

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Lagens syfte

Syftet med denna lag är att främja och möjliggöra att kunduppgifter som produceras inom social- och hälsovården och uppgifter som kunden själv producerar om sitt välbefinnande behandlas på ett informationssäkert sätt i samband med ordnandet och produktionen av hälso- och sjukvård och socialtjänster. Ett syfte med lagen är också att främja kundens möjligheter att få information om behandlingen av de egna kunduppgifterna.

2 §

Tillämpningsområde och förhållande till övrig lagstiftning

Denna lag innehåller bestämmelser som kompletterar och preciserar 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 (allmän dataskyddsförordning), nedan *dataskyddsförordningen*, när kunduppgifter inom social- och hälsovården och uppgifter som kunden själv producerar om sitt välbefinnande behandlas elektroniskt i samband med ordnandet och produktionen av hälso- och sjukvård och socialtjänster. Denna lag innehåller också bestämmelser om behandlingen av uppgifter om välbefinnande vid främjande av en persons eget välbefinnande. Om det i denna lag föreskrivs annat än i dataskyddslagen (1050/2018), tillämpas bestämmelserna i denna lag.

Till den del som denna lag inte innehåller bestämmelser om behandling av kunduppgifter föreskrivs det om saken i lagen om patientens ställning och rättigheter (785/1992), nedan *patientlagen*, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan *klientlagen*, lagen om informationshantering inom den offentliga förvaltningen (906/2019), dataskyddslagen, lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019), lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan *offentlighetslagen*, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), lagen om tillhandahållande av digitala tjänster (306/2019), lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndig-

RP 212/2020
ShUB 11/2021
RSv 71/2021

heten för digitalisering och befolkningsdata (661/2009) samt arkivlagen (831/1994). Bestämmelser om språkliga rättigheter vid behandlingen av kunduppgifter och vid ordnandet av tjänster och verksamhet enligt denna lag finns dessutom i språklagen (423/2003). Bestämmelser om produkter och utrustning som används inom hälso- och sjukvården finns i lagen om vissa medicintekniska produkter enligt EU-direktiv (629/2010).

3 §

Definitioner

I denna lag avses med

1) *kund* en sådan klient inom socialvården som avses i klientlagen och en patient som avses i patientlagen,

2) *kundhandling* en sådan klienthandling inom socialvården som avses i klientlagen och i lagen om klienthandlingar inom socialvården (254/2015), nedan *klienthandlingslagen*, och en journalhandling som avses i patientlagen,

3) *klientuppgift inom socialvården* en personuppgift som gäller en kund och som ingår i en handling som avses i klientlagen eller klienthandlingslagen,

4) *patientuppgift* en personuppgift som gäller en patient och som ingår i en journalhandling som avses i patientlagen,

5) *kunduppgift* i 3 och 4 punkten avsedda klientuppgifter inom socialvården och patientupp- gifter,

6) *informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling som det i enlighet med de egenskaper som har planerats av tillverkaren är meningen att använda för elektronisk behandling av kunduppgifter och för registrering och uppdatering av kundhandlingar eller för anslutning till de riksomfattande informationssystemtjänsterna eller med vars hjälp en yrkesutbildad person inom social- och hälsovården kan använda uppgifter om välbefinnande,

7) *tjänstetillhandahållare* en anordnare och en producent av social- och hälsotjänster,

8) *serviceanordnare* en tjänstetillhandahållare som

a) i egenskap av myndighet är skyldig att se till att kunden får sådana tjänster eller förmåner som kunden har rätt till enligt lag eller ett myndighetsbeslut, eller

b) i egenskap av privat tjänstetillhandahållare är skyldig att se till att kunden får sådana tjänster som kunden har rätt till enligt ett avtal eller konsumentskyddsbestämmelserna,

9) *tjänsteproducent* en tjänstetillhandahållare som

a) i egenskap av serviceanordnare själv producerar social- eller hälsotjänster, eller

b) för en serviceanordnares räkning producerar social- eller hälsotjänster,

10) *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 informationssäkerhet,

11) *uppgifter om välbefinnande* sådana uppgifter som en person producerat om sin hälsa och sitt välbefinnande och som personen själv har fört in i den i 12 punkten avsedda informationsresursen för egna uppgifter,

12) *informationsresursen för egna uppgifter* en inom de riksomfattande informationssystemtjänsterna upprättad centraliserad elektronisk informationsresurs för bevarande och behandling av uppgifter om välbefinnande,

13) *välbefinnandeapplikation* ett sådant program i anslutning till informationsresursen för egna uppgifter som den enskilde använder och med vilket uppgifter om välbefinnande behandlas, och till vilket en person kan få sina kunduppgifter från arkiveringstjänsten, receptcentret och informationshanteringstjänsten,

14) *arkiveringstjänst* en informationsresurs där kunduppgifter och andra för social- och hälsovården behövliga uppgifter bevaras och med vars hjälp sådana uppgifter kan användas, och som godkända informationssystem kan anslutas till,

15) *informationshanteringstjänst* en riksomfattande informationssystemtjänst genom vilken sammandrag av patientuppgifter produceras,

16) *viljeyttringstjänst* en riksomfattande informationssystemtjänst genom vilken handlingar som gäller information, tillstånd för, samtycke till och förbud mot utlämnande, andra viljeyttringar med anknytning till hälso- och sjukvård samt socialtjänster samt andra viljeyttringar med anknytning till tjänster och behandling av kunduppgifter inom social- och hälsovården förvaltas,

17) *producent av en informationssystemtjänst* den som för en tjänstetillhandahållare tillhandahåller eller genomför ett informationssystem där kunduppgifter eller uppgifter om välbefinnande behandlas och som i egenskap av tillverkare av informationssystemet, för tillverkarens räkning eller för en eller flera tillverkares del ansvarar för de krav som ställs på informationssystemet,

18) *tillverkare av ett informationssystem* den som ansvarar för planeringen och tillverkningen av ett informationssystem för social- och hälsovården,

19) *mellanhand* en tjänsteleverantör som en tjänstetillhandahållare anlitar vid produktionen av informationssystemtjänster, genomförandet av informationssystemens tekniska eller fysiska miljö eller anslutningen till de riksomfattande informationssystemtjänsterna och som i denna roll har en möjlighet att se okrypterade kunduppgifter, exempelvis i samband med underhåll, och

20) *certifiering* ett förfarande genom vilket det verifieras att informationssystem och välbefinnandeapplikationer uppfyller de väsentliga krav som ställs på dem för att de ska få användas för produktion.

2 kap.

Personuppgiftsansvar i fråga om riksomfattande informationssystemtjänster

4 §

Personuppgiftsansvarig i fråga om de riksomfattande informationssystemtjänsterna

Folkpensionsanstalten är personuppgiftsansvarig i fråga om informationsresursen för egna uppgifter, förvaringstjänsten för logguppgifterna i utlämningsloggregistret och användningsloggarna i anslutning till dess egen verksamhet. Folkpensionsanstalten har dock inte rätt att behandla uppgifter i informationsresursen för egna uppgifter i större omfattning än vad som är nödvändigt för att administrera informationsresursen eller rätt att lämna ut uppgifter ur den för andra ändamål än de som anges i 13 § 2 mom. så som föreskrivs i det momentet.

Varje tillhandahållare av social- och hälsotjänster är personuppgiftsansvarig i fråga om de användningsloggar som uppkommer i dess verksamhet.

Varje tillhandahållare av social- och hälsotjänster samt Folkpensionsanstalten är gemensamt personuppgiftsansvariga för utlämningsloggar som uppkommer inom social- och hälsovården, för informationshanteringstjänsten och för viljeyttringstjänsten. Folkpensionsanstalten ansvarar i egenskap av gemensamt personuppgiftsansvarig för tillgängligheten och integriteten i fråga om uppgifterna, datainnehållets oföränderlighet samt för förvaring och utplåning av uppgifterna på det sätt som föreskrivs i 14 §. Tjänstetillhandahållare som för in uppgifter som ska sammanställas i informationshanteringstjänsten och tjänstetillhandahållare som för in uppgifter i viljeyttringstjänsten ansvarar för att uppgifterna är korrekta och för den personuppgiftsansvariges övriga skyldigheter. Folkpensionsanstalten är den kontaktpunkt som avses i artikel 26.1 i dataskyddsförordningen.

Gemensamt personuppgiftsansvariga för användningsloggarna för gränssnittet för professionellt bruk är den yrkesutbildade personen inom hälso- och sjukvården och Folkpensionsanstalten. Folkpensionsanstalten är kontaktpunkt för användningsloggarna för det gränssnittet.

Bestämmelser om receptcentrets personuppgiftsansvariga finns i 18 § i lagen om elektroniska recept (61/2007).

5 §

Tjänsteproducenters ansvar när de handlar för serviceanordnares räkning

När en tjänsteproducent tillhandahåller social- och hälsotjänster för en serviceanordnares räkning, ansvarar tjänsteproducenten

1) för införande och registrering av kunduppgifter för serviceanordnarens räkning,
2) för beviljande av åtkomsträttigheter till kunduppgifter inom den egna organisationen,
3) för aktiv styrning och övervakning av behandlingen av personuppgifter inom den egna organisationen,
4) för att kundhandlingarna i original lämnas till serviceanordnaren utan dröjsmål, och
5) tillsammans med serviceanordnaren för att kundens rättigheter enligt dataskyddsförordningen och offentlighetslagen tillgodoses.

Serviceanordnaren och tjänsteproducenten ska avtala närmare om lämnandet av de i 1 mom. 4 punkten avsedda kundhandlingarna och om tillgodoseendet av kundens rättigheter enligt 1 mom. 5 punkten samt om andra i artikel 28 i dataskyddsförordningen avsedda frågor.

3 kap.

Utförande av riksomfattande informationssystemtjänster inom social- och hälsovården

6 §

De riksomfattande informationssystemtjänsterna inom social- och hälsovården

För bevarandet och behandlingen av kunduppgifter ska Folkpensionsanstalten ordna följande riksomfattande informationssystemtjänster:

1) en riksomfattande arkiveringstjänst för kunduppgifter,
2) en förvaringstjänst för loggregister,
3) ett gränssnitt för professionell behandling av elektroniska recept,
4) ett medborgargränssnitt,
5) en informationsresurs för egna uppgifter,
6) en informationshanteringstjänst,
7) en viljeyttringstjänst,
8) ett receptcenter,
9) en läkemedelsdatabas, och
10) en informationsförmedlings- och förfrågningsservice.

Dessutom förutsätter utförandet av de riksomfattande informationssystemtjänsterna en kodtjänst och en roll- och attributtjänst. Tillstånds- och tillsynsverket för social- och hälsovården ska förvalta roll- och attributtjänsten och kodsystem med vars hjälp tjänstetillhandahållare, apotek, Folkpensionsanstalten och Myndigheten för digitalisering och befolkningsdata, för användning och certifiering av de riksomfattande informationssystemtjänsterna, får information om rätten att vara verksam som yrkesutbildad person inom so-

cial- och hälsovården och om giltighetstiden för denna rätt. Institutet för hälsa och välfärd ansvarar för innehållet i kodtjänsten.

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare i enlighet med lagen om stark autentisering och betrodda elektroniska tjänster för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tillhandahållare av social- och hälsovårdstjänster samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Myndigheten för digitalisering och befolkningsdata har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket för social- och hälsovården få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller.

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att för skötseln av sina lagstadgade uppgifter av Myndigheten för digitalisering och befolkningsdata få information om de certifikat som centralen utfärdat enligt 3 mom.

7 §

Skyldighet att ansluta sig som användare av de riksomfattande informationssystemtjänsterna

Tjänstetillhandahållare ska ansluta sig som användare av de riksomfattande informationssystemtjänster som avses i 6 § 1 mom. 1, 6, 7 och 8 punkten.

Privata tillhandahållare av social- och hälsotjänster ska ansluta sig som användare av de riksomfattande informationssystemtjänsterna, om de använder ett informationssystem som är avsett för behandling av klient- och patientuppgifter.

Andra aktörer inom social- och hälsovården, beträffande vilkas tjänster och behandling av personuppgifter viljeyttringar förs in i den viljeyttringstjänst som avses i 6 § 1 mom. 7 punkten, kan ansluta sig som användare av viljeyttringstjänsten.

Tillhandahållare av social-, hälso- och sjukvårdstjänster i landskapet Åland kan ansluta sig som användare av de riksomfattande informationssystemtjänsterna.

8 §

Handlingar som ska sparas i den riksomfattande arkiveringstjänsten

Av en elektronisk kundhandling får det i den riksomfattande arkiveringstjänsten finnas endast ett original som är specificerat med en identifikation. För utförande av en tjänst eller av någon annan grundad anledning får det av originalet göras ett extra exemplar av vilket det ska framgå att det inte är originalet.

Efter anslutning till de riksomfattande informationssystemtjänsterna ska tjänstetillhandahållaren spara kundhandlingarna i original i den riksomfattande arkiveringstjänsten. Kundhandlingar som uppkommit före anslutningen får sparas i den riksomfattande arkiveringstjänsten. I arkiveringstjänsten får det utöver kundhandlingar även sparas andra handlingar som hänför sig till ordnandet av social- och hälsovården och till informationshanteringen.

Bestämmelser om förvaringstider för klienthandlingar inom socialvården finns i 27 § i klienthandlingslagen. Bestämmelser om förvaringstider för journalhandlingar finns i 12 § i patientlagen.

9 §

Datastrukturerna för informationssystem och kundhandlingar som hänför sig till de riksomfattande informationssystemtjänsterna

Informationssystemens och kundhandlingarnas datastrukturer ska möjliggöra användning, utlämnande, bevarande och skydd av elektroniska kundhandlingar och kunduppgifter med hjälp av de riksomfattande informationssystemtjänster som avses i 6 §.

Institutet för hälsa och välfärd meddelar föreskrifter om kundhandlingarnas datainnehåll och datastrukturer i informationssystemen för att de riksomfattande informationssystemtjänsterna ska kunna utföras samt om de kodsystem som överallt i landet ska användas i datastrukturerna.

10 §

Elektronisk underskrift av handlingar

Handlingarnas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk underskrift vid elektronisk behandling, överföring och förvaring av uppgifterna.

Vid elektronisk signering som görs av en fysisk person ska det användas en sådan avancerad elektronisk underskrift som det föreskrivs om 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. Bestämmelser om elektronisk underskrift finns också i lagen om stark autentisering och betrodda elektroniska tjänster. Vid signering som görs av en organisation och datatekniska enheter ska det användas en elektronisk underskrift av motsvarande tillförlitlighet.

11 §

Informationshanteringstjänsten

Informationshanteringstjänsten sammanställer sådana patientuppgifter i journalhandlingar som är viktiga för genomförandet av hälso- och sjukvården och producerar sammandrag av dem för tjänstetillhandahållare för genomförande av patientens vård. Viktiga patientuppgifter som informationshanteringstjänsten kan sammanställa är diagnoser och besöksorsaker, risker, laboratorieresultat, vaccinationer, åtgärder, medicineringsuppgifter, fysiologiska mätningar och bilddiagnostiska undersökningar som har antecknats enligt kodsystemet för åtgärderna, uppgifter med anknytning till funktionsförmågan, tidsbokningsuppgifter samt i 4 a § i patientlagen avsedda planer för undersökning, vård och medicinsk rehabilitering eller andra motsvarande planer. Uppgifter får lämnas ut med hjälp av informationshanteringstjänsten på det sätt som föreskrivs i 20 §. Uppgifter i informationshanteringstjänsten får behandlas inom ramen för de åtkomsträttigheter som anges i 15 §.

12 §

Viljeyttringstjänsten

I viljeyttringstjänsten ska det föras in uppgifter om information som en person har fått enligt denna lag och lagen om elektroniska recept samt om tillstånd för, samtycke till och förbud mot utlämnande som en person har meddelat i fråga om kunduppgifter.

I viljeyttringstjänsten kan det även föras in uppgift om en persons

1) andra viljeyttringar i fråga om hälso- och sjukvård eller socialtjänster än sådana som avses i 1 mom.,

2) andra viljeyttringar i fråga om tjänster inom social- och hälsovården och behandling av kunduppgifter än sådana som avses i 1 mom.

13 §

Informationsresursen för egna uppgifter

En person kan med hjälp av välbefinnandeapplikationer eller ett medborgargränssnitt föra in uppgifter om sitt välbefinnande i informationsresursen för egna uppgifter och via den använda uppgifterna för att främja sitt välbefinnande. En person har rätt att besluta om användningen av sina uppgifter, om ändring av dem och om avlägsnande av uppgifterna från informationsresursen.

En person kan ge sitt samtycke till att de uppgifter om välbefinnande som finns i informationsresursen för egna uppgifter får utlämnas till en tjänstetillhandahållare för tillhandahållande av social- och hälsotjänster.

Bestämmelser om registrering av uppgifter som påverkar vården eller tjänster i kund- eller journalhandlingarna finns i patientlagen, klientlagen och klienthandlingslagen.

De uppgifter som finns om en person i informationsresursen för egna uppgifter ska bevaras tills personen avlägsnar dem ur informationsresursen eller tills högst fem år har förflutit från personens död.

14 §

Folkpensionsanstaltens ansvar när den förvaltar riksomfattande informationssystemtjänster

De riksomfattande informationssystemtjänsterna och de införda uppgifterna ska alltid vara tillgängliga. Informationssystemtjänsterna ska ha de reservsystem som behövs med tanke på funktionsstörningar och undantagsförhållanden.

Folkpensionsanstalten svarar

1) för den tekniska realisering och de tekniska anvisningar som de riksomfattande informationssystemtjänsterna kräver,

2) för säkerställande av säkerhet på det sätt som föreskrivs i 14 § i lagen om informationshantering inom den offentliga förvaltningen i fråga om kunduppgifter, uppgifter om välbefinnande och andra uppgifter som förts in i de riksomfattande informationssystemtjänsterna samt för utplåning av uppgifterna efter det att förvaringstiden gått ut,

3) för att de riksomfattande informationssystemtjänster som anstalten ansvarar för utförs så att kunduppgifter, uppgifter om välbefinnande och andra uppgifter som har införts i de riksomfattande informationssystemtjänsterna lämnas ut endast i enlighet med denna lag och lagen om sekundär användning av personuppgifter inom social- och hälsovården,

4) för att användning och utlämnande av kunduppgifter och uppgifter om välbefinnande registreras i ett loggregister,

5) för det datatekniska utförandet av kodtjänsten,

6) för information till befolkningen med avseende på de riksomfattande informationssystemtjänsterna,

7) för testning av interoperabiliteten hos informationssystem och välbefinnandeapplikationer som ska anslutas till de riksomfattande informationssystemtjänsterna.

Folkpensionsanstalten har rätt

1) att av Tillstånds- och tillsynsverket för social- och hälsovården få sådana uppgifter om yrkesutbildade personer inom social- och hälsovården som behövs för skötseln av lagstadgade uppgifter med avseende på de riksomfattande informationssystemtjänsterna,

2) att behandla kunduppgifter och uppgifter om välbefinnande till den del det är nödvändigt med tanke på uppgifter som hänför sig till förvaltningen av de riksomfattande informationssystemtjänsterna,

3) att besluta om frågor som gäller ett systems datatekniska funktion, om inte något annat följer av denna lag eller av bestämmelser som har utfärdats med stöd av den,

4) att lämna ut handlingar som omfattas av Folkpensionsanstaltens personuppgiftsansvar, och logguppgifter över sådana handlingar, till tjänstetillhandahållare inom social- och hälsovården för uppföljning och tillsyn i fråga om användning och utlämnande av kunduppgifter, om det är uppenbart att genomförandet av säkerhetsarrangemangen inte äventyras därigenom,

5) att i syfte att öka informationssäkerheten utöva tillsyn över användningen av sina tjänster och av de uppgifter som bevaras i dessa tjänster,

6) att trots sekretessen av Myndigheten för digitalisering och befolkningsdata få nödvändig information som behövs för skötseln av uppgifter som gäller de riksomfattande informationssystemtjänsterna.

Folkpensionsanstalten kan göra och till de myndigheter som svarar för styrning, övervakning och utveckling av de riksomfattande informationssystemtjänsterna lämna ut sammanställningar över uppgifter i dessa tjänster, över handlingars metadata och över logguppgifter, om sammanställningarna har betydelse för utvecklingen och uppföljningen av de riksomfattande informationssystemtjänsterna eller för rapporteringen.

I skyddet av de riksomfattande informationssystemtjänsterna iakttas vad som föreskrivs särskilt om statliga myndigheters och kommuners informationssäkerhetsskyldigheter. Folkpensionsanstalten får inte på en utomstående överlåta behandlingen eller bevarandet av i denna lag avsedda register som har samband med ordnandet av de riksomfattande informationssystemtjänsterna, eller av loggregister som hänför sig till sådana register.

4 kap.

Behandling av kunduppgifter inom social- och hälsovården

15 §

Åtkomsträttigheter till kunduppgifter

Åtkomsträttigheterna till kunduppgifter ska grunda sig på de arbetsuppgifter som en yrkesutbildad person inom social- eller hälsovården eller någon annan som behandlar kund- och patientuppgifter sköter och de tjänster som denna person tillhandahåller, så att personen har åtkomsträtt endast till de nödvändiga kunduppgifter som han eller hon behöver i sina arbetsuppgifter och beträffande vilka han eller hon har rätt att få uppgifter. Behandlingen av kunduppgifter ska grunda sig på en kund- eller vårdrelation eller någon annan lagstadgad rätt som har säkerställts datatekniskt.

Bestämmelser om vilka uppgifter yrkesutbildade personer och andra personer som behandlar kunduppgifter får använda på grund av sina arbetsuppgifter och de tjänster som de tillhandahåller utfärdas genom förordning av social- och hälsovårdsministeriet.

Tjänstetillhandahållaren ska bestämma vilken rätt yrkesutbildade personer inom social- och hälsovården och andra personer som behandlar kunduppgifter har att använda sådana uppgifter. Tjänstetillhandahållaren ska föra register över dem som använder tjänstetillhandahållarens kundinformationssystem och kundregister och över deras åtkomsträttigheter.

16 §

Information till kunden om riksomfattande informationssystemtjänster

Tjänstetillhandahållaren ska informera kunden om kundens rättigheter, om de riksomfattande informationssystemtjänster som omfattar hans eller hennes kunduppgifter och om de allmänna principerna för hur tjänsterna fungerar. Kunden ska ges informationen senast i samband med den första kontakten.

Institutet för hälsa och välfärd svarar för sakinnehållet i informationen till kunderna, och Folkpensionsanstalten svarar för informationsmaterialet.

17 §

Identifiering av dem som behandlar kunduppgifter

Vid elektronisk behandling av kunduppgifter ska kunden, tjänstetillhandahållaren, andra parter i behandlingen av kunduppgifter och deras företrädare samt de datatekniska enheterna identifieras på ett tillförlitligt sätt. De personer som behandlar kunduppgifter, tjänstetillhandahållarna, de datatekniska enheterna och de riksomfattande informationssystemtjänsterna ska identifieras genom verifiering.

Närmare bestämmelser om de tekniska identifierings- och verifieringsmedlen får utfärdas genom förordning av social- och hälsovårdsministeriet. Innan förordningen utfärdas ska social- och hälsovårdsministeriet höra Myndigheten för digitalisering och befolkningsdata.

18 §

Tillstånd för, samtycke till och förbud mot utlämnande

En kund får meddela tillstånd för och samtycke till utlämnande enligt 20 och 21 § via riksomfattande informationssystemtjänster.

Tillstånd för utlämnande enligt 20 § 1 mom. och 21 § 1 mom. ska grunda sig på tillräcklig information som ges i ett förfarandet enligt 16 § och ska ha lämnats frivilligt. Ett tillstånd för utlämnande gäller tills vidare och kan återtas. Bestämmelser om samtycke till utlämnande enligt 20 § 2 mom. och 21 § 2 mom. finns i dataskyddsförordningen.

Om kunden saknar förutsättningar att bedöma betydelsen av ett tillstånd för eller ett samtycke till utlämnande, får kunduppgifter lämnas ut med stöd av ett tillstånd eller samtycke som lämnats av kundens lagliga företrädare. Kundens lagliga företrädare har rätt att trots tystnadsplikten få de uppgifter om kunden som är nödvändiga för att meddela och effektuera tillstånd för eller samtycke till utlämnande.

En kund har rätt att förbjuda att en personuppgiftsansvarig inom socialvården lämnar ut klientuppgifter inom socialvården om honom eller henne till en annan personuppgiftsansvarig inom socialvården via riksomfattande informationssystemtjänster. En patient har rätt att förbjuda att en personuppgiftsansvarig inom hälso- och sjukvården lämnar ut patientuppgifter om honom eller henne till ett annat register inom hälso- och sjukvården eller till en annan personuppgiftsansvarig inom hälso- och sjukvården via riksomfattande informationssystemtjänster. En vårdnadshavare eller en annan laglig företrädare har inte rätt att förbjuda utlämnande av patientuppgifter för en minderårigs räkning i situationer som avses i 13 § 3 mom. 3 punkten i patientlagen.

Ett förbud som kunden eller patienten meddelar kan gälla alla hans eller hennes klientuppgifter inom socialvården och patientuppgifter. Förbudet kan gälla en personuppgiftsansvarig inom offentlig social- och hälsovård och dess register samt en personuppgiftsansvarig inom privat socialvård och företagshälsovårdens register inom privat hälso- och sjukvård. Inom socialvården kan förbudet gälla en serviceuppgift inom socialvården eller en enskild kundhandling. Inom hälso- och sjukvården kan förbudet gälla en servicehändelse.

Genom ett förbud går det inte att förhindra en yrkesutbildad persons eller en myndighets på lag grundade och av kundens eller patientens viljeyttring oberoende rätt att få information.

Ett förbud ska grunda sig på tillräcklig information som ges i ett förfarande enligt 16 § och ska ha lämnats frivilligt. Ett förbud gäller tills vidare och får återtas.

19 §

Meddelande och återkallande av tillstånd för, samtycke till och förbud mot utlämnande

Meddelande av tillstånd för, samtycke till och förbud mot utlämnande av kunduppgifter lämnas till en tjänstetillhandahållare som har anslutit sig till den riksomfattande informationssystemtjänsten eller via ett medborgargränssitt. Tjänstetillhandahållaren ska utan dröjsmål föra in uppgift om det meddelade tillståndet, samtycket eller förbudet i viljeyttringstjänsten.

Den som tar emot ett tillstånd för, samtycke till och förbud mot utlämnande ska på begäran ge kunden en utskrift av tillståndshandlingen, samtyckeshandlingen eller förbudshandlingen eller vid behov ge kunden handlingen i fråga på ett annat sätt som är tillgängligt.

Folkpensionsanstalten fastställer innehållet i en tillståndshandling, samtyckeshandling och förbudshandling. Av tillståndshandlingen, samtyckeshandlingen respektive förbudshandlingen ska tillståndets, samtyckets eller förbudets betydelse vid behandlingen av kunduppgifter framgå.

På återkallande av tillstånd för, samtycke till och förbud mot utlämnande tillämpas vad som i 1–3 mom. föreskrivs om meddelande av tillstånd, samtycke och förbud.

20 §

Utlämnande av patientuppgifter med hjälp av riksomfattande informationssystemtjänster

Trots sekretessbestämmelserna får patientuppgifter inom hälso- och sjukvården med hjälp av de i 6 § avsedda riksomfattande informationssystemtjänsterna lämnas ut till en annan tjänstetillhandahållare inom hälso- och sjukvården eller till ett annat patientregister hos samma tjänstetillhandahållare för ordnande, produktion och tillhandahållande av hälso- och sjukvård för patienten. Patientuppgifter får dock inte lämnas ut utan att patienten meddelat tillstånd att lämna ut uppgifter eller utan någon grund som anges i 13 § 3 mom. 3 punkten i patientlagen eller i någon annan lag angiven grund som berättigar till utlämnande.

Trots sekretessbestämmelserna får patientuppgifter inom hälso- och sjukvården, om patienten samtycker, lämnas ut till en tjänstetillhandahållare inom socialvården för ordnande, produktion och tillhandahållande av socialvård. Bestämmelser om förutsättningarna för samtycke finns i artikel 7 i dataskyddsförordningen.

Uppgifter om en patient lämnas till tjänstetillhandahållare med hjälp av riksomfattande informationstjänster efter det att patienten har informerats i enlighet med 16 § och existensen av en kund- eller vårdrelation mellan patienten och den som framställt begäran om utlämnande har säkerställts datatekniskt, om inte patienten med stöd av 18 § har förbjudit att uppgifter om honom eller henne lämnas ut. Bestämmelser om åtkomsträtt till nödvändiga patientuppgifter finns i 15 §.

Patientuppgifter får lämnas ut till kunden med hjälp av en välbefinnandeapplikation eller ett medborgargränssnitt. För att få uppgifterna via välbefinnandeapplikationen ska patienten ta i bruk applikationen och godkänna att uppgifterna lämnas ut.

21 §

Utlämnande av klientuppgifter inom socialvården med hjälp av riksomfattande informationssystemtjänster

Trots sekretessbestämmelserna får klientuppgifter inom socialvården med hjälp av de i 6 § avsedda riksomfattande informationssystemtjänsterna lämnas ut till en annan tjänstetillhandahållare inom socialvården för ordnande, produktion och tillhandahållande av so-

cialvård för kunden. Klientuppgifter får dock inte lämnas ut utan kundens tillstånd eller i någon annan lag angiven grund som berättigar till utlämnande.

Trots sekretessbestämmelserna får klientuppgifter inom socialvården, om kunden samtycker, lämnas ut till en tjänstetillhandahållare inom hälso- och sjukvården för ordnande, produktion och tillhandahållande av hälso- och sjukvård. Bestämmelser om förutsättningarna för samtycke finns i artikel 7 i dataskyddsförordningen.

Utlämnande på basis av begäran av uppgifter om en kund till tjänstetillhandahållare sker med hjälp av riksomfattande informationssystemtjänster efter det att kunden har informerats i enlighet med 16 § och existensen av en kund- eller vårdrelation mellan kunden och den som framställt begäran om utlämnande har säkerställts datatekniskt, om inte kunden med stöd av 18 § har förbjudit att uppgifter om honom eller henne lämnas ut. Bestämmelser om åtkomsträtt till nödvändiga kunduppgifter finns i 15 §.

Klientuppgifter inom socialvården får lämnas ut till kunden med hjälp av en välbefinnandeapplikation eller ett medborgargränssnitt. För att få uppgifterna via välbefinnandeapplikationen ska kunden ta i bruk applikationen och godkänna att uppgifterna lämnas ut.

22 §

Förmedling av kunduppgifter med hjälp av riksomfattande informationssystemtjänster till aktörer utanför social- och hälsovården

Med hjälp av de riksomfattande informationssystemtjänsterna får intyg, utlåtanden och andra handlingar som innehåller kunduppgifter förmedlas till en aktör utanför social- och hälsovården. Handlingar får trots sekretessbestämmelserna förmedlas med stöd av kundens begäran eller mottagarens lagstadgade begäran eller utlämnarens lagstadgade uppgiftsskyldighet. Kundhandlingarna förmedlas med hjälp av den informationsförmedlings- och förfrågningsservice som hör till de riksomfattande informationssystemtjänsterna.

Institutet för hälsa och välfärd meddelar föreskrifter om vilka slags handlingar som får förmedlas med hjälp av informationsförmedlings- och förfrågningsservicen.

23 §

Användning av e-tjänster och behandling av uppgifter för någon annans räkning

En person har rätt att med stöd av en fullmakt eller med stöd av 29 § 2 mom. i lagen om förmyndarverksamhet (442/1999) för en annan persons räkning behandla sådana uppgifter om denna person som har sparats i en riksomfattande informationssystemtjänst. En vårdnadshavare har rätt att behandla sådana uppgifter om en person som vårdnadshavaren har vårdnaden om vilka har sparats i en riksomfattande informationssystemtjänst, om inte något annat följer av 11 § 3 mom. i klientlagen, 9 § 2 mom. i patientlagen, artikel 8.1 i dataskyddsförordningen, 5 § i dataskyddslagen eller 4 § 4 mom. i lagen angående vårdnad om barn och umgängesrätt (361/1983).

24 §

Medborgargränssnitt samt kunduppgifter och viljeyttringar som visas via det

En person kan avge viljeyttringar och sköta ärenden som gäller sitt kundförhållande och administreringen av kunduppgifterna och uppgifterna om välbefinnande via ett medborgargränssnitt.

Personen får via medborgargränssnittet visas eller få sådana uppgifter om sig själv som finns sparade i de riksomfattande informationssystemtjänsterna, med undantag för uppgifter som kunden enligt 11 § 2 mom. i offentlighetslagen eller enligt annan lagstiftning inte har rätt att få. Dessutom får personen via gränssnittet visas utlämningslogguppgifter och

användningsloggуppgifter som gäller behandlingen av hans eller hennes uppgifter, med undantag för mottagarens personuppgifter.

Trots det som föreskrivs i 2 mom. får en person visas namnet på en person som handlat för hans eller hennes räkning.

25 §

Uppföljning av användning och utlämnande av kunduppgifter och uppgifter om välbefinnande

En tjänstetillhandahållare ska för uppföljningen och tillsynen särskilt för varje kundregister samla in loggуppgifter om all användning och allt utlämnande av kunduppgifter.

I användningsloggregistret ska det föras in uppgifter om använda kunduppgifter och uppgifter om välbefinnande, den tjänstetillhandahållare vars kunduppgifter används, den som har använt kunduppgifter och uppgifter om välbefinnande, användningsändamålet och användningstidpunkten samt andra uppgifter som behövs för tillsynen och uppföljningen av användningen.

I utlämningsloggregistret ska det föras in uppgifter om utlämnade kunduppgifter, den tjänstetillhandahållare vars kunduppgifter lämnas ut, den som lämnat ut kunduppgifterna, utlämningsändamålet, mottagaren och tidpunkten för utlämnandet samt andra uppgifter som behövs för tillsynen och uppföljningen av utlämnandet.

Folkpensionsanstalten ska för uppföljning och tillsyn i fråga om de uppgifter som har sparats i de i 6 § avsedda riksomfattande informationssystemtjänsterna och som har lämnats ut via dem samla in dels utlämningsloggуppgifter av vilka det utlämnade datainnehållet, mottagaren, tidpunkten för utlämnandet och andra behövliga uppgifter framgår, dels användningsloggуppgifter för de uppgifter som har behandlats i gränssnittet för professionellt bruk. I den förvaringstjänst för loggregister som avses i 6 § sparas loggуppgifter om utlämnande av en tjänstetillhandahållares kundhandlingar. I förvaringstjänsten för loggregister får loggуppgifter om användning sparas.

Närmare bestämmelser om förvaringstiden för loggуppgifter får utfärdas genom förordning av social- och hälsovårdsministeriet. Institutet för hälsa och välfärd får meddela närmare föreskrifter om de uppgifter som ska föras in i loggregistren och om deras datainnehåll.

26 §

Kundens rätt att få information om behandlingen av sina egna uppgifter

En kund har för utredning eller utövande av sina rättigheter i anslutning till behandlingen av sina kunduppgifter rätt att på skriftlig begäran inom skälig tid och senast inom två månader av tjänstetillhandahållaren utifrån loggregistret avgiftsfritt få veta vem som har använt eller till vem det har lämnats ut uppgifter om honom eller henne samt grunden för användningen eller utlämnandet. Kunden har motsvarande rätt att av Folkpensionsanstalten få loggуppgifter ur informationshanteringstjänsten, viljeyttringstjänsten, receptcentret och informationsresursen för egna uppgifter, loggуppgifter för använda eller utlämnade kunduppgifter och uppgifter om välbefinnande samt uppgifter om tidpunkten för användningen eller utlämnandet till den del uppgifterna omfattas av Folkpensionsanstaltens personuppgiftsansvar.

Kunden har dock ingen rätt att få loggуppgifter, om den som ombeds lämna ut dem vet att utlämnandet av uppgifterna kan medföra allvarlig fara för kundens hälsa eller vård eller för någon annans rättigheter. Kunden har inte heller rätt att utan särskild orsak få loggуppgifter som är äldre än två år. Kunden får inte för något annat ändamål än för att utreda eller utöva sina rättigheter i anslutning till behandlingen av sina kunduppgifter använda eller lämna vidare loggуppgifter som han eller hon fått.

Om en kund på nytt begär logguppgifter som han eller hon redan har fått, får tjänstetillhandahållaren eller Folkpensionsanstalten för lämnandet av dessa logguppgifter ta ut en skälig ersättning, som inte får överstiga de direkta kostnaderna för lämnandet av uppgifterna. För tillgång till logguppgifter med hjälp av det i 24 § avsedda medborgargränssnittet får dock ingen avgift tas ut.

Om tjänstetillhandahållaren eller Folkpensionsanstalten anser att logguppgifterna inte får lämnas ut till kunden, ska det fattas ett skriftligt avslagsbeslut. Ärendet kan föras till dataombudsmannen för behandling i enlighet med 21 § 1 mom. i dataskyddslagen.

Om en kund anser att hans eller hennes kunduppgifter har använts eller lämnats ut utan tillräckliga grunder, ska den tjänstetillhandahållare som använt eller fått uppgifterna eller Folkpensionsanstalten på begäran ge kunden en redogörelse för grunderna för användningen eller utlämnandet av uppgifterna och lägga fram sin motiverade uppfattning om huruvida det har varit lagligt att använda eller lämna ut uppgifterna. Om tjänstetillhandahållaren bedömer att behandlingen av uppgifterna varit lagstridig, ska tjänstetillhandahållaren på eget initiativ vidta nödvändiga åtgärder.

5 kap.

Egenkontroll av informationssäkerhet och dataskydd

27 §

Informationssäkerhetsplan

En tjänstetillhandahållare, en mellanhand och Folkpensionsanstalten ska utarbeta en informationssäkerhetsplan med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen. Planen ska innehålla redogörelser för hur följande krav som hänför sig till behandlingen av kund- och patientuppgifterna och systemen säkerställs:

1) de som använder informationssystemen har den utbildning som användningen kräver,

2) i samband med informationssystemen finns behövliga bruksanvisningar för en korrekt användning av systemen,

3) informationssystemen används enligt anvisningar från producenten av informationssystemtjänsten,

4) informationssystemen drivs och uppdateras enligt anvisningar från producenten av informationssystemtjänsten,

5) informationssystemens driftsmiljö är lämplig för en sådan ändamålsenlig användning av informationssystemen som säkerställer informationssäkerheten och dataskyddet,

6) övriga anslutna informationssystem och andra system äventyrar inte informationssystemens prestanda eller egenskaper när det gäller informationssäkerhet och dataskydd,

7) informationssystemen installeras, drivs och uppdateras endast av personer med den yrkesskicklighet och sakkunskap som behövs,

8) informationssystem som avses i 29 § uppfyller i 34 § föreskrivna väsentliga krav som ställs enligt deras användningsändamål, och

9) tjänstetillhandahållaren, mellanhanden och Folkpensionsanstalten har en plan för hur egenkontrollen ska ordnas och genomföras inom dess verksamhet.

Innan en tjänstetillhandahållare ansluter sig som användare av de riksomfattande informationstjänsterna, ska det i tjänstetillhandahållarens informationssäkerhetsplan redogöras för hur man har tillgodosett kraven på dataskydd och en informationssäker användning av dessa riksomfattande tjänster.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om de i 1 och 2 mom. avsedda redogörelser och krav som ska tas in i informationssäkerhetsplanen och om verifiering av informationssäkerheten.

28 §

Genomförande av och ansvar för egenkontroll av informationssäkerheten

Den ansvariga föreståndaren hos en tillhandahållare av social- och hälsovårdstjänster ska se till att en informationssäkerhetsplan enligt 27 § utarbetas och iakttas. Den ansvariga föreståndaren ska meddela skriftliga instruktioner om hur kunduppgifter ska behandlas och om de förfaringssätt som ska iakttas samt se till att personalen har tillräcklig sakkunskap och kompetens för behandlingen av kunduppgifter.

För uppföljning och tillsyn i fråga om dataskyddet och informationssäkerheten har tjänstetillhandahållaren rätt att av Folkpensionsanstalten få logguppgifter för de egna kundregistren, logguppgifter som hänför sig till behandlingen av uppgifter i informationshanteringstjänsten och viljeyttringstjänsten och logguppgifter för informationsresursen för egna uppgifter till den del som den berörda tjänstetillhandahållarens anställda har läst och behandlat kundens uppgifter i informationshanteringstjänsten, viljeyttringstjänsten och informationsresursen för egna uppgifter, om det behövs för att utreda om behandlingen av kundens kunduppgifter är lagenlig.

Folkpensionsanstalten och en mellanhand ska följa genomförandet av informationssäkerhetsplanen.

Bestämmelser om utnämning av ett dataskyddsombud och om dataskyddsombudets ställning och uppgifter finns i artiklarna 37–39 i dataskyddsförordningen.

6 kap.

Informationssystemens och välbefinnandeapplikationernas användningsändamål och ibruktagande

29 §

Informationssystemens och välbefinnandeapplikationernas användningsändamål och klassificering

Producenten av en informationssystemtjänst ska utarbeta en beskrivning av informationssystemets användningsändamål och hur det uppfyller väsentliga krav. Detsamma gäller tillverkaren av en välbefinnandeapplikation i fråga om välbefinnandeapplikationen.

Informationssystemen för social- och hälsovården och välbefinnandeapplikationerna ska enligt användningsändamål och egenskaper delas in i klasserna A och B. Till klass A hör

1) de riksomfattande informationssystemtjänster som förvaltas av Folkpensionsanstalten,

2) de informationssystem och välbefinnandeapplikationer som behandlar kunduppgifter och som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna,

3) sådana andra informationssystem och välbefinnandeapplikationer och tjänster tillhandahållna av mellanhänder som i fråga om sitt användningsändamål kräver certifiering.

Andra informationssystem än de som avses i 2 mom. hör till klass B.

Institutet för hälsa och välfärd får meddela föreskrifter om klassificeringen av informationssystem. I oklara fall beslutar Institutet för hälsa och välfärd huruvida ett informationssystem hör till klass A eller klass B.

30 §

Registrering av informationssystem och välbefinnandeapplikationer

Producenten av en informationssystemtjänst ska göra en anmälan om informationssystem och tillverkaren av en välbefinnandeapplikation ska göra en anmälan om välbefinnandeapplikationer till Tillstånds- och tillsynsverket för social- och hälsovården innan informationssystemen eller välbefinnandeapplikationerna tas i användning för produktion av tjänster. Av anmälan ska informationssystemets eller välbefinnandeapplikationens tillverkare och användningsändamål framgå, och till anmälan ska det fogas i 35 och 36 § avsedda utredningar om och i 37 § avsett intyg över att de väsentliga krav som ställs på systemet eller applikationen enligt dess användningsändamål uppfylls. Om producenten av en informationssystemtjänst är någon annan än tillverkaren av informationssystemet, ska också producenten framgå av anmälan. Producenten av en informationssystemtjänst ska göra en anmälan om att en sådan version av ett informationssystem som är avsedd att användas för produktion av tjänster inte längre stöds eller att en annan aktör övertagit ansvaret för informationssystemet.

Tillstånds- och tillsynsverket för social- och hälsovården ska föra ett offentligt register över de informationssystem för social- och hälsovården samt välbefinnandeapplikationer som har anmälts till verket. Registret ska innehålla uppgifter om

1) informationssystem och välbefinnandeapplikationer som är avsedda att användas för produktion av tjänster, deras användningsändamål och de väsentliga krav som de uppfyller,

2) resultat av interoperabilitetstestningen av informationssystem och välbefinnandeapplikationer som hör till klass A och som har godkänts för användning i produktion av tjänster,

3) giltighetstiden för det intyg över bedömning av informationssäkerhet som utfärdats enligt en bedömning av informationssäkerhet för informationssystem och välbefinnandeapplikationer som hör till klass A och har godkänts för användning i produktion av tjänster, och

4) en betydande avvikelse hos ett informationssystem eller en välbefinnandeapplikation som hör till klass A och som används i produktion av tjänster, medan avvikelsen varar.

Tillstånds- och tillsynsverket för social- och hälsovården får meddela föreskrifter om innehållet i anmälan, den tid anmälan är i kraft, förnyande av anmälan och vilka uppgifter som ska antecknas i registret.

31 §

Tagande av informationssystem och välbefinnandeapplikationer i användning för produktion av tjänster

Ett informationssystem eller en välbefinnandeapplikation som hör till klass A får tas i användning för produktion av tjänster och anslutas till de riksomfattande informationssystemtjänsterna efter det att systemet eller applikationen har certifierats i enlighet med 35 §.

Ett informationssystem eller en välbefinnandeapplikation får inte tas i användning för produktion av tjänster, om det inte finns giltiga uppgifter om systemet eller applikationen i det i 30 § 2 mom. avsedda registret, eller om intyget över bedömning av informationssäkerhet för ett informationssystem eller en välbefinnandeapplikation som hör till klass A har gått ut.

32 §

Uppföljning efter ibruktagandet av informationssystem och välbefinnandeapplikationer

Producenten av en informationssystemtjänst ska genom ett uppdaterat och systematiskt förfarande följa och utvärdera de erfarenheter som fås av informationssystemet under den tid det används för produktion av tjänster. Detsamma gäller tillverkaren av en välbefinnandeapplikation i fråga om välbefinnandeapplikationen. Anmälan om betydande avvikelser från de väsentliga krav som ställs på ett informationssystem ska göras till alla tjänstetillhandahållare som använder systemet. Anmälan om betydande avvikelser i en välbefinnandeapplikation ska göras till alla som använder applikationen. Betydande avvikelser i informationssystem och välbefinnandeapplikationer som hör till klass A ska av producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation anmälas till Folkpensionsanstalten och Tillstånds- och tillsynsverket för social- och hälsovården.

Producenten av en informationssystemtjänst ska ge akt på ändringar i de väsentliga krav som ställs på informationssystemen och justera systemen i enlighet med ändringarna. Detsamma gäller tillverkaren av en välbefinnandeapplikation i fråga om välbefinnandeapplikationen. Bedömningsorganet för informationssäkerhet och Folkpensionsanstalten ska underrättas om väsentliga ändringar i informationssystem och välbefinnandeapplikationer som hör till klass A. Ett nytt intyg över bedömning av informationssäkerhet ska utfärdas eller interoperabilitetstestningen göras om, om betydande ändringar görs i ett informationssystem eller i en välbefinnandeapplikation eller om de väsentliga kraven har ändrats på ett sätt som kräver en ny certifiering.

Producenten av en informationssystemtjänst och tillverkaren av en välbefinnandeapplikation ska bevara uppgifter om interoperabilitet och informationssäkerhet samt övriga uppgifter som tillsynen kräver i minst fem år efter det att informationssystemet eller välbefinnandeapplikationen inte längre används för produktion av tjänster.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om de i 1 mom. avsedda betydande avvikelserna och om hur anmälningar om sådana ska göras.

7 kap.

Väsentliga krav på informationssystem och välbefinnandeapplikationer

33 §

Allmänna skyldigheter för tillverkare av informationssystem och välbefinnandeapplikationer och producenter av informationssystemtjänster

Tillverkaren av ett informationssystem för social- och hälsovården ansvarar för planeringen och tillverkningen av informationssystemet, oberoende av om dessa åtgärder utförs av tillverkaren själv eller av någon annan för dennes räkning. Tillverkaren av en välbefinnandeapplikation ansvarar för planeringen och tillverkningen av applikationen.

Producenten av en informationssystemtjänst ska utarbeta en beskrivning av informationssystemets användningsändamål och i samband med informationssystemet ge systemanvändarna sådana uppgifter och anvisningar om systemets ibruktagande, användning för produktion av tjänster och drift som de behöver för systemets interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. Detsamma gäller tillverkaren av en välbefinnandeapplikation i fråga om välbefinnandeapplikationen.

De uppgifter och anvisningar som ges tillsammans med informationssystemet ska finnas på finska, svenska eller engelska. De uppgifter och anvisningar som är avsedda för social- och hälsovårdspersonal som använder informationssystemet ska finnas på finska eller svenska.

Tillverkaren av ett informationssystem ska ha ett kvalitetssystem som tillämpas på planeringen och tillverkningen av informationssystemet på det sätt som informationssystemets användningsändamål förutsätter.

34 §

Väsentliga krav på informationssystem och välbefinnandeapplikationer

Ett informationssystem och en välbefinnandeapplikation som används vid behandling av kunduppgifter ska uppfylla väsentliga krav på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. En välbefinnandeapplikation ska uppfylla tillgänglighetskraven. Kraven ska uppfyllas vid användningen av ett informationssystem såväl självständigt som tillsammans med andra informationssystem som är avsedda att anslutas till det.

De informationssystem som en tjänstetillhandahållare använder ska till sitt användningsändamål svara mot tjänstetillhandahållarens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarens verksamhet. De väsentliga kraven kan uppfyllas genom en helhet som består av ett eller flera informationssystem.

Ett informationssystem uppfyller de väsentliga kraven när det har planerats och tillverkats samt fungerar i enlighet med de lagar som gäller informationssäkerhet och dataskydd och de bestämmelser som utfärdats med stöd av dessa lagar samt följer nationella bestämmelser om interoperabilitet. De väsentliga kraven på funktionalitet uppfylls om det med informationssystemet vid behandling av kund- och patientuppgifter enligt systemets användningsändamål går att utföra de funktioner som krävs i lagar och med stöd av dem utfärdade bestämmelser.

Institutet för hälsa och välfärd meddelar närmare föreskrifter om innehållet i de väsentliga kraven och om de väsentliga krav de informationssystem och välbefinnandeapplikationer som används i de olika tjänsterna ska uppfylla.

35 §

Påvisande av överensstämmelse med kraven

Överensstämmelse med kraven ska för ett informationssystem och en välbefinnandeapplikation som hör till klass A visas med certifiering, det vill säga en utredning från producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen om att systemet eller applikationen uppfyller de krav på funktionalitet som ställs enligt dess användningsändamål. Certifieringen visas med en godkänd interoperabilitetstestning och ett sådant intyg över bedömning av informationssäkerhet av ett bedömningsorgan för informationssäkerhet som avses i 37 §. Producenten av en informationssystemtjänst ansvarar för att informationssystemet är certifierat och tillverkaren av välbefinnandeapplikation ansvarar för att applikationen är certifierad.

Överensstämmelse med kraven ska för ett informationssystem som hör till klass B visas med en skriftlig utredning från producenten av informationssystemtjänsten om att informationssystemet uppfyller de väsentliga krav som ställs enligt dess användningsändamål, om det har installerats, drivits och använts på behörigt sätt. Producenten av en informationssystemtjänst svarar för bedömningen av de väsentliga kraven på funktionalitet hos informationssystem. Denna producent ska som en del av den utredning som ges om kraven försäkra att de funktioner som enligt utredningen ska ingå i systemets användningsändamål har genomförts i systemet.

Institutet för hälsa och välfärd får meddela föreskrifter om de förfaranden som ska iakttas vid påvisande av överensstämmelse med kraven och om innehållet i den utredning som ska ges. Dessutom får Folkpensionsanstalten meddela föreskrifter om de förfaranden som ska iakttas vid verifiering av interoperabiliteten i fråga om informationssystem som ska

anslutas till de riksomfattande informationssystemtjänster som avses i denna lag eller i lagen om elektroniska recept.

36 §

Interoperabilitetstestning

Ett informationssystem och en välbefinnandeapplikation som hör till klass A ska vara interoperabla med de riksomfattande informationssystemtjänsterna och med övriga anslutna informationssystem. Interoperabiliteten ska visas vid en interoperabilitetstestning som ordnas av Folkpensionsanstalten. Före interoperabilitetstestningen ska producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen lämna Folkpensionsanstalten en redogörelse för hur kraven på informationssystemets eller välbefinnandeapplikationens funktionalitet har genomförts och testats. Tidpunkten för och genomförandet av interoperabilitetstestningen ska avtalas med Folkpensionsanstalten.

Ett informationssystem som hör till klass A och har tagits i användning för produktion av tjänster ska delta i samtestningar med andra informationssystem som ska anslutas till de riksomfattande informationssystemtjänsterna, för säkerställande av informationssystemens interoperabilitet. Folkpensionsanstalten beslutar vilka informationssystem som ska delta i interoperabilitetstestningen. De producenter av informationssystemtjänster vars informationssystem deltar i interoperabilitetstestningen svarar själva för de kostnader som testningen medför för dem. Folkpensionsanstalten ger på basis av interoperabilitetstestningen ett positivt yttrande om uppfyllelsen av kraven på interoperabilitet när kraven har verifierats.

Med avvikelse från 1 mom. utförs ingen separat interoperabilitetstestning av de riksomfattande informationssystemtjänster som Folkpensionsanstalten förvaltar eller av informationssystem som hör till klass A och inte ansluts till de riksomfattande informationssystemtjänsterna.

37 §

Bedömning av informationssäkerhet

Bedömningen av överensstämmelse med de väsentliga kraven på informationssäkerhet hos de informationssystem och välbefinnandeapplikationer som hör till klass A ska göras i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet. I den bedömning av informationssäkerheten som avses i denna lag ingår emellertid ingen bedömning eller inspektion av verksamhetsställena för producenten eller tillverkaren av en informationssystemtjänst eller för användaren. Bedömningen av informationssäkerhet görs på ansökan av producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation.

Bedömningsorganet för informationssäkerhet ska utifrån sin bedömning av informationssäkerhet ge producenten av informationssystemtjänsten eller tillverkaren av välbefinnandeapplikationen ett intyg och en tillhörande kontrollrapport. Bedömningen ska göras i enlighet med de väsentliga krav som gäller informationssystemets eller välbefinnandeapplikationens användningsändamål eller i enlighet med omfattningen av de ändringar som gjorts i systemet.

Bedömningsorganet för informationssäkerhet får avkräva producenten av en informationssystemtjänst eller tillverkaren av en välbefinnandeapplikation alla uppgifter som behövs för bedömningen i syfte att upprätta intyget. På utfärdande av intyget tillämpas i övrigt 9 § i lagen om bedömningsorgan för informationssäkerhet. Intyget är giltigt i högst tre år. Intygets giltighetstid får förlängas med högst tre år i sänder.

38 §

Anmälningsskyldighet för bedömningsorgan för informationssäkerhet

Ett bedömningsorgan för informationssäkerhet ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården, Folkpensionsanstalten och Institutet för hälsa och välfärd om alla intyg som har utfärdats, ändrats eller kompletterats eller som har återkallats eller förvägrats.

Bedömningsorganet för informationssäkerhet ska på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information om de informationssystem och välbefinnandeapplikationer för vilka organet har utfärdat intyg över bedömning av informationssäkerhet.

8 kap.

Styrning och tillsyn

39 §

Styrning, övervakning och uppföljning

Den allmänna planeringen, styrningen och övervakningen av den elektroniska behandlingen av kunduppgifter inom social- och hälsovården och informationshanteringen i anslutning därtill samt beslutsfattandet om totalfinansieringen av betydande informationshanteringsprojekt hör till social- och hälsovårdsministeriets uppgifter. Den allmänna styrningen och övervakningen av den certifikattjänst som sköts av Myndigheten för digitalisering och befolkningsdata hör dock gemensamt till social- och hälsovårdsministeriets och finansministeriets uppgifter.

Institutet för hälsa och välfärd svarar för planeringen, styrningen och uppföljningen av den elektroniska behandlingen av kunduppgifter inom social- och hälsovården och informationshanteringen i anslutning därtill samt av användningen och utförandet av de riksomfattande informationssystemtjänster som avses i 6 § och de gemensamma informationsresurser som hänför sig till olika förvaltningsområden.

Tillstånds- och tillsynsverket för social- och hälsovården samt regionförvaltningsverket inom sitt verksamhetsområde styr och övervakar i enlighet med sin behörighet efterlevnaden av denna lag.

40 §

Övervakning och inspektioner av informationssystem

Tillstånds- och tillsynsverket för social- och hälsovården har till uppgift att övervaka och främja informationssystemens överensstämmelse med kraven.

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att utföra inspektioner som krävs för tillsynen. Inspektioner kan göras utan förhandsanmälan. För att utföra en inspektion har en inspektör rätt att få tillträde till alla lokaler där det bedrivs verksamhet som avses i denna lag eller där det förvaras uppgifter som är viktiga för tillsynen över efterlevnaden av denna lag. Inspektioner får dock inte utföras i utrymmen som används för boende av permanent natur. Vid en inspektion ska dessutom 39 § i förvaltningslagen (434/2003) iakttas. Om den som ska inspekteras motsätter sig inspektionen eller annars försöker försvåra den, har tillsynsmyndigheten rätt att få handräckning av polisen på det sätt som föreskrivs i 9 kap. 1 § 1 mom. i polislagen (872/2011).

Vid en inspektion ska alla handlingar som inspektören ber om och som behövs för inspektionen läggas fram. På inspektörens begäran ska dessutom kopior av de handlingar som behövs för inspektionen överlämnas till inspektören utan avgift.

Inspektionerna ska protokollföras och en kopia av protokollet ska sändas till den som saken gäller inom 30 dagar. En inspektion anses avslutad när en kopia av inspektionsprotokollet har delgetts den som saken gäller. Tillstånds- och tillsynsverket för social- och hälsovården ska bevara inspektionsprotokollet i tio år efter det att inspektionen avslutades.

41 §

Underrättelse om avvikelser från de väsentliga kraven på ett informationssystem

Om en tjänstetillhandahållare konstaterar betydande avvikelser när det gäller uppfyllandet av de väsentliga kraven på ett informationssystem, ska denne underrätta producenten av informationssystemtjänsten om saken. Om en avvikelse kan innebära en betydande risk för kundsäkerheten eller informationssäkerheten, ska tjänstetillhandahållaren, apotek, producenten av informationssystemtjänsten eller tillverkaren av informationssystemet, Folkpensionsanstalten eller Institutet för hälsa och välfärd underrätta Tillstånds- och tillsynsverket för social- och hälsovården om detta. Även andra aktörer kan underrätta Tillstånds- och tillsynsverket för social- och hälsovården om risker som de upptäcker. Om tjänstetillhandahållaren eller en annan aktör konstaterar dataskyddsavvikelser när det gäller uppfyllandet av de väsentliga kraven på ett datasystem, ska denne underrätta dataombudsmannen om saken.

42 §

Rätt att få information

För tillsynen över informationssystem inom social- och hälsovården har Tillstånds- och tillsynsverket för social- och hälsovården rätt att avgiftsfritt och trots sekretessbestämmelserna få nödvändig information av statliga och kommunala myndigheter samt av fysiska och juridiska personer som omfattas av denna lag eller av bestämmelser och beslut som med stöd av denna lag meddelats om informationssystem inom social- och hälsovården.

43 §

Rätt för Tillstånds- och tillsynsverket för social- och hälsovården att anlita utomstående experter

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att anlita utomstående experter som biträden vid bedömning av ett informationssystems överensstämmelse med kraven. Utomstående experter får delta i inspektioner som avses i denna lag samt undersöka och testa informationssystem, men de får inte fatta förvaltningsbeslut. Utomstående experter ska ha den sakkunskap och kompetens som uppgifterna kräver. På utomstående experter tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna lag. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

44 §

Föreläggande att fullgöra skyldigheter

Om en producent av en informationssystemtjänst för social- eller hälsovården eller en tillverkare av ett informationssystem, en tjänstetillhandahållare, en mellanhand eller Folkpensionsanstalten har underlåtit att fullgöra sin skyldighet enligt denna lag, får Tillstånds- och tillsynsverket för social- och hälsovården meddela ett föreläggande om att skyldigheten ska fullgöras inom utsatt tid.

45 §

Skyldigheter avseende informationssystem som är i bruk

När Tillstånds- och tillsynsverket för social- och hälsovården övervakar och inspekterar informationssystem med stöd av 40 § får verket samtidigt ålägga producenten eller tillverkaren av en informationssystemtjänst att avhjälpa brister i informationssystem som används för produktion av tjänster.

Om ett informationssystem kan äventyra kund- eller patientsäkerheten, eller om systemet inte till alla delar uppfyller de väsentliga krav som ställs på det enligt dess användningsändamål, och bristerna inte har avhjälpts inom den tid som Tillstånds- och tillsynsverket för social- och hälsovården har angett, får verket förbjuda användningen av informationssystemet till dess att bristerna har avhjälpts. Dessutom får Folkpensionsanstalten stänga förbindelser till riksomfattande informationssystemtjänster som den förvaltar, om ett anslutet informationssystem eller dess användare äventyrar den behöriga funktionen hos de riksomfattande informationssystemtjänsterna.

Tillstånds- och tillsynsverket för social- och hälsovården får ålägga producenten av en informationssystemtjänst eller en av denne befullmäktigad representant att inom den tid och på det sätt som verket bestämmer informera om förbud och förelägganden som gäller användningen av informationssystemet för produktion av tjänster.

9 kap.

Särskilda bestämmelser

46 §

Samarbete som gäller elektronisk informationshantering inom social- och hälsovården

Social- och hälsovårdsministeriet ska se till att det har ordnats samarbetsformer och samarbetsförfaranden för det samarbete som gäller elektronisk informationshantering och riksomfattande informationssystemtjänster inom social- och hälsovården. Syftet med samarbetet är att främja genomförandet av denna lag.

Statsrådet kan tillsätta delegationer och andra samarbetsorgan som behövs för det samarbete som avses i 1 mom.

Folkpensionsanstalten ska se till att det har ordnats samarbetsformer och samarbetsförfaranden kring den produktionsverksamhet som gäller informationssystemtjänster med tjänstetillhandahållare, apotek och andra intressentgrupper inom produktionsverksamheten.

47 §

Avgifter

Användningen av de riksomfattande informationssystemtjänster enligt 6 § som sköts av Folkpensionsanstalten och Myndigheten för digitalisering och befolkningsdata är avgiftsbelagd för tjänstetillhandahållarna. Den kommunala social- och hälsovårdens avgifter tas ut per sjukvårdsdistrikt hos samkommunen för sjukvårdsdistriktet. De avgifter som Folkpensionsanstalten tar ut bestäms oberoende av 10 § i lagen om grunderna för avgifter till staten (150/1992) genom förordning av social- och hälsovårdsministeriet så att de motsvarar kostnaderna för skötseln av tjänsterna. Avgifterna ska dessutom trygga likviditeten för Folkpensionsanstaltens servicefond. I fråga om de avgifter som tas ut för Myndigheten för digitalisering och befolkningsdatas prestationer föreskrivs i lagen om grunderna för avgifter till staten och med stöd av den.

Folkpensionsanstalten och Myndigheten för digitalisering och befolkningsdata ska årligen lämna social- och hälsovårdsministeriet en utredning över det föregående årets kostnader och de faktorer som påverkat kostnaderna samt en uppskattning av de totalkostnader som ligger till grund för användningsavgifterna för de följande fyra åren och av investeringsbehoven under de fyra följande åren och kostnaderna för dem.

Producenten av en informationssystemtjänst svarar för kostnaderna för certifiering. Folkpensionsanstalten har rätt att ta ut en avgift för interoperabilitetstestning enligt 36 § till ett självkostnadsvärde som avses i 6 § 1 mom. i lagen om grunderna för avgifter till staten. Registrering och införande av en i 30 § avsedd anmälan till Tillstånds- och tillsynsverket för social- och hälsovården i ett offentligt register är avgiftsbelagda. I fråga om avgifterna föreskrivs genom förordning av social- och hälsovårdsministeriet, med beaktande av vad som föreskrivs i lagen om grunderna för avgifter till staten och med stöd av den. Bestämmelser om avgifter för godkännande av bedömningsorgan för informationssäkerhet finns i 11 § i lagen om bedömningsorgan för informationssäkerhet.

48 §

Straffbestämmelser

Den som uppsåtligen eller av grov oaktsamhet

1) bryter mot identifieringsskyldigheten i 17 § 1 mom.,

2) lämnar ut kunduppgifter i strid med 20–22 § utan kundens tillstånd för eller samtycke till utlämnande eller utan lagfäst rätt, eller

3) försummar sin skyldighet att informera enligt 16 § 1 mom. och på så sätt äventyrar kundens integritetsskydd,

ska, om inte strängare straff för gärningen föreskrivs någon annanstans i lag, för *förseelse mot bestämmelserna om behandlingen av kunduppgifter inom social- och hälsovården* dömas till böter.

Bestämmelser om straff för dataintrång finns i 38 kap. 8 § i strafflagen (39/1889) och för dataskyddsbrott i 9 § i det kapitlet. Bestämmelser om brott mot sekretess finns i 1 och 2 § i det kapitlet samt i 40 kap. 5 § i den lagen.

49 §

Vite

Ett föreläggande som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat med stöd av denna lag och ett beslut som verket har fattat med stöd av denna lag kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1990).

50 §

Ändringssökande

Omprövning får begäras i fråga om ett föreläggande som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat i samband med en inspektion. Bestämmelser om begäran om omprövning finns i förvaltningslagen.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

Beslut och förelägganden som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat med stöd av denna lag ska iakttas trots begäran om omprövning eller ändringssökande, om inte den myndighet som behandlar begäran om omprövning eller förvaltningsdomstolen bestämmer något annat.

10 kap.

Ikraftträdande- och övergångsbestämmelser

51 §

Ikraftträdande

Denna lag träder i kraft den 1 november 2021.

Genom denna lag upphävs lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007).

52 §

Övergångsbestämmelser

Tjänstetillhandahållare inom den offentliga socialvården ska ansluta sig till den i 6 § 1 mom. 1 punkten avsedda riksomfattande arkiveringstjänsten för kunduppgifter senast den 1 september 2024 och tjänstetillhandahållare inom den privata socialvården senast den 1 januari 2026.

Bestämmelserna i 13 § 2 mom., vad som i 18 § 5 mom. föreskrivs om förbud som gäller alla klient- och patientuppgifter och företagshälsovården samt bestämmelserna i 20 § 2 mom. och 21 § 2 mom. tillämpas senast den 1 januari 2024.

Lagens 18 § tillämpas utom i fråga om förbud som gäller alla klient- och patientuppgifter samt register inom företagshälsovården senast från det att kundhandlingar lämnas ut från den i 6 § 1 mom. 1 punkten avsedda riksomfattande arkiveringstjänsten för kunduppgifter.

Lagens 19 § tillämpas inom socialvården från och med den 1 januari 2023 eller senast från det att kundhandlingar inom socialvården lämnas ut från den i 6 § 1 mom. 1 punkten avsedda riksomfattande arkiveringstjänsten.

Lagens 20 § 4 mom. tillämpas i fråga om välbefinnandeapplikationer senast den 1 december 2023.

Lagens 21 § 1 och 3 mom. tillämpas senast den 1 januari 2023.

Lagens 21 § 4 mom. tillämpas i fråga om välbefinnandeapplikationer senast den 1 maj 2025.

Med avvikelse från skyldigheten enligt 8 § 2 mom. att efter anslutning till de riksomfattande informationssystemtjänsterna spara kundhandlingarna i original i den riksomfattande arkiveringstjänsten ska en tjänstetillhandahållare senast den 1 oktober 2026 börja spara följande handlingar:

1) handling över tidsbeställningar inom hälso- och sjukvården som reserverats för kunden och om vilka kunden har underrättats,
2) handlingar och laboratorieresultat som anknyter till radiologisk screening,
3) intyg och blanketter som anknyter till körhälsa,
4) intyg och blanketter som anknyter till olycksfall och anmälan av yrkessjukdom,
5) läkarutlåtande om hälsotillstånd (T-intyg),
6) läkarintyg (TOD),
7) läkarintyg C, och
8) dödsattest.

Med avvikelse från skyldigheten enligt 8 § 2 mom. att efter anslutning till de riksomfattande informationssystemtjänsterna spara kundhandlingarna i original i den riksomfattande arkiveringstjänsten ska en tjänstetillhandahållare inom hälso- och sjukvården senast den 1 oktober 2029 börja spara följande handlingar:

1) uppgifter om strålbelastning,
2) video- och ljudupptagningar samt fotografier,

3) patologiskt bildmaterial,
4) biosignaler,
5) bilder tagna av enheter för mun- och tandvård, och
6) andra bilder: ritningar och illustrationer.

Med avvikelse från skyldigheten enligt 8 § 2 mom. att efter anslutning till de riksomfattande informationssystemtjänsterna spara kundhandlingarna i original i den riksomfattande arkiveringstjänsten ska en tjänstetillhandahållare inom hälso- och sjukvården senast den 1 oktober 2029 börja spara dagliga anteckningar inom vårdarbetet.

Den offentliga socialvården och tjänstetillhandahållare som arbetar för dess räkning ska börja spara klienthandlingar inom socialvården i den riksomfattande arkiveringstjänsten enligt följande:

1) handlingar som uppkommer i serviceuppgifter för barnfamiljer, personer i arbetsför ålder och äldre personer, senast den 1 september 2024,
2) handlingar som uppkommer i serviceuppgifter inom barnskyddet, senast den 1 mars 2025,
3) kundhandlingar som uppkommer i serviceuppgifter inom handikappservicen, senast den 1 september 2025,
4) kundhandlingar som uppkommer i serviceuppgifter inom missbrukarvården, senast den 1 mars 2026, samt
5) kundhandlingar som uppkommer i serviceuppgifter inom familjerättsliga tjänster, senast den 1 september 2026.

Kundhandlingar som uppkommer inom privat socialvård som grundar sig på avtal mellan tjänstetillhandahållaren och kunden ska börja sparas i de riksomfattande informationssystemtjänsterna enligt följande:

1) handlingar som uppkommer i serviceuppgifter för barnfamiljer, personer i arbetsför ålder och äldre personer samt i serviceuppgifter inom handikappservicen, senast den 1 januari 2026,
2) handlingar som uppkommer i serviceuppgifter inom missbrukarvården, senast den 1 mars 2026.

Video- och ljudupptagningar som uppkommer i serviceuppgifter inom socialvården ska dock börja sparas senast den 1 oktober 2029.

Helsingfors den 27 augusti 2021

Republikens President

Sauli Niinistö

Familje- och omsorgsminister Krista Kiuru

UTGIVARE: JUSTITIEMINISTERIET ISSN 1456-9663