LAGFÖRSLAG

1.
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 en informationssäker behandling, övervakning och användning av kunduppgifter som produceras inom social- och hälsovården och av uppgifter som kunden själv producerar om sitt välbefinnande, detta med målet att ordna, producera och utveckla social- och hälsovårdstjänsterna och främja kundens möjligheter att få information.

2 §
Tillämpningsområde

Denna lag tillämpas vid elektronisk behandling av kunduppgifter och uppgifter om välbefinnande och vid utlämnande och användning av sådana uppgifter när offentliga och privata tillhandahållare av social- och hälsovårdstjänster ordnar eller producerar social- och hälsovård.

Om inte något annat följer av denna lag tillämpas på behandlingen av kunduppgifter det som föreskrivs i lagen om patientens ställning och rättigheter (785/1992), nedan *patientlagen*, lagen om klienthandlingar inom socialvården (254/2015), nedan *klienthandlingslagen,* lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan *klientlagen*, lagen om ordnande av social- och hälsovård (x/x), lagen om produktion av social- och hälsotjänster (x/x), lagen om företagshälsovård (1383/2001), lagen om elektroniska recept (61/2007), lagen om offentlighet i

myndigheternas verksamhet (621/1999), nedan *offentlighetslagen*, förvaltningslagen (434/2003), personuppgiftslagen (523/1999), lagen om informationssäker användning av social- och hälsouppgifter (x/x), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016), lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och arkivlagen (831/1994) eller i bestämmelser som utfärdats med stöd av dem. Vid behandling av kunduppgifter och vid ordnande av tjänster och funktioner enligt denna lag ska dessutom det iakttas som föreskrivs i språklagen (423/2003) och med stöd av den. Om det informationssystem där hälso- och sjukvårdens klient- och patientuppgifter behandlas utgör en sådan produkt för hälso- och sjukvård som avses i lagen om produkter och utrustning för hälso- och sjukvård (629/2010), tillämpas på informationssystemet även den lagen och kraven i enlighet med den.

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 klienthandlingslagen och en jourhandling som avses i patientlagen,

3) *kunduppgift* en sådan uppgift om en patient som ingår i en i patientlagen avsedd journalhandling inom hälso- och sjukvården och en sådan personuppgift om en klient inom socialvården som ingår i en i klientlagen eller klienthandlingslagen avsedd klienthandling inom socialvården eller i en kundhandling som är gemensam för social- och hälsovården,

4) *servicehändelse* ett kundbesök eller en vårdperiod inom hälso- och sjukvården,

5) *serviceuppgift* en serviceuppgift som avses i 22 och 23 § i klienthandlingslagen,

6) *informationssystem* en programvara eller ett system eller delsystem i vars användningsändamål det ingår elektronisk behandling av kunduppgifter och registrering och uppdatering av

kundhandlingar, eller egenskaper som har planerats av tillverkaren för anslutning till de riksomfattande informationssystemtjänsterna,

7) *informationssystemets miljö* den tekniska, organisatoriska och fysiska miljö där en eller flera tjänstetillhandahållare använder ett informationssystem eller en informationssystemtjänst vid produktionen av social- och hälsovårdstjänster och behandlingen av kunduppgifter,

8) *tjänstetillhandahållare* en i 2 § 3 punkten i patientlagen avsedd yrkesutbildad person inom hälso- och sjukvården, en i 2 § 4 punkten i den lagen avsedd verksamhetsenhet för hälso- och sjukvård, en i 7 § 2 punkten i lagen om företagshälsovård avsedd arbetsgivare, en yrkesutbildad person inom hälso- och sjukvården som arbetar som självständig yrkesutövare, en myndighet som ordnar i 3 § 2 punkten i klientlagen avsedd socialvård, en offentlig producent av socialtjänster, en i lagen om produktion av social- och hälsotjänster avsedd tjänsteproducent samt en aktör eller person som producerar social- och hälsovård med stöd av övrig lagstiftning,

9) *tjänsteanordnare* en tjänstetillhandahållare som
a) i egenskap av myndighet är skyldig att se till att kunden får sådana tjänster eller förmåner som han eller hon 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 han eller hon har rätt till enligt ett avtal eller konsumentskyddsbestämmelserna,

10) *tjänsteproducent* en tjänstetillhandahållare som
a) i egenskap av tjänsteanordnare själv producerar social- och/eller hälsotjänster, eller
b) på basis av ett avtal med en tjänsteanordnare producerar social- och/eller hälsotjänster,

11) *bedömningsorgan för informationssäkerhet* sådana företag, sammanslutningar och myndigheter som Kommunikationsverket med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011) har godkänt att utföra bedömningar av överensstämmelse med kraven i fråga om informationssystem,

12) *informationssystems interoperabilitet* två eller flera informationssystems förmåga att utbyta information och att använda sådan information,

13) *uppgifter om välbefinnande* uppgifter om en medborgares hälsa och välbefinnande som inte ingår i kunduppgifterna och som kan föras in i datalagret för egna uppgifter,

14) *datalager för medborgares egna uppgifter* ett centraliserat elektroniskt datalager för bevarande och behandling av uppgifter om välbefinnande,

15) *program för uppgifter om välbefinnande* ett program i anslutning till datalagret för egna uppgifter med vilket uppgifter om välbefinnande och, med kundens samtycke, kunduppgifter behandlas,

16) *arkiveringstjänst* ett datalager där kunduppgifter och andra för social- och hälsovården behövliga uppgifter bevaras och som godkända informationssystem kan anslutas till,

17) *informationshanteringstjänst* en riksomfattande informationssystemtjänst genom vilken handlingar som gäller information, samtycke och förbud samt andra viljeyttringar förvaltas; dessutom kan informationshanteringstjänsten användas till att visa eller på något annat sätt behandla kunduppgifter som är viktiga med tanke på de tjänster en kund tillhandahålls,

18) *producent av en informationssystemtjänst* den som för en tjänstetillhandahållare tillhandahåller eller utför en informationssystemtjänst där kunduppgifter behandlas och som i egenskap av informationssystemets tillverkare, för tillverkarens räkning eller för en eller flera tillverkares del ansvarar för de krav som ställs på informationssystemet,

19) *mellanhand* en tjänsteleverantör som en tjänstetillhandahållare anlitar för produktion av informationssystemtjänster, genomförande av informationssystemens tekniska eller fysiska miljö eller anslutning 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 för att via interoperabilitetstestning och bedömning av informationssäkerheten verifiera att ett informationssystem uppfyller de väsentliga krav som ställs på det för att det ska få användas för produktion.

4 §

Kunduppgifternas användbarhet och bevarandet av dem

Elektroniska kunduppgifter ska vara tillgängliga och användbara och behålla sin integritet och oförvanskade form under hela sin livscykel. Den elektroniska behandlingen av kunduppgifter ska vara informationssäker.

2 kap. Registerföring av kunduppgifter och av uppgifter om välbefinnande

5 §

Registeransvarig för kunduppgifter och för uppgifter om välbefinnande

Enligt 62 § i lagen om ordnande av social- och hälsovård är ett landskap registeransvarig när det gäller klient- och patienthandlingar som uppkommer i verksamhet som omfattas av dess ansvar för att ordna social- och hälsovård. Bestämmelser om landskapens ansvar för att ordna social- och hälsotjänster finns i 9 § i den lagen. Bestämmelser om privata registeransvariga för social - och hälsotjänster finns i 33 § i lagen om produktion av social- och hälsotjänster.

Folkpensionsanstalten är registeransvarig för den informationshanteringstjänst som avses i 13 §, det datalager för medborgares egna uppgifter som avses i 14 § och det receptcenter som avses i lagen om elektroniska recept, och som samtliga ingår i de riksomfattande informationssystemtjänsterna.

6 §

Kundregister

De uppgifter om en kund som uppkommer vid ordnandet, produktionen och planeringen av social- och hälsovård förs in i social- och hälsovårdens kundregister.

Tjänsteanordnarens kundregister består av klienthandlingar inom socialvården, journalhandlingar inom hälso- och sjukvården och de kundhandlingar som upprättas inom tjänster som avses i 41 § i socialvårdslagen (1301/2014) och 32 § i hälso- och sjukvårdslagen (1326/2010) och inom social- och hälsovårdstjänster som avses i 7 § i klienthandlingslagen.

7 §

Fördelningen av ansvaret för registerföringen

När en tjänsteproducent tillhandahåller social- och hälsotjänster för en tjänsteanordnares räkning, fördelar sig den registeransvariges lagstadgade ansvar för de kundhandlingar som har upprättats och tagits emot i samband med dessa tjänster mellan tjänsteanordnaren och tjänsteproducenten på det sätt som föreskrivs i 2 och 3 mom.

I de situationer som avses i 1 mom. ansvarar tjänsteproducenten

1) för införande och registrering av kunduppgifter samt utlämnande av införda kunduppgifter för tjänsteanordnarens 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 tjänsteanordnaren enligt vad som har avtalats med stöd av 25 § 1 mom. i klienthandlingslagen, dock utan dröjsmål efter det att kundförhållandet har avslutats,
5) tillsammans med tjänsteanordnaren för att kundens rättigheter enligt personuppgiftslagen och offentlighetslagen tillgodoses,
6) för organiseringen inom den egna verksamheten av tillsynen över informationssäkerheten och av den dataskyddsansvariges verksamhet i enlighet med 27 §, och
7) i sin egenskap av den som registrerar uppgifter i en informationshanteringstjänst för att uppgifterna är korrekta och för att felaktiga uppgifter blir rättade i enlighet med 29 § i personuppgiftslagen.

I de situationer som avses i 1 mom. ansvarar tjänsteanordnaren i egenskap av registeransvarig

1) för fullgörandet av de skyldigheter som den registeransvarige har enligt personuppgiftslagen,
2) för bevarande och utplåning av handlingar,
3) för säkerställandet av att tjänsteproducenten behandlar kunduppgifterna i överensstämmelse med lagstiftning och avtal,
4) tillsammans med tjänsteproducenten för att kundens rättigheter enligt personuppgiftslagen tillgodoses samt för beslut som gäller dessa rättigheter,
5) för fullgörandet av de skyldigheter som en myndighet har enligt offentlighetslagen och för beslut som gäller åtkomst till handlingar,
6) för organiseringen inom den egna verksamheten av egenkontrollen i fråga om informationssäkerhetsplanen och av den dataskyddsansvariges verksamhet i enlighet med 27 §, och
7) för innehållet i logguppgifter som har anknytning till behandling av kunduppgifter och för att uppgifterna är korrekta.

3 kap. Utförande av riksomfattande informationssystemtjänster inom social- och hälsovården

8 §

Riksomfattande informationssystemtjänster

För bevarandet och behandlingen av kunduppgifter ska Folkpensionsanstalten för tjänstetillhandahållarnas räkning ordna riksomfattande informationssystemtjänster enligt följande:

a) en riksomfattande arkiveringstjänst,
b) en förvaringstjänst för loggregister,
c) ett gränssnitt för professionellt bruk,
d) ett medborgargränssnitt,
e) ett datalager för medborgares egna uppgifter,
f) en informationshanteringstjänst,
g) ett receptcenter,
h) en läkemedelsdatabas, och
i) en förfrågnings- och informationsförmedlingstjänst.

Övriga riksomfattande tjänster:

a) en kodtjänst, och
b) en roll- och attributtjänst.

Tillstånds- och tillsynsverket för social- och hälsovården ska förvalta den roll- och attributtjänst och de kodsystem med vars hjälp tjänstetillhandahållare, apotek, Folkpensionsanstalten och Befolkningsregistercentralen för användning och certifiering av de riksomfattande informationssystemtjänsterna får information om rätten att vara verksam som yrkesutbildad person inom social- och hälsovården och om giltighetstiden för denna rätt. Institutet för hälsa och välfärd ansvarar för innehållet i kodtjänsten.

Befolkningsregistercentralen är i lagen om stark autentisering och betrodda elektroniska tjänster avsedd certifikatutfärdare för yrkesutbildade personer och annan personal inom social- och hälsovården, tjänstetillhandahållare och organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Befolkningsregistercentralen har rätt att för

skötseln av dessa uppgifter av Tillstånds- och tillsynsverket för social- och hälsovården, ur det centralregister över yrkesutbildade personer inom social- och hälsovården som verket upprätthåller, få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat.

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att för skötseln av sina lagstadgade uppgifter av Befolkningsregistercentralen få information om de certifikat som centralen utfärdat på ovannämnda grunder. Informationen kan lämnas ut med hjälp av en teknisk anslutning.

9 §

Skyldighet att ansluta sig som användare av de riksomfattande informationssystemtjänsterna

Tjänstetillhandahållare ska ansluta sig som användare av de riksomfattande informationssystemtjänster som avses i 9 § a-, b-, f- och h-punkten. Tillhandahållare av offentliga social- och hälsovårdstjänster i landskapet Åland kan ansluta sig som användare av de riksomfattande informationssystemtjänsterna. Bestämmelser om denna anslutning ska dock utfärdas särskilt på det sätt som föreskrivs i 32 § i självstyrelselagen för Åland (1144/1991).

Bestämmelser om när socialvården senast ska anslutas som användare av de riksomfattande informationssystemen får utfärdas genom förordning av social- och hälsovårdsministeriet.

10 §

Handlingar som ska sparas i den riksomfattande arkiveringstjänsten

Av en elektronisk kundhandling ska 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 kan det av originalet göras ett extra exemplar av vilket det ska framgå att det inte är originalet.

Original av kundhandlingar som uppkommit efter anslutningen ska sparas i den riksomfattande arkiveringstjänsten. Kundhandlingar som uppkommit före anslutningen kan sparas i den riksomfattande arkiveringstjänsten.

I den riksomfattande arkiveringstjänsten kan det utöver kundhandlingar sparas uppgifter och handlingar som gäller social- och hälsovård och hänför sig till ordnande, styrning, tillsyn, utvärdering av verksamheten, utveckling och informationshantering.

Bestämmelser om när och i vilken omfattning originalhandlingar som avses i 1 mom. senast ska sparas i den riksomfattande arkiveringstjänsten får utfärdas genom förordning av social- och hälsovårdsministeriet.

11 §

Informationssystem i anslutning till de riksomfattande informationssystemtjänsterna och datastrukturerna för de kunduppgifter som ska föras in i systemen

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 8 §.

Institutet för hälsa och välfärd meddelar föreskrifter om de väsentliga krav som ställs på informationssystemen för att de riksomfattande informationssystemtjänsterna ska kunna utföras, och bestämmer kundhandlingarnas datainnehåll och datastrukturer samt de kodsystem som i hela landet ska användas i datastrukturerna.

12 §

Elektronisk signering av handlingar

Handlingarnas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk underskrift vid elektronisk behandling, överföring och bevarande 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. Vid signering som görs av en organisation och datatekniska enheter ska det användas en elektronisk underskrift med motsvarande tillförlitlighet.

13 §

Informationshanteringstjänsten

Med hjälp av informationshanteringstjänsten kan information från olika handlingar och från uppgifter om välbefinnande sammanställas samt sådan för en kunds social- och hälsovård viktig information visas som tjänstetillhandahållaren kan använda när social- och hälsovård ordnas eller produceras för kunden.

I informationshanteringstjänsten ska det föras in uppgifter om

1) information som en kund har fått och om innehållet i den,
2) förbud som en kund har meddelat,
3) en kunds och myndigheternas gemensamma välbefinnande/kundplan,
4) en kunds övriga viljeyttringar, och
5) samtycke som en kund har gett.

Institutet för hälsa och välfärd kan meddela föreskrifter om vilka uppgifter som är sådana viktiga uppgifter som ska visas via informationshanteringstjänsten.

14 §

Datalagret för egna uppgifter

En person kan i datalagret för egna uppgifter föra in sina uppgifter och information som ett program för uppgifter om välbefinnande producerat.
En person har rätt att besluta om användningen av sina uppgifter och om avlägsnande av uppgifterna från datalagret.

En person kan ge sitt samtycke till att en tjänstetillhandahållare i sitt arbete får använda sådana uppgifter om en kunds välbefinnande som finns i datalagret för egna uppgifter. En person har rätt att förbjuda att uppgifter om välbefinnande som finns i datalagret för egna uppgifter visas.

Institutet för hälsa och välfärd meddelar närmare föreskrifter om vad ett förbud att lämna ut uppgifter om välbefinnande kan gälla.

15 §

Folkpensionsanstaltens ansvar när den förvaltar riksomfattande informationssystemtjänster

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

Folkpensionsanstalten ansvarar

a) för den tekniska realisering och de tekniska anvisningar som de riksomfattande informationssystemtjänsterna kräver,
b) för användbarhet, integritet, oförvänsklighet, skydd, bevarande och utplåning i fråga om kunduppgifter, uppgifter om välbefinnande och andra uppgifter som förs in i de riksomfattande informationssystemtjänsterna,
c) för att de riksomfattande informationssystemtjänster som anstalten ansvarar för utförs så att kunduppgifter, uppgifter om välbefinnande och andra införda uppgifter lämnas ut i enlighet med denna lag och lagen om informationssäker användning av social- och hälsouppgifter,
d) för att användning och utlämnande av kunduppgifter och uppgifter om välbefinnande registreras i ett loggregister,
e) för det datatekniska utförandet av kodservern, och
f) för information till befolkningen i anslutning till de riksomfattande informationssystemtjänsterna.

Folkpensionsanstalten har rätt

a) att av Tillstånds- och tillsynsverket för social- och hälsovården få sådana uppgifter om yrkesutbildade personer inom social- och hälsovården som behövs för skötseln av anstaltens lagstadgade uppgifter i anslutning till de riksomfattande informationssystemtjänsterna,
b) att behandla kunduppgifter och uppgifter om välbefinnande till den del det är nödvändigt för förvaltningen av ett system,
c) att besluta om frågor som gäller ett systems datatekniska verksamhet, om inte något annat följer av denna lag eller av bestämmelser som har utfärdats med stöd av den,
d) att lämna ut handlingar som gäller samtyckeshantering och handlingarnas logguppgifter till berörda organisationer för dataskyddsutredningar,
e) att i syfte att öka informationssäkerheten utöva tillsyn över användningen av sina tjänster och av de uppgifter som bevaras i dessa tjänster, och
f) att lämna ut logguppgifter över handlingar som finns i Folkpensionsanstaltens register till berörda organisationer.

I egenskap av registeransvarig ska Folkpensionsanstalten i enlighet med lag lämna ut uppgifter som ingår i de riksomfattande informationssystemtjänsterna. Folkpensionsanstalten kan lämna ut handlingar som gäller samtyckeshantering och deras logguppgifter samt göra upp och lämna ut sådana sammanställningar över uppgifter i arkiveringstjänsten, över handlingars metadata och över

loggуppgifter som kan ha betydelse för utvecklingen och uppföljningen av de riksomfattande informationssystemtjänsterna eller för rapporteringen.

De riksomfattande informationssystemtjänsterna ska skyddas i enlighet med statliga myndigheters skyldigheter i fråga om informationssäkerhet på det sätt som föreskrivs i 36 § i offentlighetslagen och i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010). Folkpensionsanstalten får inte ge en utomstående i uppdrag att behandla eller bevara i x § avsedda register som har samband med ordnandet av de riksomfattande informationssystemtjänsterna, eller loggregister som hänför sig till sådana register.

4 kap. Behandling av kunduppgifter

16 §

Grund för behandlingen av kunduppgifter och uppgifter om välbefinnande

Behandlingen av kunduppgifter ska grunda sig på en kund- eller vårdrelation som avses i klientlagen eller patientlagen eller på någon annan laglig rättighet. Personal som deltar i vården eller undersökningen av en kund eller i planeringen, ordnandet eller produktionen av tjänster för kunden har rätt att i den omfattning som arbetsuppgifterna kräver behandla nödvändiga kunduppgifter som finns i ett kundregister och som personalen behöver.

Behandlingen av uppgifter om välbefinnande ska grunda sig på en kund- eller vårdrelation som avses i klientlagen eller patientlagen och på kundens samtycke.

17 §

Åtkomsträttigheter till kunduppgifter

Tjänstetillhandahållaren ska bestämma vilka åtkomsträttigheter yrkesutbildade personer inom social- och hälsovården och andra personer som behandlar kunduppgifter har till dessa uppgifter. Åtkomsträttigheter beviljas till de nödvändiga kunduppgifter som varje enskild yrkesutbildad person eller annan person som behandlar kunduppgifter behöver i sina arbetsuppgifter.

Tjänstetillhandahållaren ska föra register över dem som använder tjänstetillhandahållarens kundinformationssystem och kundregister och över deras åtkomsträttigheter.

Institutet för hälsa och välfärd meddelar föreskrifter om de grunder enligt vilka tjänstetillhandahållaren ska bestämma åtkomstsrättigheterna till kunduppgifter för den personal som behandlar sådana uppgifter.

18 §
Information till kunden

Tjänstetillhandahållaren ska informera kunden om behandlingen i enlighet med denna lag av hans eller hennes kunduppgifter och om kundens rätt att meddela förbud i enlighet med 25 § i lagen om informationssäker användning av social- och hälsouppgifter. Kunden ska ges informationen senast i samband med den första kontakten.

Det måste gå att verifiera i efterhand att informationen har getts. Om kunden redan har blivit informerad, får undantag göras från upplysningsplikten i enlighet med 24 § i personuppgiftslagen.

Folkpensionsanstalten ansvarar för innehållet i informationen till kunden.

19 §
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. Identifieringen av de personer som behandlar kunduppgifter, tjänstetillhandahållarna, de datatekniska enheterna och de riksomfattande informationssystemtjänsterna förutsätter verifiering.

Närmare bestämmelser om de tekniska identifierings- och verifieringsmedlen får utfärdas genom förordning av social- och hälsovårdsministeriet. Social- och hälsovårdsministeriet ska innan förordningen utfärdas höra Befolkningsregistercentralen till den del det gäller uppgifter som Befolkningsregistercentralen enligt 9 § ska sköta.

20 §
Kundens rätt att förbjuda att egna kunduppgifter lämnas ut och behandlas

En kund har rätt att förbjuda att en registeransvarig lämnar ut kunduppgifter om honom eller henne själv till en annan registeransvarig. Kunden har inte rätt att meddela förbud inom en och samma registeransvarig. Ett förbud som kunden meddelar kan gälla alla hans eller hennes kunduppgifter inom social- och hälsovården, en serviceuppgift eller en enskild kundhandling inom socialvården, en servicehändelse inom hälso- och sjukvården eller en serviceuppgift, en enskild kundhandling eller en servicehändelse inom de gemensamma social- och hälsovårdstjänsterna. Ett förbud gäller tills vidare och får återkallas.

I de situationer som avses i 1 mom. har en kunds lagliga företrädare rätt att med stöd av 29 § 2 mom. i lagen om förmyndarverksamhet (442/1999) förbjuda att huvudmannens uppgifter lämnas ut. En vårdnadshavare har dock inte rätt att förbjuda att kunduppgifterna för en minderårig som vårdnadshavaren har vårdnaden om lämnas ut i de situationer som avses i 1 mom.

Kunduppgifter som omfattas av ett gällande förbud får inte behandlas när hälso- och sjukvård tillhandahålls även om uppgifterna är relevanta med tanke på vården, om inte förbudet har återtagits eller patientens vilja inte kan utredas vid brådskande vård som avses i 8 § i patientlagen.

Kunduppgifter som omfattas av ett gällande förbud får inte behandlas när socialvård tillhandahålls, om inte förbudet har återtagits eller något annat föreskrivs i 17–21 § i klientlagen.

21 §

Meddelande av förbud mot behandling av kunduppgifter

Meddelande av förbud kan lämnas till en tjänstetillhandahållare som har anslutit sig till den riksomfattande informationssystemtjänsten eller via ett medborgargränssitt. Information om att meddelande av förbud har lämnats till en tjänstetillhandahållare ska utan dröjsmål ges till den riksomfattande informationssystemtjänsten.

Den som tar emot ett förbud som en kund meddelar ska på begäran ge kunden en utskrift av förbudet.

Folkpensionsanstalten bestämmer innehållet i en förbudshandling. Av förbudshandlingen ska förbudets betydelse för behandlingen av kunduppgifter framgå.

22 §

Att sköta ärenden för någon annans räkning i en e-tjänst

En person har rätt att med stöd av en fullmakt eller 29 § 2 mom. i lagen om förmyndarverksamhet för en annan persons räkning behandla kunduppgifter och uppgifter om välbefinnande som har sparats i en riksomfattande informationssystemtjänst. En vårdnadshavare har rätt att behandla sådana uppgifter som gäller en person som vårdnadshavaren har vårdnaden om och som har sparats i en riksomfattande informationssystemtjänst, om inte något annat följer av klientlagen eller 9 § 2 mom. i patientlagen.

Enligt 10 § 1 mom. i lagen om förvaltningens gemensamma stödtjänster för e-tjänster ansvarar Befolkningsregistercentralen för förmedling av uppgifter via behörighetstjänsten, om den myndighet som registrerat dessa uppgifter har gett Befolkningsregistercentralen tillstånd att förmedla uppgifterna och om verksamheten inte äventyrar tillförlitligheten hos de uppgifter som förmedlas via behörighetstjänsten. Ansvaret för registreringen av viljeyttringar kvarstår hos myndigheten i fråga.

23 §

Medborgargränssnitt samt kunduppgifter och viljeyttringar som visas via det

Ett medborgargränssnitt ska realiseras så att kunden kan avge viljeyttringar och sköta ärenden som gäller hans eller hennes kundförhållande och administreringen av uppgifterna om välbefinnande via gränssnittet. När gränssnittet realiseras ska det dessutom säkerställas att kundens integritetsskydd inte äventyras.

Kunden kan via medborgargränssnittet visas eller få sådana uppgifter om sig själv som finns sparade i de riksomfattande informationssystemtjänsterna, med undantag för uppgifter som kunden enligt 27 § 1 mom. 1–4 punkten i personuppgiftslagen eller 11 § 1 och 3 mom. i offentlighetslagen inte har rätt att få. Dessutom kan kunden via gränssnittet visas utlämningsloggуppgifter och användningsloggуppgifter som gäller honom eller henne själv.

Uppgifter om en minderårig kund kan via gränssnittet ses av kunden själv och av hans eller hennes vårdnadshavare eller av någon annan laglig företrädare. När uppgifter visas ska bestämmelserna i 9 § 2 mom. i patientlagen och 11 § 3 mom. i klientlagen beaktas.

Närmare bestämmelser om visande av kunduppgifter via ett gränssnitt får utfärdas genom förordning av social- och hälsovårdsministeriet.

24

Utlämnande av kunduppgifter ur ett kundregister

Sekretessbelagda uppgifter om en kund får av en registeransvarig som avses i 62 § i lagen om ordnande av social- och hälsovård lämnas ut till en annan registeransvarig efter det att kunden har informerats i enlighet med 18 § och existensen av en vård- eller kundrelation mellan kunden och den som framställt begäran om utlämnande har säkerställts datatekniskt, om inte något annat följer av 7 § och 13 § 3 mom. i patientlagen eller 17 och 18 § i klientlagen. Bestämmelser om utlämnande av uppgifter ur elektroniska recept finns i lagen om elektroniska recept. Bestämmelser om användning för vetenskaplig forskning av biologiska prover som uppkommer i samband med undersökning och behandling av patienter finns i lagen om medicinsk forskning (488/1999), lagen om användning av mänskliga organ, vävnader och celler för medicinska ändamål (101/2001) och biobankslagen (688/2012).

Trots bestämmelserna i 1 mom. kan kunduppgifter med hjälp av de riksomfattande informationssystemtjänsterna lämnas ut till andra än registeransvariga som nämns i det momentet. Detta förutsätter information till kunden, samtycke enligt artikel x 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 eller en bestämmelse i lag som ger rätt att lämna ut uppgifterna.

Med hjälp av de riksomfattande informationssystemtjänsterna kan intyg och utlåtanden förmedlas till den aktör utanför social- och hälsovården som handlingen har upprättats för. Övriga specificerade handlingar som bifogats till intyg och utlåtanden kan lämnas ut tillsammans med intyget. Intygen och utlåtandena förmedlas med hjälp av den informationsförmedlings- och förfrågningstjänst som hör till de riksomfattande informationssystemtjänsterna.

Institutet för hälsa och välfärd meddelar föreskrifter om vilka intyg och utlåtanden som får förmedlas med hjälp av informationsförmedlings- och förfrågningstjänsten.

25 §

Uppföljning av användning och utlämnande av kunduppgifter och uppgifter om välbefinnande

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

I användningsloggregistret förs det in uppgifter om använda kunduppgifter och uppgifter om välbefinnande, den tjänstetillhandahållare vars kunduppgifter används, den som har använt kunduppgifter och uppgifter om välbefinnande, användningsändamålet, användningstidpunkten och andra behövliga uppgifter.

I utlämningsloggregistret förs det in uppgifter om utlämnade kunduppgifter, den tjänstetillhandahållare vars kunduppgifter lämnas ut, den som lämnat ut kunduppgifterna, utlämningsändamålet, mottagaren, utlämningstidpunkten och andra behövliga uppgifter.

Folkpensionsanstalten ska i fråga om de uppgifter som har sparats i de i 8 § avsedda informationssystemtjänsterna och som har lämnats ut via anstalten samla in dels utlämningslogguppgifter av vilka det utlämnade datainnehållet, mottagaren, utlämningstidpunkten och andra behövliga uppgifter framgår, dels användningslogguppgifter om de uppgifter som har sparats i gränssnittet för professionellt bruk. I den förvaringstjänst för loggregister som avses i 8 § sparas logguppgifter om utlämnande och användning av en tjänstetillhandahållares kundregisteruppgifter.

Närmare bestämmelser om logguppgifter och uppgifter om åtkomsträttigheter och om den tid som dessa uppgifter åtminstone ska bevaras får utfärdas genom förordning av social- och hälsovårdsministeriet. Institutet för hälsa och välfärd kan meddela närmare föreskrifter om de uppgifter som ska föras in i loggregistren och om deras datainnehåll.

26 §

Kundens rätt att få information om användningen av sina egna uppgifter

Bestämmelser om kundens rätt att kontrollera uppgifter i kundregistret och om utövandet av denna rätt finns i 26–28 § i personuppgiftslagen.

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 eller inom två månader av tjänstetillhandahållaren med stöd av loggregistret avgiftsfritt få veta vem som har använt eller till vem man har lämnat ut uppgifter om honom eller henne samt grunden för användningen eller utlämnandet. Kunden har motsvarande rätt att av Folkpensionsanstalten få information om utlämnande av uppgifter som sparats i en riksomfattande informationssystemtjänst och som visas via den.

Kunden har ingen rätt att få logguppgifter, om den som lämnar ut logguppgifterna vet att utlämnandet av dem kan medföra allvarlig fara för kundens hälsa eller vård eller för någon annans rättigheter. Kunden har inte heller rätt att utan särskild orsak få logguppgifter som är äldre än två år. Logguppgifter som kunden har fått får inte användas eller lämnas vidare för något annat ändamål.

Om en kund flera gånger begär logguppgifter som gäller samma tidsperiod, kan 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 tillträde till logguppgifter med hjälp av den elektroniska förbindelse som avses i 23 § får dock ingen separat avgift tas ut.

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 utredning om grunderna för användningen eller utlämnandet av uppgifterna.

5 kap. Egenkontroll i fråga om informationssäkerhet och dataskydd

27 §
Informationssäkerhetsplan

En tjänstetillhandahållare ska utarbeta en informationssäkerhetsplan med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen. Av planen ska det framgå hur följande frågor i anslutning till användningen av klient- 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 underhålls och uppdateras enligt anvisningar från producenten av informationssystemtjänsten,

5) miljön 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, underhålls och uppdateras endast av personer med den yrkesskicklighet och kompetens som krävs,

8) informationssystem som hör till klass A eller B uppfyller i enlighet med 34 § de väsentliga krav som ställs enligt deras användningsändamål, och

9) egenkontroll i fråga om genomförandet av planen ordnas i praktiken inom tjänstetillhandahållarens verksamhet.

Om en tjänstetillhandahållare har anslutit sig som användare av de riksomfattande informationssystemtjänsterna, ska det av informationssäkerhetsplanen också framgå hur man har tillgodosett kraven på dataskydd och en informationssäker användning av dessa riksomfattande tjänster. En mellanhand som avses i X § ska utarbeta en informationssäkerhetsplan, och Folkpensionsanstalten ska utarbeta en plan för de riksomfattande informationssystemtjänster som den förvaltar.

Institutet för hälsa och välfärd kan vid behov meddela närmare föreskrifter om de i 1 och 2 mom. avsedda utredningar och krav som ska tas in i informationssäkerhetsplanen samt om registrering av mellanhänder och verifiering av informationssäkerheten.

28 §

Genomförande av och ansvar för egenkontroll i fråga om dataskydd och informationssäkerhet

Varje ansvarig föreståndare för en tjänstetillhandahållares yrkesverksamhet ska meddela skriftliga instruktioner om hur kunduppgifterna ska behandlas och om de förfaringssätt som ska iakttas samt se till att personalen har tillräcklig sakkunskap och kompetens för behandlingen av kunduppgifter. Denna föreståndare ska också se till att den informationssäkerhetsplan som avses i 27 § utarbetas och iakttas. Dessutom ska varje tjänstetillhandahållare, mellanhand och tjänsteanordnare samt Folkpensionsanstalten ha en dataskyddsansvarig för uppföljnings- och övervakningsuppgifter.

6 kap.

Informationssystemens användningsändamål och ibruktagande

29 §

Informationssystemens användningsändamål och klassificering

Producenten av en informationssystemtjänst ska beskriva informationssystemets användningsändamål och på vilket sätt informationssystemet uppfyller de väsentliga krav som ställs på det.

Social- och hälsovårdens informationssystem och program för uppgifter om välbefinnande ska enligt användningsändamål och egenskaper delas in i klasserna A och B. Till klass A hör

a) de riksomfattande informationssystemtjänster som förvaltas av Folkpensionsanstalten,
b) de informationssystem och informationssystemtjänster som används till att behandla kunduppgifter och som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna,
c) de program för uppgifter om välbefinnande som utnyttjar kunduppgifter som finns i de riksomfattande informationssystemen,

d) sådana andra informationssystem, informationssystemtjänster eller tjänster som tillhandahålls av mellanhänder som i fråga om sitt användningsändamål kräver certifiering.

Övriga informationssystem, informationssystemtjänster och program för uppgifter om välbefinnande än de som nämns i 2 mom. hör till klass B.

Institutet för hälsa och välfärd får meddela föreskrifter om klassificeringen av informationssystem, informationssystemens användningsändamål och tjänster som kräver certifiering. I oklara fall är det Institutet för hälsa och välfärd som beslutar om ett informationssystem hör till klass A eller B.

30 §

Registrering av informationssystem

Producenten av en informationssystemtjänst ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om informationssystem som hör till klass A eller B innan de tas i användning för produktion. Av anmälan ska informationssystemets tillverkare och användningsändamål framgå och till anmälan ska fogas en i 36 § avsedd utredning om att de väsentliga krav som ställs på systemet enligt dess användningsändamål uppfylls. Producenten av en informationssystemtjänst ska göra en anmälan om att en sådan version av ett informationssystem som använts för produktion inte längre stöds eller att det övergått till en annan aktör.

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

a) informationssystem som hör till klass A eller B och som är avsedda att användas för produktion, deras användningsändamål samt de väsentliga krav de uppfyller,

b) resultat för interoperabilitetstestningen av informationssystem som hör till klass A och som har godkänts för användning i produktion och den tid resultaten är i kraft, och

c) den tid det överensstämmelseintyg som utfärdats enligt en bedömning av informationssäkerhet för ett informationssystem som hör till klass A och som har godkänts för användning i produktion är i kraft.

Tillstånds- och tillsynsverket för social- och hälsovården får meddela närmare 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 i användning för produktion

Ett informationssystem som hör till klass A och ett program för uppgifter om välbefinnande som hör till klass A får tas i användning för produktion och anslutas till de riksomfattande informationssystemtjänsterna efter det att informationssystemet har certifierats.

Ett informationssystem som hör till klass A eller B får inte tas i användning för produktion, om det inte finns giltiga uppgifter om det i det register som förs av Tillstånds- och tillsynsverket för social- och hälsovården, eller om godkännandet av interoperabilitetstestningen av ett informationssystem som hör till klass A inte längre gäller eller om överensstämmelseintyget för bedömning av informationssäkerheten för ett informationssystem som hör till klass A gått ut.

Tillstånds- och tillsynsverket för social- och hälsovården kan efter ansökan bevilja ett tidsbestämt tillstånd till undantag för att ett enskilt informationssystem släpps ut på marknaden och tas i bruk, även om bedömningen av systemets överensstämmelse med kraven inte har utförts på det sätt som förutsätts enligt denna lag eller de bestämmelser eller föreskrifter som har utfärdats med stöd av den, på följande villkor:

1) systemet behövs för att lindra eller behandla en allvarlig sjukdom eller skada hos en patient,

2) inget annat, motsvarande system finns att tillgå, eller

3) sökanden visar att de väsentliga krav som gäller systemet uppfylls.

Tillstånds- och tillsynsverket för social- och hälsovården kan förena tillståndet till undantag med villkor beträffande säkerheten hos informationssystemet och dess användning.

32 §

Uppföljning efter ibruktagandet av informationssystem

Producenten av en informationssystemtjänst ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera de erfarenheter som fås av informationssystemet under den tid det används för produktion. Anmälan om betydande avvikelser från de väsentliga kraven för informationssystemet ska göras till alla tjänstetillhandahållare som använder systemet. Betydande avvikelser i informationssystem som hör till klass A ska av producenten av en informationssystemtjänst anmälas till Folkpensionsanstalten och Tillstånds- och tillsynsverket för social- och hälsovården, som vidarebefordrar informationen till bedömningsorganet för informationssäkerhet.

Producenten av en informationssystemtjänst ska ge akt på ändringar i de väsentliga krav som ställs på informationssystem och justera systemen i enlighet med ändringarna. Bedömningsorganet för informationssäkerhet och Folkpensionsanstalten ska underrättas om väsentliga ändringar i informationssystem som hör till klass A. Överensstämmelseintyget eller interoperabilitetstestningen ska förnyas om betydande ändringar har gjorts i informationssystemet eller om de väsentliga kraven har ändrats på ett sätt som kräver en ny certifiering.

Producenten av en informationssystemtjänst ska bevara uppgifter om överensstämmelse med kraven och övriga uppgifter som tillsynen kräver i minst fem år efter det att informationssystemet inte längre används för produktion.

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

7 kap.

Väsentliga krav på informationssystemen

33 §

Allmänna skyldigheter för producenter av en informationssystemtjänst

Tillverkaren ansvarar för planeringen och tillverkningen av informationssystem för social- och hälsovården, oberoende av om åtgärderna utförs av tillverkaren själv eller av någon annan för dennes räkning.

Producenten av en informationssystemtjänst ska beskriva informationssystemets användningsändamål och i samband med informationssystemet ge systemanvändarna sådana uppgifter och anvisningar om informationssystemets ibruktagande, användning för produktion och underhåll som de behöver för systemets interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. De uppgifter och anvisningar som följer med informationssystemet ska finnas på finska, svenska eller engelska. De uppgifter och anvisningar som är avsedda för social- och hälsovårdspersonal som använder informationssystemet ska dock finnas på finska och svenska.

Dessutom ska tillverkaren ha ett kvalitetssystem som tillämpas på planeringen och tillverkningen av informationssystemet på det sätt som informationssystemets användningsändamål förutsätter enligt rådets direktiv 93/42/EEG om medicintekniska produkter.

34 §

Väsentliga krav på informationssystem

Informationssystem och program för uppgifter om välbefinnande som används för behandling av kunduppgifter inom social- och hälsovården ska uppfylla väsentliga krav på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. Kraven ska uppfyllas såväl vid användningen av informationssystemet självständigt som tillsammans med andra informationssystem som är avsedda att anslutas till det.

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

Ett informationssystem uppfyller de väsentliga kraven då 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 lagarna samt följer nationella föreskrifter om interoperabilitet. De väsentliga kraven på funktionalitet uppfylls om det med informationssystemet går att utföra de funktioner som krävs i lagar och med stöd av dem utfärdade bestämmelser vid behandlingen av kund- och patientuppgifter, om behandlingen överensstämmer med sitt syfte.

För informationssystem som hör till klass A ska uppfyllandet av de väsentliga kraven verifieras genom certifiering. För certifieringen svarar producenten av en informationssystemtjänst.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om innehållet i de väsentliga kraven och om vilka väsentliga krav de informationssystem som används i de olika tjänsterna ska uppfylla. Dessutom får Folkpensionsanstalten meddela föreskrifter om de förfaranden som ska iakttas vid verifieringen av interoperabiliteten i fråga om sådana informationssystem som ska kopplas till de riksomfattande informationssystemtjänster som avses i denna lag eller i lagen om elektroniska recept.

35 §

Verifiering av överensstämmelse med kraven

Överensstämmelse med kraven för informationssystem och tjänster som hör till klass A ska verifieras med en utredning från producenten av en informationssystemtjänst om att systemet uppfyller de krav på funktionalitet som ställs enligt dess användningsändamål. Ett informationssystem av klass A ska dessutom genomgå certifiering. Att certifieringen har godkänts

ska verifieras med en godkänd interoperabilitetstestning enligt 36 § och ett sådant överensstämmelseintyg av ett bedömningsorgan för informationssäkerhet som avses i 37 §.

Överensstämmelse med kraven för informationssystem som hör till klass B ska verifieras med en skriftlig utredning från producenten av en informationssystemtjänst om att systemet uppfyller de väsentliga krav som ställs enligt dess användningsändamål om det har installerats, underhållits och använts på behörigt sätt.

Producenten av en informationssystemtjänst svarar för bedömningen av de väsentliga kraven på funktionalitet hos informationssystem som hör till klass A eller B och försäkrar som en del av den utredning som ges om kraven att de funktioner som enligt utredningen ska ingå i systemets användningsändamål har genomförts i systemet.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om de förfaranden som ska iakttas vid verifieringen av överensstämmelse med kraven och om innehållet i utredningen.

36 §

Interoperabilitetstestning

Ett informationssystem som hör till klass A ska vara interoperabelt med de riksomfattande informationssystemtjänsterna och de övriga informationssystem som är anslutna till dem. Interoperabiliteten ska visas vid en interoperabilitetstestning som utförs av Folkpensionsanstalten. En förutsättning för interoperabilitetstestning är att producenten av informationssystemtjänsten lämnar Folkpensionsanstalten en redogörelse för hur kraven på informationssystemets funktionalitet har genomförts och testats. Tidpunkten för och genomförandet av interoperabilitetstestningen ska avtalas med Folkpensionsanstalten.

Ett informationssystem av klass A som har tagits i användning för produktion ska delta i de interoperabilitetstestningar för andra informationssystem som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna för att säkerställa att informationssystemen är interoperabla. 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 föranleder. 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 centrala informationssystem som Folkpensionsanstalten förvaltar och av gränssnitten för professionellt bruk.

37 §

Bedömning av informationssäkerhet

Bedömningen av överensstämmelse med de väsentliga kraven på informationssäkerhet hos de informationssystem som hör till klass A ska göras i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet. I bedömningen av informationssäkerheten enligt denna lag ingår emellertid varken bedömning eller inspektion av vare sig tillverkarens eller användarens verksamhetsställen. Bedömningen av överensstämmelse med kraven görs på ansökan av producenten av en informationssystemtjänst.

Om ett informationssystem som hör till klass A uppfyller de väsentliga krav på informationssäkerhet som ställs enligt systemets användningsändamål, ska bedömningsorganet för informationssäkerhet utifrån sin bedömning av överensstämmelsen med kraven ge tillverkaren ett överensstämmelseintyg och en tillhörande kontrollrapport. Bedömningen eller den förnyade bedömningen ska göras i enlighet med omfattningen av de ändringar som gjorts i de väsentliga kraven på informationssystemets användningsändamål och i systemet.

Överensstämmelseintyget är giltigt i högst fem år. Den tid som intyget är i kraft kan förlängas med högst fem år i sänder. Bedömningsorganet för informationssäkerhet får avkräva tillverkaren alla uppgifter som behövs för bedömningen i syfte att upprätta överensstämmelseintyget och hålla det i kraft. På utfärdande av intyget tillämpas i övrigt vad som föreskrivs i 9 § i lagen om bedömningsorgan för informationssäkerhet.

38 §

Återkallelse av överensstämmelseintyg

Om bedömningsorganet för informationssäkerhet konstaterar att ett informationssystem inte har uppfyllt eller inte längre uppfyller de krav som föreskrivs i eller med stöd av denna lag eller att ett överensstämmelseintyg av någon annan orsak inte borde ha beviljats, ska organet uppmana tillverkaren av informationssystemet att avhjälpa bristerna. Bedömningsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tillverkaren avhjälper bristerna inom den tid som organet satt ut. När tidsfristens längd bestäms ska det beaktas att en skälig tid behövs för att ändra informationssystemet.

39 §

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 överensstämmelseintyg 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 38 §. Dessutom ska bedömningsorganet för informationssäkerhet på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

8 kap.

Tillsyn av informationssystem

40 §

Styrning, övervakning och uppföljning

Den allmänna planeringen, styrningen och övervakningen av den elektroniska behandlingen av kunduppgifter inom social- och hälsovården och informationsadministrationen i anslutning därtill

samt beslutsfattandet angående totalfinansieringen av betydande informationshanteringsprojekt hör till social- och hälsovårdsministeriets uppgifter. Den allmänna styrningen och övervakningen av Befolkningsregistercentralens certifikattjänst hör likväl 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 informationsadministrationen i anslutning därtill samt av användningen och utförandet av de riksomfattande informationssystemtjänster som avses i 8 § och de gemensamma datalager som hänför sig till olika förvaltningsområden.

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

Tillhandahållare av social- och hälsovårdstjänster, Folkpensionsanstalten, Tillstånds- och tillsynsverket för social- och hälsovården och Befolkningsregistercentralen ska följa och övervaka att det dataskydd och den datasäkerhet som hänför sig till deras tjänster förverkligas. För uppföljningen och övervakningen har tjänstetillhandahållaren rätt att få logguppgifter för sina egna kundregister från Folkpensionsanstalten, logguppgifter i anslutning till behandlingen av uppgifter i kundens informationshanteringstjänst som avses i 13 § samt logguppgifter för datalagret för medborgares egna uppgifter, till den del som anställda hos tjänstetillhandahållaren har haft åtkomst till och behandlat uppgifter i kundens informationshanteringstjänst, om det behövs för att utreda att behandlingen av kunduppgifter är lagenlig.

41 §

Tillsyn 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. 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. Under en inspektion ska dessutom iakttas vad som i 39 § 1 mom. i förvaltningslagen föreskrivs om genomförande av inspektion.

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. Inspektionen 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 att inspektionen utförts.

42 §

Meddelande om avvikelser

Om tjänstetillhandahållaren konstaterar betydande avvikelser när det gäller tillgodoseendet av de väsentliga kraven på ett informationssystem, ska denne underrätta producenten av informationssystemtjänsten om saken. Om en avvikelse kan innebära en betydande risk för patientsäkerheten, informationssäkerheten eller dataskyddet ska tjänstetillhandahållaren, producenten eller tillverkaren av informationssystemtjänsten eller Folkpensionsanstalten underrätta Tillstånds- och tillsynsverket för social- och hälsovården om detta. Andra aktörer ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om risker de upptäcker.

43 §

Rätt att få uppgifter

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att avgiftsfritt och trots sekretessbestämmelserna för tillsynen över riksomfattande informationssystem få nödvändiga uppgifter av statliga och kommunala myndigheter samt av fysiska och juridiska personer som omfattas av denna lag eller de bestämmelser och beslut om riksomfattande informationssystem som utfärdats med stöd av lagen.

44 §

Tillstånds- och tillsynsverket för social- och hälsovårdens rätt att anlita utomstående sakkunniga

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att anlita utomstående sakkunniga för bedömning av informationssystems överensstämmelse med kraven. Utomstående sakkunniga får delta i inspektioner som avses i denna lag samt undersöka och testa informationssystem. Utomstående sakkunniga ska ha den sakkunskap och kompetens som uppgifterna kräver.

På utomstående sakkunniga som utför uppgifter enligt denna lag tillämpas förvaltningslagens bestämmelser om tjänstemannajäv och bestämmelserna om straffrättsligt tjänsteansvar.

Utomstående sakkunniga får inte utan tillstånd röja vad de på grund av sin ställning, sitt uppdrag eller sitt arbete har fått veta om en persons hälsotillstånd, sjukdom eller handikapp eller om social- eller hälsovårdsåtgärder som avser personen eller andra motsvarande omständigheter. Tystnadsplikten kvarstår efter det att uppdraget har upphört.

45 §

Föreläggande att fullgöra skyldigheter

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

46 §

Skyldigheter avseende informationssystem som är i bruk

När Tillstånds- och tillsynsverket för social- och hälsovården meddelar beslut om informationssystem med stöd av 41 § får verket samtidigt ålägga tillverkaren att avhjälpa brister i informationssystem som används för produktion.

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

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

9 kap.
Särskilda bestämmelser

47 §
Delegationen för elektronisk informationsadministration inom social- och hälsovården

För behandlingen av principfrågor som gäller elektronisk informationsadministration inom social- och hälsovården, för utförandet av de riksomfattande informationssystemtjänster som avses i 8 § samt för förenhetligande och utveckling av tjänsteanvändarnas informationssystem finns i anslutning till social- och hälsovårdsministeriet delegationen för elektronisk

informationsadministration inom social- och hälsovården. Närmare bestämmelser om delegationens uppgifter och sammansättning utfärdas genom förordning av statsrådet.

48 §

Avgifter

Användningen av de riksomfattande informationssystemtjänster som avses i 8 § och som administreras av Folkpensionsanstalten och Befolkningsregistercentralen är avgiftsbelagd för tjänstetillhandahållare. Den kommunala social- och hälsovårdens avgifter tas ut per sjukvårdsdistrikt hos samkommunen för sjukvårdsdistriktet. De avgifter som Folkpensionsanstalten tar ut bestäms trots 10 § i lagen om grunderna för avgifter till staten (150/1992) genom förordning av social- och hälsovårdsministeriet så att de motsvarar beloppet av kostnaderna för skötseln av tjänsterna. Avgifterna ska dessutom trygga likviditeten för Folkpensionsanstaltens servicefond. De avgifter som tas ut för Befolkningsregistercentralens prestationer bestäms i lagen om grunderna för avgifter till staten och med stöd av den.

Folkpensionsanstalten och Befolkningsregistercentralen ska årligen lämna social- och hälsovårdsministeriet en utredning över det föregående årets kostnader och de faktorer som påverkat kostnaderna samt en bedömning av de totalkostnader som ligger till grund för användningsavgifterna för det följande året.

Tillverkare av informationssystem svarar för kostnaderna för verifieringen av överensstämmelse med kraven. Folkpensionsanstalten har rätt att ta ut en avgift för sådan interoperabilitetstestning som avses i 36 § till sådant självkostnadsvärde som avses i 6 § 1 mom. i lagen om grunderna för avgifter till staten. Registrering och införande av en i x § i denna lag avsedd anmälan i offentligt register hos Tillstånds- och tillsynsverket för social- och hälsovården är avgiftsbelagd. Avgifterna bestäms genom förordning av social- och hälsovårdsministeriet, med beaktande av vad som föreskrivs i och med stöd av lagen om grunderna för avgifter till staten. Bestämmelser om avgifter som gäller godkännande av bedömningsorgan för informationssäkerhet finns i 11 § i lagen om bedömningsorgan för informationssäkerhet.

49 §

Straffbestämmelser

Den som uppsåtligen eller av grov oaktsamhet bryter mot identifierings- eller verifieringsskyldigheten i 19 §, lämnar ut sökuppgifter i strid med 12 §, 15 § 2 mom. eller 25 § 3 mom., lämnar ut kunduppgifter utan kundens samtycke enligt 13 § eller utan att en bestämmelse i lag tillåter det eller försummar upplysningsplikten enligt 17 § 2 mom. och på så sätt äventyrar kundens integritetsskydd eller hans eller hennes rättigheter i övrigt 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 personregisterbrott i 9 § i det kapitlet. Till straff för brott mot sekretess döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte gärningen utgör brott enligt 40 kap. 5 § eller om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

50 §

Handräckning av polisen

Bestämmelser om handräckning av polisen finns i polislagen (872/2011).

51 §

Vite

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

52 §

Ändringssökande

Beslut som Tillstånds- och tillsynsverket för social- och hälsovården har fattat med stöd av denna lag får överklagas hos förvaltningsdomstolen enligt vad som föreskrivs i förvaltningsprocesslagen (586/1996). Ett beslut av förvaltningsdomstolen får överklagas genom besvär hos högsta förvaltningsdomstolen, om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Ett beslut som Tillstånds- och tillsynsverket för social- och hälsovården meddelat i samband med en inspektion får inte överklagas genom besvär. Omprövning av beslutet får begäras hos Tillstånds- och tillsynsverket för social- och hälsovården inom 30 dagar från det att inspektionen avslutats. Till beslutet ska fogas anvisningar om begäran om omprövning hos verket. Åtgärderna i beslutet ska vidtas trots begäran om omprövning. Beslut som Tillstånds- och tillsynsverket för social- och hälsovården har fattat med anledning av begäran om omprövning får överklagas genom besvär enligt 1 mom.

Beslut och förelägganden som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat med stöd av denna lag ska iakttas även om de överklagats, om inte besvärsmyndigheten bestämmer något annat.

10 kap.
Ikraftträdande- och övergångsbestämmelser

53 §
Ikraftträdande

[Ikraftträdandebestämmelserna har ännu inte beretts, de kommer att utarbetas under den fortsatta beredningen.]

54 §
Övergångsbestämmelser

[Övergångsbestämmelserna har ännu inte beretts, de kommer att utarbetas under den fortsatta beredningen.] [Genom övergångsbestämmelserna ska det vid behov även föreskrivas att de förordningar som utfärdats med stöd av den gamla lagen förblir i kraft.]

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.