Svar på skriftligt spörsmål om problem som framkommit på grund av dataintrånget i psykoterapicentret Vastaamo

Till riksdagens talman

I det syfte som anges i 27 § i riksdagens arbetsordning har Ni, Ärade talman, till den minister som saken gäller översänt följande skriftliga spörsmål SS 802/2020 rd undertecknat av riksdagsledamot Eeva-Johanna Eloranta/sd:

> *Vilka åtgärder ämnar regeringen vidta för att säkerställa och övervaka dataskyddet i patientregister,*
> *skydda offer för identitetsstöld samt uppdatera dataskyddslagstiftningen*
> *för att bland annat i stället för personbeteckning förplikta till stark autentisering till exempel i affärer, näthandeln och myndighetsärenden samt i indrivningsväsendet?*

Som svar på detta spörsmål anför jag följande:

Lagstiftningen som gäller informationssäkerhet har utvecklats under de senaste åren och utvecklas fortfarande för att allt bättre svara mot det digitala samhällets krav. Det finns reglering som gäller informationssäkerhet i flera olika lagar och den senaste lagen som trädde i kraft är lagen om informationshantering inom den offentliga förvaltningen (906/2019), vars 4 kapitel föreskriver om allmänna informationssäkerhetskrav som gäller informationssystem inom den offentliga förvaltningen. Den allmänna dataskyddslagstiftningen, som justitieministeriet ansvarar för, förnyades 2018 då man började tillämpa EU:s allmänna dataskyddsförordning (2016/679). Den allmänna dataskyddsregleringen kan anses vara tämligen uppdaterad. Den allmänna dataskyddslagstiftningen förutsätter att personuppgifter behandlas lagligt och datasäkert. Informationssystem ska planeras så att dataskydd beaktas som standard. Då behandlingen förknippas med risker till exempel för att man behandlar mycket känsliga uppgifter, ska uppgifterna skyddas särskilt noggrant. Den personuppgiftsansvarige ansvarar för och ska kunna påvisa att den har iakttagit de principer som gäller behandlingen av personuppgifter. Enligt dataskyddslagstiftningen ska även dataombudsmannen och i vissa fall incidentens offer underrättas om personuppgiftsincidenter.

Social- och hälsovårdsministeriet ansvarar för regleringen av informationssäkerheten för patientregister. Lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007, klientuppgiftslagen) föreskriver bland annat om planen för egenkontroll som gäller informationssäkerheten och dataskyddet hos tillhandahållare av socialvårdstjänster och hälso- och sjukvårdstjänster, det ansvar som tillhandahållare och tillverkare av informationssystem har, informationssäkerhetskraven på de informationssystem som behandlar klient- och patientuppgifter samt övervakning. I klientuppgiftslagen föreskrivs även om indelningen av informationssy-

stem i klasserna A och B. Till klass A hör alla de klient- och patientuppgiftssystem som ska anslutas till Kanta-tjänsten, och till klass B de system som inte är avsedda att anslutas till Kanta-tjänsten.

Informationssystem som ska anslutas till Kanta-tjänsterna ska certifieras innan de ansluts. Många krav i klientuppgiftslagen gäller emellertid alla klient- och patientuppgiftssystem. Till exempel gäller väsentliga krav på informationssystem, allmänna skyldigheter för tillverkare av informationssystem och övervakning systemen i såväl klass A som klass B. Även tjänstetillhandahållarnas ansvar för planen för egenkontroll gäller tjänstetillhandahållare som inte har anslutit sig till Kanta, och likaså även tjänstetillhandahållarens ansvar att underrätta Tillstånds- och tillsynsverket för social- och hälsovården Valvira om avvikelser i informationssystemet. Tjänstetillhandahållaren ska även följa och övervaka att det dataskydd och den datasäkerhet som hänför sig till deras service förverkligas.

I fråga om övervakning föreskrivs i klientuppgiftslagen om tjänstetillhandahållarens övervakningsskyldighet. Valviras övervakningsansvar gäller systemen i både klass A och B, och system som tillhör båda klasserna ska anmälas till Valviras informationssystemregister. Likaså är metoderna för övervakning samma för alla informationssystem, till exempel bestämmelsen om att avhjälpa brister i system som används för produktion, förbud att använda ett informationssystem och vite. Oberoende av omfattningen av övervakning som genomförs av tillsynsmyndigheter är det centrala emellertid fortfarande att tjänstetillhandahållaren har ansvaret för att informationssäkerhet uppfylls i dess egen verksamhet och egna system.

Regeringen har lämnat till riksdagen ett ändringsförslag som gäller klientuppgiftslagen (RP 212/2020 rd). I den föreslås åt alla aktörer inom social- och hälsovården som använder ett system för patient- eller klientuppgifter en skyldighet att ansluta sig som användare av Kanta-tjänster. Detta betyder att en stor grupp system i klass B som har lämnats utanför certifieringen nu övergår till klass A och att de ska genomgå en certifiering som genomförs av en extern instans.

Sätten att använda personbeteckning påverkas också av i vilken omfattning den gällande lagstiftningen ställer krav på verifiering av identitet i olika situationer då ärenden uträttas. Ärendehantering med myndigheterna utgår från förvaltningslagen. Enligt 16 § i förvaltningslagen ska av en handling som tillställs en myndighet framgå vad ärendet gäller. I handlingen ska antecknas avsändarens namn samt de kontaktuppgifter som behövs för att ärendet ska kunna skötas. Enligt 19 § i förvaltningslagen ska ett ärende inledas skriftligen genom att yrkandena jämte grunderna för dem anges. Med myndighetens samtycke får ett ärende också inledas muntligen. Denna reglering betyder att en person då ett ärende inleds inte behöver identifieras och att man till exempel då ansökningar lämnas in i pappersform inte kräver en kopia av pass eller en annan handling som verifierar identiteten som bilaga till ansökan, utan att det räcker med att sökanden kan specificeras tillräckligt tillförlitligt utifrån ansökan. Motsvarande verksamhetsmodell är möjlig också i en digital verksamhetsmiljö, där till exempel en fritt formulerad ansökan som skickats per e-post ska behandlas av myndigheten om det framgår av den vad ansökan gäller. Då man uträttar ärenden

med myndigheter med hjälp av digitala tjänster ska stark elektronisk autentisering användas om det är möjligt att få se och använda sekretessbelagt datainnehåll i en digital tjänst.

Stark elektronisk autentisering krävs i nuläget i regel redan utifrån konsumentskyddslagen (38/1978), då konsumenten ingår ett konsumentkreditavtal elektroniskt med en kreditgivare och om konsumenten inte tidigare har identifierats enligt ett sätt som förutsätts i lagen. Lagen innehåller emellertid en del undantag. Kravet på stark elektronisk autentisering gäller inte nyttighetsbundna engångskrediter som i allmänhet erbjuds som ett finansieringsalternativ i näthandeln. Dessutom innehåller betaltjänstlagen (290/2010) reglering om användning som förutsätter stark autentisering och som lämpar sig för situationer där en person via näthandeln köper en nyttighet och betalar den i sin nätbank eller med betalkort eller något annat betalningsinstrument.

Vid justitieministeriet kommer man i samband med ett projekt som gäller reform av konsumentkreditbestämmelser och som inleds under våren 2021 bedöma om reglering som gäller skyldigheten att verifiera identiteten ska skärpas genom att utvidga den till att gälla ingående av alla konsumentkreditavtal. Då bestämmelser om verifiering av identitet lades till i konsumentskyddslagen 2009, var man främst medveten om problem som gäller så kallade snabblån.

Lagen om indrivning av fordringar (513/1999) förutsätter att man vid indrivning följer god indrivningssed. Till god indrivningssed hör att lagstridiga eller klart grundlösa fordringar inte tas för indrivning (RP 199/1996, s. 12). Till god indrivningssed kan dock inte anses höra att den som tagit emot ett indrivningsuppdrag har en allmän skyldighet att börja utreda riktigheten av en fordran, inklusive om man vid ingående av det avtal som den fordran som indrivs grundar sig på har använt ett förfarande för stark elektronisk autentisering. Då man tar hänsyn till verksamhetens masskaraktär kan inte heller anses ändamålsenligt att den som tagit emot ett indrivningsuppdrag ska åläggas en sådan skyldighet.

Lagen om indrivning av fordringar föreskriver även att indrivning inte får fortsätta, om gäldenären bestrider sin betalningsskyldighet. Indrivning får fortsätta trots bestridande, om gäldenären inte anger någon grund för bestridandet eller endast åberopar en sådan grund som uppenbart inte har någon inverkan på gäldenärens betalningsskyldighet. Om en gäldenär till exempel efter att ha fått ett indrivningsbrev meddelar att han eller hon inte har företagit den rättshandling som utgör grunden för fordran i fråga, kan man i princip inte fortsätta frivillig indrivning åtminstone före närmare utredning av ärendet.

En skyddsåtgärd för att motverka missbruk är ett frivilligt kreditförbud i kreditupplysningsregistret. För närvarande är situationen den att kredituppgiftsverksamhet endast utövas av privata näringsidkare. Då kreditgivare överväger beviljande av kredit kontrollerar de regelbundet kreditsökandens kredituppgifter i dessa register som upprätthålls av privata aktörer. För närvarande används inget sådant myndighetsregister där det vore ändamålsenligt att spara uppgiften om ett frivilligt kreditförbud.

Svar på skriftligt spörsmål SSS 802/2020 rd

För närvarande förbereds emellertid vid justitieministeriet ett nytt positivt kreditupplysningsregister som ska upprätthållas av myndigheter. Som en del av beredningen av ett positivt kreditupplysningsregister är målet att genomföra möjligheten till ett frivilligt kreditförbud i registret. Då kunde det i fortsättningen vara möjligt att ta ett frivilligt kreditförbud.

För att lindra konsekvenserna av det dataintrång som psykoterapicentret Vastaamo blev utsatt för och eventuella motsvarande fall har det föreslagits inrättande av en centraliserad tjänst som drivs av myndigheter för att underlätta och förenkla verksamhetsmöjligheterna för personer som blir offer för dataintrång. Redan nu har uppgifter, anvisningar och länkar som väsentligt anknyter till ärendet samlats i tjänsten Suomi.fi som drivs av Myndigheten för digitalisering och befolkningsdata så att ett offer för identitetsstöld så enkelt och med så få åtgärder som möjligt kan få de spärrar och förbud i kraft som behövs. Dessutom inleder finansministeriet en lagstiftningsutredning om metoder för att inrätta en centrerad för den offentliga och den privata sektorn gemensam tjänst för spärrning och förbud som en del av tjänsten Suomi.fi. Målet är att personen som blivit offer för identitetsstöld ett hot om identitetsstöld ska kunna logga in i ett myndighetssystem där det är möjligt att ansöka om olika förbud och spärrar på en enda plats.

Utöver den centrerade spärrtjänsten bereder regeringen både kortsiktiga och långsiktiga åtgärder i anslutning till att ta i bruk och ändra personbeteckningar. Syftet med de kortsiktiga åtgärderna är att främja möjligheterna att använda personbeteckningen i samhället. Syftet med åtgärderna är att minska riskerna för missbruk med personbeteckningar och minska skadan för personer som utsätts fr dataskyddskränkningar och informations- och kommunikationsbrott på grund av att identitetsuppgifter som hamnat i fel händer. Regeringen inleder beredningen av en lagändring som i begränsade fall, till exempel i samband med dataintrång, ger möjlighet att ändra personbeteckningen i syfte att begränsa missbruket av identiteten. Dessutom kan åtgärder för att främja användningen av personbeteckning, till exempel gällande information till medborgarna och styrningen av goda rutiner genomföras på kort sikt i anslutning till projekt för att förnya personbeteckningen före utgången av detta år.

Helsingfors 17.11.2020

Kommunminister Sirpa Paatero