Svar på skriftligt spörsmål om informationssäkerheten och cybersäkerheten i social- och hälsovården

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 801/2020 rd undertecknat av riksdagsledamot Mia Laiho /saml:

Hur övervakas dataadministrationstjänsterna hos företag utanför Kanta-tjänsterna, deras hantering av och nivå på klientuppgifterna och datasäkerheten,

hur säkerställer regeringen att det inte finns datasäkerhetsrisker i omfattande system med information om medborgarna, såsom Kanta-tjänsterna,

har regeringen gjort en riskbedömning och lagt upp en riskhanteringsplan för vårdlanskapslösningen i fråga om datasystemen,

hur har regeringen vid beredningen av lagstiftning om social- och hälsovården beaktat frågor kring datasäkerheten i datasystem,

hur har regeringen bedömt tillräcklig datasäkerhet i de tjänster och patientdatasystem samt den personaladministration som används i social- och hälsovårdstjänsterna,

hur har datasäkerheten inom personaladministrationen beaktats i beredningen av social- och hälsovården,

hur beaktar man förutom klientuppgifternas sekretess även personalens datasäkerhet,

när ska regeringen lämna en reform av helhetslagstiftningen kring behandling av information till riksdagen,

hur har regeringen i beredningen av social- och hälsovårdslagstiftningen beaktat en högklassig datasäkerhet i den digitalisering som används i klientarbetet så att alla uppgifter hålls konfidentiella och

hur säkerställer regeringen att cyberhot och attacker mot exempelvis medicintekniska produkter, sårbarheter i programvara, mobila enheter, fjärrstyrd utrustning samt systemens användningsrutiner och lösenordspraxis som anknyter till robotik och digitaliseringen av hälso- och sjukvården beaktas i nuläget och i den planerade vårdreformen?

Svar på skriftligt spörsmål SSS 801/2020 rd

Som svar på detta spörsmål anför jag följande:

I lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007, klientuppgiftslagen) stadgas om bland annat social- och hälsovårdsproducenters egenkontrollplaner för datasäkerhet och dataskydd, serviceproducenternas och datasystemtillverkarnas ansvar samt datasäkerhetskrav på och övervakning av datasystem som behandlar klient- och patientuppgifter. I klientuppgiftslagen stadgas också om klasserna A och B för datasystem. Till klass A hör alla klient- och patientdatasystem som ansluts till Kanta-tjänsterna, och till klass B hör de system som inte är avsedda att anslutas till Kanta-tjänsterna.

Datasystem som ansluts till Kanta-tjänsterna måste certifieras innan de ansluts till Kanta-tjänsterna. Många av klientuppgiftslagens krav gäller dock alla klient- och patientdatasystem. Exempelvis de centrala kraven på datasystem, datasystemtillverkarnas allmänna skyldigheter och övervakningen gäller system i både A- och B-klassen. Även serviceproducentens ansvar för egenkontrollplanen gäller även serviceproducenter som inte är anslutna till Kanta, liksom serviceproducentens ansvar att anmäla avvikelser i datasystemen till tillstånds- och tillsynsverket för social- och hälsovården Valvira. Serviceproducenten ska också följa upp och övervaka att dataskyddet och datasäkerheten i anknytning till dess tjänster förverkligas.

Vad övervakningen beträffar regleras serviceproducentens övervakningsansvar i klientuppgiftslagen. Valviras övervakningsansvar gäller system i både A- och B-klassen, och system i båda klasserna ska anmälas till Valviras register över datasystem. Metoderna för övervakningen är också desamma för alla datasystem, exempelvis förordnanden om åtgärdande av brister i system i drift, förbud mot användning av datasystem och viten. Oberoende av omfattningen på tillsynsmyndighetens övervakning är serviceproducentens ansvar för att förverkliga datasäkerhet i sin egen verksamhet och sina egna system fortfarande centralt.

Enligt EU:s allmänna dataskyddsförordning ska dataombudsmannen övervaka att förordningen och andra lagar om behandling av personuppgifter följs. Dataombudsmannens uppgifter och befogenheter regleras i dataskyddsförordningen (artikel 55–59). Förordningen kompletteras av dataskyddslagen (1050/2018), som bland annat föreskriver en administrativ påföljdsavgift vid brott mot dataskyddsförordningen. Dataombudsmannen kan också vidta andra åtgärder, som att utfärda varningar eller anmärkningar eller ställa upp begränsningar för behandlingen.

Regeringen har lämnat en proposition om ändring av klientuppgiftslagen till riksdagen (RP 212/2020 rd). I propositionen föreslås att alla de aktörer inom social- och hälsovården som använder patient- eller klientdatasystem ska bli skyldiga att ansluta sig till Kanta-tjänsterna. Det innebär att ett stort antal system i klass B som nu lämnas utanför certifieringen flyttas till klass A och måste genomgå certifiering av en utomstående aktör.

Till de delar som klient- och patientuppgifter innehåller uppgifter om personal (t.ex. namn och ID), gäller klientuppgiftslagens bestämmelser och datasäkerhetskrav också dem. Om personuppgifter om personalen behandlas i något annat system hos serviceproducenten ska serviceproducenten följa de krav på behandlingen av personuppgifter som ingår i annan lagstiftning, såsom EU:s allmänna dataskyddsförordning och dataskyddslagen.

Svar på skriftligt spörsmål SSS 801/2020 rd

Enligt klientuppgiftslagen ansvarar Folkpensionsanstalten för förverkligandet av Kanta-tjänsterna, och Folkpensionsanstalten ansvarar därmed för lagenligt förverkligande av Kantatjänsterna och datasäkerheten i dem. Uppgifterna i Kanta-tjänsterna är skyddade på många sätt för såväl datanätverkens som databasernas och applikationernas del, och Kanta-tjänsterna är certifierade av en utomstående aktör för bedömning av datasäkerhet. Även om datasystemen har gjorts så säkra som möjligt måste Folkpensionsanstalten kontinuerligt utveckla datasäkerheten i Kanta-tjänsterna med tanke på cyberhot.

Social- och hälsovårdsministeriet har berett inledandet av en totalreform av bestämmelserna kring dataadministration. Reformen är tänkt att genomföras i flera faser. Man har som mål att lämna en regeringsproposition om den första fasen till riksdagen under denna regeringsperiod. Till de centrala innehållen i totalreformen hör förtydligande och förenhetligande av dataskyddsbestämmelserna samt reglering på lagnivå av patienthandlingar och förvaring av dokument från privata serviceproducenter vars verksamhet har avslutats.

Genom vårdreformen överförs ansvaret för ordnandet av tjänster till nya aktörer, och organisationen för serviceproduktionen förändras. Exempelvis alla skyldigheter kring digital säkerhet förblir desamma som tidigare i de nya organisationerna. Detta gäller klient- och patientuppgifter, uppgifter från personaladministrationen samt säkerheten i de tjänster som produceras. Dessa regleras i bland annat hälso- och sjukvårdslagen, klientuppgiftslagen, offentlighetslagen, informationshanteringslagen och personuppgiftslagen. Nya aktörer måste uppfylla datasäkerhets- och dataskyddskraven även framöver.

Lagstiftningsmässigt ansvarar serviceproducenten för sina tjänster, oavsett hur de förverkligas. Producenter av social- och hälsovårdstjänster ansvarar för att känsliga klient- och patientuppgifter inte avslöjas för utomstående, och detta krav måste uppfyllas även i digitala tjänster.

De digitala tjänster som används inom hälso- och sjukvården är tjänster för tidsbokning och fakturering, med undantag för huvudsakligen medicintekniska produkter, som ska uppfylla kraven på medicintekniska produkter. Till definitionerna av kraven på medicintekniska produkter bereds ett avsnitt om säkerhet, som ska förbättra produkternas cybersäkerhet.

Helsingfors 17.11.2020

Familje- och omsorgsminister Krista Kiuru