FPA / Kanta-tjänster 1.11.2021

Bilaga till förbindelsen angående kundrelationen till Kanta-tjänsterna: Beskrivning av det gemensamma personuppgiftsansvaret för tjänster i anslutning till Kanta-tjänsterna

1. Dokumentets syfte och parter som berörs av det

Syftet med detta dokument, som är en bilaga till förbindelsen angående kundrelationen till Kanta-tjänsterna, är att beskriva ansvarsområdena vid gemensamt personuppgiftsansvar enligt 4 § 3 mom. i lagen om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021, nedan kunduppgiftslagen) samt 18 § i lagen om elektroniska recept (61/2007, nedan receptlagen). I anslutning till detta specificeras i detta dokument tillvägagångssätten i anslutning till det gemensamma personuppgiftsansvaret när det gäller att tillgodose den registrerades rättigheter samt fullgöra de övriga skyldigheterna som ankommer på de personuppgiftsansvariga. Genom detta dokument eller andra inbördes arrangemang mellan de personuppgiftsansvariga går det inte att specificera eller komma överens om de personuppgiftsansvarigas ansvar på något annat sätt än vad som föreskrivs i kunduppgiftslagen eller annan lagstiftning.

I fråga om utlämningsloggуppgifter som uppkommer inom social- och hälsovården samt viljeyttringstjänsten och informationshanteringstjänsten gäller detta bilagedokument gemensamt personuppgiftsansvariga, vilka är Folkpensionsanstalten (nedan FPA) samt tillhandahållare av social- och hälsotjänster. I fråga om Receptcentret gäller detta dokument gemensamt personuppgiftsansvariga, vilka är FPA, apoteken samt tillhandahållare av social- och hälsotjänster och självständiga läkemedelsförskrivare som gör upp elektroniska recept.

I artikel 26.1 i EU:s allmänna dataskyddsförordning (Europaparlamentets och rådets förordning (EU) 2016/679, nedan dataskyddsförordningen) sägs att om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Enligt punkt 2 i samma artikel ska det arrangemang som avses i punkt 1 på lämpligt sätt återspegla de

gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

I artikel 26.3 sägs att oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

Enligt 4 § 3 mom. i kunduppgiftslagen är varje tillhandahållare av social- och hälsotjänster samt FPA gemensamt personuppgiftsansvariga för utlämningsloggar som uppkommer inom social- och hälsovården, för informationshanteringstjänsten och för viljeyttringstjänsten.

- FPA 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 § i kunduppgiftslagen.
- 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.
- FPA är i artikel 26.1 i dataskyddsförordningen avsedd kontaktpunkt för de registrerade.

Enligt 4 § 5 mom. i kunduppgiftslagen finns bestämmelser om receptcentrets personuppgiftsansvariga i 18 § i lagen om elektroniska recept. Enligt det nya 18 § 1 mom. i receptlagen (786/2021) är receptcentret ett gemensamt register för FPA och apoteken samt för tjänstetillhandahållare och självständiga läkemedelsförskrivare som gör upp elektroniska recept. I 18 § 2–4 mom. i receptlagen föreskrivs att:

- FPA ansvarar för användbarheten och integriteten hos uppgifterna i receptcentret samt för att datainnehållet är oförändrat och att uppgifterna bevaras och utplånas.
- Tjänstetillhandahållare och självständiga läkemedelsförskrivare som gör upp elektroniska recept ansvarar för riktigheten av uppgifterna i recept som lagras i receptcentret.
- Det apotek som expedierar ett läkemedel ansvarar för riktigheten av de expedieringsuppgifter som lagras i receptcentret.
- FPA ansvarar för en personuppgiftsansvarigs andra skyldigheter enligt dataskyddsförordningen än de som genom denna lag påförs apoteken samt

tjänstetillhandahållare och självständiga läkemedelsförskrivare som gör upp elektroniska recept.

- FPA är dessutom i artikel 26.1 i dataskyddsförordningen avsedd kontaktpunkt för de registrerade.

2. Definitioner

Med dataskyddslagstiftning avses i detta dokument dataskyddsförordningen med eventuella ändringar, dataskyddslagen (1050/2018) samt dataskyddsmyndigheternas eller domstolarnas beslut, anvisningar och rådgivning angående behandling av personuppgifter. Om inte något annat sägs definieras personuppgifter, behandling av personuppgifter, behandlare av personuppgifter, personuppgiftsansvarig, gemensamt personuppgiftsansvarig, registrerad, personregister, dataskyddsmyndighet och personuppgiftsincident så som i dataskyddsförordningen.

Med tillhandahållare av social- och hälsotjänster avses i detta dokument en tjänstetillhandahållare som har anslutit sig som användare av Kanta-tjänsterna och därmed använder arkiveringstjänsten, informationshanteringstjänsten samt viljeyttringstjänsten eller receptcentret. Som tillhandahållare av social- och hälsotjänster räknas också självständiga yrkesutövare med personuppgiftsansvar, som i sin verksamhet använder exempelvis informationshanteringstjänsten och viljeyttringstjänsten och därmed är gemensamt personuppgiftsansvariga för tjänsterna i fråga. Självständiga yrkesutövare är också gemensamt personuppgiftsansvariga för receptcentret, om de gör upp elektroniska recept i sin verksamhet och sparar dem i receptcentret.

3. Beskrivningar av tjänsterna och de personuppgifter som behandlas i dem

3.1 Informationshanteringstjänsten

Informationshanteringstjänsten är en del av de riksomfattande informationssystemtjänsterna enligt 6 § i kunduppgiftslagen. Informationshanteringstjänsten sammanställer från journalhandlingar de patientuppgifter som är centrala för att tillhandahålla hälso- och sjukvård och skapar sammanställningar av dem för den tjänstetillhandahållare som genomför patientens vård. Informationshanteringstjänsten kan sammanställa följande centrala patientuppgifter: diagnoser och besöksorsaker, risker, laboratorieresultat, vaccinationer, åtgärder, medicineringsuppgifter, fysiologiska mätningar och bilddiagnostiska undersökningar som dokumenterats med åtgärdskoder, uppgifter om funktionsförmågan,

tidsbokningsuppgifter. I informationshanteringstjänsten sparas också handlingar som ska upprätthållas, så som en plan för undersökning, vård och medicinsk rehabilitering enligt 4 a § i patientlagen eller någon annan motsvarande plan.

3.2 Viljeyttringstjänsten

Viljeyttringstjänsten är en del av de riksomfattande informationssystemtjänsterna enligt 6 § i kunduppgiftslagen. Enligt 12 § i kunduppgiftslagen ska det i viljeyttringstjänsten 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 andra viljeyttringar än de nämnda i fråga om hälso- och sjukvård eller socialtjänster, samt i fråga om tjänster inom social- och hälsovården och behandling av kunduppgifter.

3.3 Utlämningsloggar inom social- och hälsovården

En tjänstetillhandahållare ska för uppföljningen och tillsynen särskilt för varje kundregister samla in logguppgifter om all användning och allt utlämnande av kunduppgifter (25 § i kunduppgiftslagen). Med utlämningslogg inom social- och hälsovården avses en logg som innehåller uppgifter om utlämnande av personuppgifter mellan olika register eller personuppgiftsansvariga. 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.

3.4 Receptcentret

Receptcentret är en databas som består av elektroniska recept som lagrats av läkemedelsförskrivarna, av recept som apoteken har lagrat på de grunder som föreskrivs i 12 §, av sådana uppgifter om läkemedel som överlåtits till patienter av tillhandahållare av socialvårdstjänster och hälso- och sjukvårdstjänster på de grunder som föreskrivs i 23 §, av expedieringsuppgifter som fogats till recepten och av anteckningar som hänför sig till en bedömning av läkemedelsbehandlingen (3 § 1 mom. 4 punkten i receptlagen).

4. Grunden för behandling av personuppgifter och rätten att behandla personuppgifter

I viljeyttringstjänsten och informationshanteringstjänsten kan tillhandahållare av social- och hälsotjänster spara uppgifter endast för att genomföra patientens vård eller service. Tjänstetillhandahållare kan behandla de lagrade uppgifterna för att genomföra bara patientens vård eller service, om inte kunden har förbjudit att uppgifter om honom eller henne lämnas ut. I 18 § i kunduppgiftslagen föreskrivs bland annat om kundens tillstånd för, samtycke till och förbud mot utlämnande. I 20 och 21 § i kunduppgiftslagen och i 13 § i receptlagen föreskrivs bland annat om utlämnande av patient- och klientuppgifter via riksomfattande informationssystemtjänster.

För receptcentrets del kan apoteken behandla uppgifter i receptcentret för att expediera recept och sköta uppgifter i anslutning till detta. I 11 § i receptlagen föreskrivs om apotekens rätt att få uppgifter. Tillhandahållare av social- och hälsotjänster samt självständiga yrkesutövare kan behandla uppgifter i receptcentret för att följa upp och genomföra patientens vård och medicinering. I 13 § i receptlagen föreskrivs om utlämnande av uppgifter från receptcentret och om rätten att förbjuda utlämnande.

Grunden för behandling av de personuppgifter som avses i detta dokument och som sparats i gemensamma register är lagstiftning. Bestämmelser om åtkomsträttigheter till kunduppgifter finns i 15 § i kunduppgiftslagen samt i förordning som utfärdas med stöd av den, och för elektroniska receptuppgifters del i 4 kap. i receptlagen. Personuppgifter som sparats i de tjänster som avses i detta dokument översänds inte utanför EU/EES. Dessutom förutsätter Säkerhetskriterierna för molntjänster[1] att informationssystem som är väsentliga för en kritisk samhällsfunktion ska finnas i Finland. Likaså ska datamassor med känsliga personuppgifter finnas i Finland. Om ett apoteks- eller patientdatasystem tillhandahålls som molntjänst, ska de ovan nämnda kraven i PiTuKri beaktas.

5. Gemensamt personuppgiftsansvarigas ansvar

5.1 Allmänt om gemensamt personuppgiftsansvarigas ansvar och skyldigheter

De som är gemensamt personuppgiftsansvariga så som avses i detta dokument är personuppgiftsansvariga så som avses i dataskyddsförordningen och ansvarar därmed

[1]Säkerhetskriterier för molntjänster (PiTuKri): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf

självständigt för att deras behandling av personuppgifter är korrekt, med de ansvar som föreskrivs i kunduppgiftslagen och receptlagen. Gemensamt personuppgiftsansvariga ansvarar för att deras behandling av personuppgifter är korrekt i enlighet med gällande dataskyddslagstiftning. Gemensamt personuppgiftsansvariga är i detta dokument i enlighet med ovan sagda:

- Informationshanteringstjänsten: tillhandahållare av social- och hälsotjänster samt FPA.
- Viljeyttringstjänsten: tillhandahållare av social- och hälsotjänster samt FPA.
- Utlämningsloggar som uppkommer inom social- och hälsovården: tillhandahållare av social- och hälsotjänster samt FPA.
- Receptcentret: tillhandahållare av social- och hälsotjänster, självständiga läkemedelsförskrivare, apotek samt FPA.

Observeras bör att med avseende på det gemensamma personuppgiftsansvaret har den registrerade rätt att utöva sina rättigheter enligt dataskyddsförordningen med avseende på och emot var och en av de personuppgiftsansvariga.

5.2 Information till de registrerade och den registrerades utövande av sina rättigheter

Enligt kunduppgiftslagen och receptlagen är FPA den kontaktpunkt som avses i artikel 26 i dataskyddsförordningen med avseende på de registrerade i fråga om informationshanteringstjänsten, viljeyttringstjänsten, utlämningsloggar som uppkommer inom social- och hälsovården samt receptcentret. Beträffande personuppgifter som samlats in i de tjänster som det är fråga om i detta dokument ansvarar FPA i egenskap av kontaktpunkt för att fullgöra och genomföra den informationsskyldighet som personuppgiftsansvariga ålagts i dataskyddslagstiftningen. Vid behov ska de gemensamt personuppgiftsansvariga i samarbete bistå och ansvara för fullgörandet av skyldigheten enligt dataskyddsförordningen att informera den registrerade till den del det ankommer på den gemensamt personuppgiftsansvarige i fråga.

FPA är primär kontaktpunkt i begäranden som gäller de registrerades utövande av sina rättigheter. De registrerade informeras om FPA:s roll som kontaktpunkt i den ovan avsedda information som ska ges de registrerade. Om en registrerad tar kontakt i ett ärende som en tjänstetillhandahållare, en självständig yrkesutövare eller ett apotek ansvarar för, hänvisar FPA kunden att kontakta den tjänstetillhandahållare som kontakttagningen i fråga gäller och som har fört in den aktuella uppgiften i tjänsten i fråga, eller i vars uppgifter ärendet annars ingår.

I övrigt ska den registrerades rättigheter beskrivas i de gemensamt personuppgiftsansvarigas egna dataskyddsbeskrivningar. Det centrala innehållet även i detta dokument ska tydligt och öppet framgå av dataskyddsbeskrivningarna för tjänsten i fråga. Tjänstetillhandahållare, apotek samt självständiga yrkesutövare gör var för sig upp ett register enligt artikel 30 i dataskyddsförordningen över behandling som utförts under dess ansvar. De nämnda aktörerna ser var och en för sitt vidkommande till att registret och kontaktinformationen i det är aktuella och uppdateras vid behov. FPA gör upp ett eget register över behandling som utförts under dess ansvar med avseende på de riksomfattande informationssystemtjänsterna i fråga.

5.3 Den registrerades begäran om kontroll av uppgifter

5.3.1 Informationshanteringstjänsten

Den registrerade har rätt att kontrollera de uppgifter som sparats om honom eller henne i informationshanteringstjänsten. Tjänstetillhandahållaren är personuppgiftsansvarig för de uppgifter som uppkommit i tjänstetillhandahållarens verksamhet och ansvarar som gemensamt personuppgiftsansvarig för att de uppgifter som sammanställs från informationshanteringstjänsten är korrekta. Om den registrerade utövar sin rätt att kontrollera uppgifter, riktas samt vid behov hänvisas begäran om detta till den tjänstetillhandahållare som ansvarar för att de införda uppgifterna är korrekta samt för den personuppgiftsansvariges övriga skyldigheter. Tjänstetillhandahållaren ska förse den registrerade med de uppgifter som sparats om den registrerade i enlighet med dataskyddsförordningen. Den registrerade har möjlighet att via tjänsten Mina Kanta-sidor läsa en sammanställning av de uppgifter som sparats i informationshanteringstjänsten.

5.3.2. Viljeyttringstjänsten

Den registrerade har rätt att kontrollera de uppgifter som sparats om honom eller henne i viljeyttringstjänsten. Till den del en tjänstetillhandahållare eller en självständig yrkesutövare har fört in uppgifter i viljeyttringstjänsten, ansvarar aktören i fråga som gemensamt personuppgiftsansvarig för att de uppgifter den sparat i viljeyttringstjänsten är korrekta. Om den registrerade utövar sin rätt att kontrollera uppgifter, riktas samt vid behov hänvisas begäran om detta till den tjänstetillhandahållare som fört in uppgiften i fråga i viljeyttringstjänsten och som ansvarar för att de införda uppgifterna är korrekta samt för den personuppgiftsansvariges övriga skyldigheter. Tjänstetillhandahållaren ska förse den

registrerade med de uppgifter som sparats om den registrerade i enlighet med dataskyddsförordningen.

Den registrerade har möjlighet att via tjänsten Mina Kanta-sidor läsa en sammanställning av de viljeyttringar han eller hon meddelat. Vid behov kan FPA förse den registrerade med uppgifter som den registrerade själv har sparat i viljeyttringstjänsten. Om den registrerade inte har möjlighet att få en sammanställning från tjänstetillhandahållarna av de uppgifter som sparats i viljeyttringstjänsten, kan FPA som den registrerades kontaktpunkt vid behov lämna ut de här uppgifterna till den registrerade. I dessa situationer förser FPA den registrerade med de uppgifter som sparats om den registrerade i enlighet med dataskyddsförordningen.

5.3.3 Receptcentret

Den registrerade har rätt att kontrollera de uppgifter som sparats om honom eller henne i receptcentret. Bestämmelser om patientens rätt till information och rättelse av felaktiga uppgifter i receptcentret finns i 16 § i receptlagen. Bestämmelser om rättelse av felaktiga uppgifter i receptcentret finns i 10 § i receptlagen och i artikel 16 i dataskyddsförordningen. Om patienten eller dennes lagliga företrädare med stöd av artikel 16 i dataskyddsförordningen kräver att en uppgift ska rättas och om den felaktiga uppgiften grundar sig på läkemedelsförskrivarens eller läkemedelsexpedierarens anteckning, ska kravet på rättelse riktas till den person som gjort den felaktiga anteckningen eller den organisation där personen var anställd när felet begicks.

Till den del den registrerades begäran om kontroll av uppgifter gäller uppgifter som sparats i receptcentret ansvarar FPA för att uppfylla begäran om kontroll av uppgifter och för att den registrerades rätt att få tillgång till uppgifter tillgodoses, eftersom FPA enligt paragrafen ansvarar för övriga skyldigheter som ankommer på den personuppgiftsansvarige. FPA förser den registrerade med de uppgifter som sparats om den registrerade i enlighet med dataskyddsförordningen.

Om den registrerade önskar rätta uppgifter som sparats om den registrerade i receptcentret, riktas begäran om detta till den ansvariga tjänstetillhandahållaren i enlighet med 16 § i receptlagen.

5.3.4 Utlämningslogguppgifter som uppkommer inom social- och hälsovården samt övriga utlämningslogguppgifter

Enligt 4 § i kunduppgiftslagen är FPA och tjänstetillhandahållaren gemensamt personuppgiftsansvariga för för utlämningsloggar som uppkommer inom social- och hälsovården. FPA 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 §. Till denna del ansvarar den tjänstetillhandahållare i vars verksamhet utlämningsloggposten har uppkommit för att den sparade uppgiften är korrekt samt för begäranden om kontroll av uppgifter i anslutning till detta.

Enligt 26 § 1 mom. i kunduppgiftslagen har en kund 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. Enligt samma lagrum har kunden motsvarande rätt att av FPA få logguppgifter ur informationshanteringstjänsten, viljeyttringstjänsten, receptcentret och informationsresursen för egna uppgifter, logguppgifter för använda eller utlämnade kunduppgifter och uppgifter om välbefinnande samt uppgifter om tidpunkten för användningen eller utlämnandet till den del uppgifterna omfattas av FPA:s personuppgiftsansvar.

Enligt 16 § 3 mom. i receptlagen har patienten rätt att på begäran utifrån logguppgifter få veta vem som har behandlat eller haft åtkomst till sådan information om patienten som finns i receptcentret eller i den i 12 § i kunduppgiftslagen avsedda viljeyttringstjänsten. Patienten har dock inte rätt att få logguppgifter, om den som lämnar ut logguppgifter vet att utlämnandet kan medföra allvarlig fara för patientens hälsa eller vård eller för någon annans rättigheter. Patienten har inte heller rätt att utan särskild orsak få logguppgifter som är äldre än två år. Logguppgifter som en patient har fått får inte användas eller lämnas vidare för något annat ändamål. FPA ska lämna ut uppgifterna utan dröjsmål. Det får inte tas ut någon avgift för utlämnandet av uppgifterna. En patient som på nytt begär samma uppgifter som han eller hon redan har fått har rätt att få uppgifterna endast om det finns grundad anledning till det med hänsyn till tillgodoseendet av patientens intressen eller rättigheter. Ärendet kan föras till dataombudsmannen för behandling i enlighet med 21 § 1 mom. i dataskyddslagen. För uppgifter som lämnas ut på nytt får FPA ta ut en avgift som inte får överstiga

kostnaderna för utlämnande av uppgifterna. (Se 26 § i kunduppgiftslagen och 16 § i receptlagen).

Om den registrerades begäran om kontroll av uppgifter gäller utlämningsloggуppgifter för informationshanteringstjänsten, viljeyttringstjänsten eller receptcentret eller användningsloggуppgifter för receptcentret, är det FPA som ska uppfylla och svara på begäran. Om den registrerades begäran om kontroll av uppgifter gäller användningsloggуppgifter som uppkommit i en tillhandahållare av social- och hälsotjänsters verksamhet, ska begäran uppfyllas av den tjänstetillhandahållare i vars verksamhet användningsloggуppgiften i fråga har uppkommit (4 § i kunduppgiftslagen). Enligt 24 § 2 mom. i kunduppgiftslagen får den registrerade via Mina Kanta-sidor visas utlämningsloggуppgifter och användningsloggуppgifter som gäller behandlingen av hans eller hennes uppgifter, med undantag för mottagarens personuppgifter.

5.4 Den registrerades begäran om rättelse samt radering av uppgifter

Den tjänstetillhandahållare som ansvarar för att uppgifterna som sparats i tjänsten är korrekta ansvarar för att genomföra förfarandet för att rätta och radera uppgifter som sparats i informationshanteringstjänsten, receptcentret och viljeyttringstjänsten i enlighet med artiklarna 16 och 17 i dataskyddsförordningen. När den registrerade tar kontakt med FPA ansvarar FPA som den registrerades kontaktpunkt för att tjänstetillhandahållaren får den registrerades kontakttagning för handläggning.

Den registrerade har rätt att begära att få sina uppgifter raderade, men regelverket kring förvaring av journal- och klienthandlingar samt receptuppgifter begränsar tillgodoseendet av denna rätt. Bestämmelser om förvaringstiderna för journalhandlingar, klienthandlingar och recepthandlingar samt loggуppgifterna för dessa finns bland annat i kunduppgiftslagen, patientlagen (785/1992), förordningen om journalhandlingar (298/2009), lagen om klienthandlingar inom socialvården (254/2015) samt i receptlagen. När förvaringstiderna grundar sig på tvingande lagstiftning har den registrerade inte rätt att få sina handlingar eller uppgifter i dem eller loggуppgifter för dem raderade förrän den lagstadgade förvaringstiden gått ut.

6. Förfaranden som ska följas vid personuppgifts- och informationssäkerhetsincidenter

6.1 Allmänt om gemensamt personuppgiftsansvarigas ansvar vid personuppgiftsincidenter

Alla gemensamt personuppgiftsansvariga ska självständigt dokumentera eventuella personuppgiftsincidenter och informationssäkerhetsincidenter som gäller personuppgifter och ansvarar för sitt vidkommande för att anmäla dessa i enlighet med artiklarna 33 och 34 i dataskyddsförordningen, om incidenten är sådan att anmälan krävs. Anmälningsskyldigheten gäller både anmälan till tillsynsmyndigheten och underrättande av den registrerade i en situation där personuppgiftsincidenten sannolikt innebär en hög risk för den registrerades rättigheter och friheter. Dataskyddsförordningen innehåller bestämmelser om tidsfristerna i samband med fullgörandet av anmälningsskyldigheten.

Varje gemensamt personuppgiftsansvarig ansvarar för att förbereda sig för eventuella personuppgiftsincidenter i sin egen verksamhet och för att handlägga dem på behörigt sätt. Gemensamt personuppgiftsansvariga ansvarar i sin egen verksamhet för att deras personal har instruerats om till vem eller vart de ska vända sig vid en eventuell personuppgiftsincident. Varje gemensamt personuppgiftsansvarig ansvarar i sin egen verksamhet för sina egna processer och anvisningar i samband med personuppgiftsincidenter samt för den behövliga ansvarsfördelningen med avseende på verksamheten i fråga.

I 41 § i kunduppgiftslagen föreskrivs om skyldigheten att underrätta om avvikelser från de väsentliga kraven på ett informationssystem. Om en personuppgiftsincident beror på Kanta-tjänsternas, ett apotekssystems eller ett kund- eller patientdatasystems funktion, kan det antas att systemet inte uppfyller de informationssäkerhetskrav som ställs på systemet i kunduppgiftslagen och att det är fråga om en avvikelse från de väsentliga kraven. I en sådan situation är informationssystemets tillverkare och den tjänstetillhandahållare och det apotek som använder systemet skyldiga enligt 41 § i kunduppgiftslagen att underrätta Tillstånds- och tillsynsverket för social- och hälsovården om saken. Också FPA har bland annat ifrågavarande anmälningsskyldighet enligt 41 § i kunduppgiftslagen.

Gemensamt personuppgiftsansvariga ansvarar för att i sin egen verksamhet kunna upptäcka eventuella personuppgiftsincidenter tillräckligt snabbt och för att observationerna i samband med detta är inkluderade i den gemensamt personuppgiftsansvariges egna processer.

6.2 Ansvarsfördelningen i olika tjänster

I fråga om informationshanteringstjänsten och viljeyttringstjänsten ansvarar tjänstetillhandahållarna i enlighet med 4 § i kunduppgiftslagen för den personuppgiftsansvariges övriga skyldigheter. Därmed har tjänstetillhandahållaren i fråga det ledande ansvaret för att anmäla personuppgiftsincidenter som gäller dessa tjänster. Beträffande utlämningsloggar som uppkommer inom social- och hälsovården ansvarar FPA 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 § i kunduppgiftslagen. Till dessa delar ansvarar FPA också för eventuella personuppgiftsincidenter i tjänsten.

För receptcentrets del ansvarar FPA enligt 18 § i receptlagen för en personuppgiftsansvarigs andra skyldigheter enligt dataskyddsförordningen än de som genom denna lag påförs apoteken samt tjänstetillhandahållare och självständiga läkemedelsförskrivare som gör upp elektroniska recept. Därmed har FPA det ledande ansvaret för att anmäla personuppgiftsincidenter som gäller receptcentret. Om en personuppgiftsincident som gäller receptcentret inträffar i någon annan gemensamt personuppgiftsansvarigs egen verksamhet, till exempel vid behandlingen av receptuppgifter, har den gemensamt personuppgiftsansvarige i vars verksamhet den misstänkta incidenten har inträffat det primära ansvaret för att fullgöra anmälningsskyldigheten.

6.3 Förfaranden som ska följas

6.3.1 Utgångspunkten för anmälan av personuppgiftsincidenter i olika situationer

Oavsett vad som föreskrivits om gemensamt personuppgiftsansvarigas ansvar, kan den första observationen av en personuppgiftsincident göras av vilken aktör som helst som först upptäcker den eventuella personuppgiftsincidenten. Den som upptäcker incidenten ska ta kontakt med kontaktinstansen för personuppgiftsincidenter hos den organisation han eller hon företräder och rapportera de uppgifter som krävs enligt anvisningarna.

Om en personuppgiftsincident riktar sig mot endast en av de gemensamt personuppgiftsansvarigas verksamhet och det alltså är fråga om en intern incident inom organisationen, ska incidenten vidareutredas och lösas i enlighet med den gemensamt personuppgiftsansvariges interna process och anvisningar. Den gemensamt personuppgiftsansvarige mot vars verksamhet den eventuella personuppgiftsincidenten

riktar sig ansvarar då för att fullgöra anmälningsskyldigheten enligt artiklarna 33 och 34 i dataskyddsförordningen. Om en misstänkt personuppgiftsincident riktar sig mot eller bedöms rikta sig mot flera tjänstetillhandahållare, självständiga yrkesutövare eller apotek inom någon tjänst, men inte mot de tjänster som FPA förvaltar, ska dessa personuppgiftsansvariga tillsammans besluta om och samordna utredningsarbetet och göra en eventuell anmälan om personuppgiftsincident till tillsynsmyndigheten och vid behov underrätta den registrerade.

Om en tjänstetillhandahållare upptäcker en eventuell personuppgiftsincident i en tjänst som FPA förvaltar eller i dess verksamhet eller i någon funktion som FPA annars ansvarar för som gemensamt personuppgiftsansvarig, ska tjänstetillhandahållaren utan dröjsmål ta kontakt med FPA för att utreda saken. I dessa situationer ansvarar FPA för att fullgöra anmälningsskyldigheten enligt artiklarna 33 och 34 i dataskyddsförordningen.

Om en personuppgiftsincident riktar sig mot eller bedöms rikta sig mot både FPA och någon annan gemensamt personuppgiftsansvarig eller mot dessas verksamhet, ska de gemensamt personuppgiftsansvariga utan dröjsmål underrätta varandra om den misstänkta incidenten. För FPA:s del ska den gemensamt personuppgiftsansvarige underrätta FPA:s tekniska support om saken. Övriga gemensamt personuppgiftsansvariga ska i samband med detta meddela sin kontaktinformation i enlighet med punkt 8 i detta dokument. Om en personuppgiftsincident i dessa situationer riktar sig mot receptcentret, ansvarar FPA för att fullgöra anmälningsskyldigheten enligt artiklarna 33 och 34 i dataskyddsförordningen. Om en personuppgiftsincident riktar sig mot informationshanterings- eller viljeyttringstjänsten, är det den tjänstetillhandahållare som i situationen i fråga ansvarar för de övriga skyldigheter som ankommer på den personuppgiftsansvarige som ansvarar för att fullgöra anmälningsskyldigheten.

Om en personuppgiftsincident inträffar i en tjänst som FPA förvaltar och incidenten hänför sig till FPA:s verksamhet, ska FPA samordna och göra en eventuell anmälan till dataombudsmannens byrå och vid behov underrätta den registrerade. Om en tjänstetillhandahållare upptäcker en eventuell personuppgiftsincident i en tjänst som FPA förvaltar eller i dess verksamhet eller i någon funktion som FPA annars ansvarar för som gemensamt personuppgiftsansvarig, ska tjänstetillhandahållaren utan dröjsmål ta kontakt med FPA för att utreda saken. I dessa situationer ansvarar FPA för att fullgöra anmälningsskyldigheten enligt artiklarna 33 och 34 i dataskyddsförordningen. Om en personuppgiftsincident inträffar i en tjänst som FPA förvaltar och incidenten beror på någon annan gemensamt personuppgiftsansvarigs verksamhet, ansvarar i första hand den

gemensamt personuppgiftsansvarige i vars verksamhet incidenten har inträffat för att fullgöra anmälningsskyldigheten. Också FPA ska utan dröjsmål kontaktas angående saken.

Om incidenten till sin natur är sådan att den kräver att de gemensamt personuppgiftsansvariga underrättas, är de personuppgiftsansvariga skyldiga att utan dröjsmål underrätta den andra personuppgiftsansvarige om personuppgiftsincidenten samt även om övriga omständigheter som kan påverka den andra partens fullgörande av sina ansvar eller skyldigheter enligt 4 § i kunduppgiftslagen eller 18 § i receptlagen. Om en personuppgiftsincident också gäller något som hör till den andra personuppgiftsansvariges ansvarsområde, ska den personuppgiftsansvarige alltid underrättas om detta utan dröjsmål när en incident upptäcks. Innehållet i anmälan specificeras i punkt 6.4 i detta dokument.

6.3.2 Dokumentation av personuppgiftsincidenter och åtgärder för att förhindra att en incident sprids

Gemensamt personuppgiftsansvariga ska alltid när de upptäcker en personuppgiftsincident vidta åtgärder var och en för sitt vidkommande för att förhindra att incidenten sprids. I samband med detta ska de bedöma och undersöka om det går att begränsa personuppgiftsincidenten och om den eventuellt kan sprida sig. De ska också bedöma vilka som kan se incidenten i fråga och vilkas verksamhet den påverkar. I det här skedet ska de också preliminärt bedöma under vilka förutsättningar verksamheten i fråga kan fortgå. Det gäller bl.a. att besluta om omedelbara åtgärder som att till exempel koppla bort system från nätet, ta i bruk kontinuitetsplaner samt avdela nödvändiga resurser för att reagera.

En viktig del i handläggningen av en eventuell personuppgiftsincident är att fastställa källan till problemet. Om man misstänker eller om det framgår att det till exempel är fråga om ett brott, är det någon annan finsk myndighets, i detta fall polisens, uppgift att utreda källan till personuppgiftsincidenten. Gemensamt personuppgiftsansvariga ska dokumentera sina observationer, åtgärder och beslut i samband med personuppgiftsincidenter. Varje gemensamt personuppgiftsansvarig ska dokumentera sina egna åtgärder.

Bevismaterial ska samlas in och förvaras på ett säkert sätt och man ska bereda sig på att materialet behövs vid efterutredningar. Vid behandlingen av bevismaterialet ska materialets integritet och tidsstämplar tryggas. Bevismaterialet ska samlas in och dokumenteras så fullständigt som möjligt. Förvaringstiden för bevismaterialet fastställs på förhand i samband med personuppgiftsincidenten. För att säkerställa utredningen ska bevismaterialet emellertid förvaras i minst två år vid misstanke om vanligt brott och i minst fem år vid misstanke om

grovt brott eller tjänstebrott. När en eventuell brottsundersökning inletts ska polisens anvisningar följas.

6.4 Uppgifter som ska anges i en anmälan om personuppgiftsincident till en annan personuppgiftsansvarig

En anmälan till en annan gemensamt personuppgiftsansvarig ska innehålla följande uppgifter:

- personuppgiftsincidentens identifikationskod (om sådan finns)
- när den eventuella personuppgiftsincidenten upptäcktes och anmäldes
- om det är fråga om en personuppgiftsincident
- personuppgiftsincidentens inverkan
  - personuppgiftsincidentens nuläge (status, t.ex. misstänkt/obekräftad/bekräftad /under åtgärder varande personuppgiftsincident/utredd/rapporterad/handläggningen slutförd)
- personuppgiftsincidentens källa och orsak, om känd
- beskrivning av personuppgiftsincidenten (i vilken situation upptäcktes den och vilka tecken avslöjade den eventuella personuppgiftsincidenten)
- beskrivning av föremålen för personuppgiftsincidenten (t.ex. nätverk, servrar eller nätverkstjänster)
- övriga observationer (t.ex. avvikande datatrafik, larm eller anmälningar från användare)
- faktorer som påverkar prioriteringen av personuppgiftsincidenten (bl.a. hur viktigt det system eller den information är som är föremål för personuppgiftsincidenten)
- faktorer som minskar inverkan (t.ex. att hårddisken i en stulen dator är krypterad)
- faktorer som ökar inverkan (t.ex. att det rör sig om uppgifter som klassats som känsliga)
- vidtagna motåtgärder (t.ex. att tjänstens nättrafik förhindrats eller filtrerats eller att arbetsstationen kopplats bort från nätet)
- gemensamt personuppgiftsansvariga som redan kontaktats i anslutning till personuppgiftsincidenten

Uppgifter om personuppgiftsincidenten:

- handläggningens nuläge (status)
- personuppgiftsincidenten i sammandrag
- vilka åtgärder som vidtagits för att handlägga personuppgiftsincidenten samt de exakta tidpunkterna

- kontaktinformation till alla som deltagit i handläggningen samt dokumentation av händelserna
- en lista över insamlat bevismaterial
- handläggarens kommentarer
- grundorsaken till personuppgiftsincidenten
- kostnaderna för hantering av personuppgiftsincidenten
- personuppgiftsincidentens eventuella inverkan på affärsverksamheten

7. Upprättande av en konsekvensbedömning enligt dataskyddsförordningen

Gemensamt personuppgiftsansvariga är skyldiga att bedöma behovet av en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen. Som gemensamt personuppgiftsansvarig gör FPA en egen konsekvensbedömning av de behandlingsåtgärder FPA vidtagit. Om en tjänstetillhandahållares behandling förutsätter förhandssamråd enligt artikel 36 i dataskyddsförordningen ska tjänstetillhandahållaren sköta genomförandet av förhandssamrådsförfarandet.

8. Gemensamt personuppgiftsansvarigas samverkan och bistånd

Gemensamt personuppgiftsansvariga ser var och en för sitt vidkommande till att alla parter förmår uppfylla sina skyldigheter angående dataskyddet och att den registrerades rättigheter tillgodoses fullt ut vid gemensamt personuppgiftsansvar. Gemensamt personuppgiftsansvariga ansvarar var och en för sitt vidkommande för att parterna har den kontaktinformation som behövs för att den registrerade ska kunna utöva sina rättigheter och för att informationen alltid är uppdaterad. Gemensamt personuppgiftsansvariga ska se till att den kontaktinformation de sparat i Kanta-tjänsternas kundregister alltid är uppdaterad.

9. Dokumentets bindande natur och giltighet

Detta dokument är en del av förbindelsen angående kundrelationen till Kanta-tjänsterna. Detta dokument träder i kraft 1.11.2021.

Kommentarer angående innehållet i detta dokument har begärts av företrädare för vissa tjänstetillhandahållare samt berörda myndigheter i ett e-postmeddelande daterat 1.10.2021.