Rutin för hantering av personuppgiftsincident eller misstänkt personuppgiftsincident när det gäller Kanta-tjänsterna

Apoteken och social- och hälsovården

22.1.2019

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta-tjänsterna
PB 450, 00056 FPA

Kanta 280r 01.19
www.kanta.fi/sv
kanta@kanta.fi

Innehåll

1 Inledning 3

2 Upptäckt och anmälan av en personuppgiftsincident 4

2.1 Den som upptäckt incidenten representerar den personuppgiftsansvarige 5

2.2 Den som upptäckt incidenten representerar personuppgiftsbiträdet 5

2.3 Anmälan till FPA:s tekniska support 5

3 Dokumentering av upptäckt, åtgärder och fortsatta åtgärder 6

1 Inledning

Den här anvisningen är avsedd som stöd för apotek och tillhandahållare av social- och hälsovårdstjänster (nedan tillhandahållare av tjänster) i situationer där man har upptäckt eller misstänker en personuppgiftsincident i fråga om Kanta-tjänsterna. Apoteken och tillhandahållarna av tjänster kan utgå från detta material när de tar fram en plan för egenkontroll och separata anvisningar när det gäller datasäkerhet och dataskydd.

Vid en personuppgiftsincident eller vid misstanke om en sådan följs EU:s allmänna dataskyddsförordning och andra bestämmelser om dataskydd, såsom speciallagstiftning. Anvisningen uppdateras efter att den nya lagen om klientuppgifter och lagen om elektroniska recept trätt i kraft.

Med en personuppgiftsincident avses en händelse som leder till att personuppgifter förstörs, försvinner, ändras, lämnas ut utan lov eller hamnar i händerna på en aktör som saknar rätt att behandla dem.

Apoteken och tillhandahållarna av tjänster ska vara beredda på personuppgiftsincidenter genom att se till att personalen är medveten om rutinerna och rapporteringen kring dylika situationer.

Apoteken och tillhandahållarna av tjänster ska dessutom läsa anvisningarna för störningssituationer som finns både på webbplatserna kanta.fi och fpa.fi.

Vid en personuppgiftsincident eller vid misstanke om en sådan ska man agera enligt den modell som presenteras nedan i ett flödesschema om personuppgiftsincidenter (Bild 1). I kapitlen som följer finns korta beskrivningar av de olika skedena.

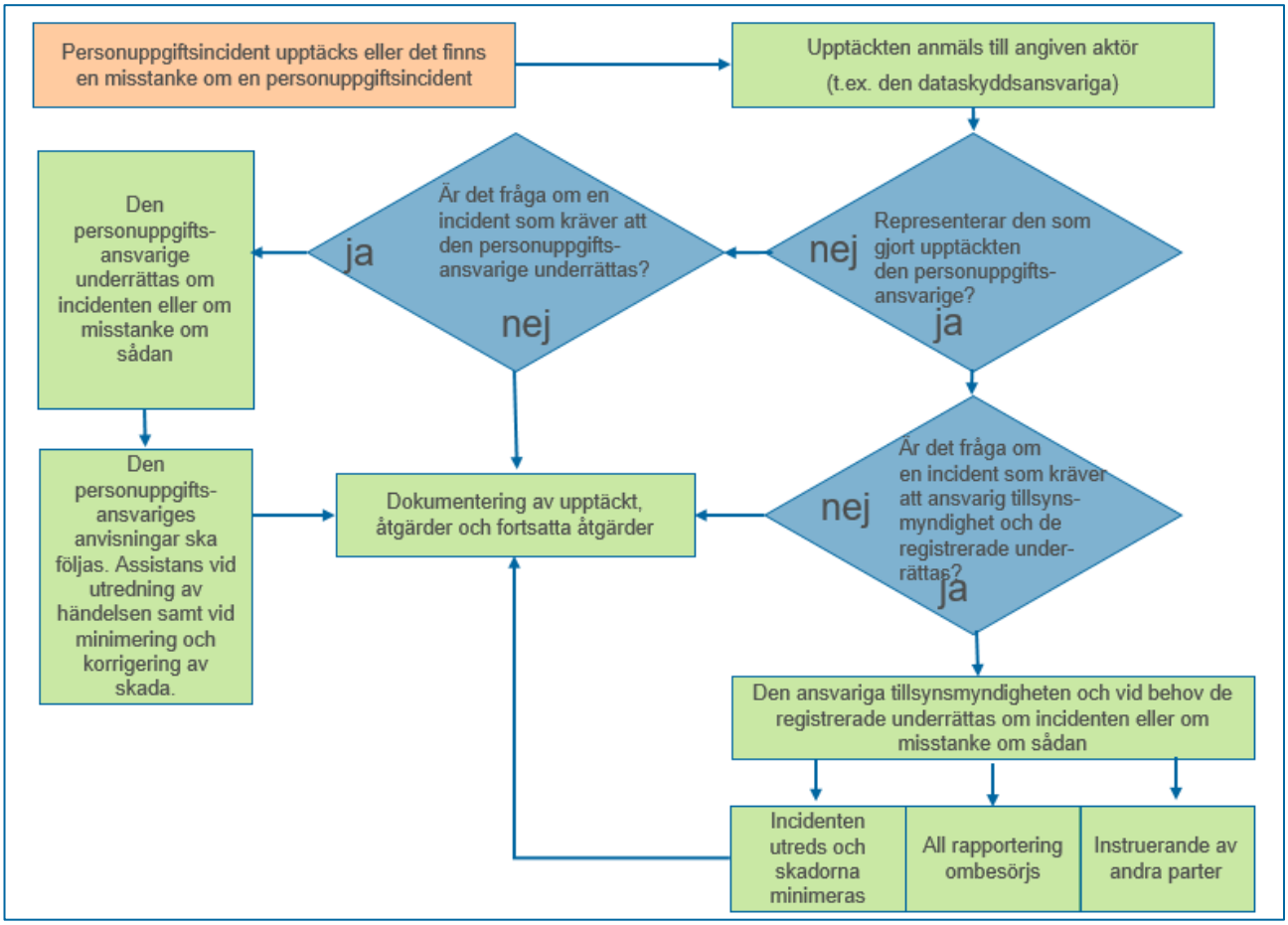

Bild 1. Handlingsplan för situationer där man upptäckt eller misstänker en personuppgiftsincident

2 Upptäckt och anmälan av en personuppgiftsincident

En personuppgiftsincident kan inträffa utan att det förekommer några tekniska störningar (t.ex. när någon snokar i personuppgifter) eller orsakas av en systemstörning (t.ex. när ett system sparar en personuppgift fel). Om incidenten orsakas av en systemstörning ska man för systemstörningens del följa anvisningarna för störningssituationer. För incidentens del gäller den process som ska följas vid personuppgiftsincidenter.

Vid upptäckt av en personuppgiftsincident eller misstanke om en sådan ska apoteket eller tillhandahållaren av tjänster utvärdera hur allvarlig risken är och huruvida den personuppgiftsansvarige, tillsynsmyndigheten och den registrerade ska underrättas.

Handlingsplanen för apotek och tillhandahållare av tjänster när det gäller en personuppgiftsincident eller misstanke om en sådan skiljer sig beroende på om incidenten upptäckts av ett personuppgiftsbiträde eller en person som representerar den personuppgiftsansvarige.

2.1 Den som upptäckt incidenten representerar den personuppgiftsansvarige

Den personuppgiftsansvarige svarar i enlighet med EU:s allmänna dataskyddsförordning för utredningen och rapporteringen kring indicenten.

Om en personuppgiftsincident eller misstanke om en sådan sannolikt medför en risk för patientens eller kundens rättigheter enligt dataskyddsförordningen ska den personuppgiftsansvarige underrätta dataombudsmannen om detta inom 72 timmar (blankett). Den registrerade ska vid behov informeras utan ogrundat dröjsmål.

Om tröskeln för anmälan inte överskrids ska incidenten dokumenteras enligt organisationens interna anvisningar.

När FPA inte är personuppgiftsansvarig men man behöver FPA:s hjälp i utredningen av en allvarlig personuppgiftsincident ska FPA:s tekniska support kontaktas, se punkt 2.3.

2.2 Den som upptäckt incidenten representerar personuppgiftsbiträdet

Personuppgiftsbiträdet underrättar den personuppgiftsansvarige att hen upptäckt en personuppgiftsincident eller misstänker en sådan.

I fråga om Receptcentret och Informationshanteringstjänsten (information, samtycken, förbud) underrättas FPA som i egenskap av personuppgiftsansvarig svarar för utredningen av incidenten och för rapporteringen i enlighet med EU:s allmänna dataskyddsförordning. FPA gör som personuppgiftsansvarig nödvändiga anmälningar till myndigheter och de registrerade.

2.3 Anmälan till FPA:s tekniska support

En personuppgiftsincident eller misstanke om sådan anmäls till FPA:s tekniska support per telefon eller skyddad e-post. En allvarlig personuppgiftsincident eller misstanke om sådan ska alltid också anmälas per telefon till FPA:s tekniska support.

FPA:s tekniska support
- telefon: 020 634 7787

Skyddad e-post skickas via adressen https://securemail.kela.fi/posti till adressen tekninentuki@kela.fi. Anvisning om hur man skickar skyddad e-post.

FPA:s tekniska support underrättas om
- vilka uppgifter som berörts av incidenten
- på vilket sätt uppgifterna har kränkts (t.ex. obehöriga har kommit åt känsliga uppgifter)
- datum och klockslag för upptäckten
- plats där incidenten inträffat
- en detaljerad beskrivning av hur man agerat i situationen

3 Dokumentering av upptäckt, åtgärder och fortsatta åtgärder

En personuppgiftsincident eller misstanke om sådan ska dokumenteras. Apoteket eller tillhandahållaren av tjänster ska registrera incidenten, konsekvenserna av den samt åtgärder som vidtagits oberoende av vilka de fortsatta åtgärderna på grund av indicenten slutligen är.

Efter anmälan till den personuppgiftsansvarige ska den personuppgiftsansvariges anvisningar samt apotekens eller tjänstetillhandahållarnas interna anvisningar följas.

I fråga om personuppgiftsincidenter bör alla parter assistera den personuppgiftsansvarige med utredningen av situationen, rapporteringen samt med minimeringen och korrigeringen av skadan.