Anvisningar för datasäkerhet i samband med Eviras elektroniska tjänster

1 Bakgrund

Evira erbjuder sina kunder webbläsarbaserade lösningar för elektroniska tjänster. En del av Eviras elektroniska tjänster är blanketter som kan fyllas i och sändas in elektroniskt. Vissa av dessa elektroniska tjänster är enkla nätblanketter, andra är elektroniska kundtjänster som består av flera delar och som går stegvis.

Blanketterna som kan laddas ner och skrivas ut är i Word- och Pdf-format. En del av dessa blanketter kan också fyllas i på datorn innan de skrivs ut. De utskrivna och ifyllda blanketterna sänds till Evira per post.

Portalerna för elektroniska tjänster öppnas från Eviras webbsidor för användare som är registrerade och identifierade som användare av systemen. Då det gäller vissa tjänster krävs det också att användarna är registrerade i ett eller flera myndighetsregister, t.ex. registret över djurhållare, registret över leverantörer av skogsodlingsmaterial eller Eviras kundregister/IACS dataregister. System för elektroniska tjänster är bland annat ett beställningssystem för sundhetscertifikat för växter, datasökning i växtskyddsmedelsregistret, svinregistret och anmälningar till får- och getregistret som togs i bruk 2008 samt registren över skogsodlingsmaterial.

2 Eviras datasäkerhetsstrategi

I dataförvaltningsstrategin definieras Eviras målsättning att utveckla datasystemen och tjänsterna på ett sådant sätt att de tjänster som kunderna erbjuds är högklassiga och datasystemen är säkra.

Vid Evira iakttas förvaltningsområdets och statsförvaltningens anvisningar och rekommendationer. Finansministeriet (FM) styr och samordnar statsförvaltningens datasäkerhet och dess utveckling. Anvisningarna utarbetas av ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) som har expertis med bred bas inom datasäkerheten. Gruppen är tillsatt av finansministeriet. VAHTI:s anvisningar för datasäkerhet täcker alla delområden. Det rekommenderas att kunderna bekantar sig med statsförvaltningens allmänna anvisningar för datasäkerhet på adressen:

http://www.vm.fi/vm/sv/13_hallinnon_kehittaminen/09_datasakerhet/index.jsp

Evira strävar med sin datasäkerhet efter kontroll över datasäkerhetsriskerna och att hålla dem på en acceptabel nivå och på så vis trygga kontinuiteten, effektiviteten och kvaliteten på

kärnverksamheten. Genom säkerhetsarrangemangen strävar man efter att ha pålitlig information och datasystem som är tillgängliga för befullmäktigade användare. Endast personer och instanser som är berättigade därtill får hantera informationen i den omfattning som deras arbetsuppgifter förutsätter. Transaktioner i anslutning till databehandlingen är spårbara i tillräcklig omfattning.

3 Användning av Eviras elektroniska tjänster

Den största delen av de elektroniska blanketterna kan användas utan identifikation. Användning av vissa tjänster förutsätter ändå identifiering.

Eviras webbtjänster förutsätter att du ingår avtal med Evira. Du får en användarkod och ett lösenord med vilka du kan logga in i tjänsten. Därtill får du eventuellt sessionsnycklar som används endast en gång.

Sköt för din del om webbtjänstens säkerhet:

- Förvara dina koder noggrant. Förvara inte användarkod, lösenord och sessionsnycklar på samma plats.
- Det är att föredra att man lär sig de permanenta användarkoderna utantill.
- För lösenord gäller grundregeln att de inte får vara lätta att gissa. Till exempel användarens eller en anhörigs namn är ett mycket dåligt lösenord. Ett bra lösenord innehåller små och stora bokstäver, siffror och andra skrivtecken.
- Ge aldrig dina koder till någon som ber om dem per telefon eller e-post, även om personen skulle uppge sig vara exempelvis en adb-stödperson.
- Försäkra dig genom tjänsteleverantörens säkerhetscertifikat om att du är på rätta sidor. Om det inte finns något certifikat, eller om det inte är i kraft, kan det vara fråga om ett försök till svindel.
- Om du använder en dator som även andra använder ska du logga ut ur alla program och tjänster innan du lämnar datorn.
- Om du har använt tjänster där konfidentiell information har behandlats, lönar det sig att också rensa webbläsarens cacheminne.

De som använder tjänsterna ska också se till att den apparat som används för tjänsterna är i ordning och att programvaran och virusskyddet är uppdaterade.