Krav på certifikatverksamheten som föranleds av dataskyddsför-ordningen

Denna bilaga är en del av registreringsanvisningen och utbildningsmaterialet. Dataskydds-förordningens krav på verksamheten med att registrera certifikat har skrivits in i denna bi-laga. Villkoren för behandling av personuppgifter och anvisningarna om hanteringen av in-formationssäkerhetsincidenter och dataskyddsincidenter hör också samman med uppfyl-landet av kraven i dataskyddsförordningen.

Kravet på inbyggt dataskydd och dataskydd som standard betyder att dataskyddsaspekten tas i beaktande i alla register, tjänster, system och funktioner redan i deras planerings-skede och att olika funktionaliteter byggs upp med dataskyddsaspekten i förgrunden. Kra-vet är kopplat till principen om ansvarsskyldighet, enligt vilken den personuppgiftsansvarige och personuppgiftsbiträdet aktivt ska kunna visa att dataskyddet har beaktats i hela verk-samheten såväl organisatoriskt som tekniskt och att dataskyddet de facto verkställs i prakti-ken.

Behandlingen av personuppgifter i anslutning till certifikat grundar sig på lagen. I lagen för-skrivs också om uttrycklig rätten att behandla personuppgifter[1]. Behandling av personupp-gifter är en förutsättning när man tillhandahåller certifikattjänster och kontrollerar elektro-niska identiteters riktighet. Personuppgifter ska endast behandlas i den omfattning som be-hövs för certifikatutfärdarens verksamhet. En registrerads personuppgifter behandlas med stöd av den registrerades certifikatansökan vid utfärdandet, produktionen och administrat-ionen av certifikatet. I samband med certifikatansökan informeras den registrerade om att personuppgifterna behandlas i certifikatprocessen.

Behandlingen av personuppgifter hör till MDB:s lagstadgade uppgift att utfärda och admini-strera certifikat. Därför kan man inte kräva en begränsning av behandlingen, och det finns inte heller någon rätt att överföra information till något annat system.

Med den registrerades rättigheter avses certifikatinnehavarens rättigheter, till exempel rätten att få veta vilka personuppgifter som finns i certifikatregistret eller i systemet för be-ställning och administration av kort och certifikat (Vartti) och för vilket ändamål personupp-gifterna behandlas, samt rätten att få felaktiga uppgifter rättade. Enligt artikel 5 i Europa-parlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med av-seende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmänna dataskyddsförordningen) ska uppgifterna vara korrekta och nödvändigt uppdaterade och otydliga och felaktiga personuppgifter ska raderas eller rättas utan dröjsmål. Enligt artikel 16 i dataskyddsförordningen har den regi-strerade rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga person-uppgifter som rör honom eller henne rättade. Den registrerade har även rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlå-tande.

En rättelse ska begäras skriftligen hos den personuppgiftsansvarige (MDB). Personen som begär rättelse ska identifieras och Myndigheten för digitalisering och befolkningsdata ska försäkra sig om identiteten hos den som begär rättelse.

Den registrerade får de personuppgifter som finns i systemet och information om vilket ändamål uppgifterna används för genom att besöka Myndigheten för digitalisering och befolkningsdata (MDB), där registreraren identifierar personen, eller i WebVartti-programmet. När den registrerade kontaktar den registeransvarige ska uppgifterna överlåtas inom en månad. Svaret till den registrerade ska vara komplett, inbegripet bl.a. de personuppgifter som finns i registret och grunderna för behandlingen av dem[2]. MDB säkerställer att den som begärt sina personuppgifter får alla uppgifter, om det inte finns något hinder för utlämnandet.

Om svaret är nej, dvs. uppgifterna ska av någon anledning inte lämnas ut, ges den registrerade en besvärsanvisning. Om personuppgifterna är felaktiga ska begäran om rättelse skickas via ett registreringsställe eller direkt till MDB.

Alla uppgifter är inte sådana som kan rättas (uppgifterna från befolkningsdatasystemet). Mer information finns i registerbeskrivningarna på MDB:s webbplats, som innehåller MDB:s principer för behandling av personuppgifter.

Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för Valttis del och- organisationernas registrerare behandlar personuppgifterna på Myndigheten för digitalisering och befolkningsdatas vägnar och för myndighetens räkning. Registrerarna har sålunda rollen som registerförare. De som registrerar certifikat ska fylla i och till MDB lämna in ett register över den behandling som personuppgiftsbiträdet utför. Registerförarens redogörelse över behandlingsåtgärderna (mall) med anvisningar finns på Dataombudsmannens webbplats: https://tietosuoja.fi/sv/register-over-behandling. Dessutom har MDB utarbetat egna anvisningar för registret.

Dessa roller (personuppgiftsansvarig, personuppgiftsbiträde) har beskrivits i dokumentationen om behandling av personuppgifter (bl.a. avtalsbilagan Villkor för behandling av personuppgifter och Register över behandling). Mer information om ämnet ges när dokumenten är klara och har publiceras på MDB:s webbplats.

MDB sörjer för att de som registrerar uppgifter regelbundet får utbildning och information för utförandet av sina arbetsuppgifter och för att uppfyllandet av de krav som ställs på registreringsställen. Utsedda anställda på MDB ansvarar för att behövliga uppdateringar görs i MDB:s dokumentation, som registreraringsanvisningen, utbildningsmaterial osv.

Frågor som gäller informationssäkerhet och dataskydd har beaktats och inkluderats i avtalsbilagor och i anvisningar och utbildningsmaterial som riktar sig till registrerare. Dessutom ska var och en själv se till informationssäkerheten och dataskyddet genom att arbeta i enlighet med lagstiftningen, avtalsvillkoren och anvisningarna.

Registreringsställena ska endast behandla sådana personuppgifter och i den omfattning som behövs för handläggningen av ansökningar och administrationen av certifikat. Personuppgifter som behövs i certifikatprocesserna är de uppgifter som frågas efter i ansökan, uppgifter som tas från befolkningsdatasystemet (BDS) och uppgifter ur Valviras register, vilka registreras i Vartti och på kortcertifikatet. Ändamålet med behandlingen av

personuppgifterna är utfärdande och administration av certifikat, spärrning av certifikat samt behandling som förutsätts för arkivering. Uppgifterna används inte för andra ändamål. I behandlingen av personuppgifter ingår inga särskilda uppgifter om personuppgiftskategorier[3].

Enligt MDB:s anvisningar ska behandlingen utföras med beaktande av konfidentialiteten, integriteten och arkiveringsrutinerna. Det innebär till exempel att uppgifterna ska skyddas mot olovlig och olaglig behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. I verksamheten ska obehörig åtkomst till uppgifterna och till den utrustning som används för behandlingen av uppgifterna förhindras.

Principen förutsätter att man sörjer för informationssäkerheten och verkställs på tillbörligt sätt när man iakttar föreskrifterna, praxisen, villkoren och anvisningarna för informationssäkerhet.

Informationsbehandlingen följs upp och övervakas för att säkerställa lämpligheten. Behandling av uppgifter och åtgärder som görs i Vartti lämnar anteckningar i loggarna. Dessa logguppgifter kan inte ändras i efterhand. MDB övervakar bl.a. genom auditeringar och granskning av logguppgifter. I och med att de som registrerar uppgifterna arbetar på tillbörligt sätt och verksamheten övervakas kan MDB säkerställa att personuppgifterna hålls intakta och oförändrade, att fel rättas till och att överträdelser anmäls till MDB utan dröjsmål.

Logguppgifterna i systemet omfattas inte av rätten att kontrollera egna uppgifter. Dataombudsmannen/tillsynsmyndigheten övervakar behandlingen av informationen. Myndigheten för digitalisering och befolkningsdata rapporterar årligen till dataombudsmannen/tillsynsmyndigheten om behandlingen av uppgifter.

Utlämnande och behandling av uppgifter ur en tjänst/ett register/ett datasystem utanför MDB sker med beaktande av uppgiftsminimering, dvs. endast sådana uppgifter lämnas ut och behandlas som behövs för ändamålet. Detta omfattar behandlingen av uppgifter om kundorganisationer, behandling av uppgifter om avtalspartner och underleverantörer samt deras anställda, till behövliga delar utlämnande av uppgifter till den registrerade själv samt utlämnande av uppgifter till kortfabriker för produktion av certifikatkort.

Lagliga ändamål för behandling av personuppgifter har skrivits in i besluten om användarbehörigheter till Vartti, och påföljderna vid verksamhet som strider mot ett ändamål har skrivits in i avtalen (avtalsvillkor om skyldigheter och ansvar samt villkor för ersättning vid verksamhet i strid med avtalet).

Information som fås vid behandling av personuppgifter behandlas inte i flera olika system för samma ändamål, om det inte finns tydliga grunder för det.

Den personuppgiftsansvarige (MDB) ska personligen meddela en registrerad om det inträffat en sådan personuppgiftsincident där konfidentialiateten i personuppgifterna har äventyrats, till exempel om uppgifter har läckt ut till utomstående. För att MDB ska kunna göra denna anmälan till den registrerade och till tillsynsmyndigheten inom den föreskrivna tiden, ska de som arbetar som registrerare för MDB:s räkning och på MDB:s vägnar meddela MDB utan dröjsmål efter att ha fått vetskap om en personuppgiftsincident. I anvisningen om

hanteringen av incidenter i anslutning till informationssäkerheten och dataskyddet, som finns som bilaga till avtalet, ges närmare villkor för anmälningsförfarandet och samarbetet.

Datakällorna för tjänsten/registret/datasystemet har specificerats och beskrivits i registerbeskrivningen. MDB:s registerbeskrivningar finns på MDB:s webbplats. Vid behandlingen av olika slags uppgifter utnyttjas i den mån det är möjligt det primära registret som informationskälla, eller så begär man informationen av personen själv.

När det gäller uppgifter i anslutning till Vartti och registreringsprocesserna hittas och rättas inexakta och felaktiga uppgifter så, att MDB:s personal och registrerare gör observationer eller de registrerade lämnar in påpekanden och begäranden om korrigering. En registrerare är skyldig att utan dröjsmål meddela MDB skriftligen om inexakta och/eller felaktiga uppgifter per e-post till adressen vartti@dvv.fi. För Varttis del kan man rätta namn, personbeteckning och e-postadress i den registrerades uppgifter eller ta bort överflödig beteckning. Uppgifterna om kortinnehavaren kommer från befolkningsdatasystemet, och därför ska en begäran om rättelse av felaktiga/ändrade uppgifter skickas till befolkningsdatasystemets underhåll. Kort som innehåller felaktiga uppgifter bör spärras i spärrtjänsten för certifikat. Om dessa behöver man inte underrätta MDB.

Förvaringen av personuppgifter grundar sig på ett utfärdat certifikat och registreringsåtgärderna i anslutning till ett certifikat. Uppgifterna ska kunna kopplas till certifikatinnehavaren. Vilka uppgifter som ska förvaras och förvaringstiden grundar sig på lagen (24 § i lagen om stark autentisering och elektroniska signaturer). Datainnehållet i certifikatet, uppgifterna om inledande identifiering/tillämpade dokument/uppgifterna om elektronisk identifiering är uppgifter som ska förvaras. Arkiveringstiden är kortets giltighetstid utökad med fem år.

Personuppgifterna i Vartti har krypterats och skyddats på tillbörligt sätt med beaktande på informationssäkerhetskraven, bland annat på följande sätt: Vartti har begränsade användarbehörigheter, alla händelser sparas i en logg och dataöverföringen till kortfabriken är krypterad.

Vid dataskyddsincidenter/personuppgiftsincidenter ska registrerarna utan dröjsmål kontakta MDB (anvisning om hantering av informationssäkerhetsincidenter och dataskyddsincidenter). Registreraren/MDB ska vidta behövliga åtgärder (eventuellt spärra certifikatet etc.) för att incidenten ska kunna tas upp till behandling och skadorna minimeras.

---

[1] Lag om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata 661/2009, 6 § Myndigheten för digitalisering och befolkningsdatas certifierade elektroniska kommunikation och dess syfte, 61 § Tjänster som tillhandahålls vid certifierad elektronisk kommunikation; lag om stark autentisering och betrodda elektroniska tjänster 617/2009, 6 § Behandling av personbeteckningar

[2] Syftet med behandlingen är att tillhandahålla certifikattjänster inom ramen för MDB:s lagstadgade uppgift. Om uppgifter lämnas ut, mottas de av certifikatinnehavarna eller kortfabriken. Förvaringstiden för uppgifterna är kortets giltighetstid + 5 år. En person har rätt att begära att den personuppgiftsansvarige rättar sina uppgifter (rätten att begära att uppgifter raderas eller att behandlingen begränsas gäller emellertid inte för MDB:s lagstadgade personregister, dvs. inte heller för certifikatregistren, eftersom behandlingen av personuppgifterna är en förutsättning för certifikatverksamheten). MDB:s certifikatregister förs för utförandet av de lagstadgade uppgifterna (tillhandahållandet av certifikattjänster), och därför existerar ingen rätt att överföra information till ett annat system. En

person har rätt att besvära sig hos tillsynsmyndigheten/dataombudsmannen (om personuppgifter inte har behandlats på det sätt som förutsätts i lagstiftningen). Om en personuppgift inte har samlats in av den registrerade, ges behövlig information om uppgiftens ursprung, till exempel en registrerare i en organisation, MDB.

[3] Behandling av särskilda kategorier av personuppgifter: Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.