E-legitimationsnämndens policy för behandling av personuppgifter

1 Bakgrund och syfte

E-legitimationsnämnden (nämnden) värnar om berörda aktörers integritet och är alltid mån om att följa gällande dataskyddsregelverk. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Nämnden har därför antagit denna Policy för behandling av personuppgifter (Policyn) för att säkerställa att alla inom organisationen följer dataskyddsreglerna. Det här dokumentet avser att ge dig som medarbetare närmare vägledning om hur du ska behandla personuppgifter.

Den 25 maj 2018 börjar EU:s allmänna dataskyddsförordning (EU) 2016/679 (dataskyddsförordningen) tillämpas. Den medför ett förstärkt skydd för de personer vars personuppgifter behandlas och den ställer fler och hårdare krav på organisationer som behandlar personuppgifter.

Om en behandling av personuppgifter skulle strida mot bestämmelserna i dataskyddsförordningen finns risken för intrång i den personliga integriteten för de registrerade, men även risken för skada för nämnden. Nämnden kan dessutom bli skyldig att utge skadestånd eller påföras en administrativ sanktionsavgift. För att undvika sådana konsekvenser är alla medarbetare skyldiga att följa dessa riktlinjer.

2 Tillämpningsområde och omfattning

Policyn gäller för nämndens alla anställda och konsulter, inom alla områden och vid var tid.

Nämnden ska se till att denna Policy efterlevs, vilket bland annat innefattar utbildning för alla anställda. Informationen till de anställda ska även innefatta information om att överträdelse av policyn kan komma att medföra t.ex. arbetsrättsliga konsekvenser.

3 Grundläggande principer

De grundläggande principer som beskrivs nedan ska alltid iakttas när personuppgifter behandlas. Nämnden svarar för och ska kunna visa att principerna efterlevs.

Laglighet, skälighet, transparens – Personuppgifter ska behandlas lagligt, korrekt och transparent i förhållande till den registrerade. Det innebär att varje typ av behandling ska baseras på en giltig s.k. laglig grund, såsom exempelvis att fullgöra en rättslig förpliktelse eller ett avtal eller att utföra en uppgift av allmänt intresse (se avsnitt 5 nedan). Kan man inte identifiera någon laglig grund som är tillämplig för behandlingen får behandlingen således inte utföras. Utgångspunkten för denna

princip är tydlig kommunikation med den registrerade om bl.a. för vilka ändamål personuppgifterna behandlas, vilken typ av behandling som utförs, om och hur personuppgifterna delas med andra, hur länge personuppgifterna lagras och hur man kommer i kontakt med nämnden. De registrerade ska alltså ges tydlig och transparent information om behandlingen av deras personuppgifter.

Ändamålsbegränsning – Personuppgifter får endast samlas in och på annat sätt behandlas för särskilda, uttryckligt angivna och berättigade ändamål och de får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Uppgiftsminimering – Personuppgifter som behandlas ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålen. Säkerställ att uppgifterna som samlas in verkligen behövs och fråga inte efter information bara för att den kanske kan vara bra att ha.

Riktighet – Personuppgifter som behandlas ska vara korrekta och om nödvändigt uppdaterade. Vidta lämpliga åtgärder för att se till att felaktiga eller ofullständiga uppgifter rättas. Undvik att lagra kopior av uppgifterna i många system i syfte att undvika felkällor och att ouppdaterad information sparas.

Lagringsbegränsning – Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs måste de gallras, vilket innebär att de antingen måste raderas eller avidentifieras. Undantag gäller dock för nämnden om det finns ett berättigat arkivändamål av allmänt intresse. Här bör också noteras att det för nämnden kan vara otillåtet att radera uppgifter om tillämplig gallringsföreskrift enligt arkivförfattningarna saknas.

Principen om *ansvarsskyldighet* innebär att nämnden måste kunna visa att dataskyddsförordningen efterlevs. Vidare ska ett register finnas över alla typer av behandlingar av personuppgifter som utförs och nämnden ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

4 Personuppgifter

Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Exempel på personuppgifter är namn, kontaktuppgifter och faktorer som är specifika för en persons fysiska, ekonomiska, kulturella eller sociala identitet. Uppgifter som enskilt inte når upp till kraven kan tillsammans ändå utgöra personuppgifter.

All behandling av personuppgifter omfattas av dataskyddsförordningen och dess regler. Med *behandling* menas en åtgärd eller kombination av åtgärder avseende personuppgifter, som utförs helt eller delvis automatiserat. Även personuppgifter i e-post och i dokument på servrar, i en enkel lista, på webbplatser och i annat ostrukturerat material omfattas.

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, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning (s.k. *särskilda kategorier av personuppgifter*) är som huvudregel förbjuden. För att sådan behandling ska vara tillåten krävs ett giltigt undantag från förbudet.

Behandling av *personnummer* får bara utföras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Behandling av uppgifter om *lagöverträdelser* (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder) får endast behandlas i vissa särskilda fall.

5 Laglig grund för behandlingen av personuppgifter

En behandling av personuppgifter är endast laglig om och i den mån någon av följande grunder är tillämplig.

Den registrerade har lämnat sitt *samtycke* till att personuppgifterna behandlas för ett eller flera specifika ändamål. Särskilda krav måste vara uppfyllda för att samtycket ska vara giltigt och denna grund kan och bör normalt inte åberopas av nämnden.

Behandlingen är nödvändig för att *fullgöra ett avtal* i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Behandlingen är nödvändig för att *fullgöra en rättslig förpliktelse* som åvilar nämnden. Som exempel kan här nämnas skyldigheten att tillhandahålla eIDAS-noden.

Behandlingen är nödvändig för att skydda intressen som är av *grundläggande betydelse* för den registrerade eller för en annan fysisk person (t.ex. när det är fara för livet).

Behandlingen är nödvändig för att utföra en *uppgift av allmänt intresse* eller som ett led i myndighetsutövning (t.ex. enligt nämndens instruktion).[1]

6 Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder. Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme. Exempel på tekniska åtgärder som måste kontrolleras är om nämnden har tillräckliga backuprutiner, tillräckliga brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor, skydd mot obehörig intern åtkomst, lösenordskrav, kryptering vid behov, loggning av åtkomst till och användning av IT-system m.m.

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att upprätta och följa en gallringsrutin för re-

[1] Det finns ytterligare en rättslig grund – en s.k. intresseavvägning – men denna grund får inte åberopas av nämnden när den utför sina uppgifter.

spektive behandling säkerställer man det strukturerade gallringsarbetet. Även personuppgifter i så kallat ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser etc. behöver raderas när ändamålet med behandlingen är uppfyllt.

7 Överföring till tredje land

För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t.ex. många online-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser m.m. och behöver analyseras särskilt. E-legitimationsnämnden överför vanligtvis inte uppgifter till tredje land, förutsatt att detta inte krävs enligt lag eller annan författning.

8 Konsekvensbedömning

Nämnden har en rutin på plats för att kunna identifiera och hantera särskilda integritetsrisker inom verksamheten och för strukturerad uppföljning. Utvecklingstakten är snabb när det gäller införandet av ny teknik inom nämndens område och särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med behandlingar i stor omfattning för att identifiera användare och skriva under elektroniskt inom hela EU och EES.

Om en ny eller ändrad personuppgiftsbehandling i visst avseende sannolikt kan komma att medföra hög risk för fysiska personers rättigheter och friheter ska rutinen följas och en bedömning göras av effekterna av de påtänkta behandlingarna för skyddet av personuppgifter innan behandlingen påbörjas.

Innan sådan personuppgiftsbehandling påbörjas ska nämndens kanslichef kontaktas för utredning om en konsekvensbedömning krävs.

9 Registerutdrag och utlämnande

Dataskyddsförordningen ger de registrerade ett flertal rättigheter vad gäller behandling av personuppgifter. Det är nämndens uppgift att uppfylla dessa rättigheter och se till att tillräckliga processer härför finns för att tillmötesgå de registrerade.

Den registrerade har rätt till *information* när personuppgifterna samlas in. Denna information ska tillhandahållas i en lättillgänglig skriftlig form med ett klart och tydligt språk. I dataskyddsförordningen föreskrivs ett antal tydliga krav som måste vara uppfyllda och kraven varierar beroende på om informationen har samlats in från den registrerade själv eller från tredje man.

Den registrerade har rätt att få bekräftelse på huruvida personuppgifter som tillhör denne behandlas, och i sådana fall få en kopia av personuppgifterna (*registerutdrag*). Denna rättighet gäller oberoende av den plats där personuppgifterna behandlas.

Om personuppgifter som behandlas är felaktiga eller ofullständiga kan den registrerade kräva att de *korrigeras*. Om den registrerade visar att ändamålet för vilket personuppgifterna behandlas inte längre är tillåtet, nödvändigt eller rimligt under omständigheterna, ska de aktuella personuppgifterna raderas, om det inte finns några lagbestämmelser som anger annat (jfr ovan om arkivförfattningarna).

Den registrerade har rätt att överföra personuppgifter som denne lämnat till annan personuppgiftsansvarig (rätt till *dataportabilitet*) om behandlingen stöds på de lagliga grunderna avtal eller samtycke. Personuppgifterna ska tillhandahållas den registrerade i ett strukturerat, allmänt använt och maskinläsbart format. Om det är tekniskt möjligt kan den registrerade begära att uppgifterna överförs direkt till annan personuppgiftsansvarig. Rätten gäller endast för de personuppgifter som den registrerade själv har lämnat till nämnden. Normalt stöder nämnden sina behandlingar av personuppgifter på en sådan rättslig grund att det inte finns någon rätt till dataportabilitet för den registrerade.

Den registrerade har i vissa fall rätt att kräva att nämnden *begränsar behandlingen* av dennes personuppgifter, d.v.s. begränsar behandlingen till vissa avgränsade syften. Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt att personuppgifterna rättas. Den registrerade kan då begära att behandlingen av personuppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den enskilde informeras om detta.

I vissa fall har den registrerade rätt att begära radering av sina personuppgifter (*”rätten att bli bortglömd”*). Ett exempel är när samtycke är den lagliga grunden för behandlingen och den registrerade återkallar sitt samtycke.

För personuppgifter som behandlas på den lagliga grunden allmänt intresse eller myndighetsutövning har den registrerade en rätt att *invända* mot behandlingen. Invändningen kan leda till att den aktuella personuppgiftsbehandlingen måste upphöra, såvida inte nämnden kan påvisa tvingande berättigade skäl som enligt nämndens bedömning väger över den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

10 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörig åtkomst till personuppgifter. Exempel på personuppgiftsincidenter kan vara stöld av register, oavsiktligt avslöjande av löneinformation via e-post till fel mottagare, en anställd tar hem en arbetsdator som senare stjäls i ett inbrott och som leder till att information om anställda eller kunder avslöjas, personuppgifter publiceras på webben av misstag, en bärbar dator innehållande personuppgifter tappas bort, m.m.

Personuppgiftsincidenter kan behöva anmälas till tillsynsmyndigheten inom 72 timmar från upptäckten av incidenten om det är sannolikt att det föreligger en risk för

fysiska personers rättigheter och friheter. Alla inträffade incidenter ska dokumenteras, oavsett om de måste anmälas till Datainspektionen, och i vissa fall kan nämnden behöva underrätta berörda registrerade om incidenten.

Vid en misstänkt personuppgiftsincident kontakta omedelbart Adam Panzer på +46 (0)10-574 19 99 eller adam.panzer@elegnamnden.se. Det är sedan nämndens kanslichef som avgör om tillsynsmyndigheten eller de registrerade behöver underrättas.

11 Övrigt

För definitioner avseende termer som används i den här policyn hänvisas till dataskyddsförordningen.

Denna policy ska uppdateras årligen eller vid behov baserat på instruktioner från nämnden.

12 Frågor

Vid frågor som anknyter till behandling av personuppgifter, vänligen kontakta Adam Panzer på +46 (0)10-574 19 99 eller adam.panzer@elegnamnden.se.

_____

Policy antagen av nämnden den 24 maj 2018.