

15.03.2021

POL-2021-1402

## **Dataskyddsbeskrivning; Det nationella systemet inom Schengens informationssystem**

### **1 Personuppgiftsansvarig**

Polisstyrelsen  
Postadress: PB 1000, 02151 Esbo  
Besöksadress: Bergsmansvägen 3, Esbo  
Telefon: 0295 480 181 (växel)  
E-post: kirjaamo.poliisihallitus@poliisi.fi

### **2 Kontaktperson i ärenden som gäller dataskydd**

Polisstyrelsen  
Päivi Laaksonen, överinspektör  
Kontaktuppgifter, se punkt 1

### **3 Polisens dataskyddsombud**

Polisstyrelsen  
Harri Kukkola, överinspektör  
Kontaktuppgifter, se punkt 1

### **4 Rättslig grund för behandling av personuppgifter**

Polisen behandlar personuppgifter för att kunna genomföra lagstadgade uppgifter, följa lagstadgade förelägganden och för att kunna använda den offentliga makt som hör till polisen i enlighet med bestämmelserna i dataskyddslagstiftningen. Enligt dataskyddslagstiftningen kan en rättslig förpliktelse grunda sig enbart på EU-lagen eller en medlemsstats lag och offentlig makt skall grunda sig på lagen eller andra rättsliga bestämmelser.

Polisens behandling av personuppgifter och behandlingens rättsliga grunder för det nationella datasystemet i Schengens informationssystem regleras i följande lagar:

- 1) Lagen om behandling av personuppgifter i polisens verksamhet (616/2019, nedan kallad polisens personuppgiftslag)

- 2) lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018, nedan kallad dataskyddslag för brottmål) samt i författningsgrunden för Schengens informationssystem.

Med författningsgrunden för Schengens informationssystem avses Europaparlamentets och rådets förordning (EG) nr 1987/2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II), rådets beslut 2007/533/RIF om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) samt Europaparlamentets och rådets förordning (EG) nr 1986/2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon, Schengenregelverket enligt punkt 2 i artikel 1 i rådets beslut 1999/435/EG från den 20 maj 1999 (nedan kallad etableringsavtal).

## **5 Syftet med behandlingen av personuppgifter, grupper av registrerade och personuppgiftsgrupper som ska behandlas**

### 5.1 Syften med behandlingen

Syftet med Schengens informationssystem skall i enlighet med förordning (EG) nr 1987/2006 vara att på medlemsstaternas territorier, med hjälp av information som överförs via detta system inom ett område med frihet, säkerhet och rättvisa i Europeiska unionen, garantera en hög säkerhetsnivå, inbegripet bevarandet av allmän säkerhet och allmän ordning och skyddet av säkerhet, samt att tillämpa bestämmelserna i förordningen avseende rörlighet för personer på deras territorium.

Schengens informationssystem innehåller nödvändiga registreringar av tredjelandsmedborgare i syfte att neka inresa eller vistelse. Uppgifterna får inte användas för administrativa ändamål. Med undantag för detta, kan också nationella rättsliga myndigheter, inbegripet de som är ansvariga för att väcka allmänt åtal inom ramen för ett brottmålsförfarande och för utredningar som föregår åtal samt samordnande myndigheter, när de utför sina uppgifter i enlighet med nationell lagstiftning ha rätt att få tillgång till uppgifter som sparats i Schengens informationssystem och rätt att direkt söka efter sådana uppgifter.

Uppgifter i polisens personregister får trots sekretessbestämmelserna behandlas även för laglighetsövervakning, analys, planering och utveckling. Uppgifter får

också användas för utbildning, om de är nödvändiga för att utbildningen ska kunna genomföras.

5.2 Schengens uppgiftskategorier och personuppgiftsgrupper som behandlas via gränssnittet för i det nationella datasystemet i Schengens informationssystem presenteras i följande avsnitt.

- I förordningen (EG) nr 1987/2006 specificeras att endast följande uppgifter får lagras av gällande registreringar av tredjelandsmedborgare i syfte att neka inresa eller vistelse samt personer med införd registrering:
  - a) namn- och efternamn, namn vid födelsen och tidigare använda namn samt alias, som kan inregistreras separat
  - b) specifika, permanenta fysiska särskilda kännetecken
  - c) födelsedatum och -plats
  - d) kön
  - e) fotografier
  - f) fingeravtryck
  - g) medborgarskap
  - h) om personen ifråga är beväpnad, våldsam eller har rymt
  - i) orsak till efterlysning
  - j) myndighet som efterlyser
  - k) hänvisning till beslut, baserat på vilken efterlysningen har gjorts
  - l) åtgärd som skall genomföras
  - m) länk eller länkar till övriga registreringar i SIS II i enlighet med artikel 37
- I rådets beslut 2007/533/RIF specificeras dessutom följande syften för registreringar:
  - registreringar om personer som är efterlysta för gripande eller utlämning baserat på europeisk arresteringsorder
  - efterlysning av försvunna personer
  - registreringar om personer som söks för att delta i ett rättsligt förfarande
  - registreringar om personer och föremål som omfattas av diskreta kontroller eller särskilda kontroller
  - registreringar om föremål som skall beslagtas eller användas som bevis i brottmål

Av de registreringssyften som anges i rådets beslut 2007/533/RIF – som dock ej inkluderar utbyte av tilläggsuppgifter och bevarande av förordningar gällande

kompletterande uppgifter – av personer som har registrerats, får endast följande uppgifter lagras:

- a) namn- och efternamn, namn vid födelsen och tidigare använda namn samt alias, som kan inregistreras separat
- b) specifika, permanenta fysiska särskilda kännetecken
- c) födelsedatum och -plats
- d) kön
- e) fotografier
- f) fingeravtryck
- g) medborgarskap
- h) om personen ifråga är beväpnad, våldsam eller har rymt
- i) orsak till efterlysning
- j) myndighet som efterlyser
- k) hänvisning till beslut, baserat på vilken efterlysningen har gjorts
- l) åtgärd som skall genomföras
- m) länk eller länkar till övriga registreringar i SIS II i enlighet med artikel 52
- n) brottets art.

Dessutom fastställs i rådets beslut följande gällande registreringar som skall utföras för olika syften:

- Personer som är efterlysta för utlämning eller för att gripas och överlämnas till följd av en europeisk arresteringsorder (artikel 26)
  - den medlemsstat som lägger in registreringen skall också lägga in en kopia av originalet av den europeiska arresteringsordern i SIS II.
  - Den medlemsstat som har lagt in registrering i SIS II för gripande och överlämnande baserat på europeisk arresteringsorder skall överlåta alla uppgifter till medlemsstaterna med utbyte av tilläggsuppgifter
- Efterlysningar av försvunna personer som behöver ställas under beskydd och/eller vars vistelseort man behöver få reda på (artikel 32). Information om försvunna personer som tillhör följande grupper får lagras:
  - a) försvunna personer, som behöver ställas under beskydd för att skydda dem eller för att förebygga hot samt
  - b) försvunna personer som inte behöver ställas under beskydd
- Registreringar om personer som söks för att delta i ett rättsligt förfarande (artikel 34). På begäran av behörig myndighet skall uppgifter om följande

kategorier av personer läggas in i SIS II, i syfte att upplysa om deras vistelseort eller hemvist:

- a) vittnen
  - b) personer som har kallats eller personer som söks för att kunna kallas att inställa sig i rätten i samband med ett brottmålsförfarande för att stå till svars för gärningar som de åtalas för
  - c) personer som skall delges en dom i ett brottmål eller andra handlingar i samband med ett brottmålsförfarande, för att stå till svars för gärningar som de åtalas för
  - d) personer som skall delges en kallelse att inställa sig för verkställighet av ett frihetsberövande straff.
- Registreringar om personer och föremål som omfattas av diskreta kontroller eller särskilda kontroller. I överensstämmelse med nationell lagstiftning i den medlemsstat som lägger in registreringen skall uppgifter införas om personer eller fordon, fartyg, luftfartyg och containrar för diskret kontroll eller särskild kontroll i enlighet med artikel 37.4 (artikel 36). Registreringar om fordon, fartyg, luftfartyg och containrar får införas när det finns tydliga tecken på att de har samband med ett grovt brott eller ett allvarligt hot. En sådan registrering får göras i syfte att bekämpa brottslighet och förebygga hot mot den allmänna säkerheten om:
    - a) det finns tydliga tecken på att en person avser att begå, eller redan begår ett grovt brott.
    - b) om den allmänna uppfattningen om en person, särskilt på grundval av redan begångna brott, leder till misstanke om att denne även i framtiden kommer att begå grova brott.

I syfte att utföra diskreta kontroller eller särskilda kontroller kan samtliga eller vissa av nedanstående uppgifter insamlas och översändas till den myndighet som lagt in registreringen när gränskontroller eller andra polis- och tullkontroller utförs inom medlemsstaten:

- a) påträffande av en person eller ett fordon, ett fartyg, ett luftfartyg eller en container som efterlysts i en registrering
- b) plats, tidpunkt eller skäl för kontrollen
- c) resväg och målet för resan
- d) personer i de berörda personernas sällskap eller passagerare i fordonet, fartyget eller luftfartyget som rimligen kan förväntas ha anknytning till de berörda personerna

- e) fordon, båt, flygplan eller container som använts
  - f) transporterade varor
  - g) omständigheter kring påträffandet av personen eller fordonet, fartyget, luftfartyget eller containern.
- Följande lätt identifierbara föremålskategorier samlas in och anges i registreringarna, som görs om föremålen som antingen skall beslagtas eller användas som bevis i brottmål (artikel 38):
    - a) motorfordon med en cylindervolym överstigande 50 cm<sup>3</sup> samt fartyg och luftfartyg
    - b) släpvagnar med en tjänstevikt överstigande 750 kg samt husvagnar, industritillbehör, utombordsmotorer och containrar
    - c) skjutvapen
    - d) stulna, bortförda eller försvunna officiella blankodokument.
    - e) stulna, bortförda, försvunna eller ogiltigförklarade utfärdade identitetshandlingar, till exempel pass, ID-kort, körkort, uppehållstillstånd och resehandlingar
    - f) stulna, bortförda, försvunna eller ogiltigförklarade registreringsbevis för fordon och nummerplåtar för fordon
    - g) sedlar (registrerade sedlar)
    - h) värdepapper och betalningsmedel som checkar, kreditkort, obligationer och aktier som stulits, bortförts, försvunnit eller ogiltigförklarats.
  - Uppgifter om en person vars identitet har missbrukats får användas endast i följande syften:
    - för att göra det möjligt för den behöriga myndigheten att skilja mellan den person vars identitet har missbrukats och den person som faktiskt avses i registreringen
    - för att göra det möjligt för den person vars identitet har missbrukats att styrka sin identitet och fastställa att den har blivit missbrukad.

## 6 Normalt utlämnande av uppgifter

### 6.1 Utlämnande av personuppgifter ur det nationella datasystemet i Schengens informationssystem

Polisen får trots sekretessbestämmelserna lämna ut uppgifter ur det nationella datasystemet i Schengens informationssystem till behöriga Schengenmyndigheter, med iakttagande av författningsgrunden för Schengens

informationssystem. Uppgifterna får också lämnas ut genom en teknisk anslutning eller som en datamängd.

## 6.2 Utlämnande av personuppgifter till stater som använder Schengens informationssystem och till Schengens informationssystem

Polisen får trots sekretessbestämmelserna, lämna ut uppgifter som avses i författningsgrunden för Schengens informationssystem till Schengenstaternas behöriga myndigheter, om uppgifterna behövs för ändamål som anges i författningsgrunden för Schengens informationssystem. Den tilläggsinformation som avses i författningsgrunden för Schengens informationssystem skall lämnas ut genom förmedling av Sirenekontoret. Sirenekontoret i Finland utgörs av Centralkriminalpolisen. Uppgifterna får också lämnas ut genom en teknisk anslutning eller som en datamängd.

## 7 Raderande och arkivering av personuppgifter

Avlägsnande av information i Schengens informationssystem regleras på följande sätt i författningsgrunden:

- I enlighet med beslutet (EG) nr 1987/2006/RIF i SIS II skall lagrade registreringar om personer lagras endast under så lång tid som behövs för att uppnå det syfte för vilket de tillhandahölls. Den medlemsstat som infört registreringen skall inom tre år efter att registreringen infördes, se över om registreringen behöver bevaras. Den medlemsstat som fört in registreringen får inom tidsfristen för översynen efter en övergripande individuell bedömning som skall arkiveras, besluta att registreringen skall lagras längre om detta visar sig nödvändigt för det syfte i vilket den förts in. I förekommande fall skall varje medlemsstat bestämma kortare tidsfrister för denna översyn i enlighet med sin nationella lagstiftning.
- Registreringar gällande personer vilka lagrats i enlighet med beslut 2007/533/RIF i SIS II, lagras endast under så lång tid som behövs för att uppnå det syfte för vilket de tillhandahölls. Den medlemsstat som infört registreringen skall inom tre år efter att registreringen infördes, se över om registreringen behöver bevaras. Tidsfristen för registreringarna som gäller de personer som avses i artikel 36 uppgår emellertid till ett år. Den medlemsstat som fört in registreringen får inom tidsfristen för översynen efter en övergripande individuell bedömning som skall arkiveras, besluta att registreringen skall lagras längre om detta visar sig nödvändigt för det syfte i vilket den förts in.

- Registreringar gällande föremål som lagrats i enlighet med beslut 2007/533/RIF i SIS II, lagras endast under så lång tid som behövs för att uppnå det syfte för vilket de tillhandahölls. I enlighet med artikel 36 bevaras registreringar gällande lagrade föremål i maximalt fem år och i enlighet med artikel 38 bevaras uppgifter om lagrade föremål i maximalt tio år med undantag för registreringar gällande betalmedel vars giltighetstid uppgår till ett år. Förvaringstiden gällande de förutnämnda registreringarna kan förlängas, om det är nödvändigt för de syften för vilka registreringen upprättades.
- Kompletterande uppgifter för att komma till rätta med missbruk av identitet skall avlägsnas samtidigt som motsvarande registrering eller tidigare om personen, vars identitet har missbrukats, kräver detta.
- Personuppgifter som registrerats hos Sirenekontoret till följd av informationsutbyte, skall lagras endast under så lång tid som kan behövas för att uppnå de ändamål för vilka de tillhandahölls. De skall under alla omständigheter tas bort senast ett år efter det att registreringen med anknytning till personen har tagits bort i SIS II.
- Logguppgifter måste tas bort minst ett år och senast tre år efter att de har upprättats. Logguppgifter som innehåller registreringskedan skall avlägsnas ett till tre år efter att registreringen tagits bort. Logguppgifter får förvaras längre om de behövs i redan påbörjade övervakningsförfaranden.

## 8 Den registrerades rättigheter

För att säkerställa öppen information samt för att främja den registrerades användning av sina rättigheter har polisen inrättat ett omfattande informationsmaterial på [www.poliisi.fi/sv](http://www.poliisi.fi/sv) -webbplatsen. På webbplatsen finns detaljerad information bland annat om hur den registrerade kan kontrollera sina uppgifter, inskränkning i rätten till insyn, hur och med vilka förutsättningar uppgifterna kan rättas eller raderas, hur polisen behandlar loginformation och hur polisen som personuppgiftsansvarig ser till de registrerades rättigheter och den interna övervakningen av behandlingen av personuppgifterna.

För att säkerställa att ovannämnda informationsmaterial finns till allas förfogande även på andra ställen har det i varje av polisens servicepunkter placerats en personregister-mapp, där motsvarande informationsmaterial avsett för de registrerade finns i pappersform.



## 8.1 Rätt till insyn / rätt att få tillgång till uppgifter

Enligt författningsgrunden i Schengens informationssystem skall personers rätt att få tillgång till uppgifter om sig själva och som har lagts in i SIS II, utövas i enlighet med den nationella lagstiftningen i den medlemsstat i vilken de åberopar denna rätt. Enligt författningsgrunden får inte uppgifter överlåtas till den registrerade, om det är oundvikligt för att genomföra de rättsliga åtgärder som anges i registreringen eller för att skydda övriga personers rättigheter eller friheter.

I princip har alla rätt att få information från den personuppgiftsansvarige om huruvida ens personuppgifter behandlas, och om ifrågavarande uppgifter behandlas har den registrerade rätt att på begäran få de uppgifter som nämns i 23 § i dataskyddslagen avseende brottmål från den personuppgiftsansvarige.

Vid utövande av rätten till insyn skall den registrerade framställa en personlig begäran till den personuppgiftsansvarige eller till polisinrättningen samt styrka sin identitet. Den registrerade kan ha ett biträde med sig. Begäran ska specificeras med sådan noggrannhet att det i den framgår med tillräcklig noggrannhet till vilket personuppgiftsregister eller vilken del av den begäran riktar sig.

Enligt författningsgrunden i Schengens informationssystem skall personen ifråga meddelas så snabbt som möjligt men senast 60 dagar från det att vederbörande begär ut sina uppgifter eller tidigare, om så regleras i den nationella lagstiftningen.

Den registrerade själv har inte rätt till insyn i uppgifter från informationskällor, personuppgifter som gäller hemlig övervakning och särskild kontroll i Schengens informationssystem, sådana uppgifter om polisens taktiska eller tekniska metoder, observationsuppgifter, uppgifter om informationskällor eller uppgifter som används för teknisk undersökning, som ingår i de personuppgifter som avses i 5–8 § i polisens personuppgiftslag, eller personuppgifter som erhållits genom de inhämtningsmetoder som avses i 5 kap. i polislagen och 10 kap. i tvångsmedelslagen samt med stöd av 157 § i lagen om tjänster inom elektronisk kommunikation.

Den registrerades rätt till insyn kan begränsas om det med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd i syfte att:

- a) undvika menlig inverkan på förebyggande, avslöjande, utredning av brott eller på åtgärder som avser åtal för brott eller på verkställighet av straffrättsliga påföljder
- b) trygga andra undersökningar, utredningar eller motsvarande förfaranden hos myndigheter
- c) skydda den allmänna säkerheten
- d) skydda den nationella säkerheten eller
- e) skydda andra personers rättigheter.

Om den registrerades rätt till insyn skjuts upp, begränsas eller vägras, ska den personuppgiftsansvarige utan obefogat dröjsmål informera den registrerade om detta genom ett skriftligt intyg. Även grunderna för uppskovet, begränsningen eller vägran ska uppges, utom i det fall att lämnandet av denna information skulle äventyra syftet med vägran eller begränsningen. Om den personuppgiftsansvarige inte inom tre månader efter att begäran framställts har gett den registrerade ett skriftligt svar, betraktas detta som att insyn har vägrats.

Den registrerade har rätt att be dataombudsmannen kontrollera lagenligheten i personuppgifter och behandlingen av dem, om den registrerades rätt till insyn har skjutits upp, begränsats eller vägrats med stöd av dataskyddslagen avseende brottmål. Begäran ska framställas personligen till dataombudsmannen, den personuppgiftsansvarige (Polisstyrelsen) eller polisinrättningen och den som lämnar in begäran ska styrka sin identitet.

En registrerad har rätt att föra ett ärende till dataombudsmannen för behandling (begäran om åtgärder), om den registrerade anser att någon vid behandlingen av hans eller hennes personuppgifter bryter mot dataskyddslagen för brottmål eller någon annan lag som gäller behandling av personuppgifter.

**Dataombudsmannens byrå:**

Besöksadress: Fågelviksgränden 4, 00530 Helsingfors

Postadress: PB 800, 00531 Helsingfors

Växel: 029 566 6700, Fax: 029 566 6735

E-post (registratorskontor): tietosuoja@om.fi

## 8.2 Rättelse eller utplåning av personuppgifter eller begränsning av behandlingen

Enligt författningsgrunden för Schengens informationssystem har alla rätt att få felaktiga uppgifter som lagrats i SIS II om sig själv korrigerade eller utplånade om de har lagrats olagligt. I enlighet med författningsgrunden skall den berörda

personen så snart som möjligt informeras om vilka åtgärder som vidtas till följd av begäran om rättelse eller utplåning, dock senast tre månader räknat från dagen för begäran om rättelse eller utplåning, eller tidigare om en kortare tidsfrist följer av nationell lagstiftning.

Den personuppgiftsansvarige skall på eget initiativ eller på begäran av den registrerade utan ogrundat dröjsmål rätta till eller komplettera sådana personuppgifter om den registrerade som är oriktiga eller bristfälliga med hänsyn till ändamålet med behandlingen.

Den personuppgiftsansvarige skall på eget initiativ eller på begäran av den registrerade utan ogrundat dröjsmål avlägsna personuppgifter som rör den registrerade, om deras behandling motstrider kravet på lagenlighet i dataskyddslagen för brottmål, bundenhet till användningsändamålet, relevanskrav, felfrihetskrav eller förordningar som gäller särskilda personuppgiftskategorier.

I stället för utplåning skall den personuppgiftsansvarige dock begränsa behandlingen om:

- a) den registrerade bestrider personuppgifternas korrekthet och det inte kan fastställas huruvida de är korrekta, eller felaktiga (den personuppgiftsansvarige skall innan denna begränsning avlägsnas, meddela detta till den registrerade) eller
- b) personuppgifterna måste bevaras som bevisning.

Den registrerade kan framföra en begäran om rättelse eller utplåning av personuppgifter och begränsning av behandlingen till den personuppgiftsansvarige eller annan polisenhet. Begäran skall preciseras med tillräcklig noggrannhet så att det av begäran framgår vems personuppgifter det rör sig om, till vilka av polisens personuppgifter som begäran om rättelse, utplåning eller begränsning av behandling är riktade till, varför uppgifterna ifråga enligt den registrerade är bristfälliga, oklara eller felaktiga vad gäller behandlingens syfte och vilka förändringar den registrerade kräver skall genomföras samt varför begränsning av personuppgifternas behandling borde införas. Den personuppgiftsansvarige har rätt att begära ytterligare information i syfte att styrka identiteten.

Den registrerades rättigheter avseende rättelse eller utplåning av personuppgifter eller begränsning av behandlingen kan begränsas om det med beaktande av den registrerades rättigheter är en proportionell och nödvändig åtgärd i syfte att:

- a) undvika menlig inverkan på förebyggande, avslöjande, utredning av brott eller på åtgärder som avser åtal för brott eller på verkställighet av straffrättsliga påföljder
- b) trygga andra undersökningar, utredningar eller motsvarande förfaranden hos myndigheter
- c) skydda den allmänna säkerheten
- d) skydda den nationella säkerheten eller
- e) skydda andra personers rättigheter.

Om den personuppgiftsansvarige inte godkänner den registrerades begäran om rättelse, komplettering eller utplåning av personuppgifter eller begränsning av behandlingen av dem, ska den personuppgiftsansvarige genom ett skriftligt intyg informera den registrerade om vägran och grunderna för vägran. Den personuppgiftsansvarige får helt eller delvis låta bli att lämna den registrerade information om grunderna för vägran, om det är nödvändigt på de grunder som nämns ovan.

Den registrerade har rätt att be dataombudsmannen kontrollera lagenligheten i personuppgifter och behandlingen av dem, om den registrerades rätt till insyn har skjutits upp, begränsats eller vägrats med stöd av dataskyddslagen avseende brottmål eller någon annan lag eller om den personuppgiftsansvarige inte godkänner den registrerades yrkande om rättelse, komplettering eller utplåning av personuppgifterna eller begränsning av behandlingen av dem (kontaktuppgifter ovan).

Den personuppgiftsansvarige ska anmäla varje rättelse av oriktiga personuppgifter till den myndighet från vilken de oriktiga personuppgifterna kommer. Om personuppgifter har rättats eller utplånats eller behandlingen av dem har begränsats med stöd av 25 § i dataskyddslagen avseende brottmål, ska den personuppgiftsansvarige informera de mottagare om saken till vilka den personuppgiftsansvarige har lämnat ut uppgifterna. Mottagarna ska rätta eller utplåna de personuppgifter de har eller begränsa behandlingen av dem.

I enlighet med polisens personuppgiftslag får en uppgift som konstaterats vara felaktig bevaras tillsammans med den korrigerade uppgiften, om det behövs för att trygga de rättigheter som den registrerade, någon annan part eller en person

som hör till polispersonalen har. En uppgift som konstaterats vara felaktig får emellertid inte lagras i det nationella datasystemet i Schengens informationssystem.

### 8.3 Den registrerades övriga rättigheter

Den registrerades rätt att motsätta sig behandling av uppgifterna, rätt att flytta uppgifterna från ett system till ett annat och rätt att inte bli föremål för automatiserat beslutsfattande tillämpas inte då polisen behandlar personuppgifter i samband med polisens lagstadgade uppgifter i syfte att utföra undersöknings- och övervakningsuppgifter samt vid användande av polisens offentliga makt.

Alla har rätt att be den övervakningsmyndighet som avses i Schengens allmänavtal, säkerställa att den insamling, lagring, behandling och användning av vederbörandes personuppgifter i det arkiv som upprätthålls av enheten för tekniskt stöd i Schengens informationssystem, sker lagenligt och korrekt. Den registrerade skall personligen framställa en begäran till personuppgiftsansvarig eller polisinrättning och den registrerade skall kunna styrka sin identitet. En begäran om kontroll som lämnats till polisen skall utan dröjsmål sändas till dataombudsmannen.

### 8.4 De registrerades möjligheter att utöva sina rättigheter samt avgiftsfria åtgärder

Meddelanden och information som de registrerade ska få enligt med dataskyddslagen för brottmål samt behandlingen av begäranden som de registrerade framställt är i regel avgiftsfria för de registrerade. Om en registrerads begäranden på grund av att de upprepats eller av någon annan orsak är uppenbart orimliga eller ogrundade, får den personuppgiftsansvarige dock för åtgärden ta ut en avgift. Bestämmelser om grunderna för avgiftens belopp finns i lagen om grunderna för avgifter till staten (150/1992). Om den personuppgiftsansvarige tar ut en avgift med stöd av ovannämnda grunder, ska den personuppgiftsansvarige vid behov visa att begäran har varit uppenbart ogrundad eller orimlig.

## 9 Kontroll och skydd av personuppgifter hos polisen

Den personuppgiftsansvarige och personuppgiftsbiträdet ska genom tekniska och organisatoriska åtgärder se till att personuppgifterna är tillräckligt skyddade med hänsyn till den risk för den registrerades rättigheter som behandlingen medför. Personuppgifterna ska särskilt skyddas för obehörig behandling och mot

förlust, förstöring eller skada genom olyckshändelse. Åtgärderna ska planeras och genomföras med beaktande av:

- 3) den senaste tekniska utvecklingen
- 4) kostnaderna för att genomföra åtgärderna
- 5) behandlingens art, omfattning, sammanhang och ändamål
- 6) riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter.

Grunden för polisförvaltningens tekniska, administrativa och organisatoriska datasäkerhet utgörs av Polisens datasäkerhets- och dataskyddspolicy, vilken innehåller en definition av målen för skyddet av uppgifter, ansvaren och genomförandemetoderna vid polisförvaltningen. Datasäkerhets- och dataskyddspolicyn revideras i flera separata föreskrifter och anvisningar.

Polisstyrelsen har gett ut en anvisning om polisens interna laglighetsövervakning och om vissa andra rättsliga frågor inom polisen, vilka skapar förutsättningar för planering och genomförande av polisens laglighetsövervakning samt rapportering av resultaten i samband med användningen av informationssystemet och övervakningen av behandling av personuppgifterna.

I laglighetsövervakningen av personuppgiftsregistrets användning och personuppgifternas behandling ägnas särskild uppmärksamhet vid korrekthet och nödvändighet, ändamålsenlig användning av uppgifterna, användarrättigheternas korrekthet och aktualitet, samt vid att uppgifterna behandlas i enlighet med klassificeringskrav för sekretessbelagda.

datamängder. Vid behandling av personuppgifter som hör till särskilda kategorier av personuppgifter ska särskild uppmärksamhet ägnas åt att lämpliga tekniska och organisatoriska skyddsåtgärder genomförs ändamålsenligt och att ifrågavarande personuppgifter endast behandlas då det är nödvändigt för utförande av de uppgifter som polisen ålagts genom lag.

## **10 Tillgång till dataskyddsbeskrivningarna**

Polisens dataskyddsbeskrivningar finns tillgängliga för alla i elektroniskt format i polisens nationella nätverk ([www.poliisi.fi/sv](http://www.poliisi.fi/sv)), polisens interna nätverk (Intranet) samt i pappersform vid alla polisens servicepunkter.

Dataskyddsbeskrivningarna lagras i polisens ärendehanterings-, beslutsfattande- och arkiveringssystem (Acta) för administrativ ärendehantering.