

Samkommunen Helsingforsregionens trafik

Dataskyddspolicy

17.4.2018

version 1.1

Innehåll

1	Tarkoitus ja taustaa	Virhe. Kirjanmerkkiä ei ole määritetty.
2	Sovellettava lainsäädäntö ja määritelmät.....	Virhe. Kirjanmerkkiä ei ole määritetty.
2.1	Lainsäädäntö.....	Virhe. Kirjanmerkkiä ei ole määritetty.
2.2	Määritelmät	Virhe. Kirjanmerkkiä ei ole määritetty.
3	Tietosuojaperiaatteet.....	Virhe. Kirjanmerkkiä ei ole määritetty.
3.1	Lainmukaisuus, kohtuullisuus ja läpinäkyvyys	Virhe. Kirjanmerkkiä ei ole määritetty.
3.2	Käyttötarkoitussidonnaisuus	Virhe. Kirjanmerkkiä ei ole määritetty.
3.3	Tietojen minimointi	Virhe. Kirjanmerkkiä ei ole määritetty.
3.4	Tietojen täsmällisyys	Virhe. Kirjanmerkkiä ei ole määritetty.
3.5	Tietojen säilytyksen rajoittaminen	Virhe. Kirjanmerkkiä ei ole määritetty.
3.6	Tietojen eheys ja luottamuksellisuus	Virhe. Kirjanmerkkiä ei ole määritetty.
3.7	Rekisterinpitäjän osoitusvelvollisuus.....	Virhe. Kirjanmerkkiä ei ole määritetty.
4	Tietosuojan hallintamalli	Virhe. Kirjanmerkkiä ei ole määritetty.
5	Tietosuojapolitikan hyväksyminen ja päivittäminen	Virhe. Kirjanmerkkiä ei ole määritetty.

1 SYFTE OCH BAKGRUND

I denna dataskyddspolicy förklaras de syften, ansvar och riktlinjer för dataskydd som HRT har definierat. HRT förstår betydelsen av dataskydd och integritetsskydd av de registrerade som en del av sin verksamhet och förbinder sig till dataskydd på det sätt som beskrivs i denna dataskyddspolicy. Datasekretess är en del av verksamhetens överensstämmelse med reglerna, dataskydd och riskhantering.

Definiering av syften och betydelsen av dataskyddet samt av verksamhetsprinciperna inom dataskyddsarbetet, dokumentering och information till HRT:s anställda utgör en viktig del av HRT:s dataskyddskultur. Med hjälp av denna dataskyddspolicy och de noggrannare anvisningarna som baserar sig på dataskyddspolicyn informeras HRT:s anställda och samarbetspartner om HRT:s dataskyddsprinciper. Med högklassigt dataskyddsarbete säkerställs för sin del att målen för dataskydd uppfylls. HRT:s dataskyddspolicy definierar principerna som gäller dataskydd och dataskyddsarbete.

2 TILLÄMPLIG LAGSTIFTNING OCH DEFINITIONER

2.1 Lagstiftning

EU:s allmänna dataskyddsförordning (2016/679), den nationella personuppgiftslagstiftningen samt övriga lämpliga specialbestämmelser tillämpas i HRT:s dataskydd och i behandling av personuppgifterna. HRT:s grundavtal, strategi, förvaltningsstadga samt interna anvisningar styr HRT:s dataskyddsarbete och HRT:s dataskyddspolicy, ISO/IEC 27001 & 27002 standarderna samt den goda praxisen HRT:s dataskydd.

I HRT:s verksamhet beaktas förvaltningens offentlighet och den registrerades integritetsskydd som är föreskrivna i grundlagen. HRT samordnar dessa grundläggande rättigheter på det sätt som bestäms i lagstiftningen.

2.2 Definitioner

I denna dataskyddspolicy används definitioner som är i enlighet med EU:s allmänna dataskyddsförordning.

Med personuppgift avses i förordningen varje upplysning som avser en identifierad eller identifierbar fysisk person dvs. den registrerade. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller manuellt, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med personuppgiftsbiträde avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Ett register är en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden. **Med registeransvarig** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den registeransvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. **Med samtycke av den registrerade** avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. **Med profilering** avses varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

3 DATASKYDDSPRINCIPER

Behandling av personuppgifterna styrs med principer som är i enlighet med EU:s allmänna dataskyddsförordning så att kraven i förordningen uppfylls och den registrerades rättigheter skyddas. I behandlingen av personuppgifterna ska alla nedanstående principer beaktas. Dataskyddsprinciperna ska iaktas under personuppgiftsbehandlingens hela livscykel.

3.1 Laglighet, korrekthet och öppenhet

Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De registrerade ska veta hur personuppgifter som rör dem insamlas och behandlas. All information och kommunikation i samband med behandlingen av personuppgifterna ska vara lättillgänglig och lättbegriplig. Den registrerade ska känna till den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Den registeransvarige ska kunna ange information till de registrerade om hur deras personuppgifter behandlas samt hur den registeransvarige säkerställer en rättvis och öppen behandling av personuppgifterna.

3.2 Ändamålsbegränsning

Insamling av personuppgifterna ska vara ändamålsbegränsad dvs. de ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De insamlade uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Ytterligare behandling av personuppgifterna för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som avses i EU:s allmänna dataskyddsförordning (artikel 89 punkt 1) ska inte anses vara oförenligt med de ursprungliga ändamålen.

3.3 Uppgiftsminimering

Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Den period under vilken personuppgifterna kommer att lagras ska vara så kort som möjligt. Personuppgifterna ska behandlas endast om det inte är möjligt att rimligt utföra uppgiften med något annat medel. Den registeransvarig ska sätta tidpunkten för när personuppgifterna kommer att raderas. Om det inte är möjligt att sätta en utsatt tidpunkt ska registeransvarige ge de kriterier som används för att fastställa tidpunkten för radering av personuppgifterna.

3.4 Uppgifternas korrekthet

Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. Den registrerade har rätt att komplettera ofullständiga personuppgifter, bland annat genom att lämna in en tilläggsutredning.

3.5 Lagringsminimering av uppgifterna

Personuppgifterna ska förvaras i en sådan form där den registrerade kan identifieras endast så länge det är nödvändigt för behandling av uppgifterna. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

3.6 Uppgifternas integritet och konfidentialitet

I behandlingen av personuppgifterna ska säkerställas adekvat dataskydd dvs. uppgifternas integritet, konfidentialitet och tillgänglighet. Uppgifterna ska skyddas mot obehörig eller olaglig behandling och mot förlust, förstöring eller skada genom olyckshändelse.

3.7 Registeransvariges ansvarsskyldighet

Med ansvarsskyldighet avses att den registeransvarige ska kunna visa till de registrerade och dataskyddsmyndigheterna hur dataskyddsprinciper efterlevs. Detta sker bland annat genom utarbetande av dataskyddsbeskrivningar, informering av de registrerade, interna anvisningar inom organet, samt genom att behandlingsprocesser av personuppgifterna dokumenteras noggrant. Den registeransvarige ska regelbundet utvärdera hur principerna verkställs i den egna verksamheten.

4 HANTERINGSMODELL

Enligt HRT:s förvaltningsstadga ansvarar styrelsen om dataskyddet och utser dataskyddsombudet. Dataskyddsombudet ansvarar för de uppgifter som bestäms i dataskyddsförordningen och i dataskyddets hanteringsmodell.

Hanteringsmodellen definierar HRT:s dataskyddsuppgifter och –ansvar i enlighet med förvaltningsstadgan och dataskyddspolicyn. Den verkställande direktören godkänner HRT:s hanteringsmodell för dataskydd.

Avdelningsdirektörerna ansvarar för att verksamheten i avdelningen genomförs i enlighet med dataskyddspolicy vad gäller genomförandet av dataskydd. Detta gäller också tjänster för behandling av personuppgifterna som utförs på entreprenad. Om behandling av personuppgifterna som utförs på entreprenad ingås alltid ett skriftligt avtal där parterna kommer överens om ansvar och skyldigheter som gäller behandling av personuppgifterna i enlighet med EU:s allmänna dataskyddsförordning. Avdelningsdirektörerna ansvarar för att konsekvensbedömning av behandling med avseende på personuppgifterna utförs. Konsekvensbedömningen ska utföras om behandlingen sannolikt kan innebära en hög risk för registrerades rättigheter och friheter. För konsekvensbedömningen bör frågas råd från dataskyddsansvarige.

Verkställande direktör och avdelningsdirektörerna ser till att det finns tillräckliga och nödvändiga resurser för dataskyddsarbetet.

Dataskyddsskyldigheterna gäller HRT:s anställda och HRT:s samarbetspartner.

HRT:s dataskydd utvärderas regelbundet i enlighet med hanteringsmodellen. Dataskyddsombudet rapporterar avdelningsdirektörerna om dataskyddsincidenter samt regelbundet avdelningsdirektörerna och styrelsen i enlighet med principerna i hanteringsmodellen.

HRT:s anställda och samarbetspartner är skyldiga att meddela om de har upptäckt brister, förfarandefel eller övriga hot mot dataskydd.

5 GODKÄNNANDE OCH UPPDATERING AV DATASKYDDSPOLICYN

HRT:s styrelse har godkänt innehållet i denna dataskyddspolicy. Vad dataskyddspolicyn innehåller granskas och uppdateras vid behov. HRT:s dataskyddsombuds uppgift är att utvärdera uppdateringsbehov av dataskyddspolicyn och uppdateringsförslag lämnas till HRT:s styrelse för godkännande.

Godkänt av styrelsen 17.4.2018