Södertörns brandförsvarsförbund

TJÄNSTEUTLÅTANDE 2019

2019-01-25

Dnr: 2019-000411

Dataskyddspolicy – interna riktlinjer för hantering av personuppgifter

Sammanfattning

Efter revisorernas granskning av IT-verksamheten hos Södertörns brandförsvarsförbund under hösten 2017 konstaterades att det saknades aktuella dokumenterade riktlinjer för IT-området. Det i samband med införandet av nya dataskyddsförordningen GDPR den 26 maj 2018 kräver att vi har ett tydligt styrdokument som visar hur vi hanterar olika typer av personuppgifter inom Södertörns brandförsvarsförbund.

Ett förslag till dataskyddspolicy med interna riktlinjer för hantering av personuppgifter har tagits fram som beskriver på ett övergripande plan hur personuppgifter kan och får behandlas, för vilka syften och på vilket sätt.

Ärendets beredning

Förslaget till dataskyddspolicy har arbetats fram av administrativ chef Susanne Nilsson, tillsammans med dataskyddsombud Froukje Bouius, på uppdrag av brandchef Lars-Göran Uddholm.

Bilagor

Bilaga 1 Förslag till Dataskyddspolicy – interna riktlinjer för hantering av personuppgifter.

Förslag till beslut

1. Direktionen fastställer föreslagen Dataskyddspolicy med interna riktlinjer för hantering av personuppgifter.

Susanne Nilsson

Administrativ chef

Södertörns brandförsvarsförbund

Mogårdsvägen 2
143 43 Vårby

Tfn: 08-721 22 00
Fax: 08-721 22 23

www.sbff.se
brandforsvaret@sbff.se

Org.nr.: 222000-0737

Södertörns brandförsvarsförbund

Dataskyddspolicy - interna riktlinjer för hantering av personuppgifter

Dnr: 2019-000411

Datum: 2019-01-25

Syftet med denna policy

Alla individer vars personuppgifter behandlas inom ramen för Södertörns brandförsvars verksamhet ska vara trygga med hur vi hanterar deras uppgifter.

Policyn beskriver på ett övergripande plan hur personuppgifter kan behandlas, för vilka syften och på vilket sätt av Sbff.

Denna policy ska säkerställa att Sbff:

- följer gällande dataskyddslagstiftning
- lagrar och hanterar personuppgifter på ett korrekt och enhetligt sätt
- kommunicerar tydligt och öppet gällande hur personuppgifter hanteras i verksamheten
- kan tillmötesgå anställdas, kunders och andra intressenters rättigheter
- skyddar den egna verksamheten mot hot och därmed minimerar integritetsrisker

Omfattning

Policyn har tagits fram av administrativ chef tillsammans med dataskyddsombud och omfattar all behandling av personuppgifter som utförs inom organisationen.

Denna policy gäller samtliga, oavsett vems personuppgifter som Sbff behandlar och oavsett sammanhang. Policyn ska kompletteras med riktlinjer och rutiner för informationssäkerhet samt andra specifika verksamhetsområden.

Riktlinjerna ska efterlevas av ledning, anställda och likaså av andra personer som arbetar på uppdrag av eller under översyn av Sbff, exempelvis konsulter eller partners.

Gällande dataskyddslagstiftning

Hanteringen av och skyddet för personuppgifter regleras övergripande av EU:s allmänna dataskyddsförordning (GDPR - Europaparlamentets och rådets förordning [EU] 2016/679) samt kompletterande svensk lagstiftning i form av den kompletterande dataskyddslagen och tillhörande förordning (SFS 2018:218 och SFS 2018:219).

Ytterligare relevant lagstiftning kan tillkomma i form av exempelvis registerförfattningar inom specifika branschområden.

Inom ramen för Sbff:s verksamhet är huvudsakligen följande lagar och bestämmelser tillämpliga:

- EU:s allmänna dataskyddsförordning
- Den kompletterande svenska dataskyddslagen
- Kommunallagen
- Offentlighet- och sekretesslagen
- Lagen om skydd mot olyckor
- Lag om brandfarliga och explosiva varor

Viktiga begrepp och definitioner

Denna policy rör hantering av personuppgifter. Personuppgifter är all information som kan användas för att identifiera en enskild person, direkt eller indirekt. Begreppet personuppgifter inkluderar (men är inte begränsat till):

- Namn
- Personnummer
- E-postadress
- Telefonnummer
- IP-adress
- Kundnummer
- Bilder (på personer)

I uttrycket **behandling av personuppgifter** inkluderas allting som görs där personuppgifter förekommer, exempelvis administration av, kommunikation med och lagring av sådana uppgifter för olika ändamål och i olika sammanhang.

I den mån **känsliga personuppgifter** förekommer i Sbff:s verksamhet gäller särskilda regler för dessa. Känsliga personuppgifter är:

- Uppgifter som avslöjar ras eller etniskt ursprung,
- Uppgifter som avslöjar politiska åsikter,
- Uppgifter som avslöjar religiös eller filosofisk övertygelse,
- Uppgifter om medlemskap i fackförening,
- Uppgifter om hälsa,
- Uppgifter om sexualliv eller sexuell läggning,
- Genetiska uppgifter, och
- Biometriska uppgifter för att entydigt identifiera en fysisk person.

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas.

Sbff är **personuppgiftsansvarig** för de flesta av de personuppgiftsbehandlingar som förekommer i verksamheten. Med detta menas att organisationen är den juridiska person som är ytterst ansvarig för personuppgifterna, och som bestämmer över ändamål och medel. I specifika fall kan det vara så att någon annan än Sbff är personuppgiftsansvarig. Roller och

ansvarsfördelning mellan organisationen och eventuella **personuppgiftsbiträden** ska framgå för varje behandling i registerförteckningen.

Ändamål med behandling av personuppgifter

Inom Södertörns brandförsvarsförbund hanterar vi personuppgifter i många olika sammanhang. Det är information som vi behöver för att tillhandahålla det stöd och den service vi ansvarar för. Det kan till exempel vara för att:

- Utföra vårt uppdrag inom vår förebyggande verksamhet, t ex hantera olika tillstånd och ansökningar.
- Tillhandahålla utbildning.
- Utöva tillsyn inom brandskyddsområdet enligt Lagen om skydd mot olyckor och Lag om brandfarliga och explosiva varor.
- Direktionen ska kunna fatta beslut i ärenden och personuppgifter kan t ex förekomma i underlag för beslut, kallelse och protokoll.
- Ta hand om initiativ, synpunkter och frågor från enskilda.
- Administrera uppgifter om kunder och leverantörer, till exempel för att hantera fakturor, inbetalningar och utbetalningar.
- Administrera upphandlingar och avtal med olika leverantörer.
- Hantera krav, försäkringsärenden och rättsliga tvister.
- Informera om och kommunicera räddningstjänstens verksamhet i olika sammanhang.
- Rekrytera nya medarbetare, med flera.

Generella riktlinjer

Utbildning

Alla anställda ska få grundläggande dataskyddsutbildning, för att säkerställa förståelse för vikten av att hantera personuppgifter korrekt. Ansvarig för att utbildningen genomförs är administrativ chef.

Närmsta chef ansvarar för att berörda medarbetare får ta del av sådana instruktioner och rutiner som är relevanta för dem, och sådan information som behövs för att var och en ska kunna utföra sitt arbete i linje med dataskyddslagstiftningen. Detta inkluderar, men är inte begränsat till, utbildning av nyanställda.

Registerförteckning

Detaljerad information om varje slags behandling av personuppgifter som förekommer i processer, IT-system och på olika avdelningar inom ramen för Sbff:s verksamhet ska finnas dokumenterad i organisationens registerförteckning. Förteckningen ska löpande hållas uppdaterad och fungera som ett heltäckande register över alla personuppgiftsbehandlingar, i enlighet med kraven i artikel 30 GDPR.

Registerförteckningen administreras av administrativ chef. System- och informationsägare samt avdelningsansvariga kan komma att tilldelas ansvar för specifika delar av registerförteckningen i samarbete med administrativ chef. Förteckningen kan visas upp för tillsynsmyndigheten på begäran.

Rättslig grund

Varje behandling av personuppgifter ska ha en specificerad så kallad **rättslig grund** för att det ska vara lagligt att hantera personuppgifterna. Inga personuppgifter får behandlas hos Sbff utan att det finns en identifierad och lämplig rättslig grund. En godtagbar rättslig grund kan exempelvis vara ett avtal som ska uppfyllas, ett berättigat intresse, en laglig skyldighet (till exempel enligt bokföringslagen eller arkivlagen) eller ett faktiskt samtycke från de registrerade. Alla de olika möjliga rättsliga grunderna finns listade i artikel 6 GDPR.

Det är inte tillåtet att behandla känsliga personuppgifter förutom i specifika undantagsfall, som i så fall ska finnas beskrivna i registerförteckningen samt i kompletterande policydokument/rutinbeskrivningar.

Ändamålsbegränsning och uppgiftsminimering

Personuppgifter får endast behandlas för specifika syften, i den utsträckning de behövs och i enlighet med dataskyddslagstiftningen.

Endast sådana personuppgifter som faktiskt behövs får samlas in och sparas. Inga uppgifter får sparas med lösa motiveringar såsom att de ”kanske kan vara bra att ha”.

Behandling av personuppgifter i nya sammanhang (för nya ändamål) måste alltid på förhand utvärderas och kontrolleras med dataskyddsansvariga, för att säkerställa att den nya hanteringen inte riskerar att kränka de registrerade personernas integritet eller på annat sätt bryta mot dataskyddslagstiftningen.

Behörighetsbegränsning

De personuppgifter som förekommer i verksamheten ska endast vara tillgängliga för personer som specifikt behöver dem i sitt arbete. För känsliga personuppgifter ska en snävare behörighetstilldelning generellt sett gälla än för mer harmlösa uppgifter.

Lagringsminimering

Personuppgifter som inte längre behövs (och som man inte heller är skyldig att spara) ska gallras löpande. Observera att det kan finnas lagkrav på att arkivera och spara uppgifter, men det ska finnas gallringsrutiner för varje process och varje system där personuppgifter förekommer. Var och en som arbetar där är skyldig att följa dessa rutiner.

Personuppgifter får inte användas på annat sätt eller överföras till och/eller behandlas på annan plats (system/lagringsställe/enhet) än vad som följer av gällande rutiner och instruktioner.

Information till registrerade

Alla vars personuppgifter hanteras av Sbff har rätt till information om hur deras personuppgifter hanteras. Detta gäller såväl anställda som kunder och andra grupper. Informationen ska vara lättillgänglig samt tillräckligt utförlig för att motsvara kraven i dataskyddslagstiftningen. Informationen ska lämnas på ett klart och tydligt sätt.

Informationen lämnas i huvudsak via intranätet (för anställda) och på den offentliga webbplatsen i form av en informationssida riktad till kunder och användare.

De registrerades rättigheter

Sbff ska ha rutiner och instruktioner på plats för hur organisationen ska fullgöra sina skyldigheter gentemot de registrerade. De registrerades rättigheter framgår av 3 kapitlet i dataskyddsförordningen (artiklarna 12-23), och dessa rättigheter ska Sbff vara beredda att tillmötesgå i alla situationer där det krävs. Detta omfattar ovan nämnda informations-skyldighet, men också rätten till tillgång (begäran om registerutdrag), rättelse, radering, begränsning, dataportabilitet samt rätten att invända.

Lagring och informationssäkerhet

Alla personuppgifter som finns hos Sbff ska skyddas genom säkra servrar och andra lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32 GDPR. Känsliga personuppgifter kräver generellt högre säkerhet än mer harmlösa uppgifter. Vidare specifikationer gällande informationssäkerhet inom Sbff finns i separat IT-policy/Informationssäkerhetspolicy.

Utlämnande av personuppgifter till tredje part

Det kan hända att Sbff behöver lämna ut personuppgifter till tredje part.

Att lämna ut uppgifter på det sättet är i sig en behandling av personuppgifter. Det ska alltid finnas en laglig grund för ett sådant utlämnande och de registrerade ska ha fått information om att deras uppgifter lämnas ut utanför Sbff.

Biträdesavtal

Sbff anlitar endast personuppgiftsbiträden som garanterar lämpliga tekniska och organisatoriska åtgärder och på andra sätt kan ge garantier för att kraven i dataskyddsförordningen uppfylls också när en annan aktör behandlar personuppgifter för vår räkning. Det ska finnas skriftliga biträdesavtal med samtliga leverantörer och andra personuppgiftsbiträden. Dataskyddsansvarig ansvarar tillsammans med respektive informationsägare för att kontrollera att biträdesavtal finns och speglar kraven i artikel 28 GDPR.

Incidentrapportering

Var och en som upptäcker eller misstänker en incident som skulle kunna innebära en integritetsrisk, ska rapportera detta vidare till dataskyddsanasvariga. En personuppgiftsincident kan vara allt ifrån att någon har tappat en mobiltelefon till en hackerattack där kundinformation och kontokortsinformation blivit stulna. Rutiner kring hantering av incidenter ansvarar dataskyddsansvarig för hos Södertörns brandförsvarsförbund. Mer information finns i separat Informationssäkerhetspolicy.

Roller och ansvar

Varje anställd som hanterar personuppgifter i sitt uppdrag måste säkerställa att uppgifterna behandlas i enlighet med denna policy samt följer kompletterande uppsatta instruktioner.

Var och en som arbetar inom ramen för Sbff:s verksamhet är skyldig att följa denna policy samt att samarbeta med ansvariga personer när det är relevant.

Tillsynsmyndighet

Södertörns brandförsvarsförbund har gjort bedömningen att ansvarig tillsynsmyndighet för verksamheten är Datainspektionen.

Enskilda personer som har klagomål gällande Sbff:s hantering av personuppgifter har rätt att kontakta Datainspektionen.

Kompletterande policyer och instruktioner

Vidare riktlinjer och instruktioner som rör Sbff:s personuppgiftsbehandling finns i följande dokument:

- IT-policy
- Informationssäkerhetspolicy
- Kommunikationspolicy

Dokumentets historia

Upprättad/ reviderad:	Upprättad/ reviderad av:	Kontrollerad av 1:	Kontrollerad av 2:	Godkänd av:	Ersätter:
SUN		LU	AE	Direktionen 2019-02-08 §5	