DET HÄR ÄR ETT STYRDOKUMENT

RIKTLINJE

Riktlinje för dataskydd och hantering av personuppgifter

BOTKYRKA LÅNGT IFRÅN LAGOM BOTKYRKA

Dokumentkategori:	**Normerande**
Beslutad av:	Kommunstyrelsen
Antagen:	2024-03-11
Diarienummer:	KS/2023:00743
Dokumentet gäller för:	Samtliga nämnder och förvaltningar
Dokumentansvarig	Kommunstyrelseförvaltningen
Ansvar för revidering:	Centralt dataskyddsombud
Giltigt till och med:	Tillsvidare

BOTKYRKA KOMMUN

Innehåll

1. Inledning

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), gäller som lag i Sverige sedan den 25 maj 2018 och ersätter tidigare personuppgiftslagen, PuL (1998:204). I Sverige kompletteras även dataskyddsförordningen av den nya dataskyddslagen samt verksamhetsspecifik lagstiftning.

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra krav på ökad dokumentation. Det finns möjligheter för tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY), att i vissa fall döma ut en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter.

I Botkyrka kommun hanteras en stor mängd personuppgifter och det behöver säkerställas att kommunens hantering är i enlighet med gällande lagstiftning.

2. Syfte

Riktlinjens syfte är dels att främja att Botkyrka kommun hanterar personuppgifter på ett lagenligt sätt, dels att visa för allmänhet och anställda att de kan vara trygga med att deras personuppgifter hanteras på ett respektfullt sätt samt att inga personuppgifter hanteras i onödan eller riskerar att hamna i orätta händer.

Avsikten med riktlinjen är vidare att skapa en enhetlig vägledning på detta område i Botkyrka kommun. Denna riktlinje gäller för kommunens samtliga nämnder. Det åvilar dock respektive nämnd/förvaltning att ta fram verksamhetsspecifika rutiner och mallar som komplement till denna riktlinje då detta är nödvändigt.

3. Dokumentet gäller för

Botkyrka kommuns nämnder, förvaltningar, medarbetare och förtroendevalda. I tillämpliga fall även för andra som hanterar personuppgifter för kommunens räkning.

4. Ansvarsfördelning och organisation

Dataskyddsförordningen kräver ett tydligt fastställande om vem som bär ansvar. I Botkyrka kommun är varje nämnd och styrelse personuppgiftsansvariga för sina personuppgiftsbehandlingar.

4.1 Personuppgiftsansvar

Varje nämnd och styrelse inom Botkyrka kommun är personuppgiftsansvarig för behandlingen av personuppgifter inom sitt verksamhetsområde.

Nämnderna ansvarar för att kraven som ställs på personuppgiftsansvariga i dataskyddsförordningen uppfylls. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att bland annat:

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas.
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med nödvändig säkerhet.
- Kunna visa att krav i lagstiftning är uppfyllda genom noggrann dokumentation.
- Säkerställa att riskanalyser genomförs och dokumenteras.
- Säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet.
- Säkerställa att personuppgiftsincidenter rapporteras till IMY.
- Tillgodose registrerades rättigheter gällande information, tillgång (registerutdrag), rättning, begränsning, dataportabilitet och invändning.
- Föra register över behandlingar av personuppgifter i för ändamålet avsett register (registerförteckning).

4.1.1 Särskilt om kommunstyrelsen

Kommunstyrelsen har ett ansvar för att leda, samordna och ha uppsikt över kommunens arbete med att uppfylla kraven i dataskyddsförordningen. Kommunstyrelsen har genom sin uppsiktsplikt över nämnderna ett särskilt ansvar för kommunens behandling av personuppgifter. Kommunstyrelsen ska inom ramen för uppsiktsplikten vid behov ge nämnderna råd,

anvisningar och förslag på åtgärder. Kommunstyrelsen utfärdar riktlinjer samt vid behov kommungemensamma regler och rutiner för att säkerställa att kommunen hanterar personuppgifter på ett lagenligt och enhetligt sätt.

Kommunstyrelsen ansvarar vidare för att utse centralt dataskyddsombud och svara för att denne har förutsättningar och den kunskap som krävs för att fullgöra sitt uppdrag.

4.2 Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och ska säkerställa att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde och dess medarbetare får bara behandla personuppgifter enligt instruktion från den personuppgiftsansvarige.

Det åligger varje personuppgiftsansvarig att säkerställa att personuppgiftsbiträdesavtal (PUB-avtal) tecknas med aktörer utanför kommunens organisation som ska behandla personuppgifter för kommunens räkning. Personuppgiftsansvarig ska även hålla PUB-avtalen samlade och ordnade.

4.3 Dataskyddsombud

Hos Botkyrka kommun ska det finnas en central dataskyddsombudsfunktion hos Kommunstyrelsen. Denna har, utöver nedan angivna arbetsuppgifter, en samordnande roll och ansvarar för att samordna det kommungemensamma dataskyddsnätverket för att främja enhetlighet i kommunen samt stöttar Kommunstyrelsen i arbetet att ta fram kommungemensamma styrdokument.

Ett dataskyddsombud har en revisorsliknande och rådgivande funktion vars uppgifter framgår tydligt av dataskyddsförordningen.

Dataskyddsombud har i huvudsak följande uppgifter:

- Informera och ge råd till den personuppgiftsansvarige och anställda om skyldigheterna enligt dataskyddsförordningen.

- Övervaka efterlevnad av förordningen, inbegripet fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning.
- Ge råd vid konsekvensbedömningar.
- Samarbeta med tillsynsmyndigheten.
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter,
- Företräda de registrerade.
- Delta i frågor som rör skyddet av personuppgifter. Får även ha andra uppgifter om det inte leder till intressekonflikt. Det är den personuppgiftsansvarige som ska säkerställa att ingen intressekonflikt föreligger.

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet:

- På ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.
- Tillhandahålls de resurser och det stöd som krävs för att fullgöra sina uppgifter.
- Inte blir föremål för sanktioner eller avsätts på grund av att ombudet utför sitt uppdrag.
- Inte bli föremål för otillbörlig påverkan i utövande av sitt uppdrag.

Dataskyddsombudet ska när denna anser det nödvändigt ges tillträde till aktuell förvaltnings ledningsgrupp. Personuppgiftsansvarige bör av detta skäl meddela dataskyddsombud om sammankomster som avhandlar data- och integritetsskydd eller alternativt informationssäkerhetsaspekter. Förvaltningsledningarna ska säkerställa att dataskyddsombud involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling av personuppgifter kan komma i fråga.

Dataskyddsombud ska årligen redovisa för aktuell nämnd/styrelse det arbete som verksamheten gör gällande efterlevnaden av GDPR, nationell dataskyddslagstiftning och lokala styrdokument. Av den årliga redovisningen ska det minst framgå:

- Vilka interna och externa utbildningsåtgärder som förvaltningen genomfört på området,
- Resultat av Dataskyddsombudets granskningar,
- Antal personuppgiftsincidenter som inträffat under året inklusive eventuella analyser av dessa,

- Övriga iakttagelser.

Det innebär att Dataskyddsombud: samlar in information om hur de personuppgiftsansvariga behandlar personuppgifter, kontrollerar efterlevnaden av dataskyddsförordningen, rutiner och andra interna styrdokument som berör hantering av personuppgifter, sammanställer resultat av granskningen i en rapport och kommunicerar granskningsrapporten med aktuell personuppgiftsansvarig.

4.4 Dataskyddsamordnare

Som stöd i dataskyddsarbetet ska det hos varje förvaltning finnas en utsedd dataskyddssamordnare. Denna ska bland annat ha följande arbetsuppgifter:

- Delta i dataskyddsnätverket som leds av dataskyddsombudet.
- Bistå vid interrevisioner som dataskyddsombudet genomför.
- Verka för att centrala styr- och stöddokument efterlevs hos förvaltningen.
- Vara operativt stöd till förvaltningen vid genomförande av till exempel konsekvensbedömningar och vid incidentrapporter.
- Stötta dataskyddsombudet med att implementera dataskyddsarbetet och utföra utbildningar för förvaltningens medarbetare.
- Fungerar som förvaltningens kontaktperson till dataskyddsombudet, samordnar framtagande av underlag för dataskyddsombudets granskningar och ingår i kommunövergripande nätverk för dataskyddsfrågor
- Svarar på löpande GDPR-frågor, ger råd och praktiskt stöd till den förvaltningen som denne jobbar på
- Stöttar sin förvaltning vid implementering av kommunövergripande rutiner/styrning från dataskyddsombudet och i den praktiska efterlevnaden av dataskyddsförordningen inom förvaltningen
- Samordnar uppdatering av sin nämnds registerförteckning
- Samordnar hantering av förvaltningens personuppgiftsincidenter (enligt Riktlinje för dataskydd) och ansvarar för att dessa anmäls till IMY
- Samordnar arbetet med att tillgodose de registrerades rättigheter, exempelvis hantering av begäran om registerutdrag, på den egna förvaltningen

- Samordnar förvaltningens arbete med PUB-avtal
- För förvaltningens talan i GDPR-frågor

5. Laglig behandling av personuppgifter

I enlighet med artikel 6 i dataskyddsförordningen får personuppgifter endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden ska fastställas innan behandling påbörjas enligt någon av nedan punkter:

- Samtycke – *ska vara informerat, frivilligt och specifikt samt kunna uppvisas.*
- Behandlingen är nödvändig för att fullgöra ett avtal.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har.
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person.
- Behandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

All behandling av personuppgifter ska dokumenteras i enlighet med dataskyddsförordningen. Ansvarsskyldigheten är en grundläggande princip vilken ställer krav på att den personuppgiftsansvarige ska kunna visa att krav och principer följs och på vilket sätt detta görs.

Innan behandling av personuppgifter påbörjas krävs följande:

1. Dokumentera ändamål/syfte med behandlingen samt under hur lång tid behandlingen beräknas pågå,
2. Fastställ rättslig grund,
3. Inhämta samtycke vid behov (används enbart i undantagsfall),
4. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna i artikel 5 GDPR, kommunens dataskyddspolicy samt denna riktlinje,
5. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomför en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen,
6. Om riskanalys visar att behandlingen kan leda till en hög risk för de registrerade ska en konsekvensbedömning genomföras och

dokumenteras. Rådgör med dataskyddsombudet vid konsekvensbedömningen,
7. Samråd med tillsynsmyndighet om hög risk inte kan åtgärdas inför behandling av personuppgifter,
8. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från riskanalys och konsekvensbedömning,
9. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändigt,
10. Upprätta personuppgiftsbiträdesavtal vid behov,
11. Anteckna ny behandling av personuppgifter i nämndens registerförteckning.

6. Registerförteckning

Varje nämns ska löpande föra ett samlat register över verksamhetens pågående personuppgiftsbehandlingar. Registret ska förvaras i kommunens diariesystem Public 360, och ska fastställas årligen av nämnden.

Som utgångspunkt kan Mall för registerförteckning med fördel användas.

7. Konsekvensbedömning

Enligt GDPR ska en konsekvensbedömning göras om en viss personuppgiftsbehandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.

Konsekvensbedömningar handlar om att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Målet är att minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för enskilda personers fri- och rättigheter samt göra en bedömning om behovet av behandlingen och det intrång den utgör står i proportion till syftet.

Det åligger varje medarbetare att genomföra en konsekvensbedömning i det fall det är nödvändigt. Exempel på när det är aktuellt är bl.a. vid inköp av nya system eller vid införande av kameraövervakning eller automatiserade beslut. För genomförande av konsekvensbedömning ska kommunens Mall för konsekvensbedömning användas. I mallen finns utvärderingsfrågor som hjälper medarbetaren att avgöra om en konsekvensbedömning är nödvändig. Konsekvensbedömningen ska vara väldokumenterad och eventuella risker ska hanteras och följas upp av ansvarig chef eller den som chef delegerat till. Vid genomförande av konsekvensbedömning ska kommunens dataskyddsombud involveras.

Vid planerat inköp av nytt system ska en konsekvensbedömning alltid genomföras innan upphandling. Även en informationsklassificering av den planerade informationshanteringen måste göras innan upphandling, för att få fram lämpliga säkerhetskrav. Informationsklassificering genomförs i KLASSA. Upphandlingsenheten ska ha rutiner på plats för att kontrollera att verksamheten har genomfört dessa åtgärder innan en upphandling får annonseras.

8. Personuppgiftsincident

I dataskyddsförordningen definieras en personuppgiftsincident som "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".

Alla organisationer är enligt dataskyddsförordningen skyldiga att ha rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Varje förvaltning ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten.

8.1 Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har:

- blivit förstörda.
- gått förlorade på annat sätt.
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter. En personuppgiftsincident kan få allvarliga konsekvenser för registrerade personerna. De kan råka ut för till exempel ekonomisk skada eller kränkning av sina friheter och rättigheter.

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan också påverka tilltron till den organisation som behandlar personuppgifter. Bristande hantering av personuppgiftsincidenter kan också leda till sanktionsavgifter.

8.2 Vad ska du göra?

Varje anställd och förtroendevald har ett ansvar att rapportera personuppgiftsincidenter under följande förutsättningar

- Anställd/förtroendevald **vet** att en incident har inträffat
- Anställd/förtroendevald **misstänker** att en incident har inträffat
- Anställd/förtroendevald ser en **risk** för att en incident ska inträffa

Om du upptäcker eller misstänker en personuppgiftsincident så ska du rapportera detta omedelbart. På Botwebb finns information om hur du gör: Rapportera personuppgiftsincident - Botwebb (botkyrka.se). Tänk på att ange så utförlig information som möjligt om incidenten. Observera även att detta ska ske mycket skyndsamt.

Inskickad rapport ska levereras till förvaltningens dataskyddsombud som kontaktar ansvarig chef för incidenten. Ansvarig chef för incidenten är enhets- avdelnings- eller verksamhetschef där incidenten har inträffat. Dataskyddsombudet lämnar en rekommendation till chefen som ska besluta om incidenten ska anmälas till tillsynsmyndighet eller inte. En sådan anmälan ska göras till IMY inom 72 timmar från att incidenten upptäcktes.

Rapport, beslut och eventuell anmälan till tillsynsmyndighet ska diarieföras i Public 360.

9. Personuppgiftsbiträdesavtal

Varje nämnd ska teckna personuppgiftsbiträdesavtal (PUB-avtal) när denne uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter för nämndens räkning.

Vem som kan teckna personuppgiftsbiträdes avtal ska framgå av förvaltningens delegationsordning.

Personuppgiftsbiträdets (biträdet) behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige.

I avtalet ska anges:

- Vem som är personuppgiftsansvarig respektive personuppgiftsbiträde.
- Vad behandlingen avser, dess varaktighet, art, ändamål, typ av personuppgifter samt kategori av registrerade.
- Den ansvariges skyldigheter och rättigheter.
- Att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion.
- Att biträdet iakttar nödvändig konfidentialitet och tystnadsplikt.
- Att biträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa adekvat skydd för personuppgifterna samt att detta kan visas genom att ge ansvarige tillgång till vederbörlig information.
- Att biträdet ska bistå den ansvarige i att uppfylla sina förpliktelser enligt förordningen.
- Att biträdet inte får anlita underleverantör för behandling av den ansvariges personuppgifter utan den ansvariges skriftliga medgivande till detta. Om biträdet anlitar underleverantör ska personuppgiftsbiträdesavtal upprättas även mellan dessa parter.
- Att överföring till tredje land inte får ske utan att adekvata säkerhetsåtgärder är uppfyllda.
- Reglering om inom vilken tid radering eller överflyttning av personuppgifter sker vid avtalets upphörande.

I Botkyrka kommun är huvudregeln att SKR:s framtagna standardavtal (personuppgiftsbiträdesavtal) ska användas. Annan typ av biträdesavtal får endast användas efter godkännande från ansvarig chef.

10. De registrerades rättigheter

10.1 Information till allmänheten

GDPR syftar bland annat till att skydda fysiska personer med avseende på behandling av personuppgifter. Därför är det viktigt att Botkyrka kommun visar allmänheten att kommunen följer GDPR och hänvisar till platser där ytterligare information finns att hämta. Detta sker på kommunens hemsida där kommunen ger information om hur kommunen behandlar personuppgifter. Där ska också kontaktuppgifter till dataskyddsombuden publiceras. I kommunens utgående mail och svarsmail ska följande text finnas:

”Personuppgifter hanteras enligt dataskyddsförordningen (GDPR), läs mer på Hantering av personuppgifter - Botkyrka kommun.

E-post som kommer till Botkyrka kommun blir allmän handling enligt offentlighetsprincipen.”

10.2 Tillgång, rättelse, radering och begränsning

Varje förvaltning ska ha kapacitet att hantera begäranden från registrerade om att utöva sina rättigheter. I de fall kommunövergripande rutiner saknas ska förvaltningarna ha egna rutiner för att hantera begäranden som avser:

- Få tillgång till information om dennes personuppgifter (registerutdrag),
- Rätta eller komplettera sina uppgifter,
- Radera sina uppgifter,
- Begränsa behandlingen av sina uppgifter,
- Invända mot automatiserade beslut,
- Utnyttja möjligheten till dataportabilitet om sådan möjlighet finns.

Det ska av respektive nämnds delegationsordning framgå vem som äger rätt att fatta beslut enligt dataskyddsförordningen och tillämplig nationell dataskyddslagstiftning.