VAXHOLMS STAD

Riktlinje för dataskydd och hantering av personuppgifter i Vaxholms stad

Antagen av kommunstyrelsen 2020-10-29 §150

Giltighetsperiod: Tillsvidare
För revidering och uppföljning ansvarar: Kansli- och servicechef

Post: 185 83 Vaxholm
Besök: Eriksövägen 27
Telefon: 08-541 708 00
Fax: 08-541 708 57
E-post: kansliet@vaxholm.se
Webb: www.vaxholm.se
Org nr: 212000-2908
Bankgiro: 5302-9435

Innehåll

Dokumenthierarki 4
Inledning 4
Syfte 4
Dokumentet gäller för 4
Nämndernas ansvar 4
Särskilt om kommunstyrelsen 5
Laglig behandling av personuppgifter 5
Ansvarsfördelning och organisation 6
Innebörd av personuppgiftsansvar 6
Personuppgiftsbiträde 7
Dataskyddsombud 7
Förvaltningschef 8
Dataskyddssamordnare 8
Dataskyddsnätverk 9
Personuppgiftsincident 9
Incidentrapportering 9
Vad är en personuppgiftsincident? 9
Vad ska rapporteras? 10
Anmälan inom 72 timmar 10
Registrering 10
Vem ska anmäla incidenten? 10
Anmälan till Datainspektionen 10
Information till registrerade personer 11
Information dataskyddsombud 11
Information personuppgiftsansvarig 11
Övriga riktlinjer 11
Särskilt vid inköp och upphandling 11
Konsekvensbedömning avseende dataskydd 11
Säkerhet i samband med behandling av personuppgifter 12
Kontroll över personuppgiftsbehandlingar 12
Register över personuppgiftsbehandlingar 13
Personuppgiftsbiträdesavtal 13
De registrerades rättigheter 13
Information till allmänheten 13

Tillgång, rättelse, radering och begränsning 14
Bilaga 1 15
Begreppsförklaringar 15
Behandling av personuppgift 15
Den registrerade 15
Känsliga personuppgifter 15
Personuppgift 15
Personuppgiftsansvarig 15
Personuppgiftsbiträde 15
Personuppgiftsbiträdesavtal 15
Samtycke 15

Dokumenthierarki

I enlighet med antaget dokument ”Struktur för kommungemensamma styrande och stödjande dokument i Vaxholms stad” ska kommunstyrelsen fastställa kommunövergripande riktlinjer. Riktlinjer är en detaljerad vägledning och anger ramarna för handlingsutrymme inom ett visst område. Riktlinjer ger vägledning för att följa övergripande styrdokument (se dataskyddspolicy för Vaxholms stad).

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 (Datainspektionen) att i vissa fall döma ut en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter.

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

Syfte

Riktlinjens syfte är dels att Vaxholms stad hanterar personuppgifter på ett lagenligt sätt men också 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 Vaxholms stad. Denna riktlinje gäller för stadens samtliga nämnder. Det åvilar dock respektive nämnd/förvaltning att ta fram verksamhetsspecifika rutiner och mallar som komplement till denna riktlinje då detta är nödvändigt.

Dokumentet gäller för

Vaxholms stads nämnder, förvaltningar, verksamheter, bolag och medarbetare. I tillämpbara fall även för andra som hanterar personuppgifter i organisationer där Vaxholms stad har det rättsligt bestämmande inflytandet (tex styrelser, bolag, privata utförare, inhyrd personal eller andra aktörer som hanterar personuppgifter för Vaxholms stads räkning).

Nämndernas ansvar

Av det nämndgemensamma reglementet framgår att varje nämnd i Vaxholms stad är personuppgiftsansvarig för behandlingen av personuppgifter inom sitt verksamhetsområde. Detsamma gäller även stadens helägda bolag. 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.
- Utse dataskyddsombud och svara för att denne har förutsättningar och den kunskap som krävs för att fullgöra sitt uppdrag.
- 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 samt verifierande tester.
- Att riskanalyser finns och är dokumenterade.
- Säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet.
- Säkerställa att personuppgiftsincidenter rapporteras till tillsynsmyndigheten (Datainspektionen).
- Tillgodose registrerades rättigheter gällande information, tillgång (registerutdrag), rättning, begränsning, dataportabilitet och invändning.
- Föra register över behandlingar av personuppgifter i Vaxholms stads kommungemensamma registerverktyg (Draftit).

Särskilt om kommunstyrelsen

Kommunstyrelsen har ett ansvar för att leda, samordna och ha uppsikt över stadens 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 för att säkerställa att staden hanterar personuppgifter på ett lagenligt sätt.

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 visas.
- 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. Dokumentation av ändamål och syfte samt under hur lång tid behandlingen beräknas pågå.
2. Fastställ rättslig grund.
3. Inhämta samtycke vid behov.
4. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna i artikel 5, Vaxholms stads dataskyddspolicy samt denna riktlinje.
5. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomföra en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen.
6. Rådgör med dataskyddsombudet vid konsekvensbedömningar av behandling av personuppgifter som kan leda till en hög risk för de registrerade.
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.
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 kommunens registerverktyg (Draftit).

Ansvarsfördelning och organisation

Dataskyddsförordningen kräver ett tydligt fastställande om vem som bär ansvar. Vaxholms stad har med dessa riktlinjer fördelat ansvar och preciserat uppgiftsfördelning för att behandling av personuppgifter ska uppnå rättssäkerhet. Det lagstadgade kravet på ansvarsfördelning är att det ska finnas personuppgiftsansvariga, personuppgiftsbiträden och dataskyddsombud. Vaxholms stad utökar detta med ansvar för förvaltningschef och uppgifter för dataskyddssamordnare. Det ska också finnas ett internt dataskyddsnätverk. I Vaxholms stad är varje nämnd, revisorerna och kommunstyrelsen personuppgiftsansvariga och i vissa fall personuppgiftsbiträden. Personuppgiftsbiträdesavtal (PUB-avtal) tecknas med aktörer utanför kommunens organisation. Varje personuppgiftsansvarig har ett dataskyddsombud. Varje förvaltning har en eller flera dataskyddssamordnare

Innebörd av personuppgiftsansvar

Personuppgiftsansvaret innebär att ta ansvar för att alla personuppgiftsbehandlingar sker enligt bestämmelser i GDPR. Respektive personuppgiftsansvarig ansvarar för att ha kännedom om i vilka system/register som personuppgifter förekommer samt att upprätta och hålla ett aktuellt register över dessa system och tillhörande personuppgiftsbiträdesavtal (PUB-avtal). Personuppgiftsansvarig ansvarar också för att det finns aktuell förteckning över personuppgiftsbehandlingar (i Draftit) och incidenter (i Evolution/Castor). Personuppgiftsansvarig ska säkerställa att dataskyddsombudet i god tid och på ett korrekt sätt deltar i alla frågor som rör skydd av personuppgifter. Det åligger varje personuppgiftsansvarig att ha rutiner för hantering av personuppgifter och, vid behov, kunna visa

hur personuppgiftsansvaret utövas. För att kunna utöva ansvaret på ett effektivt sätt ges personuppgiftsansvariga stöd i form av dataskyddssamordnare.

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. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige. Det åligger varje personuppgiftsansvarig att följa den mall för personuppgiftsbiträdesavtal som är beslutad (företrädelsevis SKR:s standardmall) av respektive personuppgiftsansvarig samt att hålla ett aktuellt register över personuppgiftsbiträden.

Dataskyddsombud

Dataskyddsombudet har en revisorsliknande och rådgivande funktion vars uppgifter framgår tydligt i dataskyddsförordningen.

Dataskyddsombudet 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.
- Upprätthålla ombudets sakkunskap.
- 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 förvaltningarnas ledningsgrupper samt den kommunövergripande ledningsgruppen som leds av kommunchefen. Den personuppgiftsansvarige bör av detta skäl meddela dataskyddsombud om sammankomster som avhandlar data och integritetsskydd eller alternativt informationssäkerhetsaspekter.

Förvaltningsledningarna ska säkerställa att dataskyddsombudet involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling av personuppgifter kan komma ifråga.

Dataskyddsombudet ska årligen redovisa för de personuppgiftsansvariga nämnderna det arbete som verksamheten gör gällande efterlevnaden av dataskyddsdirektivet, nationell dataskyddslagstiftning och lokala styrdokument. Av den årliga redovisningen ska det minst framgå:

- Vilka interna och externa utbildningsåtgärder som förvaltningen genomfört på området.
- Vid vilka ledningsgruppsmöten som dataskyddsombudet har beretts tillfälle närvara vid för att avlägga rapport över förvaltningens hantering av personuppgifter.
- Dataskyddsombudets granskningar
- Personuppgiftsincidenter.
- Övriga iakttagelser.

Det innebär att dataskyddsombudet: samlar in information om hur Vaxholms stad som helhet behandlar personuppgifter, kontrollerar att kommunen som helhet följer GDPR, rutiner och andra interna styrdokument som berör hantering av personuppgifter, sammanställer resultat av granskningen i en rapport, kommunicerar granskningsrapporten med respektive personuppgiftsansvarig, redovisar granskningsrapporten för kommunstyrelsen.

Dataskyddsombudet har inget eget ansvar för att Vaxholms stad följer GDPR. Det ansvaret ligger alltid hos den personuppgiftsansvariga. GDPR preciserar dataskyddombudets uppgifter. Vad avser uppgifter har Vaxholms stad ett tillägg till dataskyddsombudets arbetsuppgifter i form av att vara sammankallande för Vaxholms stads interna dataskyddsnätverk där dataskyddsamordnare från respektive förvaltning deltar.

Förvaltningschef

Förvaltningschef är ansvarig för att förse personuppgiftsansvarig och personuppgiftsbiträden med administrativt, tekniskt och organisatoriskt stöd. Förvaltningschef utser (via delegering från nämnden) dataskyddsombud samt tillser att förvaltningen har minst en dataskyddssamordnare som stöd för personuppgiftsansvariga.

Dataskyddssamordnare

Dataskyddssamordnares ansvar och uppgifter framgår inte av GDPR. I Vaxholms stad ger dataskyddssamordnaren stöd till personuppgiftsansvarig. Dataskyddsamordnare inom förvaltningen ska fungera som förvaltningens kontaktperson för dataskyddsfrågor med uppgift att fungera som en länk mellan förvaltningens verksamheter och dataskyddsombudet gällande dataskyddsfrågor. Dataskyddsamordnare har vidare följande uppgifter:

- upprätta och á jourhålla de register och andra dokument som personuppgiftsansvarig behöver för att kunna utöva sitt ansvar,
- handlägga alternativt bistå annan handläggare vid begäran om registerutdrag inkommen till förvaltningen,
- registrera samt samordna registrering av pågående behandlingar i registerförteckningen (i Draftit) och löpande följa upp att den verksamhet man representerar har ett ifyllt register över behandlingar,
- ge råd och stöd till verksamhetens ledning och berörd personal i frågor rörande behandling av personuppgifter,

- stödja verksamheten i frågor som gäller information till registrerade, stödja vid upprättande av skriftliga avtal med personuppgiftsbiträden, omvärldsbevaka området för behandling av personuppgifter,
- rådfråga och samråda med dataskyddsombud,
- bidra till utvecklingen av gemensamma rutiner och arbetssätt för att uppfylla dataskyddslagstiftningen,
- följa rutinerna för incidentrapportering

Dataskyddsnätverk

Vaxholms stad har ett internt dataskyddsnätverk. Nätverket är en kontaktyta för dataskyddssamordnare och dataskyddsombud. Deltagarna i dataskyddsnätverket ska vara:

- Dataskyddsombud (sammankallande)
- Dataskyddssamordnare

Nätverket syftar till erfarenhetsutbyte och utvecklingsinsatser för personuppgiftshantering.

Personuppgiftsincident

Incidentrapportering

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. (Se Vaxholms stads process för personuppgiftsincident)

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

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.

Vad ska rapporteras?

Samtliga personuppgiftsincidenter ska rapporteras till dataskyddsombudet.

När det har inträffat en personuppgiftsincident måste förvaltningen först fastställa sannolikheten och allvaret, och den därmed följande risken för människors rättigheter och friheter, d v s vilka konsekvenser personuppgiftsincidenten kan leda till.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre. Förvaltningen är skyldig att begränsa skadorna för de registrerade så fort som möjligt.

Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste förvaltningen anmäla detta till Datainspektionen. Men om det är osannolikt att en personuppgiftsincident medför risker behöver förvaltningen inte meddela Datainspektionen.

Se ytterligare information i Rutin för hantering av personuppgiftsincident.

Anmälan inom 72 timmar

Anmälan ska göras till Datainspektionen inom 72 timmar från det att personuppgiftsincidenten upptäcktes. Skickas anmälan in senare än så ska förseningen motiveras. Rapportering till Datainspektionen behöver emellertid inte göras om det är osannolikt att incidenten kan komma att medföra en risk för de registrerades grundläggande fri- och rättigheter. Vid osäkerhet rådfråga Dataskyddsombudet.

Registrering

Alla personuppgiftsincidenter ska registreras i kommunens ärendehanteringssystem, Evolution/Castor (dvs även incidenter som inte anmäls till Datainspektionen). Förslagsvis används Datainspektionens anmälningsblankett som finns att hämta på intranätet eller Datainspektionens hemsida.

Vem ska anmäla incidenten?

Anmälan görs av chef hos den personuppgiftsansvariges verksamhet, det vill säga den nämnd som bestämmer ändamål och medel för behandlingen. Men det finns också en skyldighet för den som har anlitats som personuppgiftsbiträde att uppmärksamma den personuppgiftsansvarige på en säkerhetsincident så fort den upptäckts.

Anmälan till Datainspektionen

Personuppgiftsincidenter anmäls genom Datainspektionens e-tjänst ”Anmälan om personuppgiftsincident”. E-tjänsten återfinns på Datainspektionens hemsida.

Information till registrerade personer

Om personuppgiftsincidenten är allvarlig så ska förvaltningen utan onödigt dröjsmål även informera de registrerade om personuppgiftsincidenten. Detta gäller alltså om det är sannolikt att personuppgiftsincidenten leder till en hög risk för fysiska personers rättigheter och friheter.

Följande punkter är ett minimikrav när information ska ges till registrerade utifrån en inträffad personuppgiftsincident:

- Orsaken till personuppgiftsincidenten klart och tydligt.
- Namn och kontaktuppgifter till dataskyddsombudet.
- De sannolika konsekvenserna av personuppgiftsincidenten.
- Vilka åtgärder förvaltningen gjort och/eller tänker göra, för att hantera personuppgiftsincidenten.
- I förkommande fall: Beskriv vad förvaltningen har gjort för att mildra eventuella negativa effekter.

Information dataskyddsombud

Dataskyddsombud ska alltid informeras om uppstådda personuppgiftsincidenter.

Information personuppgiftsansvarig

Ansvarig nämnd ska informeras vid nästkommande sammanträde, alternativt vid större incidenter via ordföranden. Förvaltningschef beslutar om vilken information som ska lämnas vid respektive tillfälle.

Övriga riktlinjer

Särskilt vid inköp och upphandling

Vid inköp och upphandlingar (av produkter och tjänster) ska särskilt utredas om användandet av det som inköpet avser eller annars som en följd av avtalsrelationen kan komma att leda till behandling av personuppgifter. Förvaltningarna ska ha en rutin för under vilka förutsättningar dataskyddsombudet ska engageras vid inköp och upphandlingar och när under inköpsprocessen som denne bör kontaktas.

Vid inköp och upphandlingar av produkter och tjänster som kan komma att leda till behandling av personuppgifter ska krav ställas på att all utrustning lever upp till kraven i dataskyddsförordningen och annan lagstiftning inom dataskyddsområdet.

Vid utredning av vilka tekniska säkerhetskrav som bör ställas ska, vid behov, samråd ske med IT-enheten.

Konsekvensbedömning avseende dataskydd

En konsekvensbedömning ska enligt dataskyddsförordningen 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.

Som stöd för genomförande av konsekvensbedömningar i Vaxholms stad finns en egen modul i kommunens gemensamma system för hantering av personuppgiftsbehandlingar (Draftit). Vid genomförande av konsekvensbedömning ska kommunens dataskyddsombud involveras, och vid behov förvaltningens dataskyddsamordnare.

Säkerhet i samband med behandling av personuppgifter

Varje nämnd ansvarar för att en fullgod säkerhetsnivå upprätthålls vid behandling av personuppgifter. Förvaltningarna ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå utifrån de kriterier som anges i dataskyddsförordningen.

Säkerhet utgörs av:

- Inbyggt dataskydd och dataskydd som standard vilket för personuppgiftshanteringen bl.a. innebär:
    - Att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder.
    - Säkerställa att säkerhetsåtgärder i enlighet med informationsklassningens åtgärdsplan vidtas.
    - Om möjligt använda åtgärder som pseudonymisering, anonymisering eller kryptering.
    - Säkerställa särskilda personuppgifters konfidentialitet och riktighet genom att bl.a. använda kryptering samt stark autentisering.
    - Använda åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsmimimering och åtkomstbegränsning.
- Införande och tillämpning av rutiner för att:
    - Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder.
    - Vid behov kunna ge incidentinformation till berörda registrerade.
    - Vid behov kunna involvera och rådgöra med dataskyddsombudet.

För frågor som gäller tekniska åtgärder gällande IT-verksamhet ansvarar IT-enheten.

Vid planering av verksamheten ska särskild hänsyn tas till att personuppgifter inte behandlas i högre utsträckning eller under längre tid än vad som är nödvändigt. Anställda som på något sätt kan komma att behandla personuppgifter i sitt arbete ska genomgå utbildning för att säkra att personuppgifter hanteras på ett lagligt och respektfullt sätt.

Kontroll över personuppgiftsbehandlingar

Nämnderna ansvarar för att av de personuppgifter som behandlas inom ramen för dess verksamhet sker på ett lagenligt sätt.

Register över personuppgiftsbehandlingar
Varje nämnd ska löpande föra ett register över vilka personuppgifter som behandlas i den egna verksamheteten i de kommungemensamma registersystemet (Draftit).

Registret ska föras utifrån instruktioner från kommunledningskontoret, kansli- och serviceenheten.

Personuppgiftsbiträdesavtal

Varje nämnd ska teckna personuppgiftsbiträdesavtal när denne uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter för nämndens räkning. Vem som får underteckna personuppgiftsbiträdesavtalet ska framgå av nämndens delegationsordning.

Förvaltningarna ska föra en förteckning över aktuella personuppgiftsbiträdesavtal och därtill hörande underbiträdesavtal.

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

De registrerades rättigheter

Information till allmänheten

GDPR syftar bl a till att skydda fysiska personer med avseende på behandling av personuppgifter. Därför är det viktigt att Vaxholms stad visar allmänheten att kommunen följer GDPR och hänvisar till platser där ytterligare information finns att hämta. Detta sker på kommunens hemsida där Vaxholms stad ger information om hur kommunen behandlar personuppgifter. Där ska också kontaktuppgifter till dataskyddsombud publiceras. I kommunens utgående mail och svarsmail ska

följande text finnas:
”*Vaxholms stad hanterar dina personuppgifter i enlighet med dataskyddslagstiftningen.För mer information, besök www.vaxholm.se/gdpr*”

Tillgång, rättelse, radering och begränsning

Varje förvaltning ska ha rutiner för hantering av begäranden från registrerade om att utöva sina rättigheter att:

- Få tillgång till information om dennes personuppgifter (rgisterutdrag)
- Rätta eller komplettera sina uppgifter.
- Radera sina uppgifter.
- Begränsa behandlingen av sina uppgifter.
- 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.

Övergripande kommungemensamma rutiner ska i så stor utsträckning som möjligt tas fram.

Bilaga 1

Begreppsförklaringar

Behandling av personuppgift

Behandling av personuppgift omfattar varje åtgärd som vidtas i fråga om personuppgifter. Begreppet är teknikneutralt vilket innebär att det kan handla om manuell eller automatiserad/datoriserad behandling. Det kan enligt lagen vara fråga om insamling, registrering, organisering, lagring, bearbetning eller ändring, utlämnande, utplåning eller förstöring, sammanställning eller samkörning etc.

Den registrerade

Den registrerade är den person som en personuppgift avser.

Känsliga personuppgifter

Känsliga personuppgifter är uppgifter som behöver särskilt skydd vilka betecknas som särskilda kategorier av personuppgifter i lagtexten. *Detta är exempelvis personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.*

Personuppgift

Personuppgift är all slags information som direkt eller indirekt kan hänföras till fysisk person som är i livet. Det kan även uttryckas som att en person är identifierbar eller sökbar utifrån de uppgifter som förs.

Personuppgiftsansvarig

Personuppgiftsansvarig är den som bestämmer ändamålen med och/eller medlen för behandling av personuppgifter, dvs. kommunstyrelsen och ansvariga nämnder i egenskap av självständiga förvaltningsmyndigheter. Personuppgiftsansvaret kan aldrig överlåtas.

Personuppgiftsbiträde

Personuppgiftsbiträde avses såväl en fysisk som juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. De biträden som anlitas ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Personuppgiftsbiträdesavtal

När personuppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett personuppgiftsbiträdesavtal.

Samtycke

Samtycke måste vara en fråga om frivillig, specifik och otvetydig viljeyttring genom den registrerade, efter att ha fått information, godtar behandling av den registrerades personuppgifter. Den registrerade kan när som helst återkalla sitt samtycke vartefter behandling inte vidare kan ske.