



LANDSKRONA
STAD

Beslutas av: Kommunstyrelsen **Datum:** 2022-01-13

Dokumentet gäller för: Landskrona stad

Dokumentansvarig: Stadsledningsförvaltningen, juridiska
avdelningen

Revideras: Vid behov

Diarienummer: KS 2021/3400

Riktlinjer för personuppgifts- behandling

Riktlinje



Innehåll

1. Viktiga begrepp	4
1.1 Personuppgift och registrerad	4
1.2 Känsliga personuppgifter och andra kategorier av personuppgifter	4
1.3 Dataskyddsförordningen och dataskyddslagstiftning	5
1.4 Personuppgiftsbehandling och personuppgiftsincident	5
1.5 Personuppgiftsansvarig	5
1.6 Personuppgiftsbiträde och personuppgiftsavtal	6
1.7 Dataskyddsombud och dataskyddssamordnare	6
1.8 Inbyggt dataskydd och dataskydd som standard	6
1.9 Tredjelandsoverföring	6
2. Ansvar och organisation	7
2.1 Personuppgiftsansvarig	7
2.2 Dataskyddsombudets roll	8
2.3 Dataskyddssamordnarens roll	8
3. Rättsliga grunder för behandling	9
3.1 De olika rättsliga grunderna	9
3.2 Om behandlingen rör känsliga personuppgifter	11
4. Grundläggande principer vid personuppgiftsbehandling	12
4.1 Laglighet, korrekthet och öppenhet	12
4.2 Ändamålsbegränsning	12
4.3 Uppgiftsminimering	12
4.4 Riktighet	12
4.5 Lagringsminimering	13
4.6 Integritet och konfidentialitet	13
4.7 Ansvarsskyldighet	13
5. Process vid ny personuppgiftsbehandling	13
5.1 Riskanalys och konsekvensbedömning	13
5.2 Registerförteckning	14
5.3 Tekniska system och lagring	14
5.4 Tredjelandsoverföring	15

5.5 Personuppgiftsbiträdesavtal	15
5.6 Om personuppgiftsincident inträffar	16
6. Den registrerades rättigheter	16
6.1 Rätt till information	16
6.2 Rätt till registerutdrag	17
6.3 Rätt till rättelse	17
6.4 Rätt till radering	18
6.5 Rätt att invända eller begränsa personuppgiftsbehandling	19
6.6 Rättighet vid automatiserade beslut	19
6.7 Rätt att klaga	19
7. Rensning och gallring	20
8. Informationssäkerhet och dataskydd	20
9. Personuppgifter i e-post och sociala medier	20
10. Personuppgifter i fritextfält	21
11. Relevanta styrdokument	21

1. Viktiga begrepp

1.1 Personuppgift och registrerad

Med begreppet personuppgift menas det alla uppgifter direkta eller indirekta som kan knytas till en levande fysisk person.

Den registrerade är den fysiska personen vars personuppgifter ämnas att behandlas.

1.2 Känsliga personuppgifter och andra kategorier av personuppgifter

1.2.1 Känsliga personuppgifter

Känsliga personuppgifter utgör sådana personuppgifter som anses vara av sin natur ytterst känsliga för en individ och har därför ett starkare skydd än det som gäller för behandling av andra ”vanliga” personuppgifter. Det är som huvudregel förbjudet att behandla känsliga personuppgifter. Den typ av personuppgift som kan anses vara är känslig är uppgift om:

- Ras eller etniskt ursprung.
- Biometriska uppgifter som används för att entydigt identifiera en person. Ett exempel på en biometrisk uppgift är fingeravtryck. Fotografi kan utgöra denna typ av uppgift om det behandlas med ansiktsgenkänningsprogram.
- Genetiska uppgifter.
- Sexualliv eller sexuell läggning.
- Hälsa.
- Medlemskap i fackförening.
- Politiska åsikter.
- Religiös eller filosofisk övertygelse.

1.2.2 Integritetskänsliga personuppgifter

Utöver ”vanliga” och känsliga personuppgifter finns det också de som kan kallas integritetskänsliga. Dessa är personuppgifter som anses var särskilt skyddsvärda. De ställer därmed ett högre säkerhetskrav vid sin behandling men är till skillnad från känsliga uppgifter inte som huvudregel förbjudna att behandla. Denna typ av integritetskänsliga personuppgifter har dock en stor verkan vid bedömningen av en personuppgiftsincident eller på en konsekvensbedömning. Exempel på dessa integritetskänsliga personuppgifter kan vara:

- löneuppgifter

- uppgifter om lagöverträdelse
- värderande uppgifter, såsom från utvecklingssamtal eller personlighetstester
- information som rör en registrerads personliga sfär
- uppgifter om den registrerades sociala förhållanden.

1.3 Dataskyddsförordningen och dataskyddslagstiftning

Dataskyddsförordningen (GDPR) är den europeiska förordning som ligger till grund för stora delar av den lagstiftning som rör personuppgiftsbehandling. Dess fullständiga namn är: Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

När det talas om dataskyddslagstiftning i denna text så syftas det på dataskyddsförordningen samt annan lagstiftning som påverkar personuppgiftsbehandling. Ett exempel på sådan lagstiftning går att finna i, lag med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218).

1.4 Personuppgiftsbehandling och personuppgiftsincident

Personuppgiftsbehandling (behandling) syftar på när en åtgärd genomförs där personuppgifter används eller beträffas. Det utgör en behandling av personuppgifter oavsett om det är automatiserat eller ej. Även vissa slagbara manuella pappersregister kan utgöra personuppgiftsbehandling som omfattas av dataskyddslagstiftningen.

En personuppgiftsincident inträffar när en säkerhetsincident leder till en brytning av konfidentialiteten, tillgängligheten eller integriteten av de personuppgifter som behandlas. Ett exempel på en sådan säkerhetsincident är när personuppgifter förstörs oavsett om det är avsiktligt eller ej. Om en personuppgiftsincident kan anses som allvarlig ska den anmälas till tillsynsmyndigheten inom 72 timmar från incidenteten. I Sverige agerar Integritetskyddsmyndigheten som tillsynsmyndighet.

1.5 Personuppgiftsansvarig

En personuppgiftsansvarig (PUA) är den fysiska personen, juridiska personen, myndighet, institutionen eller annat organ som bestämmer för vilka ändamål och hur personuppgifterna ska behandlas. I Landskrona stad är varje nämnd,

kommunstyrelsen och kommunfullmäktige personuppgiftsansvarig när de behandlar personuppgifter.

1.6 Personuppgiftsbiträde och personuppgiftsavtal

Ett personuppgiftsbiträde är den som utför behandling av personuppgifter på den personuppgiftsansvarigas vägnar.

Med personuppgiftsavtal menas det avtal som en personuppgiftsansvarig ska säkerställa existerar mellan den och ett personuppgiftsbiträde där omfattningen och andra instruktioner av behandlingen detaljeras.

1.7 Dataskyddsombud och dataskyddssamordnare

Dataskyddsombud är en fysisk eller juridisk person som har utsetts av personuppgiftsansvarig för att kontrollera att dataskyddsförordningen följs av den personuppgiftsansvariga. Detta kan göras genom exempelvis informationsinsatser och kontroller. Den agerar även som kontaktpunkt för personuppgiftsbehandlingen. Dataskyddsombuds position gäller för all personuppgiftsbehandling gjort av personuppgiftsansvarig eller dess biträde. För Landskrona stad utgör Security Solution AB dataskyddsombud.

Dataskyddssamordnare är en person inom den egna organisation eller nämnden som sammanställer och lämnar vissa råd gällande behandlingen av personuppgifter. Agerar inom Landskrona stad som stöd för den personuppgiftsansvariga i frågor gällande personuppgiftsbehandling. Inte att likställa med dataskyddsombud. Denna roll måste finnas inom den egna organisationen enligt policy för personuppgiftsbehandling i Landskrona stad.

1.8 Inbyggt dataskydd och dataskydd som standard

Principen om inbyggt dataskydd innebär att vid skapandet av system och rutiner tar i åtanke integritetskyddsreglerna som gäller. Även kallat Privacy by Design. Exempel på sådana åtgärder är kryptering och pseudonymisering av personuppgifter.

Principen dataskydd som standard syftar på att den som behandlar personuppgifter ska säkerställa att de håller den säkerhet som behövs och inte samlar in uppgifter i onödan. Exempel kan vara att förvalda inställningar i en tjänst inte samlar in mer personuppgifter än absolut nödvändigt för tjänsten. Även kallat Privacy by Default.

1.9 Tredjelandsoverföring

När det talas om en tredjelandsoverföring så syftas det till när en överföring av personuppgifter sker till ett land utanför EU/EES. Detta kan ske om uppgifter

lagras i en molntjänst vars infrastruktur tex server är belägna utanför EU/EES. Eller om någon utanför EU/EES får tillgång till personuppgifter lagrade inom EU/EES. Att publicera på internet är inte automatiskt en tredjelandsoverföring.

2. Ansvar och organisation

2.1 Personuppgiftsansvarig

Varje nämnd och styrelse är personuppgiftsansvarig för all personuppgiftsbehandling i sin verksamhet. Ansvaret gäller för all behandling av personuppgifter såsom anställningsuppgifter eller kontaktnummer till förtroendevalda. Ansvaret kvarstår även vid sådan personuppgiftsbehandling som sker för stadens räkning via ett personuppgiftsbiträde (PuB), oftast en leverantör.

Personuppgiftsansvaret är omfattande och följande lista tjänar som vägledning för vad som ingår. Listan är ej uttömmande. Personuppgiftsansvarig svarar för att:

- Rådande lagstiftning som omfattar personuppgiftsbehandling följs.
- Upprätthålla förteckning över samtliga processer/behandlingar av personuppgifter inklusive system och kataloger/lagringsytor där personuppgifter lagras och behandlas.
- Utse och anmäla dataskyddsombud, stödja ombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens.
- Försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning.
- Säkerställa att medarbetarna har nödvändig kompetens för att kunna följa personuppgiftslagstiftningen.
- Säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning.
- Säkerställa att det finns ett register över den behandling som sker. Registret ska bland annat innehålla information om ändamålet med behandlingen samt de olika kategorierna av personuppgifter och registrerade. Exempel på behandling som ska registreras är om det skapas en lista i ett word-dokument eller pappersregister som är sökbara.

För att säkerställa att de uppgifter vi behandlar är korrekta sker ibland kontroll mot folkbokföringsdatabaser. Den personuppgiftsansvarige svarar för att de uppgifter som hämtas från sådana databaser inte är fler än nödvändigt

och att antalet personer som har behörighet att genomföra hämtningar inte är fler än vad som krävs för arbetets utförande.

2.2 Dataskyddsombudets roll

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen är självständig vilket säkerställs genom tillgång till egen budget. Ombudet har i uppdrag att bland annat granska efterlevnaden av dataskyddslagstiftningen och vara rådgivande i arbetet. Dataskyddsombudet ska utföra detta arbete för Landskrona stad:

- Informera och ge råd till personuppgiftsansvariga gällande dataskyddslagstiftning.
- På begäran ge råd vad gäller konsekvensbedömningar.
- Bistå i utredning om personuppgiftsincident om detta begärs, Agera kontakt mot enskilda och Integritetsskyddsmyndigheten.
- Utöva tillsyn över den personuppgiftsbehandling som sker.
- Rapportera till Landskrona stad om dataskyddsfrågor och utvecklingsfrågor samt ge förslag på vilka åtgärder som kan behöva vidtas.
- På begäran bistå i andra dataskyddsfrågor.

2.3 Dataskyddssamordnarens roll

Dataskyddssamordnare är en funktion i Landskrona stad som ska finnas inom varje nämnd enligt policy för personuppgiftsbehandling i det fall den behandlar personuppgifter. Rollen kan kombineras med andra arbetsuppgifter om det bedöms möjligt. Det är upp till varje nämnd att säkerställa att dataskyddssamordnare får tillräckligt med tid och resurser att genomföra sitt uppdrag. Dataskyddssamordnaren är en stödfunktion. Ansvaret att lagstiftning efterlevs vilar alltid på personuppgiftsansvarig. Dataskyddssamordnaren stöttar verksamhet och personuppgiftsansvarig och ska åtminstone utföra följande uppgifter för den personuppgiftsansvarigas räkning:

- löpande uppdatera och följa upp registerförteckningen,
- administrera begäran om registerutdrag,
- ge råd och stöd och påtala brister till verksamhetens ledning och berörd personal i frågor rörande dataskydd och personuppgiftsbehandling,
- följa upp att verksamheten genomför grundutbildning för varje medarbetare och i övrigt föreslå och följa upp kompetensutveckling,
- vara ett stöd vid upprättande av personuppgiftsbiträdesavtal,
- hålla sig underrättad om utveckling av lagstiftningen och praxis inom området, rådfråga och samråda med dataskyddsombudet för verksamhetens räkning,

- bidra till utvecklingen av stadsgemensamma rutiner och arbetssätt,
- vara dataskyddsombudets och stadsledningskontorets kontaktperson i dataskyddsfrågor samt delta i stadens dataskyddsnätverk. Nätverket består av alla dataskyddssamordnare Landskrona stad.

3. Rättsliga grunder för behandling

För att en behandling ska vara laglig enligt dataskyddsförordningen krävs det en rättslig grund. I detta kapitel kommer de olika lagstadgade rättsliga grunderna presenteras och vilka som i första hand bör användas av Landskrona stad.

3.1 De olika rättsliga grunderna

Det finns i dataskyddsförordningen sex olika rättsliga grunder. Enbart en rättslig grund kan användas på en behandling. Det är därmed inte möjligt att byta rättslig grund under den tid personuppgiftsbehandlingen pågår. Valet av rättslig grund för behandlingen gives därmed en stor vikt vid frågor kring personuppgiftsbehandling.

3.1.1 Myndighetsutövning eller allmänt intresse

Med uppgift av allmänt intresse eller myndighetsutövning menas att personuppgifterna måste behandlas för att utföra myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse. Ett allmänt intresse kan vara ett frivilligt åtagande som Landskrona stad gör. Främjande av lokal kulturverksamhet kan vara ett sådant åtagande av allmänt intresse för Landskrona stad.

Det som faller inom den kommunala kompetensen kan anses utgöra myndighetsutövning. Exempel på sådant är handläggning av bygglov. När det kommer till myndighetsutövning bör det vara något inom den kommunala kompetensen.

Ett exempel på när allmänt intresse kan agera som rättslig grund är när kommunen behandlar personuppgifter inom verksamhet, såsom badhus eller evenemang. Denna rättsliga grund är en av de som bör främst användas av Landskrona stad i dess personuppgiftsbehandling. Anledningen är att grunden inte är möjlig att återkalla som samtycke.

Utöver detta faller det ofta inom antingen myndighetsutövning eller uppgift av allmänt intresse i de fall en kommun behöver behandla personuppgifter. Bör vara första alternativet som rättslig grund för Landskrona stad om inte rättslig förpliktelse går att använda som grund för behandlingen.

3.1.2 Avtalsförpliktelse

Avtalsförpliktelse syftar på att den registrerade har ingått eller ska ingå ett avtal med den personuppgiftsansvariga och behandlingen av uppgifterna är nödvändig för att fullgöra avtalet. Denna rättsliga grund kan användas i vissa situationer inom Landskrona stad. Ett exempel på en sådan situation är behandlingen av anställdas personuppgifter.

Ett annat fall är när någon av kommunens verksamheter behöver behandla uppgifter för att uppfylla sina avtalsskyldigheter eller fakturera för en tjänst. Exempel på detta är badhus eller en kulturskola som behandlar elevernas personuppgifter.

3.1.3 Rättslig förpliktelse

Med denna rättsliga grund behövs det lag eller annan författningsgrundade regel som orsakar att personuppgiftsansvarig måste behandla personuppgifterna i sin verksamhet. Exempel på sådan rättslig förpliktelse kan vara en arbetsgivares skyldighet att redovisa skatter och sociala avgifter.

Denna förpliktelse bör användas av Landskrona stad när det finns sådana rättsliga tvång framför annan rättslig grund såsom allmänt intresse. Anledningen till detta är att det är en stark rättslig grund som inte kan återkallas såsom samtycke. Ett vanligt exempel på när rättslig förpliktelse bör användas som rättslig grund är faderskapsutredningar.¹ I det fall behandlingen krävs av lag ska denna grund användas före myndighetsutövning.

3.1.4 Intresseavvägning

Personuppgiftsansvarig får behandla personuppgifterna utan samtycke om dess intressen väger tyngre än den registrerades och behandlingen är nödvändig för ändamålet. Denna grund bör inte användas av myndigheter eller andra offentliga organ. Intresseavvägning är alltså inte lämplig som rättslig grund för personuppgiftsbehandling som görs av Landskrona stad.

3.1.5 Grundläggande intresse

Denna rättsliga grund får bara användas för att skydda en registrerad som inte kan lämna samtycke. Exempel på sådan situation när denna grund kan användas är vid medvetlöshet. Vård som planerats anses inte utgöra ett grundläggande intresse om personen inte kan lämna samtycke vid det givna tillfället. Bör inte användas av Landskrona stad om inte absolut nödvändigt och en situation att likställa vid medvetlöshet uppstår.

¹ 12 § förordning (2001:637) om behandling av personuppgifter inom socialtjänsten.

3.1.6 Samtycke

Samtycke föreligger när den registrerade har blivit informerad och efter det tydligt och frivilligt sagt ja till behandlingen av personuppgifterna med ett specifikt ändamål. Ett samtycke kräver att personen förstår att behandlingen sker och får inte leda till någon nackdel. Samtycke kan alltid återkallas när som helst av den registrerade. Detta samtycke ska ges tydligt till exempel genom tydlig underskrift där det framgår vad den registrerade samtycker till.

Samtycke bör inte användas när det förekommer en stor obalans i makt mellan de två parterna. Exempel på sådant förhållande kan vara ett anställningsförhållande. Barn under 13 år kan inte lämna samtycke själva. I det fallet måste vårdnadshavare kontaktas.

Samtycke är det sista alternativet för rättslig grund som bör användas av Landskrona stad. En anledning till detta är för att det kan dras tillbaka när som helst. Utöver detta har Landskrona stad ett ojämnt maktförhållande med en enskild vilket kan riskera frivilligheten av samtycket, vilket är ett krav för dess giltighet. En brukare i en verksamhet driven av Landskrona stad har ett sådant förhållande att frivillighet kan ifrågasättas. Ett samtycke gäller inte utöver de uttryckliga behandlingar det har givits för.

3.2 Om behandlingen rör känsliga personuppgifter

I det fall den tilltänkta personuppgiftsbehandlingen involverar känsliga personuppgifter gäller det även att något av underliggande scenarion föreligger för att behandlingen ska vara laglig:

- Den registrerade har lämnat sitt uttryckliga samtycke.
- Behandlingen är nödvändig för att fullgöra någon av parternas skyldigheter och utöva sina rättigheter inom områdena arbetsrätten, social trygghet eller socialt skydd.
- Grundläggande intresse föreligger och den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
- Behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse.
- Behandlingen är nödvändig med hänsyn till ett allmänt intresse på folkhälsoområdet.
- Behandlingen är nödvändig för arkivändamål av allmänt intresse eller lag.

4. Grundläggande principer vid personuppgiftsbehandling

Dessa principer skall tas i åtanke vid varje personuppgiftsbehandling som genomförs inom Landskrona stad. Dessa principer ska anse vara en grund som all behandling skall utgå ifrån.

4.1 Laglighet, korrekthet och öppenhet

All behandling av personuppgifter måste vara laglig. Med detta menas att det alltid måste finnas en rättslig grund för behandlingen. För de rättsliga grunderna se kapitel 3. Behandlingen ska också vara korrekt och öppen, med detta menas att den ska vara skälig, rättvis, rimlig och proportionerlig i förhållande till den registrerade. Utöver detta ska den vara öppen mot den registrerade och informera denna att uppgifterna behandlas och hur. Behandlingen får därmed inte ske på dolda eller manipulerande sätt.

4.2 Ändamålsbegränsning

Innan behandling ska ske måste det angivas ett särskilt och uttryckligt angivet ändamål för personuppgiftsbehandlingen. Ändamålet måste alltså vara tydligt och specifikt i sin utformning samt berättigat. Detta ändamål bestämmer inom vilka ramar behandlingen får ske. Det får inte skapas ett nytt ändamål efter det att behandlingen påbörjats. I det fall man önskar behandla personuppgifterna på ett nytt sätt måste detta vara förenligt med det ursprungliga ändamålet annars rör det sig om en ny personuppgiftsbehandling. Dessa ändamål ska dokumenteras och de registrerade ska informeras om vad ändamålet är.

4.3 Uppgiftsminimering

De insamlade och behandlade personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till det angivna ändamålet. Det kan därmed sägas att ändamålet bestämmer vilken mängd av personuppgifter som får samlas in. Det är inte tillåtet att samla in personuppgifter för obestämda framtida behov.

4.4 Riktighet

Det är den personuppgiftsansvariga eller personuppgiftsbiträdet som ska säkerställa att de personuppgifter som behandlas ska vara riktiga och om nödvändigt uppdaterade. Uppgifterna ska hållas uppdaterade i den mån det kan anses rimligt.

4.5 Lagringsminimering

Personuppgifter får enbart sparas så länge de behövs för det ändamål som har angivits vid behandlingen påbörjan. De får inte sparas för ett senare tillfälle som inte omfattas av det ursprungliga ändamålet. När personuppgifterna senare inte behövs för ändamålet ska de raderas eller avidentifieras om inte annat är föreskrivet i lag eller rutin för Landskrona stad.

4.6 Integritet och konfidentialitet

Vid behandling av personuppgifter ska de behandlas på ett bra sätt genom att lämpliga skyddsåtgärder har vidtagits. Exempel på en skyddsåtgärd är kryptering eller pseudonymisering gällande tekniken och åtkomstbegränsning för organisatorisk skyddsåtgärd.

4.7 Ansvarsskyldighet

Den som är personuppgiftsansvarig eller personuppgiftsbiträde är ansvarig för att de grundläggande principerna för personuppgiftsbehandling följs. Det måste även vara möjligt att kunna bevisas att principerna följs.

5. Process vid ny personuppgiftsbehandling

Personuppgiftsbehandling ska följa samma procedur för samtliga av Landskrona stads nämnder. Innan behandlingen påbörjas eller tekniska hjälpmedel köps in ska ändamålet och den rättsliga grunden för behandlingen vara fastställt. Mängden uppgifter som samlas in ska inte vara fler än vad som är nödvändigt i förhållande till ändamålet och den rättsliga grunden.

Om processen involverar externa aktörer ska dessa lyda under avtal om sekretess och tystnadsplikt. Viktigt att ha i åtanke är att genom hela denna process ska principerna för personuppgiftsbehandling hållas i åtanke samt den registrerades rättigheter.

5.1 Riskanalys och konsekvensbedömning

Behandlingen ska analyseras i en riskanalys och möjligen en konsekvensbedömning om detta anses nödvändigt. För detta arbete är förvaltningens dataskyddssamordnare behjälplig. Analysen kräver att personuppgifterna klassificeras utifrån såväl dataskyddslagstiftning och offentlighets- och sekretesslagen som utifrån informationssäkerhet. Klassningen och analysen ligger till grund för vilka säkerhetskrav som ska ställas.

För behandlingar som kan medföra allvarliga risker för de registrerades rättigheter krävs också att det genomförs en konsekvensbedömning.

Landskrona stad har en rutin för hur konsekvensbedömningar ska genomföras.² Om konsekvensbedömning görs ska även dataskyddsombud antingen granska den slutförda konsekvensbedömningen eller rådgöras i ärendet.

5.2 Registerförteckning

Både personuppgiftsansvarig och personuppgiftsbiträde är skyldiga enligt dataskyddslagstiftning att föra antingen ett register eller en förteckning över de behandlingar av personuppgifter som sker. I Landskrona stad förs detta register genom att behandlingen ska registreras i varje nämnds registerförteckning. Själva registreringen av behandlingen görs i programmet Draftit Records av personuppgiftsansvarig. Den personuppgiftsansvarigas registrering ska innehålla följande uppgifter:

- namn och kontaktuppgifter för den personuppgiftsansvariga, dess företrädare och dataskyddsombudet
- en beskrivning av kategorierna av registrerade och de olika kategorierna av personuppgifter
- de kategorier av mottagare till vilka uppgifterna har lämnats ut
- om möjligt, överföringar till tredje land av uppgifter
- om möjligt, den förutsedda tiden innan radering av uppgifterna
- om möjligt, en beskrivning av de säkerhetsåtgärder som vidtagits för behandlingen.

5.3 Tekniska system och lagring

För tekniska system där personuppgifter behandlas ska principerna om Dataskydd som standard och Inbyggt dataskydd beaktas. Ett exempel kan vara att standardinställningarna för systemet inte behandlar personuppgifter som inte kan anses som absolut nödvändiga och att enbart de som är behöriga har tillgång till information i systemet.

Lagringsminimering ska tillämpas vilket innebär att personuppgifterna inte förvaras i en form som möjliggör identifiering under längre tid än nödvändigt. Lagring över längre perioder ska följa lagstadgade krav och riktlinjer. Vid bedömning av gallringsfrister i informationshanteringsplaner ska principen om lagringsminimering beaktas. Att ta bort uppgifter ska följa regler och rutiner för rensning och gallring.

² Rutin för konsekvensbedömning se kap 11.

5.4 Tredjelandsoverföring

Om personuppgiftsbehandlingen innebär att tredjelandsoverföring av personuppgifter sker, säkerställ att någon av dessa undantag föreligger för giltighet av överföringen:

- Standard Contractual Clauses (SCC) används och håller en tillräcklig hög säkerhetsgrad i det tredje landet för att förhindra att informationen läcks. Ett exempel är att SCC inte ger tillräckligt skydd mot USA i skrivande stund med hänsyn till att det inte säkras att landets myndigheter tar del av personuppgifterna.
- Överföringen är tillfällig och nödvändig. Den kommer därmed inte ske regelbundet. Den ska även tas i åtanke om den är nödvändig med utgångspunkt i den registrerades intressen. Exempel på sådan situation är nedladdning eller uppdatering av ett system som härstammar från ett tredjeland. Detta undantag kan inte utnyttjas om överföringen sker inom ramen för kommunens myndighetsutövning.
- Landet finns på den lista av länder som har en adekvat säkerhetsnivå enligt den europeiska kommissionen enligt artikel 45 GDPR.³

I det fall ingen av de ovanstående undantagen kan göras på en eventuell tredjelandsoverföring så ska den inte genomföras, då överföringen anses vara ogiltig och inte i enlighet med GDPR. Detta kan hindra personuppgiftsbehandlingen i det fall den är beroende av denna överföring.

5.5 Personuppgiftsbiträdesavtal

Vid anlitan av personuppgiftsbiträde ska ett personuppgiftsbiträdesavtal skrivas. Avtalet kan ligga som en bilaga till huvudavtalet eller ingå som klausuler i huvudavtalet. Personuppgiftsansvarig ansvarar för att verksamheten har biträdesavtal. Den som är behörig att teckna huvudavtal med leverantören för nämnden är också behörig att teckna biträdesavtalet. För hur ett personuppgiftsbiträdesavtal ska se ut se mall för personuppgiftsbiträdesavtal.

I det fall det rör sig om ett personuppgiftsbiträdeförhållande mellan nämnder, kommunstyrelse eller fullmäktige inom Landskrona stad så finns det en rättsakt som reglerar detta i stället för ett personbiträdesavtal. Denna rättsakt agerar som ersättning för dessa avtal genom att säkerställa förhållandet och de instruktioner som behövs när ett

³ <https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/>

personbiträdesförhållande föreligger.⁴ Därmed behövs inget avtal om det rör personuppgiftsansvarig och personuppgiftsbiträde inom Landskrona stad.

5.6 Om personuppgiftsincident inträffar

Personuppgiftsincidenter är en typ av informationssäkerhetsincident där tillgängligheten, riktigheten eller konfidentialiteten av personuppgifterna har riskerats. Denna typ av incident ska följa en viss formalia i dess hantering.

Rapportering av personuppgiftsincidenter ska för Landskrona stads nämnder ske i stadens centrala inrapporteringssystem Flexite för risker, tillbud och skada. Inrapporteringen ska analyseras kontinuerligt och åtgärder vidtas som en naturlig del i det skadeförebyggande arbetet.

Dataskyddsombudet för Landskrona stad ska meddelas vid händelser där personuppgiftsincident är av sådan grad att en anmälan till tillsynsmyndigheten upprättas. En personuppgiftsincident ska i samband med upptäckt rapporteras vidare inom 72 timmar till Integritetskyddsmyndigheten om det inte kan anses vara osannolikt att incidenten har medfört en risk för de registrerade.

6. Den registrerades rättigheter

Den registrerade ges genom dataskyddslagstiftningen vissa rättigheter som måste säkerställas att de uppfylls vid en personuppgiftsbehandling. Dessa rättigheter ger den registrerade en rätt att få information om hur och när deras personuppgifter behandlas, kontroll över de egna rättigheterna och få uppgifterna rättade, raderade eller blockerade.

6.1 Rätt till information

En registrerad har rätt till information kring behandlingen av dess uppgifter. Den registrerade har rätt att få veta följande saker på begäran:

- varför uppgifterna kommer att behandlas
- i vissa fall den rättsliga grunden för behandlingen
- hur länge uppgifterna kommer att lagras
- vem som tar del av uppgifterna
- de egna rättigheterna enligt dataskyddsförordningen
- om uppgifterna kommer att överföras till ett tredjeland
- rätten att lämna klagomål
- hur samtycke kan återkallas om detta har använts

⁴ För mer information om exakta instruktioner se, rättsakt för Landskrona stad nämnder emellan, bilaga 1 policy för personuppgiftsbehandling.

- kontaktuppgifterna till den organisation som ansvarar för att behandla personuppgifterna och dess dataskyddsombud.

Personuppgiftsansvarig är skyldig att informera den registrerade om personuppgiftsbehandlingen. Ovanstående punkter måste i Landskrona stad besvaras av personuppgiftsansvarig om det begärs, och är möjligt enligt gällande lagstiftning att lämna ut informationen.⁵ Utöver detta måste personuppgiftsansvarig informera om behandlingen och dess ändamål vid första kontakttillfället eller vid insamlingen.

Om begäran är uppenbart ogrundad eller orimlig, exempelvis om samma information begärs många gånger, behöver inte personuppgiftsansvarig lämna ut informationen. Hur den registrerade ska informeras bedöms utifrån vad som är lämplig. Medarbetare inom Landskrona stads organisation informeras i samband med anställning och via arbetsnätet.

6.2 Rätt till registerutdrag

Registerutdrag fås ut på begäran av den registrerade. En begäran görs via e-tjänst eller skriftligen till den personuppgiftsansvarige. Den registrerade ska legitimera sig både vid sin begäran om utdrag och vid uthämtandet. Utlämnade ska ske inom en månad av begäran.

Registerutdraget ska innehålla information om vilka uppgifter som behandlas, Hur de behandlas, ändamålet med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnats ut till. Uppgifterna i registerutdraget ska sekretessprövas enligt offentlighet- och sekretesslagen innan det lämnas ut. Det skall också undersökas om annan lagstiftning kan förhindra att informationen i registerutdraget ska lämnas ut eller utelämnas från utdraget, detta ska ske i enlighet med gällande lagstiftningen och riktlinjer.

Överföring av registerutdrag till den registrerade sker genom *Mina meddelanden* i e-tjänsten för registerutdrag, genom post till folkbokföringsadress eller vid känsliga uppgifter genom rekommenderat brev samt genom avhämtning i reception. Registerutdrag mejlas inte till den registrerade.

6.3 Rätt till rättelse

Den som är registrerad har en rättighet att vända sig till en personuppgiftsansvarig och be att få felaktiga uppgifter om den rättade. Detta

⁵ Hur Landskrona stad behandlar personuppgifter enligt dataskyddsförordning.

inkluderar en registrerads rätt att komplettera med sådana uppgifter som saknas och är relevanta för det givna ändamålet av behandlingen.

Det åligger den personuppgiftsansvarige att inom rimlig tid och både på begäran och självmant rätta uppgifter som innehåller sakliga fel eller uppgifter som inte får behandlas. I samband med att en rättelse genomförts har personuppgiftsansvarig en skyldighet att se till att tidigare felaktiga uppgifter tas bort.

Om uppgifterna lämnats ut ska personuppgiftsansvarig informera om de nya och korrekta uppgifterna till de som uppgifterna lämnats ut till. Detta behövs inte göras om denna handling skulle vara omöjlig eller medföra en alltför betungande instans för personuppgiftsansvarig.

6.4 Rätt till radering

Den registrerade har en rätt att vända sig till en personuppgiftsansvarig och be att de uppgifter som rör personen ska raderas. Uppgifterna ska raderas av personuppgiftsansvariga i följande fall:

- de inte längre behövs för det insamlade ändamålet
- om behandlingen grundar sig på ett samtycke som sedan återkallas
- om behandlingen sker för direktmarknadsföring som den registrerade motsätter sig
- om radering krävs för att uppfylla en rättslig skyldighet
- om personuppgifterna har behandlats olagligt
- om personuppgifterna avser barn och har samlats in i samband med att barnet skapat en profil i ett socialt nätverk.

I det fall uppgifterna har raderats är det personuppgiftsansvarig som är skyldig att informera om detta i det fall uppgifterna har lämnats ut. Detta gäller inte om arbetet skulle vara omöjligt eller onödigt betungande för personuppgiftsansvarig. En offentlig myndighet som har mottagit uppgifterna inom ramen för ett särskilt uppdrag är inte en mottagare som måste underrättas om raderingen.

Flera av dessa rättigheter till radering är begränsade för en offentlig myndighet då det undantas ofta från radering om dessa personuppgifter är nödvändiga för att tillgodose andra viktiga rättigheter. Exempel på sådan rättighet är rättslig förpliktelse för en kommun, utföra en uppgift i allmänt intresse eller som ett led i myndighetsutövningen.

En begäran från den registrerade ska prövas och den registrerade ska få ett beslut som kan överklagas om begäran nekas. Vilka beslut som kan överklagas framgår av 7 kap. 2 § dataskyddslagen (2018:2018).

6.5 Rätt att invända eller begränsa personuppgiftsbehandling

En registrerad har i vissa fall en rätt att kräva att behandlingen av personuppgifter ska begränsas. Med en begränsning menas det att de markeras så att uppgifterna enbart får behandlas i vissa specificerade syften. Ett exempel på en sådan begränsning är vid utredningen av uppgifternas korrekthet.

Utöver detta har en registrerad även en rätt att invända mot personuppgiftsbehandling i vissa fall hos en nämnd. Detta gäller när uppgifterna behandlas för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. I dessa fall får personuppgiftsansvarig fortsätta att behandla uppgifterna enbart om den kan påvisa att det finns berättigade skäl till behandlingen av uppgifterna som väger tyngre än den enskildes intressen, rättigheter och friheter eller att behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

6.6 Rättighet vid automatiserade beslut

Ett automatiskt beslut innebär att beslutsfattandet sker utan involvering av en fysisk person i ärendet. Ett exempel på detta kan vara ett automatiskt avslag på en ansökan via internet. I det fall ett beslut tas automatiskt har den registrerade vissa rättigheter. Den personuppgiftsansvariga måste i dessa fall säkerställa att dessa punkter efterlevs:

- Informera den registrerade att behandlingen och beslutet är automatiskt.
- Ge den registrerade en möjlighet att få beslutet granskat av en fysisk person. Exempelvis en handläggare som arbetar med denna typ av beslut.
- Den registrerade måste ges möjligheten att bestrida beslutet.

6.7 Rätt att klaga

Den registrerade kan lämna klagomål som avser hantering av personuppgifter till i först hand personuppgiftsansvarig, i andra hand till dataskyddsombudet och slutligen till Integritetskyddsmyndigheten. Den kan även vända sig direkt till Integritetskyddsmyndigheten om det är det val som vill göras. Det rekommenderas dock att först vända sig till personuppgiftsansvarig så de kan bemöta eller ordna upp det eventuella problemet.

7. Rensning och gallring

Gallring alternativt bevarande, ska följa fastställda informationshanteringsplaner och gällande lagstiftning. Den personuppgiftsansvarige svarar för att rutiner och regler följs. När informationshanteringsplaner revideras ska hänsyn tas till dataskyddslagstiftning. Detta görs med hänsyn till principen om lagringsminimering vid personuppgiftsbehandling.

8. Informationssäkerhet och dataskydd

Personuppgifter är information som utöver dataskyddslagstiftning omfattas av Landskrona stads Informationssäkerhetspolicy samt dess underliggande styrdokument.

Behörighetskontroll ska finnas för samtliga system som hanterar personuppgifter. Arbetsmetoder och rutiner hur verksamheten ger åtkomst till personuppgifter ska upprättas skriftligt. För personuppgifter som är säkerhetsskyddsklassade ska finnas särskilda krav för behörighet.

Loggning redogör för historiken i ett system. Loggningen ska följas upp och skyddas mot ändringar. I loggen ska det framgå detaljerad information som kan användas vid utredning om personuppgifter använts felaktigt, obehörigt eller om uppgiften blivit föremål för ändring.

9. Personuppgifter i e-post och sociala medier

Hantering av personuppgifter i e-post ska följa verksamhetens informationshanteringsplan. Informationen ska behandlas på samma sätt som annan information. E-posten är inte en lämplig permanent lagringsyta och informationen ska i stället överföras till exempelvis dokument- och ärendehanteringssystemet.

Om personuppgifter ska mejlas eller på annat sätt överföras digitalt ska uppgiften skyddas mot obehörig åtkomst, förändring och förstöring. Känsliga och integritetskänsliga uppgifter ska i de fall de bedöms kunna e-postas skyddas med kryptering. Gällande hantering av personuppgifter inom e-post så ska detta göras i enlighet med de riktlinjer som finns inom Landskrona stad.

Behandling av personuppgifter i sociala medier och för marknadsföring regleras av Landskrona stads kommunikationspolicy med tillhörande riktlinjer och tillämpningsanvisningar. Utöver de grunder för personuppgiftsbehandling som återfinns i policy för behandling av personuppgifter med tillhörande riktlinjer.

10. Personuppgifter i fritextfält

Med ett fritextfält menas ett utrymme i ett system, på en hemsida eller ett dokument där en person kan skriva vad de önskar. Ett vanligt sätt att använda dess fritextfält är för personliga anteckningar eller för att lyfta sådana frågor som inte kommit fram tidigare. Ett annat syfte med fritextfält kan vara att besvara tidigare ställda frågor i ett formulär på ett vis som kan ge ett mer helhetligt svar. Fritextfält kan utgöra källor för personuppgifter och därmed falla under dataskyddslagstiftningen.

När Landskrona stad använder sig av fritextfält måste därför vissa frågor och anvisningar tas i beaktning:

- Är fritextfält nödvändigt för detta typ av ärende?
- Om personuppgifter förekommer faller de inom någon rättslig grund?
- Vad är ändamålet med informationen i fältet?
- Inga värderingar eller kränkande skrivelser ska återfinnas som kan kopplas till en person och utgöra en personuppgift.
- Inga omdömen eller uppgifter om en namngiven tredje person ska förekomma.
- Personnummer eller andra personuppgifter får endast antecknas om det kan anses vara nödvändigt för ärendets handläggning.
- Säkerställ att inga känsliga personuppgifter förekommer i den mån det är möjligt.
- Uppgifterna som antecknas i ett fritextfält ska bara sparas så länge de är nödvändiga.

Utöver detta måste man tänka på att all personuppgiftsbehandling som sker i dessa fält måste följa de regler och principer som presenteras i dataskyddslagstiftningen samt den policy och de riktlinjer som kan appliceras på det aktuella området gällande personuppgiftsbehandlingen som sker i dessa fritextfält.

11. Relevanta styrdokument

Nedan finns en lista med andra styrdokument som har en stark koppling till personuppgiftsbehandling och behövs beaktas inom respektive område.

- Informationssäkerhetspolicy
- Handbok för sociala medier
- Kommunikationspolicy
- Riktlinjer för bild och film
- Rutin för konsekvensbedömning

- Riktlinje för e-posthantering
- Instruktion för begäran om registerutdrag
- Hur Landskrona stad behandlar personuppgifter enligt dataskyddsförordning
- Policy för personuppgiftsbehandling.