LINDESBERGS KOMMUN

KS 2018/63-4

Lindesbergs kommuns arbete med dataskydds-förordningen

Strategi
Plan/program
›› Riktlinje
Regler och instruktioner

Fastställt av: Kommunstyrelsen
Datum: 2018-04-23 § 63
För revidering ansvarar: Dataskyddsombudet
För eventuell uppföljning och tidplan för denna ansvarar: Kommundirektör
Dokumentet gäller för: Alla nämnder och bolag
Dokumentet gäller till och med: 2020

1 Innehåll

1 Inledning

Den nya dataskyddsförordningen börjar gälla som lag i Sverige i maj 2018 och kompletteras av en svensk dataskyddslag.

Mycket av det som finns i den nya förordningen återfinns i nuvarande personuppgiftslagen, men det finns också en del stora förändringar och också en del nya bestämmelser.

EU:s nya dataskyddsförordning är ett omfattande regelverk och ingår i en större dataskyddslagstiftning. Däri ingår även ett direktiv som reglerar hur personuppgifter får hanteras i den brottsbekämpande verksamheten.

Den nya förordningen innehåller 99 artiklar och flera av dessa innebär nyheter och förändringar av gällande rätt. Några av förändringarna är:

- Rätt att bli raderad (bortglömd)
- Rätt till dataportabilitet (Den som har lämnat sina personuppgifter har i vissa fall rätt att få ut och använda sina personuppgifter på annat håll till exempel i en annan social medietjänst)
- ”Privacy by design” – krav på inbyggt dataskydd i IT- system
- Nya krav på behandlingar av personuppgifter i ostrukturerat material
- En skyldighet att anmäla personuppgiftsincidenter till tillsynsmyndigheten
- Utökade krav på information till registrerad
- Utökade krav på personuppgiftsansvarig och personuppgiftsbiträde
- Vid överträdelse av reglerna ev. skyldighet att betala administrativa sanktionsavgifter

1.1 Vad är en personuppgift?

Dataskyddsförordningen definierar personuppgift mer detaljerat än personuppgiftslagen och tar upp exempel på vilka uppgifter som definieras som personuppgifter.

Med personuppgift menas all slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Det avgörande är om en person på något sätt kan identifieras av någon annan.

Exempel på personuppgifter är

- namn
- personnummer
- fotografi
- ljudinspelning
- telefonnummer
- registreringsnummer på fordon
- diarienummer
- IP-adress.

Namn och personnummer är exempel på *direkta* personuppgifter. Telefonnummer, registreringsnummer på fordon, diarienummer och IP-adress är exempel på så kallade *indirekta* personuppgifter. För att veta vilken person som en indirekt personuppgift avser behöver man ytterligare information såsom t.ex. uppgift om vem som är ägare till ett fordon med ett visst registreringsnummer.

Ibland kan uppgifter vara så detaljerade att det går att förstå vilken person som avses utan att någon direkt eller indirekt personuppgift anges, t.ex. ”kyrkvaktmästaren i XX församling”. En sådan uppgift är också en personuppgift. Även uppgifter som är krypterade och olika slags elektroniska identiteter som t.ex. e-postadresser eller IP-adresser är personuppgifter om de kan knytas till en person.

1.2 Känsliga personuppgifter

Vissa personuppgifter anses vara extra känsliga ur integritetssynpunkt. Med detta menas personuppgifter som

- avslöjar ras eller etniskt ursprung
- avslöjar politiska åsikter
- avslöjar religiös eller filosofisk övertygelse
- avslöjar medlemskap i fackförening
- rör hälsa eller sexualliv.

Exempel på känsliga personuppgifter kan vara

- uppgift om en persons medlemskap i ett trossamfund
- uppgift om att en person har lämnat bidrag till ett politiskt parti
- uppgift om att en person har skadat sin fot eller är sjukskriven
- uppgifter om allergier, intoleranser
- uppgifter om matpreferenser så som t. ex. kosher eller halal-mat.

Det finns särskilda bestämmelser för om och i så fall hur känsliga personuppgifter får behandlas.

1.3 Vad är ett system/behandling?

Datainspektionens definition på behandling:

Alla former av åtgärder med personuppgifter är personuppgiftsbehandling, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Dataskyddsförordningen gäller för helt eller delvis automatiserad behandling av personuppgifter. Den gäller också för manuell behandling av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett manuellt register som är sökbart enligt särskilda kriterier.

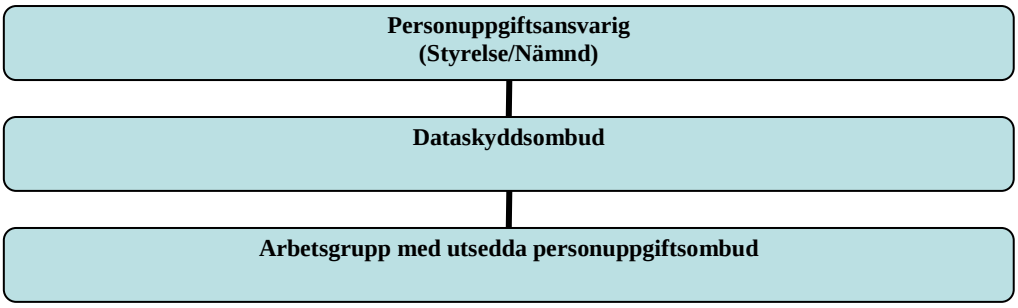
2 Ansvar för dataskyddsfrågor i Lindesberg kommun

Den nya förordningen ställer krav på att det ska finnas ett dataskyddsombud i varje organisation.

Den som ska utses ska ha tillräcklig kunskap om dataskydd och få det stöd och befogenheter som behövs för att utföra uppdraget på ett effektivt och oberoende sätt.

Det är styrelsen eller nämnden som är personuppgiftsansvariga och dataskyddsombudet arbetar på uppdrag av dessa.

Till sin hjälp ska dataskyddsombudet ha en central arbetsgrupp med utsedda representanter från verksamheterna. Dataskyddsombudet ska leda arbetsgruppen och personerna i gruppen, som vi väljer att kalla för personuppgiftsombud, ska fungera som stöd till dataskyddsombudet och vara vägen in i verksamheterna i frågor gällande dataskyddsarbete. Dessa har inte samma ansvar för dataskyddsarbetet som dataskyddsombudet.
Vid behov kan fler personuppgiftsombud utses av nämnderna.



3 Vad behövs göras?

När den nya dataskyddsförordningen börjar gälla som lag i Sverige i maj 2018 ska följande vara genomfört eller påbörjat.

1. Kommunstyrelsen ska utse ett **dataskyddsombud.**

2. **Information om lagstiftningen** ska ges till följande grupper:

    - Kommunens ledningsgrupp
    - IT-avdelningen
    - Kommunens dataskyddsombud
    - Nämndsekreterare/registratorer

3. **Kartläggning** - Varje nämnd ska fatta ett beslut om vilka personuppgifter som behandlas enligt de rutiner som finns och överlämna detta till dataskyddsombudet för att bli till en central förteckning.

Inventering av de system som innehåller personuppgifter och rättigheterna ovan kan uppfyllas.
I och med att missbruksregeln för behandling av ostrukturerat material försvinner behöver sådan behandling gås igenom. Detta görs av dataskyddsombudet tillsammans med övriga personuppgiftsombud.

4. **Information till registrerade.** Bland annat ska kommunen informera om den rättsliga grunden för behandlingen, hur länge personuppgifterna lagras och möjligheten att lämna klagomål till tillsynsmyndigheten.

5. Framtagande av **nya rutiner**.

6. Hantering av **dataintrång**.

7. Den nya förordningen ställer särskilda krav på behandling av personuppgifter som kan medföra stora integritetsrisker för enskilda. Dataskyddsombudet ska undersöka tillsammans med övriga personuppgiftsombud om det finns sådana register. Hantering av personuppgifter för barn är exempel på en sådan behandling.

8. **Leverantörer och avtal** – Inbyggt dataskydd ska finnas i de system som utvecklas och som införskaffas, t. ex det ska inte finnas mer information än vad som behövs och att den inte ligger kvar längre än nödvändigt. Vid utveckling av system ska även konsekvensanalyser göras.
IT-avdelning och upphandlingsansvarig informeras om att dessa krav ska finnas med i upphandling av både utveckling och inköp av kommande IT-system.

9. **Dokumentera** kommunens arbete med dataskydd.

3.1 Information om EU:s nya dataskyddsförordning

Beslutsfattare och nyckelpersoner ska vara medvetna om att personuppgiftslagen kommer att ersättas av dataskyddsförordningen och hur organisationen påverkas och inom vilka områden det måste vidtas åtgärder.
Därför ska information ges till:

- Kommunens ledningsgrupp
- IT-avdelningen
- Kommunens dataskyddsombud
- Nämndsekreterare/registratorer

Rent praktiskt är det dataskyddsombudet som har det största ansvaret för att se till att varje myndighet ser till att de anpassningar på systemnivå som är nödvändiga genomförs.

3.2 Vilka personuppgifter hanteras?

En samlad förteckning av vilka personuppgifter som hanteras sammanställs utifrån befintligt underlag.

Samtliga nämnder ska enligt de rutiner som finns sedan tidigare ha fattat beslut om vilka personuppgifter som hanteras, hur insamlingen går till och till vem uppgifterna lämnas ut.

Denna förteckning gås igenom av personuppgiftsombud, korrigeras och beslutas av nämnden. Därefter expedieras beslutet till dataskyddsombudet som sammanställer listan.

Beslutet i nämnden kompletteras med att nämnden vid förändringar i hanteringen av personuppgifter, dvs. nya system, förändringar av hantering av personuppgifter i befintliga system etc. ska fatta nytt beslut om hanteringen av personuppgifter om att meddela detta till kommunstyrelsens personuppgiftsombud och dataskyddsombud.

Syftet med att ha en central förteckning är att uppfylla kravet på att rättningar av felaktiga uppgifter ska kunna göras. Detta går inte genomföra om det inte finns en förteckning på vilka uppgifter som hanteras, varifrån de kommer och till vem de lämnas ut.

3.3 Missbruksregeln

I nuvarande lagstiftning är behandling av ostrukturerat material, t. ex. löpande text på kommunens hemsida eller intranätet undantagen så länge inte behandlingen utgör en kränkning av den registrerades personliga integritet. Denna regel upphör när den nya förordningen träder i kraft.

Det är viktigt att om denna regel har utnyttjats undersöka vilken rättslig grund som finns för behandlingen, att de grundläggande kraven uppfylls och att de registrerade informeras på ett korrekt sätt. I annat fall ska personuppgiften tas bort.

Dataskyddsombudet tillsammans med övriga nämnders personuppgiftsombud undersöker förutsättningarna och tar fram nya rutiner om det behövs.

3.4 Vilken information lämnas?

När personuppgifter samlas in måste kommunen enligt dataskyddsförordningen lämna viss information, till exempel om identitet och ändamålet med behandlingen.

Dataskyddsförordningen innehåller utökade krav på vilken information som ska lämnas till de registrerade. Bland annat behöver vi informera om den rättsliga grunden för behandlingen, hur länge personuppgifterna lagras och möjligheten att lämna klagomål till tillsynsmyndigheten (som i Sverige är Datainspektionen). Det behöver även lämnas information om hur gallring sker.

Informationen ska vara kortfattad, lättbegriplig och utformad på ett tydligt sätt.

Dataskyddsombudet tar fram riktlinjer för hur den nya informationen ska utformas och informerar övriga personuppgiftsombud om de ändringar som ska genomföras och när de senast ska vara genomförda.

3.5 De registrerades rättigheter

Kommunen ska se över rutinerna för att säkerställa att alla rättigheter som de registrerade har enligt dataskyddsförordningen uppfylls. Exempelvis hur personuppgifter raderas (när det inte finns lagkrav på att de ska sparas) och hur uppgifter lämnas ut elektroniskt i ett allmänt använt format (dataportabilitet).

De viktigaste rättigheterna för de registrerade är:

- få tillgång till sina personuppgifter
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat
- beslutsfattande och profilering
- flytta personuppgifterna (dataportabilitet)

Det som är nytt är rätten att flytta uppgifterna – övriga rättigheterna bedöms kommunen redan kunna uppfylla i de allra flesta fall. En flytt av uppgifter innebär att de ska kunna tas ut i ett allmänt och maskinläsbart format. Detta är vara aktuellt om uppgifterna kommer från den registrerade p.g.a. samtycke eller avtal. I annat fall finns ingen dataportabilitetskyldighet för kommunen.

Dataskyddsombudet inventerar de system som innehåller personuppgifter och rättigheterna ovan kan uppfyllas.

3.6 Med vilket rättsligt stöd behandlas personuppgifter?

Datainspektionen påpekar att det är viktigt att det rättsliga stödet för behandling av personuppgifter är angivet och beslutat eftersom det ska informeras innan behandlingen av personuppgifter. Detta ingår redan i de rutiner som finns för nämnderna i Lindesberg kommun.

Kommunstyrelsens personuppgiftsombud se till att övriga personuppgiftsombud tar med detta i den förnyade inventering av system och personuppgifter som görs.

3.7 Hur inhämtas samtycke och när?

Det måste finnas en frivillig, specifik och otvetydig viljeriktning där den registrerade godkänner registreringen.

Dataskyddsombudet informerar övriga personuppgiftsombud om att det ska finnas en tydlig godkännandefunktion för samtliga system som registrerar personuppgifter.

3.8 Behandlas personuppgifter om barn?

Dataskyddsförordningen innebär ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk.

Dataskyddsombudet undersöker om det finns internettjänster som sociala nätverk och säkerställer att medgivande inhämtas.

3.9 Personuppgiftsincidenter

Dataskyddsförordningen innehåller nya bestämmelser om vad kommunen måste göra vid dataintrång eller vid förlust av kontrollen över de uppgifter som behandlas.

Sådana händelser måste dokumenteras och om händelsen medför risker för enskildas fri- och rättigheter måste den anmälas till datainspektionen inom 72 timmar.

Dataskyddsombudet informerar övriga personuppgiftsombud och IT-avdelningen om de nya reglerna och kompletterar rutinbeskrivningarna på insidan med information hur dataintrång ska hanteras.

3.10 Vilka särskilda integritetsrisker finns med behandlingen?

Den nya förordningen ställer särskilda krav på behandling av personuppgifter som kan medföra stora integritetsrisker för enskilda. T ex storskaliga register som innehåller känsliga uppgifter, profilering eller omfattande övervakning på allmän plats. Åtgärder som kan bli aktuella är pseudonymisering eller kryptering.

Dataskyddsombudet undersöker tillsammans med övriga personuppgiftsombud om det finns sådana register.

3.11 Leverantörer och avtal

Dataskydd ska finnas i de system som utvecklas och som införskaffas, t. ex. ska det inte finnas mer information än vad som behövs och att den inte ligger kvar längre än nödvändigt. Vid utveckling av system ska även konsekvensanalyser göras.

Dataskyddsombudet ska tillsammans med systemansvariga se över aktuella avtal och säkerställa att de är uppdaterade med personuppgiftsbiträdesavtal och instruktioner som är anpassade till dataskyddsförordningen.

Verksamhetsansvariga ska med stöd av dataskyddsombudet kontrollera att pågående upphandlingar tar med aktuella krav och personuppgiftsbiträdesavtal.

Systemansvariga ska ta kontakt med leverantörer för att säkerställa att kunskap om det nya regelverket finns och att det finns samstämmighet om roller och ansvarsfördelning.

3.12 Dokumentera

Samla systematisk och fortlöpande dokumentation som visar hur vi följer dataskyddsförordningen, utöver registerförteckningen.
Besluta en övergripande policy för dataskydd som beskriver mål, styrning, organisation och ansvar för dataskyddsarbetet.

Se till att dokumentation om dataskydd hålls på ett ordnat och systematiskt sätt och att rutiner finns för att hålla det uppdaterat.

Dataskyddsförordningen ställer krav på att den personuppgiftsansvariga organisationen ska kunna visa att man följer reglerna och även hur man följer reglerna. Detta kräver utöver registerförteckningen och konsekvensanalyser att flera analyser ska dokumenteras, till exempel riskanalyser om säkerhetsåtgärder.