KIRUNA KOMMUN

Dokumenttyp	Policy
Dokumentansvarig	Kommunkontoret
Upprättad	2018-08-06
Antagen	Ks 2018-09-24, § 97
Senast reviderad	
Dokumentet gäller för	Kiruna kommunkoncern

Dataskyddspolicy

Hur vi inom Kiruna kommunkoncern ska behandla personuppgifter

Syfte

Alla personer vars personuppgifter behandlas inom ramen för Kiruna kommunkoncerns verksamhet ska vara trygga med hur deras personuppgifter hanteras.

Policyn beskriver på ett övergripande plan hur personuppgifter ska behandlas, för vilka syften och på vilket sätt och riktar sig till samtliga anställda.

Denna policy ska säkerställa att Kiruna kommunkoncern:

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

Omfattning

Policyn omfattar all behandling av personuppgifter som utförs inom Kiruna kommunkoncern.

Denna policy gäller samtliga, oavsett vems personuppgifter som behandlas och oavsett sammanhang. Policyn ska kompletteras med styrdokument för informationssäkerhet samt andra specifika verksamhetsområden.

Policyn ska efterlevas av ledning, anställda och likaså av andra personer som arbetar på uppdrag av eller under översyn av Kiruna kommunkoncern, exempelvis konsulter eller partners. Detta uppnås med bland annat information, styrdokument och personuppgiftsbiträdesavtal.

Gällande dataskyddslagstiftning

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

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

Viktiga begrepp och definitioner

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

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

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

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

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

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

Varje nämnd inom Kiruna kommun och styrelserna i de kommunala bolagen är **personuppgiftsansvarig** för de personuppgiftsbehandlingar som förekommer i deras verksamhet.

Ändamål med behandling av personuppgifter

Den information Kiruna kommunkoncern samlar in, inklusive personuppgifter, behandlas för att kommunen ska uppfylla de lagstadgade krav eller myndighetsutövning, alternativt för att erbjuda en tjänst. I de fall information samlas in via blanketter eller e-tjänster lämnas upplysning om laglig grund för insamling av personuppgifter direkt på blankett/e-tjänst.

Personuppgifter som har samlats in för bearbetning i system eller i processer hanteras av aktuell handläggare och lagras i respektive system inom Kiruna kommunkoncern. I vissa fall tar vi hjälp av tjänsteleverantörer för våra IT-system. Dessa tjänsteleverantörer får endast behandla personuppgifter i enlighet med våra instruktioner. De är även skyldiga att vidta tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifter i samma utsträckning som Kiruna kommunkoncern gör.

Den information vi samlar in från den registrerade kan användas för att:

- Serva medborgare med aktuell information
- Kunna ta emot ansökningar och behandla dessa
- Få förslag på förbättringar som kan göras i kommunen

Utbildning

Alla anställda ska genomgå grundläggande dataskyddsutbildning, för att säkerställa förståelse för vikten av att hantera personuppgifter korrekt. Utbildningen genomförs som en e-learning. Ansvariga för att utbildningen genomförs är dataskyddssamordnarna inom varje nämnds verksamhet.

Varje dataskyddsamordnare ansvarar för att berörda medarbetare får ta del av sådana instruktioner och styrdokument som är relevanta för dem och sådan information som behövs för

att var och en ska kunna utföra sitt arbete i linje med dataskyddslagstiftningen. Detta inkluderar, men är inte begränsat till, utbildning av nyanställda.

Registerförteckning
Detaljerad information om varje slags behandling av personuppgifter som förekommer i processer, IT-system och på olika avdelningar inom ramen för Kiruna kommunkoncerns verksamhet ska finnas dokumenterad i organisationens registerförteckning. Kiruna kommun har egen registerförteckning och bolagen har sina egna. Förteckningen ska löpande hållas uppdaterad och fungera som ett heltäckande register över alla personuppgiftsbehandlingar, i enlighet med kraven i artikel 30 GDPR.

Registerförteckningen administreras av dataskyddsamordnarna. System- och informationsägare kan komma att tilldelas ansvar för specifika delar av registerförteckningen i samarbete med dataskyddsamordnare. Förteckningen ska kunna visas upp för tillsynsmyndigheten på begäran.

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

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

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

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

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

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

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

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

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

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

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

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

Utlämnande av personuppgifter till tredje part
Huvudregeln för Kiruna kommunkoncern är att inte lämna ut personuppgifter till tredje part. De registrerades information kan komma att delas med utförare och leverantörer med kravet att dessa parter godkänner att hålla informationen konfidentiell. Vi kan komma att dela personuppgifter till utförare av kommunala tjänster för att de i sin tur ska utföra delar av våra åtaganden gentemot de registrerade.

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

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

Incidentrapportering
Var och en som upptäcker eller misstänker en incident som skulle kunna innebära en integritetsrisk, ska rapportera detta vidare till dataskyddsamordnare eller dataskyddsombud. Dataskyddsamordnare ska vara behjälplig vid bedömning av risker med incidenten. Det finns

riktlinjer för hur personuppgiftsincidenter ska hanteras inom Kiruna kommunkoncern. En personuppgiftsincident kan vara allt från att någon har tappat en mobiltelefon till en hackerattack där information om medborgare eller kontokortsinformation blivit stulna. Mer information finns även i separat Informationssäkerhetspolicy.

Roller och ansvar
Följande personer har särskilt ansvar för delar av dataskyddsarbetet:

- IT-chef
  Ansvarar för: Informationssäkerheten och upprättande av styrdokument på området
- Kommunchef/VD
  Ansvarar för: att samtliga förvaltningschefer får den information som är nödvändig avseende dataskyddsarbetet så att dessa kan bedöma behov inom sin verksamhet
- Dataskyddsombud
  Ansvarar för: se befintlig arbetsbeskrivning
- Dataskyddsamordnare
  Ansvarar för: att förvaltningarna fortlöpande arbetar med dataskyddsfrågor och att registerförteckning upprättas

Varje förvaltning och avdelning måste säkerställa att uppgifterna behandlas i enlighet med denna policy samt följer kompletterande uppsatta instruktioner.

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

Tillsynsmyndighet
Den ansvariga tillsynsmyndigheten för verksamheten är Datainspektionen.

Enskilda personer som har klagomål gällande Kiruna kommunkoncerns hantering av personuppgifter har rätt att kontakta Datainspektionen.

Kompletterande styrdokument
Vidare riktlinjer och rutiner som rör Kiruna kommunkoncerns personuppgiftsbehandling ska finnas i följande dokument:

- Integritetspolicy
- Informationssäkerhetspolicy
- Riktlinjer och rutiner vid personuppgiftsincidenter
- Riktlinjer och rutiner för fritextfält
- Rutiner och riktlinjer för postöppning och registrering av allmänna handlingar
- Policy för e-posthantering
- Riktlinjer för hantering av sociala medier
- Rutiner för webb
- Rutiner för att hantera begäran om registerutdrag
- Rutiner för information till de registrerade
- Dokumenthanterings- och gallringsplan

Styrdokument upprättas eller revideras fortlöpande vid behov.