

Tjänsteutlåtande

Kommunstyrelsens kontor

Till Kommunstyrelsen

Datum 2018-08-16

Dnr KS 2018/0244

Personuppgiftspolicy

Sammanfattning

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016) för hantering av personuppgifter i Sverige och i hela EU. Dataskyddsförordningen har till syfte att bl.a. att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, samt att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. I dataskyddsförordningen ställs bland annat krav på att den personuppgiftsansvarige ska kunna visa att behandlingen av personuppgifter görs i enlighet med dataskyddsförordningen. Syftet med denna policy är att klargöra Österåkers kommuns övergripande mål och intentioner för hantering av personuppgifter i kommunens verksamheter.

Beslutsförslag

Kommunstyrelsens arbetsutskott föreslår Kommunstyrelsen föreslå Kommunfullmäktige besluta

Anta Personuppgiftspolicy i enlighet med förvaltningens tjänsteutlåtande daterat 2018-08-16.

Bakgrund

Idag är registrering och behandling av personuppgifter är på många områden nödvändig för en fungerande verksamhet. Det är därför viktigt att dessa uppgifter behandlas i enlighet med gällande regelverk i dataskyddsområdet och att den enskildes personliga integritet respekteras samt värnas.

I dataskyddsförordningen finns ett antal viktiga grundläggande principer som har tagits med i denna policy som mål och intentioner för behandling av personuppgifter i Österåkers kommun. Principerna gäller för all personuppgiftsbehandling inom hela kommunens verksamhetsområde.

Förvaltningens slutsatser

Personuppgiftspolicyn ska utgöra en grund för god dataskyddskultur i Österåkers kommun. Kommunens interna styrdokument ska säkra att behandling av personuppgifter sker med hänsyn till den enskildes rättigheter och personlig integritet. Behandlingen ska även ske korrekt med beaktande av gällande dataskyddslagstiftning samt med hög nivå av dataskydd.

Denna policy ska kompletteras med riktlinjer och rutiner på övergripande- och vid behov på förvaltningsnivå. De nämnd- eller förvaltningsövergripande riktlinjerna samt rutinerna för behandling av personuppgifter fastställs av kommunstyrelsens kontor. Varje förvaltning ska även, när det behövs, fastställa riktlinjer och rutiner för behandling av personuppgifter inom sitt specifika ansvarsområde. Varje förvaltning ansvarar för att verkställa samt implementera de övergripande interna styrdokumenterna inom dataskyddsområdet med stöd av kommunstyrelsens kontor.

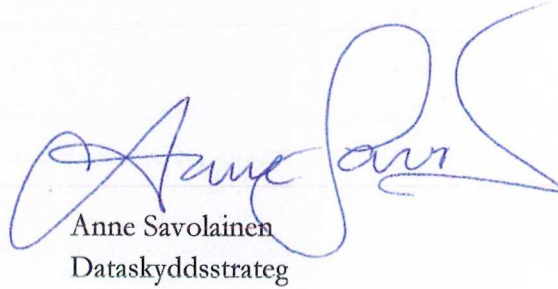
Tjänsteutlåtande

Bilagor

1. Personuppgiftspolicy



Jan-Olof Friman
Kommundirektör

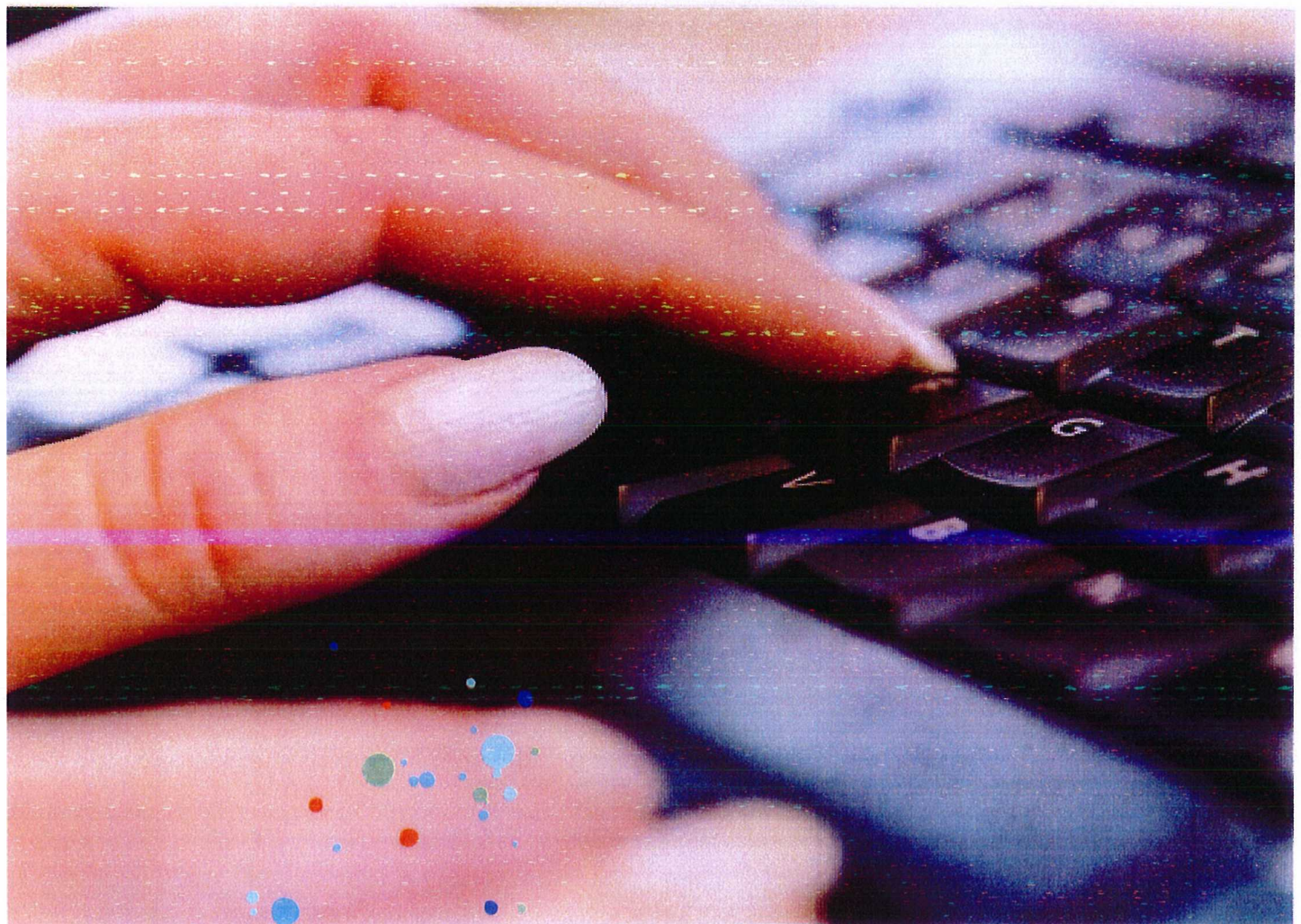


Anne Savolainen
Dataskyddsstrateg

Expedieras

- Akt

Personuppgiftspolicy



Personuppgiftspolicy

Detta dokument gäller för Österåkers kommuns samtliga nämnder samt styrelser och fastställer övergripande mål och intentioner för hantering av personuppgifter i kommunens verksamheter. Dessa mål och intentioner ska även tas i hänsyn i samband med upphandlingar och köp av tjänster.

Skyddet för personuppgifter samt personlig integritet framgår bland annat av EU:s stadga om de grundläggande rättigheterna, Europakonventionen, Regeringsformen samt av EU:s dataskyddsförordning som har till syfte att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. I Österåkers kommun ska personuppgifter skyddas samt den personliga integriteten värnas genom hög nivå av dataskydd samt laglig och ändamålsenlig behandling av personuppgifter. Målet är att de, som på olika sätt är i kontakt med kommunen, bor eller är anställda i kommunen, ska känna sig trygga hur information om dem hanteras.

Grundläggande principer

Vid behandling av personuppgifter ska följande grundläggande principer tillämpas:

- Behandlingen ska vara *laglig, korrekt* och *öppen* gentemot den registrerade
- Personuppgifter ska endast behandlas för berättigat ändamål som är fastställt innan behandlingen påbörjas – *ändamålsbegränsning*
- Personuppgifter som samlas in ska vara *riktiga*, uppdaterade, samt relevanta
- Insamlingen får inte vara mer omfattande än nödvändigt – *uppgiftsminimering*
- Insamlade personuppgifter får bara bevaras i identifierbar form så länge det är nödvändigt för ändamålet – *lagringsminimering*
- Personuppgifter ska raderas när de inte längre behövs
- Endast behöriga ska få åtkomst till personuppgifter – *åtkomstbegränsning*
- Tekniska och organisatoriska åtgärder baserade på riskanalyser och informations- och säkerhetsklassningar ska skydda personuppgifterna – *integritet* och *konfidentialitet* – samt att inbyggt dataskydd och lämpliga säkerhetsmekanismer ska användas
- Vid varje behandling av personuppgifter ska ett sådant förhållningssätt iakttas så att risk för skada för den registrerade minimeras
- Det ska säkerställas att alla medarbetare har relevanta kunskaper om lagar och förordningar på dataskyddsområdet
- Den personuppgiftsansvarige ska kunna *visa* att behandlingen sker med följsamhet till principerna och att man lever upp till de fastställda dataskyddskraven – *ansvarsskyldighet*
- Varje personuppgiftsansvarig ska utse ett dataskyddsombud