



KRISTINESTAD
KRISTIINANKAUPUNKI

Informationssäkerhetspolicy

Kristinestad

Daterad 17.9.2019



PB 13, 64101 KRISTINESTAD
PL 13, 64101 KRISTIINANKAUPUNKI
Tel. / Puh. +358 (0)6 221 6200
kristinestad@krs.fi / kristiinankaupunki@krs.fi
WWW . kristinestad.fi
kristiinankaupunki.fi



PB 13, 64101 KRISTINESTAD
PL 13, 64101 KRISTIINANKAUPUNKI
Tel. / Puh. +358 (0)6 221 6200
kristinestad@krs.fi / kristiinankaupunki@krs.fi

WWW kristinestad.fi
kristiinankaupunki.fi

INNEHÅLL

UTGÅNGSPUNKTEN FÖR FÖRESKRIFTERNA.....	3
DATASÄKERHET OCH DATASKYDD	3
MÅLET MED DATASÄKERHETS- OCH DATASKYDDSARBETET	3
BEHANDLING AV PERSONUPPGIFTER.....	3
FAKTORER SOM STYR VERKSAMHETEN.....	4
ORGANISERING OCH ANSVAR	4
FÖRVERKLIGANDE AV DATASÄKERHETSARBETET.....	6
HANTERING AV DATASÄKERHETSRISKER	6
INFORMERING	6
VERKSAMHETEN I UNDANTAGSFÖRHÅLLANDEN	6





PB 13, 64101 KRISTINESTAD
PL 13, 64101 KRISTIINANKAUPUNKI
Tel. / Puh. +358 (0)6 221 6200
kristinestad@krs.fi / kristiinankaupunki@krs.fi

WWW.kristinestad.fi
WWW.kristiinankaupunki.fi

UTGÅNGSPUNKTEN FÖR FÖRESKRIFTERNA

Kristinestads Informationssäkerhetspolicy är ett ställningstagande som stadens ledning godkänt och som definierar och stöder förverkligandet och utvecklandet av datasäkerhetsarbetet samt hur målen för detta uppnås i organisationen.

DATASÄKERHET OCH DATASKYDD

Med datasäkerhet avses skyddande av hantering och arkivering av information, informationens hanteringsprocesser, metoder och redskap som används för skyddande av information samt utrymmenas datasäkerhetsegenskaper.

Med dataskydd avses skydd av personuppgifter från olovligt missbruk som skadar person. I dataskyddet ingår privata personers integritetsskydd samt de rättigheter och förmåner som tryggar detta vid hanteringen av personuppgifter.

MÅLET MED DATASÄKERHETS- OCH DATASKYDDSARBETET

I staden Kristinestads serviceproduktion hanteras stadens interna, kundernas och intressentgruppernas uppgifter. En del av uppgifterna är känsliga eller konfidentiella och en del är offentliga.

Det primära målet med datasäkerhetsarbetet är att på ett ändamålsenligt sätt hantera all information som behandlas och upprätthålls i stadens funktioner och service samt bevara konfidentialiteten och att datasystemen och datakommunikationen skyddas med administrativa och tekniska åtgärder under normala- och undantagsförhållanden. På så sätt säkerställs en störningsfri funktion och förhindras obehörig användning, oavsiktlig eller avsiktlig förstörelse eller förvrängning av information.

Målet med dataskyddsarbetet är att i alla skeden av databehandlingen från den tidpunkt då informationen skapas ända tills den arkiveras och förstörs skydda personens integritet och personuppgifter för obehörig användning som skadar personen.

BEHANDLING AV PERSONUPPGIFTER

Europeiska unionens allmänna dataskyddsförordning (GDPR) trädde i kraft i maj 2016 och den tillämpas nationellt från den 25 maj 2018. Den allmänna



dataskyddsförordningen är direkt tillämplig lagstiftning, som också ska följas i kommunernas verksamhet. I och med detta preciseras och förenhetligas reglerna för behandling av personuppgifter i EU:s medlemsländer. Dataskyddsförordningen tillämpas på behandlingen av personuppgifter både inom den offentliga och den privata sektorn. Syftet med förordningen är att säkerställa människors rätt till skydd av sina personuppgifter och därmed deras rätt till skydd för privatlivet också i digitaliseringens tid.

Kristinestads stad behandlar personuppgifter på rättsligt samt behörigt sätt och i enlighet med bestämmelserna i EU:s dataskyddsförordning samt andra lagar som föreskriver säker behandling av personuppgifter. De register över personuppgifter eller behandlingar som berör personuppgifter som kommunen hanterar behövs för hanteringen av de tjänster som kommunen erbjuder, handhar och ansvarar för. Varje personuppgiftsbehandling som kommunen utför innehåller endast sådana uppgifter som är absolut nödvändiga för ett specifikt ändamål. Registren innehåller främst personuppgifter som namn, personsignum, adress, telefonnummer och elektroniska adresser. Enligt dataskyddsförordningen ska den registrerade på begäran få veta vilka personuppgifter om honom eller henne som lagras i ett register och på vilka rättsliga grunder de behandlas. Genom att utöva sin rätt till insyn kan den registrerade även kräva att en felaktig uppgift korrigeras.

FAKTORER SOM STYR VERKSAMHETEN

Stadens datasäkerhetsarbete styrs av lagstiftningen, myndighetsbestämmelser, anvisningar samt allmänna datasäkerhetsstandarder och dessa förpliktar också staden att följa datasäkerhetsföreskrifterna.

ORGANISERING OCH ANSVAR

Stadsstyrelsen godkänner föreskrifterna och de föreslagna ändringarna och följer upp förverkligandet av datasäkerhets- och dataskyddsarbetet i staden.

Stadsdirektören har det övergripande ansvaret för datasäkerhets- och dataskyddsarbetet samt rapporteringen till stadsstyrelsen. Stadsdirektören äger och godkänner föreskrifterna samt övriga därtill direkt anslutna anvisningar och riktlinjer på stadsnivå. Centrala ledningsgruppen stöder stadsdirektören i datasäkerhetsärendena.

Dotterbolagens styrelser och verkställande direktörer ansvarar inom sina organisationer för förverkligandet av datasäkerheten och dataskyddet.

Serviceområdets direktör svarar för riskhantering och beredskap samt informationssäkerheten och dataskyddet inom sitt serviceområde.

Förmannen ansvarar inom sitt eget ansvarsområde för att datasäkerheten och dataskyddet förverkligas. Förmannen har till uppgift att implementera datasäkerhetsföreskrifterna och datasäkerhetsansvaren som ingår i de anställdas arbetsuppgifter i organisationen. Då ett anställningsförhållande upphör eller en person övergår till andra uppgifter ansvarar förmannen dessutom för att data och annan egendom återbördas till staden samt att åtgärder som behövs för att avlägsna den anställdas användarrättigheter och -behörigheter vidtas.

Personalen och alla tjänsteinnehavare och arbetstagare som hanterar stadens uppgifter samt andra användare av datasystemen har skyldighet och ansvar att bekanta sig med givna anvisningar och användningsregler samt att iaktta dem. Alla som använder datasystemen har dessutom skyldighet att rapportera problem som upptäcks i anslutning till datasäkerheten och dataskyddet, misstänkt missbruk av eller brott mot datasäkerheten till ledningen för sin egen organisation.

Utomstående leverantörer och serviceproducenter ska förbinda sig att följa de datasäkerhetsanvisningar som staden fastställt och om dessa överenskomms då serviceavtal ingås. Utomstående leverantörer och serviceproducenter rapporterar till kontaktpersonen som ansvarar för beställningen/avtalet.

Dokumentförvaltningen ansvarar för klassificeringen av informationen och säkerställande av enhetligheten samt lagring i den miljö som klassificeringen förutsätter.

Datasystemets/processens ägare ansvarar för riskhanteringen och förverkligandet av datasäkerheten och dataskyddet i anslutning till datasystemet och dess information. Datasystemets ägare godkänner användarrättigheterna till datasystemet på basis av förmannens ansökan.

ICT-direktören främjar förverkligandet av datasäkerheten i staden. Han/hon ansvarar för den tekniska datasäkerheten samt beredningen och upprätthållandet av föreskrifterna och övriga anvisningar. ICT-direktören rapporterar om datasäkerhetens förverkligande till stadsdirektören och ansvarar för kommunikationen i anslutning till datasäkerheten.



PB 13, 64101 KRISTINESTAD
PL 13, 64101 KRISTIINANKAUPUNKI
Tel. / Puh. +358 (0)6 221 6200

kristinestad@krs.fi / kristiinankaupunki@krs.fi

WWW.kristinestad.fi
WWW.kristiinankaupunki.fi

Personalförvaltningen ansvarar för och främjar förverkligandet av datasäkerheten och dataskyddet i personalprocessen samt stöder anvisningen av personalen för upprätthållande av datasäkerhets och dataskyddsnivån.

FÖRVERKLIGANDE AV DATASÄKERHETSARBETET

Förverkligandet av målen med datasäkerhetsarbetet främjas genom stadens interna anvisningar, information och tekniska ändringar. Målet är att säkerställandet av datasäkerheten och dataskyddet ska vara en naturlig del av stadens tjänster och å sin sida en del av den enskilde användarens arbetsätt.

HANTERING AV DATASÄKERHETSRIKER

Datasäkerhetsrisker utvärderas på basis av hur de inverkar på verksamheten. Hot mot datasäkerheten som eventuellt berör organisationen övervakas fortlöpande och målet är att aktivt minska eller helt eliminera inverkningarna av identifierade risker.

INFORMERING

Föreskrifterna som fastställts av staden liksom även de senaste versionerna av därtill hörande anvisningar finns kontinuerligt tillgängliga för alla stadens anställda.

VERKSAMHETEN I UNDANTAGSFÖRHÅLLANDEN

I undantagsförhållanden vidtas åtgärder som fastställts i föreskrifterna i mån av möjlighet. Målet är att också i undantagssituationer med både tekniska och administrativa lösningar bevara datasäkerhetsnivån, trygga kontinuiteten för de mest kritiska funktionerna och återställa verksamheten till normal nivå med så små skador som möjligt.

