**KASKÖ STADS DATASÄKERHETSPOLICY / UTKAST**

1. **Inledning**

Information är en central resurs i Kaskö stads verksamhet och serviceproduktion. För att information ska kunna utnyttjas effektivt, ska informationshanteringen och -behandlingen fungera ändamålsenligt i alla situationer.

I detta dokument fastställer stadens ledning principer, linjeringar, ansvar och mål som gäller informationsskydd och datasäkerhet. Dokumentet utgör en grund för anvisningar som gäller stadens informationsskydd och datasäkerhet. Anvisningarnas syfte är att specificera innehållet i detta dokument och att fungera som hjälp vid dess tillämpning i praktiken.

Datasäkerhetspolicyn gäller alla stadens anställda och representanter för intressentgrupper, som i sitt arbete eller i anslutning till sina uppdrag behandlar uppgifter som ägs eller förvaltas av staden.

Datasäkerhetspolicyn tillämpas på all information och annan data (senare data) oberoende av hur data framställs, i vilken form, dess skyddsnivå, skedet av livscykeln, omgivningen där den förekommer eller transmissionsvägen.

1. **Överensstämmelse och syfte**

Utöver förpliktande lagstiftning ställer också stadens verksamhetsmiljö vissa krav på stadens informationsskydd och datasäkerhet. Förutom stadens egna anvisningar och direktiv styrs informationsskyddet och datasäkerheten av följande författningar, bestämmelser och anvisningar:

* EU:s Allmänna Dataskyddsförordning: (EU) 2016/679 samt Dataskyddlag 1050/2018
* Statsrådets förordning om informationssäkerheten inom statsförvaltningen: 681/2010, 5§
* Ledningsgruppens för datasäkerheten inom statsförvaltningen (VAHTI) anvisningar

Syftet med kommunens informationssäkerhets- och dataskyddsarbete är att likrikta kommunens interna säkerhetspraxis genom att utveckla kommunens säkerhetskultur.

Inom organisationen, i processer, i projekt och inom datasystem bör man sörja för hanteringen av risker i anslutning till informationssäkerhet och dataskydd samt informationsteknik i allmänhet.

1. **Informationssäkerhet och dataskydd**

Med informationssäkerhet i kommunen avses administrativa, tekniska och andra medel för skyddande av data som kommunen äger eller administrerar i normal- och störningssituationer samt i undantagsförhållanden.

För att realiseras kräver informationssäkerheten förverkligande av följande värden, vars betydelse varierar från fall till fall:

-Konfidentialitet: Informationen finns till hands endast för dem som har befogenheter för det.

-Integritet: Informationen har inte ändrats avsiktligt eller oavsiktligt, och informationen har inte ändrats till följd av tekniska störningar.

-Tillgänglighet: Informationen, datasystemet eller tjänsten finns till hands och är tillgänglig då de behövs, för personer och system som har befogenheter för det.

-Obestridlighet: Samlande av bevis för att säkerställa, att ingen part som tagit del i behandling eller överföring av information kan bestrida sin andel i detta.

Med dataskydd i kommunen avses åtgärder i enlighet med förpliktande dataskyddsbestämmelser, med vilka man tryggar personens tillräckliga integritetsskydd och övriga rättigheter vid behandling av hens personuppgifter.

Personuppgifter som kommunen samlar in och behandlar i egenskap av registeransvarig beskrivs på kommunens dataskyddssidor.

Informationssäkerhet och dataskydd samt till dem anslutna krav som kommunen fastställt, bör beaktas i ett så tidigt skede som möjligt när verksamheten, anskaffningar och tekniska system planeras.

1. **Hot mot informationssäkerhet**

Hoten mot informationssäkerhet utgör en risk för konfidentialitet, integritet och användbarhet av data, datasystem eller telekommunikation.

Personers eventuella inkompetens, vårdslöshet eller likgiltighet utgör de ansenligaste hoten mot organisationens informationssäkerhet.

Dessutom föranleds hot av avsiktligt missbruk av information, dataintrång, fel fungerande program och anordningar, virus, skadeprogram, överbelastningsattacker samt tekniska problem.

Betydande hot kan också ha att göra med produktion av utomstående tjänster, om man inte gjort avtal med serviceproducenter om beaktande av angelägenheter i anslutning till informationssäkerhet, dataskydd och beredskap samt sanktioner i samband med överträdelser.

1. **Övergripande säkerhet**

Med övergripande säkerhet avses av kommunen definierade delområden av säkerhet, riskhantering och beredskap, som tillsammans med informationsskydd och datasäkerhet bildar en solid helhet som skydd för kommunens information:

-Cybersäkerhet: Åtgärder med vilka cyberverksamhetsmiljöns konfidentialitet, integritet, tillgänglighet och kontinuitet tryggas.

-Fysisk säkerhet: Åtgärder, system och strukturer med hjälp av vilka stadens utrymmen, i dem befintliga människor, transporter, researbete samt information och annan egendom skyddas mot fysiska och fastighets- och miljöskador, skadeförsök och oberättigade personer.

-Personlig säkerhet: Åtgärder som påverkar informationssäkerheten som utförs under personalprocessen före anställningsförhållandet, under det och i anslutning till dess upphörande.

-Riskhantering: Systematisk verksamhet för riskhantering så, att riskerna står i optimalt förhållande till kostnaderna för riskbegränsning, samtidigt som målen ställda för kommunens verksamhet kan uppnås.

-Beredskap: Tekniska arrangemang och handlingssätt genom vilka kontinuiteten i kommunens verksamhet och service tryggas i normala förhållanden, störningssituationer och undantagsförhållanden.

- Genom tillbörliga och uppdaterade avtal säkerställs förverkligandet av i denna policy beskrivna principer även när det gäller samarbetet med våra intressentgrupper.

1. **Organisation, roller och ansvar**

Allmänt konstateras, att ansvaret för att informationssäkerheten och dataskyddet förverkligas och att datasäkerhetspolicyn följs ligger hos var och en, även om förvaltningen svarar för utveckling och koordinering av den allmänna informationssäkerheten och dataskyddet. **I angelägenheter i anslutning till informationssäkerhet och dataskydd är var och en ansvarig för risker i anslutning till hens kompetens eller beslut.**

Roller och ansvar i anslutning till informationssäkerhet och dataskydd har organiserats på följande sätt i kommunen:

**Stadsstyrelsen** följer upp förverkligandet av informationssäkerheten och dataskyddet i kommunen. Stadsstyrelsen godkänner datasäkerhetspolicyn. Dessutom är stadsstyrelsen ansvarig för ordnandet av stadens interna kontroll och riskhantering.

**Stadsdirektören** har det övergripande ansvaret för förverkligandet av informationssäkerheten och dataskyddet och för rapportering om deras förverkligande till stadsstyrelsen. Dessutom svarar stadsdirektören för stadens säkerhetsplanering och beredskap.

**Förvaltningsdirektören** koordineras datasäkerhetsadministrationen inom stadens organisation. Förvaltningsdirektören fungerar som ledande tjänsteinnehavare för arkivfunktionen och leder arkivarbetsgruppen, som också fungerar som datasäkerhetsgrupp.

**Enhetscheferna** svarar för informationssäkerheten och dataskyddet inom sin enhet samt för den övergripande säkerheten hos enhetens processer.

**Dotterbolagens styrelser och verkställande direktörer** svarar för förverkligandet av informationssäkerheten och dataskyddet samt förverkligandet av den övergripande säkerheten inom sina egna organisationer.

**Förmannen** svarar för förverkligandet av informationssäkerheten och dataskyddet i personalprocessens alla skeden inom sitt eget ansvarsområde.

Förmannens viktigaste uppgifter är att sörja för:

-introduktion av sin organisation i kommunens informationssäkerhets- och dataskyddsanvisningar samt i informationssäkerhets- och dataskyddsansvaret i anslutning till samtliga anställdas arbetsuppgifter;

när arbetstagarens anställningsförhållande upphör eller när personen övergår till andra uppgifter:

-att kommunens information/data och annan egendom återlämnas

-att meddela till huvudanvändaren eller den it-producerande samarbetsparten att arbetstagarens användarrättigheter och -fullmakter ska upphävas.

**Personalen** svarar för sin egen del för att föreskrifter och anvisningar följs. Det är dessutom varje anställds plikt att omedelbart meddela om avvikelser, hot och risker till sin egen förman, den dataskyddsansvarige eller förvaltningsdirektören/it-producerande samarbetsparten.

**Ägaren** till datasystemet eller någon annan teknisk helhet svarar för riskhantering och beredskap i anslutning till sitt system och informationen/data som systemet innehåller, samt för att informationssäkerheten och dataskyddet förverkligas.

**Huvudanvändaren** svarar för sitt systems del för förverkligandet av informationssäkerheten och dataskyddet under ledning av datasystemets ägare.

**Ägaren av data** svarar för klassificering av informationen (definition av offentlighet och sekretess) och säkerställande av integritet samt sparande i den omgivning som klassificeringen förutsätter. När det gäller t.ex. ärenden som behandlas i förtroendeorgan ligger ansvaret hos föredraganden (stadsdirektören, avdelningschefer).

**Den dataskyddsansvarige** främjar förverkligandet av informationssäkerheten och dataskyddet i kommunen. Den dataskyddsansvarige är en oberoende aktör som följer med hur lagstiftningen som styr dataskyddet följs i kommunen. Dessutom samarbetar den dataskyddsansvarige med övervaknings- och andra myndigheter samt ger stöd och råd i informationssäkerhets- och dataskyddsfrågor. Den dataskyddsansvarige rapporterar till stadsdirektören om förverkligandet av informationssäkerheten och dataskyddet samt svarar tillsammans med förvaltningsdirektören för kommunikationen i samband med informationssäkerheten och dataskyddet. Till uppgiften som dataskyddsansvarig har stadsstyrelsen i Kaskö valt det utomstående bolaget Oy Black Label Bytes Ab.

**Dataskyddsgruppen** fungerar som stöd för den dataskyddsansvarige. Dataskyddsgruppen följer med informationssäkerhetens och dataskyddets allmänna utveckling, hot och risker samt förverkligandet av informationssäkerheten och dataskyddet i kommunen. Gruppen analyserar och bedömer den ovan nämnda helheten och ger på basis av detta förslag till förbättringar angående kommunens informationssäkerhet och dataskydd. Dessutom fungerar gruppen, tillsammans med den dataskyddsansvarige, som stöd för kommunen i informationssäkerhet- och dataskyddsfrågor. Dataskyddsgruppen utses av stadsstyrelsen. Som dataskyddsgrupp fungerar stadens arkivarbetsgrupp.

**Den interna kontrollen** svarar för att informationssäkerheten förverkligas på vederbörligt sätt, i tillräcklig omfattning och att den granskas.

**Ledningsgruppen** svarar för kommunens säkerhetsplanering och beredskap.

Yttre **intressentgrupper** svarar för sin del för förverkligandet av informationssäkerheten och dataskyddet i enlighet med de krav som kommunen ställt och beskrivit i avtalen.

1. **Användning av data och datasystem**

I kommunens datasystemomgivning används av stadsstyrelsen godkända datasystem, anordningar och programvara, som är avsedda för skötseln av arbetsuppgifter. Endast stadsdirektören eller av stadsdirektören befullmäktigad person får göra ändringar i kommunens datasystemomgivning. Rätt till tillträde till kommunens datanät och -system samt nyttjanderätt till data som ägs och förvaltas av kommunen beviljas i den omfattning som skötseln av arbetsuppgifterna kräver.

1. **Förverkligande av informationssäkerhet och dataskydd**

Informationssäkerheten och dataskyddet förverkligas genom lednings- och annan praxis vars mål är en ständig förbättring. Centralt i detta förverkligande är, att staden ska ha tillräckliga färdigheter att upprätthålla sin säkerhetskultur bl.a. på följande sätt:

-Informationssäkerheten och dataskyddet leds systematiskt

-Personalens kunnighet upprätthålls genom kontinuerlig skolning

-Verksamhetsmiljöns tillstånd uppföljs aktivt

-Hot- och riskmiljön bedöms regelbundet och man reagerar på det sätt som situationen förutsätter

-Man förbereder sig på avvikelser och störningar genom att upprätthålla, öva och testa nödvändiga kontinuitets- och andra planer.

1. **Kaskö stads datasäkerhetspraxis vid behandling av personuppgifter**

**Behandling av personuppgifter i ärenden som hör till kommunens kompetensområde**

I kommunen kan man anhängiggöra ett ärende skriftligt, per email eller i undantagsfall muntligt. Handlingar i anslutning till anhängiggjorda ärenden förvaras av ärendets beredare eller beslutsfattare tills ärendet avgjorts, varvid de överförs till kommunens arkiv.

Ändamålet för användning av uppgifter är behandling av anhängiggjorda ärenden på det sätt som förutsätts i lagstiftningen, eller planering och förverkligande av myndighetsverksamhet och annan verksamhet.

Förvaringstider för personuppgifter i anslutning till anhängiggjorda ärenden som kommunen behandlar definieras enligt arkivlagen (831/1994), arkivverkets bestämmelser (AL16465/07.01.01.03.02/2016) och kommunens arkivbildningsplan.

**Vilka uppgifter behandlas av kommunen**

Ärenden som anhängiggjorts i kommunen ges till ärendets beredare eller beslutsfattare, som förvarar ärendet i ett låst utrymme tills ärendet avgjorts eller överförts vidare.

Omfattningen av uppgifter som behandlas beror på ärendets natur och vilka uppgifter i anslutning till ärendet som tillställts kommunen.

Vanligtvis behandlas åtminstone följande uppgifter:

* namn på den som anhängiggjort ärendet
* kontaktuppgifter som anhängiggöraren gett till kommunen, t.ex. telefonnummer, e-mailadress och/eller postadress
* ärendets beskrivning
* uppgifter gällande ärendets behandlingsskeden

**Vad baserar sig uppgiftsbehandlingen i kommunen på**

Vi behandlar personuppgifter för att utföra uppgifter som gäller det allmänna bästa och för att använda till kommunen hörande offentlig makt:

-Dataskyddsförordningen (EU 2016/679) artikel 6

Vi behandlar särskilda personuppgiftsgrupper på basis av det allmänna bästa i stöd av nationell lagstiftning:

- Dataskyddsförordning (EU 2016/679) artikel 9 punkt 2

- Personuppgiftslag (523/1999) 12 § 1 mom. punkt 5

Om kommunens uppgifter och befogenheter stadgas:

-KommunalL 410/2015

**Utlämnande av uppgifter**

Uppgifter utlämnas vanligen inte.

Uppgifter utlämnas på begäran enligt lagen om offentlighet i myndigheternas verksamhet. Uppgifter och handlingar är offentliga om de inte uttryckligen i lagen stadgas att de ska hållas hemliga.

-OffentlighetsL 621/1999

**Dataskyddsrättigheter i samband med behandling av personuppgifter**

**Rätt till information om behandling av personuppgifter**

-Kunden har rätt att få veta för vilka ändamål och på vilka sätt vi behandlar hans/hennes personuppgifter.

**Rätt till tillgång**

-Kunden har rätt att få veta om vi behandlar personuppgifter som gäller honom/henne. Om så är fallet, har kunden rätt att få en kopia av dessa uppgifter, om kommunen inte har laga grund till att vägra att ge ut uppgifterna.

**Rätt till rättelse**

-Om kundens personuppgifter som vi behandlar är felaktiga, kan kunden begära rättelse av uppgifterna av kommunen

-Om kommunen rättar uppgifter på kundens begäran är kommunen skyldig att i mån av möjlighet meddela om rättelsen till alla som man utlämnat uppgifter åt tidigare.

**Rätt till begränsning av behandling**

-Om kunden anser att de uppgifter om honom/henne som kommunen behandlar är felaktiga, att behandlingen är olaglig eller om den registrerade har invänt mot behandling av sina uppgifter, kan han/hon begära begränsning av deras användning.

Härvid kan kommunen behandla kundens uppgifter endast

* med den registrerades samtycke
* om kommunen behöver uppgifter för att uppgöra, framställa eller försvara rättsliga anspråk
* för skäl som rör ett viktigt allmänintresse, eller
* för att skydda någon annan persons rättigheter
* om kommunen begränsar behandlingen av uppgifter på kundens begäran, är kommunen skyldig att i mån av möjlighet underrätta var och en som uppgifter tidigare lämnats ut åt

**Rätt att göra invändningar**

I vissa fall kan kunden också göra invändningar mot behandling av sina personuppgifter, m. a. o. begära att uppgifterna inte behandlas överhuvudtaget.

Invändningar kan göras om registratorn behandlar kundens uppgifter p.g.a. allmänt intresse eller av myndighetsskäl eller på basis av sina berättigade intressen. Kunden kan göra invändningar mot behandling av sina uppgifter av skäl som hänför sig till hans/hennes specifika situation.

Begäran angående dataskyddsrättigheter ska tillställas kommunen per email (info@kaskinen.fi), per post eller inlämnas personligen (Kaskö stad, Rådhusgatan 34, 64260 Kaskö).

På begäran ska uppges

-vill kunden begränsa eller motsätta sig behandlingen av sina personuppgifter

-motiveringat för begränsning eller motsättning av behandlingen

-kundens namn

-kundens kontaktuppgifter (t.ex. e-mailadress eller telefonnummer).

Begäran behandlas i kommunen och om begäran fattas ett tjänsteinnehavarbeslut.

Kommunen gör ingen profilering på basis av de behandlade personuppgifterna.

**Alla ansökningar om uppgifter och rättelser av personuppgifter inlämnas antingen personligen eller egenhändigt undertecknade, eller i något annat på ett tillförlitligt sätt bekräftat dokument, till Kaskö stads förvaltningsavdelning, adress Rådhusgatan 34, 64260 Kaskö.**

1. **Underhåll av dokument**

För regelbunden utvärdering och uppdatering av denna handling svarar stadsdirektören eller av honom/henne utsedd part. Dokumentet finns fritt att få i adressen www.kaskinen.fi.

Stadens informationssäkerhets- och dataskyddsdokumentation i sin helhet finns tillgänglig för personalen i kommunens interna informationskanaler i den omfattning som arbetsuppgifterna förutsätter.