

|                                  |                 |                     |                           |                        |
|----------------------------------|-----------------|---------------------|---------------------------|------------------------|
| UTFÄRDARE<br>Ali Ababneh         |                 |                     | DOKUMENTTYP<br>Riktlinjer |                        |
| BESLUTAD AV<br>KOMMUNFULLMÄKTIGE | DIARE<br>NUMMER | DATUM<br>2023-01-25 | VERSION<br>1.0            | DOKUMENTIDENTIFIKATION |

**Dataskyddss riktlinjer i Haparanda stad.**



**PROGRAM**

Uttrycker värdegrund och önskvärd utveckling av verksamheten.

**POLICY**

Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

**STRATEGI**

Konkretiserar ett program eller en policy och utgör en grund för prioritering.

**HANDLINGSPLAN**

Beskriver konkreta mål och åtgärder.

**RIKTLINJER**

Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande

## Innehållsförteckning

|   |    |
|---|----|
| INLEDNING.....  | 5  |
| DEFINITIONER.....   | 5  |
| ANSVARSFÖRDELNING.....  | 6  |
| HAPARANDA KOMMUNS HANTERING AV PERSONUPPGIFTER.....             | 7  |
| Personuppgiftsansvarig.....                                     | 7  |
| GDPR-arbetsgrupp.....   | 7  |
| Behandling av personuppgifter.....                              | 7  |
| Personuppgiftsincidenter.....                                   | 8  |
| Personuppgiftsbiträdesavtal.....                                | 8  |
| Att tänka på vid upphandling.....                               | 8  |
| Lagring och arkivering av personuppgifter.....                  | 9  |
| Information till den registrerade.....                          | 9  |
| Gallring och arkivering i Office 365.....                       | 10 |
| E-post.....   | 10 |
| Chat och inlägg i Microsoft Teams.....                          | 10 |
| Behörighet till personuppgifter.....                            | 11 |
| Grund för behandling av personuppgifter.....                    | 11 |
| PUBLICERING AV PERSONUPPGIFTER PÅ INTERNET.....                 | 12 |
| Ansvar över publiceringen.....                                  | 12 |
| Kontroll före publicering.....                                  | 12 |
| Publicering av personuppgifter i form av foto/film.....         | 13 |
| Förbud mot publicering.....                                     | 13 |
| PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER.....                | 13 |
| Kommunens arbete med efterlevnad av dataskyddsförordningen..... | 13 |
| Information och registerutdrag.....                             | 14 |
| Principer för insamlande av personuppgifter.....                | 14 |
| Korrekta personuppgifter.....                                   | 14 |
| Lagringstid för personuppgifter.....                            | 14 |
| Säkerhet som princip.....                                       | 15 |
| Dataskyddsförordningen och offentlighetsprincipen.....          | 15 |
| Skyddsvärda/integritetskänsliga personuppgifter.....            | 15 |
| Känsliga personuppgifter.....                                   | 16 |
| KONSEKVENSBEDÖMNING.....  | 17 |
| INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD.....               | 17 |
| INFORMATION OCH KOMMUNIKATION.....                              | 17 |
| DEN REGISTRERADES RÄTTIGHETER.....                              | 18 |
| Rätt till insyn.....  | 18 |
| Rätt till ändring.....  | 18 |
| Rätten att bli bortglömd.....                                   | 18 |
| Rätt till begräsning.....                                       | 18 |
| Rätt till dataportabilitet.....                                 | 18 |
| Återkallande av samtycke.....                                   | 18 |
| Invända mot behandling.....                                     | 18 |

|   |    |
|---|----|
| Rätt att lämna klagomål.....                          | 18 |
| SANKTIONSAVGIFTER.....                                | 19 |
| ÖVERFÖRING TILL TREDJE LAND.....                      | 19 |
| särskilda regler för överföring utanför EU/EES? ..... | 19 |
| När är överföring utanför EU/EES tillåten?.....       | 20 |
| KONTAKT, FRÅGOR ELLER MER INFORMATION.....            | 20 |
| KLAGOMÅL.....   | 20 |
| MER OM DATASKYDDSFÖRORDNINGEN.....                    | 20 |

## INLEDNING

Detta dataskyddsdokument är uppdelad i två avsnitt, ett som reglerar hur Haparanda kommuns anställda ska hantera personuppgifter och ett som informerar hur Haparanda kommun behandlar personuppgifter. Dokumentets båda delar är dock bindande för Haparanda kommuns personuppgiftsansvariga.

Dataskyddspolicyn utgår från bestämmelserna i Europaparlamentet och rådets förordning (EU) 2016/679 av 27.4.2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan Dataskyddsförordningen eller GDPR).

Genom dataskyddsförordningen kommer den personuppgiftsansvariges ansvar och skyldigheter att förtydligas och de registrerades rättigheter kommer att förstärkas. En anpassning till den nya förordningen kräver att kommunen ser över och tar fram riktlinjer för hur personuppgifter hanteras.

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra krav på ökad dokumentation.

## DEFINITIONER

### Personuppgift

Med personuppgift avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Typiska personuppgifter är personnummer, namn, adress, e-postadress och telefonnummer. Bilder, filmer och ljudupptagningar av individer kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer och cookies, räknas som personuppgifter om de kan kopplas till fysiska personer. Även information som har kodats, krypterats eller pseudonymiserats men som kan hänföras till en fysisk person med hjälp av kompletterande uppgifter är personuppgifter.

### 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.

### Den registrerade

Den registrerade är den person vars personuppgifter behandlas inom våra olika verksamheter. Exempel på registrerade är exempelvis anställda, förtroendevalda, förskolebarn, elever, brukare, äldre och medborgare i kommunen.

### Personuppgiftsbiträde

Ett personuppgiftsbiträde behandlar personuppgifter på uppdrag av den personuppgiftsansvarige. Exempel på en biträdessituation är när en IT-leverantör behandlar personuppgifter genom att tillhandahålla support till ett system eller en tjänst

# ANSVARSFÖRDELNING

## Nämnden är personuppgiftsansvarig

Varje nämnd och revisionen är personuppgiftsansvarig för all personuppgiftsbehandling i sin verksamhet. Ansvaret kan inte delegeras.

Ansvaret gäller såväl uppgifter om anställda och förtroendevalda som uppgifter om medborgare, barn/elever, brukare/klienter, kunder och affärskontakter. Ansvaret omfattar även personuppgiftsbehandling som sker för kommunens räkning via ett personuppgiftsbiträde.

Personuppgiftsansvaret är omfattande och följande lista tjänar som vägledning för vad som ingår.

**Listan är inte uttömmande.**

Personuppgiftsansvarig ansvarar bland annat för att:

- all personuppgiftsbehandling alltid följer rådande dataskyddslagstiftning,
- försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
- upprätthålla registerförteckning över samtliga personuppgiftsbehandlingar i den ansvariges verksamhet,
- säkerställa att medarbetarna har nödvändig kompetens för att kunna följa dataskyddslagstiftningen,
- säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning,
- säkerställa att personuppgiftsincidenter hanteras i enlighet med lagstiftningens krav,
- utse dataskyddsombud och anmäla dess kontaktuppgifter till tillsynsmyndigheten,
- stödja dataskyddsombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens.

## Kommunsledningsförvaltning

Kommunsledningsförvaltning har central stödfunktion för nämnderna och ansvarar för att erbjuda samverkan, stöd och hjälp, grundläggande utbildning samt verktyg för att upprätta registerförteckning. Kommunsledningsförvaltning ansvarar för att sammankalla och leda kommunens dataskyddsarbetsgrupp.

## Ledningen

Kommundirektören och förvaltningscheferna har det övergripande ansvaret för att dessa riktlinjer integreras i organisationens dagliga arbete. Förvaltningschefer ansvarar för att respektive verksamhet har relevanta rutiner och/eller arbetsinstruktioner samt för att förvaltningen har en representant i kommunens dataskyddsarbetsgrupp.

## Dataskyddssamordnare

Dataskyddssamordnare är en funktion som ska finnas inom varje förvaltning. Rollen kan kombineras med andra arbetsuppgifter om det bedöms möjligt. Dataskyddssamordnaren är en stödfunktion och är förvaltningens representant i kommunens dataskyddsarbetsgrupp.

Ansvaret för att lagstiftning efterlevs vilar alltid på den personuppgiftsansvarige och ansvaret kan inte delegeras.

Dataskyddssamordnaren stöttar verksamhet, ledningen och personuppgiftsansvarig genom lämpligtvis men inte uteslutande följande uppgifter:

- löpande uppdatera och följa upp registerförteckningen,
- löpande följa upp att samtliga personuppgiftsbehandlingar analyseras i en risk- och konsekvensbedömning,
- löpande följa upp att konsekvensbedömning avseende dataskydd (DPIA) genomförs i de fall lagstiftningen kräver detta,

- administrera begäran om registerutdrag,
- ge råd och stöd och påtala brister till verksamhetens ledning och berörd personal i frågor rörande dataskydd,
- följa upp att verksamheten genomför grundutbildning för varje medarbetare och i övrigt föreslå och följa upp kompetensutveckling,
- vara stöd vid upprättande av personuppgiftsbiträdesavtal,
- hålla sig underrättad om utveckling av lagstiftningen och praxis inom området,
- löpande följa upp att de kommunövergripande och förvaltningsspecifika rutinerna för hantering och anmälan av personuppgiftsincidenter är kända i verksamheten,
- bidra till utvecklingen av kommungemensamma rutiner och arbetssätt,
- föreslå förvaltningsspecifika rutiner och arbetsinstruktioner i de fall det behövs,
- rådfråga och samråda med dataskyddsombudet för verksamhetens räkning,
- vara dataskyddsombudets och kommunkontorets kontaktperson i dataskyddsfrågor samt delta i kommunens dataskyddsarbetsgrupp.

### **Dataskyddsombud**

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Funktionen ska agera självständigt och får inte ta emot instruktioner eller bli föremål för sanktioner för att utfört sina arbetsuppgifter. Dataskyddsombudet har bland annat i uppdrag att övervaka efterlevnaden av dataskyddslagstiftningen genom granskning och att informera och vara rådgivande i dataskyddsarbetet. Dataskyddsombudets kontaktuppgifter ska anmälas till tillsynsmyndigheten.

### **Övriga chefer och medarbetare**

Samtliga medarbetare har ett ansvar för att behandlingen av personuppgifter utförs på ett korrekt och lagligt sätt. Riktlinjer, rutiner och arbetsinstruktioner ska vara kända inom organisationen och det åligger varje chef att förmedla vikten av att följa gällande styrdokument.

## **HAPARANDA KOMMUNS HANTERING AV PERSONUPPGIFTER**

### **Personuppgiftsansvarig**

Det är respektive nämnden eller styrelsen i den förvaltning eller det bolag i kommunen som är personuppgiftsansvarig för de personuppgifter som behandlas inom verksamhetsområdet.

### **GDPR-arbetsgrupp**

Haparanda kommun har en GDPR-grupp som består av medarbetare från varje förvaltning och olika enheter. Gruppens uppgift är att se till att GDPR efterlevs och följa den framtida utvecklingen inom dataskyddsförordningens regler och avsikter. Gruppen ser över och tar fram riktlinjer för hur personuppgifter hanteras inom Haparanda kommuns verksamheter. I uppgiften ingår att informera, utbilda, bistå medarbetare samt utreda eventuella incidenter relaterade till dataskyddsförordningen.

### **Behandling av personuppgifter**

Som behandling av personuppgifter räknas enligt dataskyddsförordningen en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med lagring avses inte arkivering utan avser lagring av aktuella personuppgifter. När något arkiverats anses personuppgiften inte längre vara under behandling.

Personuppgifter är bara sådana uppgifter som kan härledas till en fysiskt levande person. Uppgifter om avlidna är inte en personuppgift och uppgifter som härleds till juridiska personer är inte heller personuppgifter.

Haparanda kommun har tagit framme en GDPR-guide<sup>1</sup> och Handbok<sup>2</sup> för alla medarbetare och publicerade på hemsidan och intranätet

## Personuppgiftsincidenter

En personuppgiftsincident enligt artikel 4.2 i GDPR är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel på personuppgiftsincident:

- Personuppgift som på något sätt har gått förlorad
- Personuppgift som kommit i orätta händer.

Det har ingen betydelse om ovanstående har skett med eller utan avsikt. Det är i båda fallna personuppgiftsincidenter. En personuppgiftsincident kan innebära risker för den vars personuppgifter det handlar om. Riskerna kan handla om till exempel identitetsstöld, bedrägeri, finansiell förlust, diskriminering eller skadlig ryktesspridning. Om det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter ska den anmälas till tillsynsmyndigheten.

En personuppgiftsincident ska anmälas till tillsynsmyndigheten inom 72 timmar efter att den har upptäckts. Det åligger varje anställd att utan dröjsmål rapportera en personuppgiftsincident i samråd med överordnad. Personuppgiftsincidenten ska även rapporteras till den personuppgiftsansvarige.

Haparanda kommun har tagit fram tydliga incidenthanteringsplaner och processer. De finns tillgänglig på intranätet<sup>3</sup> och personalen ska rapportera en incident så snabbt så möjligt via en e-tjänst<sup>4</sup>.

## Personuppgiftsbiträdesavtal

Ett biträde är den som behandlar personuppgifter för den personuppgiftsansvarig. Ett personuppgiftsbiträdesavtal är ett avtal som ska skrivas mellan personuppgiftsansvarig och kommunens personuppgiftsbiträden. Ett personuppgiftsbiträde är således en aktör som på uppdrag av Haparanda kommun behandlar personuppgifter. Vid behov av personuppgiftsbiträdesavtal bör den personuppgiftsansvarige meddela detta till aktören. Haparanda kommun använder SKR standard personuppgiftsbiträdesavtal mall.

## Att tänka på vid upphandling

Innan inköp av system eller tjänster i vilka personuppgifter kommer att behandlas ska beställaren kartlägga, analysera och ställa krav så att lagstiftningen beaktas. Utgångspunkt för detta är den risk- och konsekvensbedömning som ska genomföras. Personuppgiftsbiträdesavtal ska alltid tecknas i de fall ett personuppgiftsbiträde anlitas.

Innan personuppgiftsbehandlingen påbörjas eller tekniska hjälpmedel köps in ska ändamålet med behandlingen samt den rättsliga grunden vara fastställd. Antalet uppgifter som behandlas ska inte vara fler än vad som är nödvändigt i förhållande till ändamålet, beställaren ska även säkerställa att uppgifterna som samlas in är korrekta.

Lagringsminimering ska tillämpas vilket innebär att personuppgifterna inte förvaras i en form som möjliggör identifiering under längre tid än nödvändigt. Lagring över längre perioder ska följa lagstadgade krav och riktlinjer. Vid bedömning av gallringsfrister i dokumenthanteringsplan ska principen om lagringsminimering beaktas. Att ta bort uppgifter ska följa regler och rutiner för rensning och gallring.

---

<sup>1</sup> <https://www.haparanda.se/kommun-och-politik/om-personuppgifter>

<sup>2</sup>

<https://www.haparanda.se/download/18.4e1a93b016d8b57a913906f9/1572419276541/Handbok%20GDPR.pdf>

<sup>3</sup> <https://www.haparanda.se/intranat/personalrummet/for-mitt-arbete/gdpr-guide-hantera-personuppgifter-ratt>

<sup>4</sup> <https://insidanhaparanda.enamnd.se/oversikt/overview/1679>



För tekniska system där personuppgifter behandlas ska principerna om Dataskydd som standard och Inbyggt dataskydd beaktas. Dataskydd som standard (Privacy by default) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan.

Det kan till exempel handla om att de förvalda inställningarna i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Inbyggt dataskydd (Privacy by design) innebär att hänsyn ska tas till integritetsskyddsreglerna redan när IT-system och rutiner utformas.

## **Lagring och arkivering av personuppgifter**

En av de grundläggande principerna i GDPR är principen om lagringsminimering. Haparanda kommun ska således endast samla in sådana uppgifter som behövs för att kunna utföra kommunens åtagna uppgifter.

När en personuppgiftsansvarigs grund för behandling av personuppgifter upphör (t.ex. när ett barn inte längre är i barnomsorg) ska uppgiften arkiveras alternativt gallras beroende på arkivbestämmelserna. För närvarande sker all arkivering genom papper och elektronisk arkivering är inte möjlig. Arkivering ska ske på separat plats, man kan således inte ha arkiverade personuppgifter på samma plats i till exempel kontoret som man har aktuella personuppgifter.

Kommunens hantering av information omfattas av offentlighetsprincipen och det svenska regelverket kring allmän handling. Det betyder att personuppgifter kommer att hanteras den tid som det behövs och i vissa fall för all framtid enligt bestämmelser i tryckfrihetsförordningen, offentlighets- och sekretesslagen och arkivlagen

## **Information till den registrerade**

Varje registrerad har rätt att veta vilka personuppgifter som en myndighet behandlar. Haparanda kommun är således skyldig att vid förfrågan ge ut uppgifter till den registrerade. Uppgifter som ska ges ut är både strukturerade data och ostrukturerade data. Undantag är personuppgifter som återfinns i löpande text som utgör ett utkast eller en minnesanteckning.

Vid förfrågan från den registrerade ska följande information delges den berörda:

- Ändamål med behandlingen
- Vilka personuppgifter som behandlas
- Till vilka Haparanda kommun lämnat eller kommer att lämna ut uppgifterna
- Om möjligt, en uppskattning hur länge personuppgifterna kommer att behandlas, eller om detta inte är möjligt, de kriterier som används för att fastställa hur länge vi behandlar uppgifterna
- Rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling
- Rätten att inge klagomål till en tillsynsmyndighet
- Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.

Varje personuppgiftsansvarig bör vara beredd på förfrågningar och således ha klara och tydliga motiveringar varför behandling av personuppgifterna sker.

## **Gallring och arkivering i Office 365**

För alla applikationer i Office 365 är det varje systemanvändare ansvarar för att information hanteras korrekt enligt upprättande rutiner och att sekretessmaterial eller skyddsvärd information inte lagras och hanteras i Office 365. All information och kommutation anhållet i Office 365 är allmänna handlingar och vid en begäran kan innehållet efter en sekretessprövning lämnas ut.

## E-post

GDPR påverkar hur användningen av e-post får ske inom Haparanda kommun. Grundregel är att hantering av personuppgifter ska ske utanför e-post i system eller strukturerade dokument som är skyddade från obehöriga.

All e-post som inkommer till Haparanda kommun är en allmän handling. E-post som är av betydelse för verksamheten ska diarieföras, övrig e-post av rutinmässig karaktär ska gallras så fort den är inaktuell i enlighet med kommunens dokumenthanteringsplaner. E-posten är inget dokumentarkiv för lagring av uppgifter.

Ett e-postmeddelande med personuppgifter får inte ligga kvar i inkorgen eller i skickat mappen hur länge som helst. När behandlingen av personuppgiften är klar ska informationen flyttas till ett system eller till ett strukturerat dokument alternativt raderas. Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum.

- I e-post får man inte behandla eller spara personuppgifter som är känsliga eller sekretessbelagda. Om känsliga eller sekretessbelagda personuppgifter inkommer får man till exempel inte vidarebefordra eller svara på e-posten så att uppgifterna sänds vidare. Ifall Haparanda kommun behöver de inkomna uppgifterna för att utföra kommunens uppgifter ska man:
  - skriva ut e-posten och sedan radera den, eller
  - flytta uppgifter från e-posten till ett lämpligare system, eller
  - Gallra så fort den är inaktuell

Känsliga personuppgifter ska aldrig skickas via e-post om det inte finns tillräckliga skyddsåtgärder på plats som exempelvis krypterad e-post, till exempel uppgifter om någons hälsa, religiösa åsikter eller politiska åsikter. Undvik även att skicka andra integritetskänsliga och extra skyddsvärda uppgifter som exempelvis lönebesked, värderingar av en person såsom social förmåga eller provresultat via e-post. Undantagna från denna regel är registratorer som får skicka känsliga personuppgifter till interna e-postadresser, då de vidareförmedlar e-post som inkommit i kommunens brevlåda.

Vid besvarande av ett inkommande e-post som innehåller integritetskänsliga/känsliga personuppgifter är det viktigt att ta bort dessa uppgifter innan svaret skickas iväg.

E-post ska användas för att kommunicera, inte för att lagra uppgifter. Man ska således inte spara e-post bara för att det eventuellt kan vara bra att ha i framtiden. Mer information om hantering e-post finns i Riktlinjer för e-postdokument

## Chat och inlägg i Microsoft Teams

Microsoft Teams används för att samarbeta kring arbetsmaterial och innehåller information i form av dokument, chattar och gruppmessages. Även inspelningar från möten sparas i Teams.

Chatt/inlägg är en enklare form av mejl och följer samma grundprinciper. Funktionen är endast avsedd för information av tillfällig art som inte ska arkiveras. Det är användaren ansvar att arkivera och diarieföra konversationer, om det faller inom ramen för allmän handling som ska diarieföras. Chatten och inlägg sparas den lika länge som e-post.

Känsliga personuppgifter, skyddsvärd och sekretessklassad information ska inte hanteras i Teams eller andra Office 365 applikationer. Känsliga personuppgifter ska aldrig skickas via Teams. Personnummer är betrakta som skyddsvärd information.

## Behörighet till personuppgifter

Bara den som behöver kunna behandla personuppgifterna ska kunna utföra sådan behandling. Därmed ska behörighet till olika system eller mappar spegla en anställds faktiska behov för att utföra sina arbetsuppgifter.

## Grund för behandling av personuppgifter

När personuppgifter behandlas i Haparanda kommun, eller på uppdrag av kommunen, ska de grundläggande principerna i GDPR vara uppfyllda. Principerna anges i artikel 5 i GDPR.

I enlighet med GDPR:s princip om laglighet, korrekthet och öppenhet ska Haparanda kommun behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den vars personuppgifter registreras av Haparanda kommun. Med detta menas att kommunen alltid ska vara tydlig och konkret i sin beskrivning av hur personuppgifter behandlas.

Haparanda kommun ska alltid se till att personuppgifter behandlas på en utpekad rättslig grund och att annan lagstiftning som inverkar på behandlingen efterlevs. All behandling av personuppgifter som Haparanda kommun utför måste vila på minst en rättslig grund, i annat fall är behandlingen olaglig. Nedan följer de rättsliga grunder som behandlingen ska vila på:

- Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Grunden för Haparanda kommuns behandling av personuppgifter vilar oftast på att behandlingen är nödvändig för att fullgöra kommunens rättsliga förpliktelser. Som exempel är ett register över barn i barnomsorg ett sådant register som Haparanda kommun behöver för att kunna fullgöra förpliktelserna i barnomsorgslagen.

Några exempel på sådant är när du söker bygglov, startar en restaurang eller får ett klagomål riktat mot dig. En sådan behandling får göras utan att samtycke behöver hämtas från den vars personuppgifter registreras. De personuppgifter som registreras ska vara tillräckliga för att kunna hantera en ansökan eller ett klagomål.

Ett ytterligare typfall av ändamål för en behandling av personuppgifter kan vara att förbättra förvaltningens framtida handläggning. Det kan då röra sig om att uppgifter som ni har lämnat in kan komma att användas för intern statistisk bearbetning eller användas i enkätundersökning riktad till er av Haparanda kommun eller av företag på uppdrag av Haparanda kommun.

I vissa fall är det dock nödvändigt för Haparanda kommun att begära in samtycke från de registrerade för att kunna behandla personuppgifter. Det kan till exempel vara ett nyhetsbrevs utskick eller något annat som är helt valfritt att vara del i för den registrerade. Samtycken ska inte hämtas in om det finns någon annan rättslig grund för behandlingen.

## **PUBLICERING AV PERSONUPPGIFTER PÅ INTERNET**

Haparanda kommun publicerar i regel alla organs protokoll på webbplatsen och kommunen publicerar även annat material på webbplatsen. Vid all publicering måste man dock ta hänsyn till individers rättigheter.

Publicering av anställdas personuppgifter, såsom namn, befattning, telefonnummer och e-postadress till arbetet och liknande arbetsplatsrelaterade personuppgifter kan normalt publiceras utan den registrerades samtycke om publiceringen är nödvändig för att informera om kommunens verksamhet. Den rättsliga grunden för publiceringen är i sådant fall utföra uppgift av allmänt intresse. Uppgifter om familjeförhållanden, bostadsadress, telefonnummer och fritidsintressen **får inte** publiceras.

Publicering av förtroendevaldas personuppgifter, såsom namn, typ av uppdrag, e-postadress (enbart

@haparanda.se) och telefonnummer som tillhandahålls av Haparandas kommun får publiceras med stöd av den rättsliga grunden utföra uppgift av allmänt intresse. Partitillhörighet är en känslig personuppgift enligt dataskyddsförordningen men denna uppgift får publiceras med stöd av den rättsliga grunden eget offentliggörande. Den förtroendevaldes privata telefonnummer får enbart publiceras om hen har samtyckt till publiceringen. Samtycket ska vara skriftligt dokumenterat. Om samtycket återkallas ska publiceringen upphöra.

## **Ansvar över publiceringen**

I Haparanda kommun är det kommunikatören som oftast publicerar något på kommunens webbplats. Dock ligger ansvaret över det som publiceras på den som begär att det ska publiceras och denne ska se till att felaktiga personuppgifter tas bort eller rättas. Förvaltningschefer och enhetschefer ansvarar för information om hur Haparanda kommun hanterar personuppgifter och det nedanföljande ska kommuniceras ut på kommunens webbplats och finnas tillgängligt på kommunens verksamhetsenheter.

## **Kontroll före publicering**

I första hand ska material som ska publiceras på webbplatsen skrivas på ett sådant sätt att det inte innehåller några personuppgifter. I fall det inte går att undvika ska personuppgifter maskeras.

Protokoll innehåller ofta personuppgifter och som även är nödvändiga för beslutsfattandet, många personuppgifter som återfinns i protokoll är också offentliga uppgifter. Det ska dock ur ett informationsperspektiv finnas mycket goda grunder för att lägga ut personuppgifter på webbplatsen och således ska personuppgifter i protokoll maskeras innan publicering om inte berörd personen gett sitt samtycke. Det finns dock vissa undantag på personuppgifter som inte behöver maskeras:

Tjänstemäns och förtroendevaldas personuppgifter får publiceras om uppgifterna har samband med deras tjänsteutövning eller uppdrag.

- Beslut om att till exempel utdela ett stipendium, ge någon fullmakt eller bygglov.
- Offentliga personuppgifter, om offentliggörandet tjänar kommunens intresse att ge information, dvs. om uppgifterna är av allmänt intresse.

Bygglov är tillståndsbeslut som innehåller personuppgifter och som hör till anslagsförfarandet enligt en speciallag och som ska vara offentligt framlagda endast under den tid som krävs i lagen. Således kan till exempel uppgifter om vem som har fått bygglov publiceras på webben enligt 2 punkten ovan förutsatt att lagens villkor för anslagsförfarandet följs noggrant. Kontaktuppgifter till den som fått bygglov ska dock inte publiceras om inte berörd har gett sitt samtycke till detta.

Punkten ovan förutsätter prövning från fall till fall. I fall en personuppgiftsansvarig anser att en personuppgift är av så stort allmänt intresse att den bör publiceras bör denne ta kontakt med kommunens dataskyddsombud för att rådgöra.

## **Publicering av personuppgifter i form av foto/film**

För webbpublicering av fotografier där identifierbara levande personer förekommer krävs samtycke. Det krävs samtycke från en enskild person för att det ska vara lagligt att publicera bild och film på till exempel en webbsida. Samtycket ska inhämtas från den enskilda personen innan publiceringen.

Ansvaret för att samtycke inhämtas ligger på den som vill att bildmaterialet ska publiceras. I nästa steg ska kommunikatören kontrollera att samtycke finns innan publicering. Alla samtycken förvaras i stadshuset. Det är kommunikatören som ansvarar för detta register.

Foto/film där enskilda medborgare, såväl vuxna som barn, inte kan identifieras (så kallade mingelbilder) får publiceras med stöd av den rättsliga grunden utföra uppgift av allmänt intresse. Om en medborgare kontaktar kommunen och anser att hen är identifierbar på en mingelbild och motsätter sig publiceringen bör publiceringen upphöra.

## Förbud mot publicering

Följande uppgifter får inte publiceras på Haparanda kommuns webbplats:

- Känsliga uppgifter enligt dataskyddsförordningen:
  - Etnisk tillhörighet
  - Politiska åsikter (gäller ej förtroendevalda)
  - Religiös eller filosofisk övertygelse
  - Medlemskap i fackförening
  - Uppgifter som rör hälsa eller sexualliv
- Uppgifter som omfattas av sekretess eller tystnadsplikt
- Personbeteckning
- Uppgift om lagöverträdelse
- Personnummer eller samordningsnummer
- Uppgifter om lagöverträdelser
- Integritetskänslig information, till exempel uppgifter om enskildas personliga förhållanden eller sådant som ha en nära koppling till den enskildas privata sfär.

Känsliga personuppgifter får publiceras om det finns ett samtycke från den personen eller om denne själv på ett tydligt sätt offentliggjort uppgifterna. Detta gäller till exempel fackliga företrädare.

## PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

Varje nämnd i Haparanda kommun är personuppgiftsansvarig och därmed ytterst ansvarig för sin behandling av personuppgifter.

Dataskyddsförordningen, även kallad GDPR, har till syfte att skydda den grundläggande mänskliga rättigheten, rätten till ett privatliv. En människas personliga integritet ska inte kränkas i samband med behandlingen av personuppgifter.

Till personuppgifter räknas all slags information som kan knytas till en fysisk person som är i livet. Exempel på personuppgift är personbeteckning, namn, adress, foton, registreringsnummer, fastighetsbeteckning, identifikationer online, personers fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

### Kommunens arbete med efterlevnad av dataskyddsförordningen

När personuppgifter behandlas (all hantering av personuppgifter utgör behandling) i kommunen, eller på uppdrag av kommunen, ska de grundläggande principerna i dataskyddsförordningen vara uppfyllda. Nedan ges några exempel på hur Haparanda kommun arbetar med att efterleva förordningen.

I enlighet med Dataskyddsförordningens princip om laglighet, korrekthet och öppenhet ska Haparanda kommun behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den vars personuppgifter registreras av Haparanda kommun. Med detta menas att kommunen alltid ska vara tydlig och konkret i sin beskrivning av hur personuppgifter behandlas.

Haparanda kommun ska alltid se till att personuppgifter behandlas på en utpekad rättslig grund och att annan lagstiftning som inverkar på behandlingen efterlevs. All behandling av personuppgifter som Haparanda kommun utför måste vila på minst en rättslig grund, i annat fall är behandlingen olaglig.

Kommunen ska alltid ha avvägningen mellan den registrerades integritet och den egna verksamhetens effektivitet i åtanke.

För de uppgifter som hämtas in av kommunens olika enheter är samtycke i de flesta fall inte nödvändigt. Det beror på att uppgifterna används i samband med exempelvis myndighetsutövning, för att kunna fullgöra en skyldighet som åligger kommunen eller att ett avtalsförhållande föreligger. Alla kommunala nämnder har ett ansvar för att personuppgifter behandlas på ett korrekt sätt.

## Information och registerutdrag

Den registrerade har rätt att få information när dennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av Haparanda kommun både när uppgifterna samlas in och när den registrerade begär det.

Önskas information om vilka av ens personuppgifter som behandlas av Haparanda kommun ska man ta kontakt med kommunkansliet. Elle via e-tjänster <sup>5</sup>på kommunens hemsida. För att få ut personuppgifterna behöver man kunna styrka sin identitet.

## Principer för insamlande av personuppgifter

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Med detta menas att Haparanda kommun hela tiden känner till och dokumenterar anledningen till att en viss personuppgift hanteras och personuppgifterna inte senare används för en helt annan anledning som går emot den ursprungliga.

Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Med detta menas att Haparanda kommun endast ska använda sig av de personuppgifter som krävs för att uppnå målet med hanteringen. Kan samma mål uppnås genom att använda färre personuppgifter eller mindre känsliga sådana ska så ske.

## Korreakta personuppgifter

Personuppgifterna som Haparanda kommun hanterar ska vara korrekta och om nödvändigt uppdaterade. Åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga raderas eller rättas utan dröjsmål.

Med detta menas att Haparanda kommun alltid måste verka för att personuppgifter som är felaktiga rättas och att det finns rutiner för hur så ska ske.

## Lagringstid för personuppgifter

Personuppgifter får inte förvaras identifierbara under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Med detta menas att personuppgifterna inte får sparas längre än vad som behövs utifrån målet med behandlingen. När målet är uppnått ska arkivering, gallring eller avidentifiering av personuppgifterna alltid övervägas.

## Säkerhet som princip

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna, inklusive skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder enligt kommunens informationssäkerhetspolicy

Med detta menas att personuppgifter ska skyddas genom tekniska och organisatoriska åtgärder på en nivå som motsvarar uppgifternas skyddsvärde. Är uppgifterna av känslig eller särskilt skyddsvärd art ska också högre tekniska och organisatoriska krav ställas. Utgångspunkten ska alltid vara att endast behöriga personer ska ges tillgång till skyddsvärd information.

För att minska riskerna för att ni missar något viktigt eller gör misstag som kan leda till kostsamma säkerhetsincidenter. Haparanda kommun har tagit framme tydliga, interna informationssäkerhetspolicy-och rutiner samt följer de internationella informationssäkerhetsstandard SS-ISO/IEC 27001.

---

<sup>5</sup> <https://www.haparanda.se/kommun-och-politik/om-personuppgifter>

## Dataskyddsförordningen och offentlighetsprincipen

För kommunens verksamhet gäller offentlighetsprincipen. Offentlighetsprincipen innebär en rätt för var och en att hos Haparanda kommun ta del av allmänna handlingar.

Detta innebär att även personuppgifter kan begäras och lämnas ut som en del av allmän handling oavsett för vilket ändamål personuppgiften ursprungligen behandlades. Denna rätt gäller dock inte om handlingarna innehåller uppgifter som är belagda med sekretess enligt gällande lagstiftning.

GDPR hindrar inte kommunen att lämna ut en allmän handling enligt offentlighetsprincipen. Däremot behöver handlingen lämnas ut på ett säkert sätt. Om den som begär ut uppgifterna vill ha den digitalt måste en bedömning göras om uppgifterna kan lämnas ut på ett säkert sätt, annars får utlämningen ske på papper. Det finns inte någon skyldighet att lämna ut uppgifter enligt offentlighetsprincipen annat än på papper.

Vissa personuppgifter i ett dokument kan vara offentliga och andra sekretessbelagda. Det kan finnas behov av att maskera uppgifter innan handlingen lämnas ut. Maskering av sekretessbelagda uppgifter innebär dock ett nekande av att lämna ut de uppgifterna i handlingen. Det framgår av delegeringsordningen vem som har rätt att fatta beslut om att inte lämna ut de uppgifter eller den handling som är sekretessbelagd.

## Skyddsvärda/integritetskänsliga personuppgifter

### Personnummer/Samordningsnummer

Personnummer (ÅÅMMDD-XXXX) och samordningsnummer är extra skyddsvärda personuppgifter. Samordningsnummer är ett tillfälligt identitetsnummer för personer som inte är folkbokförda i landet men som har kontakt med landets myndigheter. Användningen av samordnings- och personnummer regleras i den svenska dataskyddslagen<sup>6</sup>. Där står det bland annat att personnummer endast får användas om det är nödvändigt att säkerställa att det är rätt person som behandlas, om behandlingen kan vara motiverad utifrån ändamålet eller om det finns ett inhämtat samtycke.

Slentrianmässig användning och onödig exponering av person- och samordningsnummer ska undvikas. Om personnummer används i en behandling ska det motiveras. Om det inte kan motiveras så bör det inte användas. Där det går kan exempelvis födelsedatum (ÅÅMMDD) användas istället.

Personnummer ska som huvudregel inte heller användas som användaridentitet vid inloggning i olika typer av verksamhetssystem. Om det finns behov av att använda personnummer som inloggning så ska dataskyddsombudet tillfrågas.

## Barns uppgifter

Barns personuppgifter är extra skyddsvärda, eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig sina uppgifter samt förstå sina rättigheter.

## Andra integritetskänsliga uppgifter

Förutom personnummer/samordningsnummer och barns personuppgifter så finns det många andra integritetskänsliga personuppgifter som är extra skyddsvärda, så som:

- Löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala eller ekonomiska förhållanden
- personuppgifter som omfattas av sekretess eller tystnadsplikt

---

<sup>6</sup> Dataskyddslagen 3 kap. 10§.

## Känsliga personuppgifter

Vissa personuppgifter är till sin natur mer känsliga än andra. I dataskyddsförordningen anses följande särskilda kategorier av personuppgifter kräva ett särskilt legalt skydd:

- Etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Haparanda kommun ska endast behandla känsliga personuppgifter när det finns särskilt stöd i lag eller om den registrerade särskilt samtyckt till den specifika behandlingen.

Känsliga personuppgifter får enligt undantagen i artikel 9.2 a-j i GDPR och 3 kap 2–7§§ dataskyddslagen enbart behandlas om något av följande uppfylls:

- vid uttryckligt samtycke
- om uppgifterna offentliggjorts av den registrerade
- för att den personuppgiftsansvariga ska kunna fullgöra sina skyldigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd
- den registrerades vitala intressen ska kunna skyddas
- ideella organisationers behandling av medlemmars personuppgifter (politiskt, filosofiskt, religiöst, fackligt syfte)
- för att fastställa eller tillvarata rättsliga anspråk eller domstols rättskipande verksamhet
- viktigt allmänt intresse
- hälso- och sjukvård och social omsorg
- allmänt intresse på folkhälsoområdet
- när det är nödvändigt av skäl som hör samman med förebyggande
- hälso- och sjukvård och yrkesmedicin
- vid bedömning av en arbetstagares arbetskapacitet
- när rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras
- för medicinska diagnoser

## KONSEKVENSBEDÖMNING

Om en behandling av personuppgifter som kan leda till en hög risk för de registrerade (t.ex. en omfattande hantering av känsliga personuppgifter eller risk att särskilda krav avseende skydd inte kommer att kunna uppnås) planeras genomföras måste Haparanda kommun enligt dataskyddsförordningen först genomföra en så kallad konsekvensbedömning avseende dataskydd.

Om en sådan konsekvensbedömning innebär att de bedömda höga riskerna kvarstår måste Haparanda kommun samråda<sup>7</sup> med Integritetsskyddsmyndigheten som är tillsynsmyndigheten innan behandlingen påbörjas.

För att kunna bedöma riskerna för enskildas friheter och rättigheter måste ni ta ett helhetsgrepp om situationen och titta på många olika faktorer i personuppgiftsbehandlingen.

Haparanda kommun har tagit fram en mall och process för konsekvensbedömning och arbetar med att ta fram en e-tjänst för Konsekvensbedömnings processen.

---

<sup>7</sup> <https://www.imy.se/verksamhet/utfora-arenden/begar-forhandssamrad/>



Fyra grundläggande krav på vad en konsekvensbedömning ska innehålla:

1. En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
2. En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
3. En bedömning av riskerna för de registrerades rättigheter och friheter.
4. De åtgärder som ni planerar för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.
5. Redogöra med dataskyddsombud
6. Inhämta synpunkter från de registrerade eller deras företrädare när det är lämpligt.

## **INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD**

Inbyggt dataskydd och dataskydd som standard är ett krav för alla personuppgiftsansvariga, och gäller alla verksamheter.

Genomförandet av inbyggt dataskydd och dataskydd som standard varierar beroende på behandlingen i det enskilda fallet. Oavsett storlek kan genomförandet av inbyggt dataskydd och dataskydd som standard gynna både den personuppgiftsansvariga och den registrerade.

Inbyggt dataskydd innebär att den personuppgiftsansvariga tar hänsyn till integritetsskyddsreglerna redan när IT-system och rutiner utformas. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas.

Kravet på dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas.

## **INFORMATION OCH KOMMUNIKATION**

Haparanda kommun ska tillhandahålla information till registrerade i enlighet med dataskyddsförordningens krav. Information ska ges om hur Haparanda kommun behandlar de registrerades personuppgifter och om vilka rättigheter som de registrerade har enligt dataskyddsförordningen.

Information som ges ska vara koncis, klar, tydlig och begriplig och den ska ges i ett lättillgängligt format. Språket ska vara klart och tydligt, och vara anpassat till mottagaren, exempelvis om informationen är särskilt riktad till barn.

Informationen ska tillhandahållas skriftligt och kan när det är lämpligt ges i elektronisk form. Om den registrerade begär det ska informationen tillhandahållas muntligt, under förutsättning att den registrerade har styrkt sin identitet.

Det här innebär att den som ansvarar för behandlingen alltid måste ta ställning till om den information om behandlingen som krävs ges till den registrerade på ett tillräckligt sätt.

## **DEN REGISTRERADES RÄTTIGHETER**

Alla registrerade har rättigheter gentemot den som är personuppgiftsansvarig. Vissa av rättigheterna är beroende av vilken rättslig grund som den aktuella behandlingen av personuppgifter vilar på. Detta innebär att vissa rättigheter bara kan göras gällande under vissa förutsättningar. Haparanda kommun ska möjliggöra för de registrerade att utöva sina rättigheter.

### **Rätt till insyn**

Den registrerade har rätt att få tillgång till de personuppgifter som behandlas. Detta innebär att Haparanda kommun på begäran måste kunna tillhandahålla dessa uppgifter till den registrerade.

## Rätt till ändring

Den registrerade har rätt att begära att felaktiga personuppgifter rättas och att ofullständiga personuppgifter kompletteras. Vissa personuppgifter som behandlas i enlighet med viss lagstiftning får dock till exempel endast justeras under vissa förutsättningar.

## Rätten att bli bortglömd

Beroende på omständigheter i det enskilda fallet och vilken rättslig grund som personuppgiftsbehandlingen görs kan den registrerade även ha rätt till radering av sina personuppgifter. Rättigheten har begränsad tillämpning inom offentlig förvaltning eftersom merparten av personuppgiftsbehandlingarna vilar på en rättslig grund där rättigheten inte är tillämplig.

## Rätt till begräsning

Beroende på omständigheter i det enskilda fallet kan den registrerade ha rätt till att behandlingen av personuppgifterna begränsas till endast lagring under den tid det tar att utreda en invändning från den registrerade.

## Rätt till dataportabilitet

Beroende på omständigheter i det enskilda fallet och på vilken rättslig grund som personuppgiftsbehandlingen grundar sig på har den registrerade i vissa fall rätt att få tillgång till personuppgifterna i ett sådant format som möjliggör överförande till en annan personuppgiftsansvarig. Rättigheten har begränsad tillämpning inom kommuner eftersom merparten av personuppgiftsbehandlingarna vilar på en rättslig grund där rättigheten inte är tillämplig.

## Återkallande av samtycke

Om den rättsliga grunden för behandling av personuppgifter är ett samtycke från den registrerade så har denne rätt att återkalla samtycket. Ett återkallande av samtycket påverkar dock inte lagligheten av personuppgiftsbehandlingen för tiden innan samtycket återkallades.

## Invända mot behandling

Om den lagliga grunden för behandlingen av personuppgifter baseras på berättigat intresse (intresseavvägning) eller allmänt intresse har en registrerad under vissa förutsättningar rätt att invända mot hur dennes personuppgifter behandlas.

## Rätt att lämna klagomål

Den registrerade har alltid rätt att vända sig till tillsynsmyndigheten med klagomål om denne inte är nöjd med hur Haparanda kommun hanterar den registrerades personuppgifter. Tillsynsmyndighet är Integritetsskyddsmyndigheten.

## SANKTIONSAVGIFTER

Vid en överträdelse av GDPR och dataskyddslagen kan tillsynsmyndigheten utfärda en reprimand, föreläggande eller förbud mot den personuppgiftsansvarige. Tillsynsmyndigheten har även befogenhet att påföra administrativa sanktionsavgifter. För offentliga myndigheter kan avgiften som mest vara tio miljoner kronor för allvarigare överträdelser. För de något mindre allvarliga överträdelserna gäller ett maxbelopp på fem miljoner kronor.

|   |                 |
|---|-----------------|
| <b>Vid överträdelse av följande bestämmelser (mindre allvarliga överträdelser) är maxbeloppet för en myndighet som högst 5 miljoner kronor.</b> |                 |
| <b>Artikel</b>  | <b>Innehåll</b> |

|  |  |
|--|--|
| 8,11, 25–39, 42 och 43 i GDP   | Personuppgiftsansvarigas/personuppgiftsbiträdens skyldigheter, exempelvis utförande av konsekvensbedömning |
| 42–43 i GDPR   | Certifieringsorganets skyldigheter   |
| 41.4 i GDPR  | Övervakningsorganets skyldigheter  |
| <b>Vid överträdelser av följande bestämmelser (allvarliga överträdelser) är maxbeloppet för en myndighet som högst 10 miljoner kronor.</b> |  |
| 5,6,7 och 9 i GDPR   | Grundläggande principer, inklusive villkoren om samtycke   |
| 12–22 i GDPR   | Registrerades rättigheter  |
| 44–49 i GDPR   | Överföring av personuppgifter till tredjeland m.m.   |
| 3 kap. 10§ dataskyddslagen   | Behandling av personnummer/samordningsnummer   |
| 58,2 c-h och j i GDPR  | Underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten.                               |
| 58.1 i GDPR  | Underlåtelse att ge tillsynsmyndigheten tillgång till uppgifter.   |

## ÖVERFÖRING TILL TREDJE LAND

Dataskyddsförordningen reglerar särskilt aspekten kring delning av personuppgifter med tredje land, det vill säga länder som inte är en del av den Europeiska unionen. Om vi behöver överföra dina uppgifter till tredje land ska du få reda på det.

### Särskilda regler för överföring utanför EU/EES?

Genom dataskyddsförordningen har alla EU:s medlemsstater ett likvärdigt skydd för personuppgifter och personlig integritet. Detta gäller även EES-länderna. Därför kan personuppgifter föras över fritt inom detta område utan begränsningar.

Utanför EU/EES däremot finns inga generella regler som ger motsvarande garantier.

Dataskyddsförordningen innehåller därför regler om under vilka förutsättningar det är tillåtet att föra över personuppgifter till länder utanför EU/EES.

### När är överföring utanför EU/EES tillåten?

Under vissa förutsättningar är det tillåtet att överföra personuppgifter utanför EU/EES:

- Det finns ett beslut från EU-kommissionen om att exempelvis ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå<sup>8</sup>.
- Ni har vidtagit lämpliga skyddsåtgärder, till exempel bindande företagsbestämmelser (så kallade Binding Corporate Rules, BCR) eller standardavtalsklausuler (så kallade Standard Contractual Clauses, SCC).
- Särskilda situationer och enstaka fall.

<sup>8</sup><https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/adekvat-skyddsniva/>

Om skyddsnivån i mottagarlandet inte är tillräcklig kan ni behöva vidta ytterligare skyddsåtgärder utöver till exempel standardavtalsklausuler. I vissa fall kan inga skyddsåtgärder kompensera för bristerna och göra överföringen tillåten. I sådana fall behöver ni avstå ifrån eller avbryta överföringen. Europeiska dataskyddsstyrelsen (EDPB) har antagit rekommendationer om när ytterligare skyddsåtgärder kan behövas och vad sådana åtgärder kan vara.

## KONTAKT, FRÅGOR ELLER MER INFORMATION

För att göra invändningar mot Haparanda kommuns personuppgiftsbehandlingar eller om man vill ha rättelse, begära överföring (dataportabilitet), begära begränsning av behandlingen eller begära radering av sina personuppgifter begär man det på adressen:

**Haparanda kommun  
Torget 9, 953 85 Haparanda**

Man kan även göra begäran genom att skicka en e-post till [kommunen@haparanda.se](mailto:kommunen@haparanda.se)

För kontakt med Haparanda kommuns dataskyddsombud:

**Postadress: Haparanda kommun, Torget 9, 953 85 Haparanda  
E-post: [Dataskyddsombud@haparanda.se](mailto:Dataskyddsombud@haparanda.se)**

## KLAGOMÅL

Har du synpunkter eller klagomål på hur Haparanda stad hanterar dina personuppgifter så är du välkommen att kontakta Haparanda kommuns dataskyddsombud som utreder det inträffade och ser till att eventuella fel åtgärdas.

Känner du dig ändå inte nöjd eller inte kan eller vill kontakta dem som du tycker har gjort fel så kan du alltid lämna klagomål till tillsynsmyndigheten, Integritetsskyddsmyndigheten. Besök [Integritetsskyddsmyndighetens webbplats](#)

## MER OM DATASKYDDSFÖRORDNINGEN

Dataskyddsförordningen (GDPR) är till för att förhindra att din personliga integritet kränks genom felaktig behandling av personuppgifter. Dina personuppgifter får bara behandlas om du har godkänt det eller om det finns stöd i dataskyddsförordningen, DSF eller annan lag.

[Läs mer om dataskyddsförordningen på Integritetsskyddsmyndighetens webbplats](#)