HEDEMORA KOMMUN	**STYRDOKUMENT**	Sida 1(7)
Skapad av: Säkerhetschefen	Datum 2021-11-22	Diarienummer: KS178-21 003
	Giltighet fr o m: 2022-05-17	Senast reviderad: KS 2018-11-06, § 129 (2018-09-14)
Godkänt/antaget av: Kommunstyrelsen den 17 maj 2022 § 47		
Dokumentansvarig: Kommunsekreterare		

Riktlinje för GDPR-arbetet i Hedemora kommuns nämnder och bolag

Dok. Kategori:	Riktlinjer
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Riktlinjen beskriver hur Hedemora kommuns nämnder och bolag ska arbeta och organisera kommunens GDPR-arbete och vilket förhållningssätt man ska ha till detsamma.

Hedemora kommuns olika styrdokument

Organiserade styrdokument	**Aktiverande styrdokument**
Visar tydligt roll och ansvarsfördelning. - Reglemente - Delegationsordning - Bolagsordning	Visar vad kommunen vill förändra och uppnå. - Strategi - Mål och budget - Program - Ägardirektiv - Handlingsplan och övrig plan - Förvaltningarnas verksamhetsplan - Bolagens affärsplan - Aktivitetsplan
Normerande styrdokument Tydliggör kommunens förhållningssätt och arbetssätt. - Policy - Riktlinje - Rutin och vägledning	**Regler för dem som bor och verkar i Hedemora kommun** Tydliggör villkoren för kommunal service och vilka krav kommunen ställer på de som bor och verkar i kommunen. - Avgifter (inkl. taxor) - Regler (inkl. lokala föreskrifter och lokala ordningar

Mer information om de olika styrdokumenten finns i Hedemora kommuns riktlinje ”Riktlinjer för styrdokument”.

Globala målen – Agenda 2030

Mål 16 i Agenda 2030 *handlar om Fredliga och inkluderande samhällen. Fredliga samhällen och frihet från våld utgör både ett mål och ett medel för hållbar utveckling. En väl fungerande statsförvaltning med ansvarsfulla institutioner, transparens och rättsstatens principer har alla ett fundamentalt egenvärde. De utgör grund för god samhällsstyrning inklusive korruptionsbekämpning och är viktiga drivkrafter för utveckling. Alla människor är lika inför lagen och ska ha lika tillgång till rättvisa samt ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för utveckling. Begreppen demokrati och de mänskliga rättigheterna återfinns inte uttryckligen under mål 16. Dessa begrepp förekommer dock tydligt i den politiska deklarationen i 2030-agendan.*

Delmål i mål 16

16.10 Säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal.

1. Inledning

EU:s dataskyddsförordning (General Data Protection Regulation - GDPR), som trädde i kraft den 25:e maj 2018, gäller som lag i Sverige. Förordningen kompletteras sedan med en svensk dataskyddslag (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och en svensk förordning (Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning). GDPR är överordnad olika svenska sektorsspecifika nationella lagar/förordningar (särlagstiftning) och den svenska dataskyddslagen och förordningen, men den svenska dataskyddslagen är underordnad de svenska sektorsspecifika lagarna/förordningarna.

Ändamålet med lagstiftningen är respekt för människans integritet. Syftet med GDPR är att stärka integritetsskyddet för enskilda personer, ge enskilda personer kontroll över sina personuppgifter, harmonisera lagstiftningen i Europa, anpassa lagstiftningen till den ökade digitaliseringen, minska byråkratiseringen och skapa förutsättningar för den inre digitala marknaden.

Skyddet för den personliga integriteten vid behandling av personuppgifter är ett samhällsbehov och det är också frågor som adresseras i särskilda lagar och/eller regler över hela världen.

Den personliga integriteten har olika fokus:

- Rätten att bli lämnad i fred
- Rätten till en personlig sfär
- Rätten till sina egna personuppgifter

Det handlar om att respektera den enskilde individen och hens rättigheter när det gäller personuppgifter. På så sätt kan man skapa en nödvändig tilltro till den offentliga verksamheten och uppfylla invånarnas förväntningar inom detta område.

Alla personuppgifter som på något sätt behandlas i kommunens verksamheter omfattas av GDPR med följande undantag:

- privat behandling, som därmed saknar koppling till yrkes- eller affärsmässig verksamhet,
- uppgifter om avlidna,
- om de strider mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,
- journalistiska ändamål, akademiskt, konstnärligt och litterärt skapande,
- tillgången till allmänna handlingar – offentlighetsprincipen,
- nationell säkerhet och gemensam utrikes- och säkerhetspolitik,
- brottsbekämpande myndigheter.

GDPR omfattar inte bara nya personuppgiftsbehandlingar från när GDPR trädde ikraft utan även äldre information om personuppgifter som fanns och behandlades i kommunens verksamheter innan förordningen trädde ikraft.

Hedemora kommun är skyldig att följa och VISA att kommunen följer GDPR, varför det är viktigt att alla anställda (medarbetare och chefer) och förtroendevalda i kommunen tar ansvar för att personuppgifter hanteras på rätt sätt. Att dokumentera vad man gör och varför är helt avgörande för att kunna visa hur kommunen följer GDPR. En förutsättning för att man ska kunna hantera personuppgifter på rätt sätt är också att verksamheterna har och följer en aktuell dokumenthanteringsplan och gallringsbeslut.

Kommunen ska i alla sina verksamheter arbeta utifrån principerna om **inbyggt dataskydd** och **dataskydd som standard**. Inbyggt dataskydd innebär att verksamheterna hela tiden ska arbeta för att förbättra sig tekniskt och organisatoriskt. Man ska använda sig av tillgängliga tekniska lösningar och organisera sig med beaktande av GDPR. Dataskydd som standard innebär att personuppgiftsansvarige ska se till att personuppgifter i standardfallet inte behandlas i onödan.

Dataskyddsarbetet i organisationen handlar om ett förändringsarbete som ska genomsyra hela verksamheten med att bygga system och processer som uppfyller GDPR:s krav. Det kräver ett proaktivt arbete från nämndens/styrelsens och ledningens sida och ett gott ledarskap. En modern förvaltning förutsätter ett gott skydd för den personliga integriteten. Förutom att det handlar om värderingar och människosyn handlar det också om hur man kan skapa effektivitet och kvalitet i arbetet som innebär mervärden utöver inbyggt dataskydd.

2. Dataskyddskultur

I och med den rådande samhällsutvecklingen som går emot ett digitaliserat samhälle ser alltfler organisationer och företag betydelsen av att lägga fokus inte bara på legala överväganden utan även etiska sådana. Behovet av transparens och hur man informerar till den enskilde om olika behandlingar av personuppgifter får en ny betydelse. En god behandling av personuppgifter är en förutsättning för den digitala samhällsutvecklingen.

En nyckel för att lyckas med detta arbete är att kommunens verksamheter skapar en dataskyddskultur. Med att bygga en dataskyddskultur menas att skapa normer, värderingar och attityder som skapar vissa beteenden hos medarbetarna i en organisation. Det är lämpligt att skapa en dataskyddskultur som är en del av organisationskulturen, dvs den ska ligga inbäddad naturligt i det arbete som görs i organisationen.

När det finns en dataskyddskultur ställer sig medarbetarna naturligt vissa frågor, exempelvis:

- Ägnar jag/vi oss åt en ANSVARSFULL databehandling här?
- Behandlar jag/vi bara de personuppgifter som är NÖDVÄNDIGA?
- Följer jag/vi de RUTINER och ANDRA STYRDOKUMENT kommunen har?
- Hur skulle jag känna om jag var den registrerade och fick vetskap om hur personuppgifterna behandlas nu?
- Kan jag/vi göra något för att skydda personuppgifterna på ett bättre sätt?

Dataskyddsarbetet är en del av kommunens värdegrundsarbete. För att uppnå en god dataskyddskultur behöver man från ledningens och styrelsens sida arbeta strategiskt med dataskyddsaspekter inom organisationen.

En sund dataskyddskultur borgar för att organisationen och dess medarbetare på ett bättre sätt kan uppfylla kraven på en ansvarsfull databehandling och kan visa att de grundläggande principerna i GDPR efterlevs.

3. Grundläggande principer

Ett antal grundläggande principer genomsyrar hela dataskyddslagstiftningen (artikel 5 GDPR).

De grundläggande principerna måste alltid efterlevas och består av:

- **Laglighet =** Man måste alltid ha en rättslig grund (laglig grund) för all personuppgiftsbehandling och man måste följa övriga principer och bestämmelser i GDPR och i annan kompletterande lagstiftning.
- **Korrekthet** = Behandlingen av personuppgifter ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade.
- **Öppenhet/transparens** = Personuppgiftsbehandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt. GDPR ska skydda människors värdighet vid behandling av deras personuppgifter genom att behandla dem med respekt och göra det möjligt för dem att utöva självbestämmande över sina liv. Självbestämmandet när det gäller personuppgifter handlar i hög grad om att kunna välja själv vilka som ska få behandla ens personuppgifter. För att kunna göra sådana val måste de registrerade först och främst känna till vem som avser att behandla deras personuppgifter, för vilka ändamål osv. De registrerade ska informeras om personuppgiftsbehandlingen. Transparenskravet är starkt, men inte absolut.
- **Ändamålsbegränsning** = Personuppgifter får endast behandlas för ett specifikt (konkreta), legitimt och uttryckligt angivet ändamål. Personuppgifterna får bara användas för det ändamål de samlades in och som anges i registerförteckningen för den specifika behandlingen.
- **Uppgiftsminimering** = Att de personuppgifter som behandlas ska vara adekvata, relevanta och begränsade till vad som är NÖDVÄNDIGT för de ändamål som de behandlas för. Onödiga data får inte samlas in, och i det fall det blir onödigt under tiden som det förvaras ska det utplånas (obs! arkivlagen bestämmelser måste beaktas, vilket innebär att vissa personuppgifter ska bevaras). ”Man får inte behandla personuppgifter som inte är nödvändiga för att jag ska kunna utföra mina arbetsuppgifter – Ingen uppgift får sparas för att den kan ”vara bra att ha”.
- **Riktighet =** Personuppgifter som behandlas ska vara riktiga och , om nödvändigt, uppdaterade.
- **Lagringsminimering =** Man får bara spara personuppgifter så sänge som de behövs för ändamålet med personuppgiftsbehandlingen.
- **Integritet – Konfidentialitet** = När man behandlar personuppgifter måste man se till att uppgifterna skyddas på ett bra sätt genom att vidta lämpliga säkerhetsåtgärder (tekniska och organisatoriska åtgärder).
- **Ansvarsskyldighet =** Personuppgiftsansvarig ansvarar för att följa de grundläggande principerna om personuppgiftsbehandling. Man måste också kunna visa att man följer dem och på vilket sätt man gör det.

4. Strategiska frågeställningar för ledningen och nämnden/styrelsen

Exempel på frågeställningar för ledningen och nämnden/styrelsen:

- Vilka mål har vi för verksamheten och hur kan dataskydd och behandling av personuppgifter stödja dessa mål?
- Hur ser den inbyggda risken ut i organisationens olika behandlingar och dataflöden och vilken nivå på risken är acceptabel? Dataskyddsarbetet handlar om att arbeta utifrån ett riskbaserat förhållningssätt och att arbetet ska dokumenteras.
- Vad betyder inbyggt dataskydd för vår verksamhet och hur kan vi åstadkomma det?
- Hur skapar vi en effektiv dataorganisation som är anpassad för vår verksamhet? Hur vill vi bygga upp vår förvaltnings/bolagsorganisation för dataskydd för att kunna möta kraven och de målsättningar vi väljer?
- Vilken infrastruktur kan och vill vi använda och är den intern eller extern?

5. Organisation och styrdokument

Hedemora kommun har en handlingsplan - Handlingsplan för informationssäkerhet, dataskydd och digitaliseringsutveckling – styrning - som beskriver kommunens dataskyddsorganisation. Organisationen ska visa hur kommunen genom sin organisation ska ta tillvara den enskilde individens rättigheter och ange mål på lång- och kort sikt för dataskyddsarbetet. Kommundirektören beslutar om handlingsplanen efter samråd med koncernledningsgruppen/kommunledningsgruppen.

De styrdokument som reglerar kommunens dataskyddsarbete är strategi, budget, riktlinjer, rutiner, handlingsplan och utbildningsplan. Strategin, handlingsplan och riktlinjer är kommunövergripande. Rutinerna och utbildningsplan kan vara både kommunövergripande och sektorsspecifika.

Varje nämnd/bolag ska arbeta fram en GAP-analys för sitt dataskyddsarbete. En GAP-analys visar på nuläget och ”målläge”. För skillnaden, dvs gapet, ska verksamheterna upprätta en åtgärdsplan. Åtgärdsplanen ska hållas uppdaterad. Åtgärdsplanen är bl a till för att minimera riskerna.

En GAP-analys med en grundlig nulägesanalys är en viktig framgångsfaktor för en GDPR-anpassning. Målet med nulägesanalysen är att kartlägga hur verksamheten behandlar personuppgifter och fastställa hur den uppfyller de legala kraven enligt GDPR. Nulägesanalysen bör omfatta följande aspekter:

- System: Hur behandlas personuppgifter i IT-systemen? Vilken behandling gör underleverantörer?
- Ostrukturerat material (mail, word, excel, papper, hemsida, intranät m.fl.): Hur behandlas personuppgifter i ostrukturerat material? Vilket åtkomstskydd finns för det ostrukturerade materialet? Efter genomgången kan verksamheten identifiera vad som bör förbättras och vilka åtgärder bör prioriteras.
- Governance: Vilka styrdokument och processer finns på plats? Vilken organisation finns att hantera frågorna?
- IT-säkerhet och annan informationssäkerhet: Vilket åtkomstskydd finns i de aktuella IT-systemen och för annan information än system, t ex papper? Genomgång av organisationens personuppgiftsbehandlingar och system görs normalt med hjälp av ett systemstöd (SKL:s KLASSA 1). Efter genomgången kan verksamheten identifiera vilka områden som bör förbättras och vilka åtgärder som bör prioriteras.

6. Kompetensutveckling

En viktig faktor för GDPR-anpassningen är att medarbetare och chefer kontinuerligt erbjuds utbildning inom GDPR och informationssäkerhet.
Koncernledningsgruppen/Kommunledningsgruppen beslutar årligen om en kommunövergripande utbildningsplan för kommunens medarbetare. Dessutom ska förvaltnings/bolagsspecifika utbildningsplaner finnas.

7. Barnrättsperspektiv

Genom GDPR införs ett förstärkt skydd för barns personuppgifter när det gäller kommersiella internettjänster som sociala nätverk (informationssamhällets tjänster inkl. social medier). Eftersom barn enligt förordningen förtjänar särskilt skydd måste all den information som riktar sig till barn vara skriven på ett tydligt och enkelt sätt som barn förstår. Barns skyddsvärda

ställning ska också vägas in vid en intresseavvägning. Kommunens verksamheter ska beakta barnrättsperspektivet i all verksamhet.

8. Personuppgiftsincidenter

Hantering av personuppgiftsincidenter och rapportering av desamma är ett fundament i dataskyddsarbetet. Alla medarbetare och chefer ska ha kännedom om vad en personuppgiftsincident är och känna till kommunens organisation kring incidenthantering. Synsättet ska vara att medarbetare ska uppmuntras att anmäla incidenter eller misstänkta incidenter i enlighet med kommunens styrdokument. Principen som gäller är ”hellre en gång för mycket än en gång för lite”. Förutom den lagliga skyldigheten att anmäla personuppgiftsincidenter till Datainspektionen och skyldigheten att dokumentera samtliga personuppgiftsincidenter oberoende om de ska anmälas till Datainspektionen eller inte är en god incidenthantering ett viktigt verktyg i kommunens effektiviserings- och kvalitetsarbete samt kommunens arbete med Inbyggt dataskydd. Personuppgiftsincidenter kan identifiera svagheter och risker som en organisation har och på så sätt vara viktiga i verksamhetens lärande och arbete med ständiga förbättringar.

9. Information om kommunens dataskyddsarbete

Information om kommunens dataskyddsarbete återfinns på intranätet under Informationssäkerhet och GDPR. Information till invånarna om hur kommunen behandlar deras personuppgifter återfinns på kommunens hemsida www.hedemora.se under Dataskydd eller på respektive bolags hemsida. Information till nämndernas anställda hur kommunen behandlar deras personuppgifter finns i personalhandboken eller motsvarande för kommunens bolag.

Registerförteckningen för respektive verksamhet återfinns i dataskyddsombudets diarium (DSO-diariet) i Ciceron. Åtkomsten till diariet är behörighetsstyrt och varje verksamhet kan endast se sina egna behandlingar och annan information som tillhör den egna nämnden/bolaget. Genom diariet kan verksamheterna även bl a följa DSO:s arbete med personuppgiftsbehandlingarna, DSO:s årliga rapporter och få kännedom om vilka personer som genomgått GDPR-utbildningar arrangerade av dataskyddsombudet.