PLAN

Strategi GDPR 2025-2028

Fastställd av miljö- och byggnämnden
Framtagen av samhällsbyggnadsförvaltningen
Datum framtagande 2024-11-15
Gäller 2025-2028
Ärendenr MBN 2024/2318
Version [1.0]

Region Gotland
Besöksadress Visborgsallén 19
Postadress SE-621 81 Visby
Telefon +46 (0)498 26 90 00
E-post regiongotland@gotland.se
Org nr 212000-0803
Webbplats www.gotland.se

Innehåll

1. Om GDPR

Dataskyddsförordningen General Data Protection Regulation (GDPR) gäller som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Införandet av GDPR innebär att den enskildes rättigheter stärkts kring personlig integritet och därmed också en skärpning kring behandlingen av personuppgifter.

Det övergripande syftet med GDPR är att säkerställa och stärka medborgarnas kontroll över sina personuppgifter och därmed rätten till skydd för privatlivet. Ett annat mål är att dataskyddet ska efterlevas bättre än tidigare.

Tillsynsmyndighet är Integritetsskyddsmyndigheten, IMY.

1.1 Miljö- och byggnämnden

Miljö- och byggnämnden är personuppgiftsansvarig och kan inte delegera ansvaret, men däremot de arbetsuppgifter som gäller GDPR.

Miljö- och byggnämndens ordförande ska informeras varje gång det inträffar en personuppgiftsincident. Miljö- och byggnämnden får information om och beslutar om samhällsbyggnadsförvaltningens dokument Strategi GDPR när det uppdateras, vilket kommer att ske var fjärde år (enligt önskemål från nämndens ledamöter, tidigare togs ny plan fram varje år) och vanligtvis i december. Tidigare var strategi- och handlingsplanen ett dokument, men handlingsplanen behöver uppdateras varje år och därför är den nu separerad från strategin för GDPR.

Det finns inga formella krav på hur ofta återrapportering till nämnd ska ske, men nämnden ska vara uppdaterad om förvaltningens arbete med GDPR. Rapporter och remisser gällande GDPR hanteras i miljö- och byggnämnden, oftast som informationsärenden.

1.2 Förvaltningens anpassning

GDPR kräver bred anpassning från samhällsbyggnadsförvaltningen i hur personuppgifter behandlas, hanteras, sparas, gallras och sprids i myndighetsutövningen. Nedan följer strategin för anpassning och argumentation kring personuppgiftshantering på förvaltningen.

2. Strategi

Samhällsbyggnadsförvaltningen (SBF) har arbetat pappersintensivt under många år, och har därför haft en hel del ostrukturerad data.

Ett omfattande digitaliseringsarbete har genomförts på förvaltningen under de senaste åren, genom olika projekt som till exempel Digital Samhällsbyggnad (DiSa) och Digital Dialog. Det aktiva arbetet med digitalisering bidrar till en ökad grad av efterlevnad av GDPR på SBF. Personuppgifter som digitaliseras minskar risken för att personuppgifterna används på ett olämpligt sätt och det blir lättare att kontrollera var uppgifterna finns och hur de används. SBF arbetar löpande med anpassningen till GDPR. Arbete med personuppgiftsincidenter, en uppdaterad registerförteckning och objektförvaltning har prioriterats. Utbildning sker fortlöpande inom informationssäkerhet där GDPR ingår som en del. Förvaltningarna inom Region Gotland samverkar och delar erfarenheter inom informationssäkerhet på nätverksmöten och regiongemensamma aktiviteter.

2.1 Definition av en personuppgift

En personuppgift är all slags information som avser en identifierad eller identifierbar levande fysisk person. I SBF:s verksamhet är det nedanstående personuppgifter som behandlas och som är relevanta i SBF:s arbete med anpassning till GDPR.

- Namn
- Personnummer
- Telefonnummer
- Postadress
- E-postadress
- Fastighetsbeteckning
- Registreringsnummer på fordon
- Foto på person eller fastighet (om personen/fastigheten kan identifieras)
- Diarienummer
- Ärendenummer

2.2 Ändamål

SBF behandlar personuppgifter när lagstiftning krävs inom olika verksamhetsområden eller när det är nödvändigt för att utföra den uppgift, det vill säga ändamålet, som avses. På SBF hanteras personuppgifter på följande sätt:

Internt

- Hantering av personalfrågor
- Hantering av avtal
- Vid bokföring
- Hantering av skattefrågor och annan administration
- I samband med verksamhetsutveckling

Externt

- Prövning av bygglov, förhandsbesked med mera
- När karttjänster erbjuds
- Beslut om översiktsplaner och detaljplaner
- Vid inspektioner inom miljö- och hälsoskydd
- Vid inspektioner inom livsmedel och alkohol

2.3 Rättslig grund

SBF:s behandling av personuppgifter villkoras av de rättsliga grunder som fastslås i GDPR. Behandlingen stödjer sig på följande rättsliga grunder:

Rättslig grund enligt GDPR	Definition	Exempel i SBF:s verksamhet

Myndighetsutövning och uppgift av allmänt intresse	Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.	Handläggning, beslutsfattande, kartinformation, personalinformation, samrådsprocesser.
Rättslig förpliktelse	Det finns lagar eller regler som gör att den personuppgifts-ansvarige måste behandla vissa personuppgifter i sin verksamhet.	Bokföringsskyldighet, arkivhållning, register på skatter och sociala avgifter.
Avtal	Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige.	Anställningsavtal för personal.

Sammanfattningsvis behandlar vi personuppgifter i följande sammanhang:

Behandling av personuppgifter:	**Rättslig grund:**
SBF behandlar personuppgifter i bred utsträckning i samhällsbyggnadsprocessen	Myndighetsutövning och uppgift av allmänt intresse, även serviceskyldigheten
SBF hanterar de anställdas personuppgifter	Avtal
SBF hanterar personuppgifter i sitt arkiv	Rättslig förpliktelse, myndighetsutövning samt uppgift av allmänt intresse
SBF hanterar personuppgifter i bokföringsprocessen och i ekonomisystemet	Rättslig förpliktelse

3. Rättssäker hantering av personuppgifter hos SBF

Personuppgifter förekommer i flera av SBF:s processer och är nödvändiga för SBF:s uppdrag att skapa en god livsmiljö på Gotland. Genom rättssäker behandling och god internkontroll säkerställs det att arbetet på SBF utförs i linje med GDPR.

3.1 Ledningssystemet för informationssäkerhet, LISa

Alla system och objekt som behandlar personuppgifter på SBF, det vill säga alla register, är upplagda i systemet LISa. De ska vara kompletta med förvaltningsplaner, risk- och sårbarhetsanalyser och ha en tillsatt objektägare samt minst en objektförvaltare med ansvar för systemet/objektet. LISa är nyckeln till att kunna hitta var den registrerades personuppgifter förekommer. Alla ärenden som rör begäran om registerutdrag, rättelse och radering hanteras i LISa och det krävs en uppdaterad registerförteckning för att SBF ska klara kravet kring dataportabilitet. Nya system ska klassas i LISa och utfasade system ska avvecklas och raderas. Ett stort arbete har gjorts med registerförteckningen i LISa och arbetet med objektförvaltning fortsätter kontinuerligt för att förbättra innehållet och hålla det uppdaterat.

3.2 Personuppgiftsbiträdesavtal (PUB-avtal) eller samordningsavtal

Alla avtal som SBF har ingått måste ha ett PUB-avtal (eller samordningsavtal) i tillägg, om det krävs på grund av personuppgiftsbehandling.

Om en leverantör inte vill ingå ett PUB-avtal, men hanterar personuppgifter i en biträdessituation, kan och bör leverantören väljas bort. I enstaka fall kan ett samordnat ansvar med leverantör förekomma. Då blir både Region Gotland och leverantören

personuppgiftsansvariga och ett samordningsavtal ska upprättas istället för ett PUB-avtal. PUB-avtal/samordningsavtal ses över vid behov, till exempel om det tillkommer en ny underleverantör eller om något annat förändras.

3.3 Ostrukturerad information

När GDPR började gälla försvann den så kallade missbruksregeln, vilket betyder att SBF inte längre har rätt att hantera ostrukturerade personuppgifter om det saknas rättslig grund för behandlingen. Alla personuppgifter behöver förvaras på ett spårbart, identifierbart och säkert sätt. Det innebär att alla personuppgifter måste läggas in i ett system som är klassat i LISa. I en övergångsfas klassas även fysiska papper, men målet är att det som finns i pappersformat på sikt ska arkiveras eller gallras.

3.4 Arkivering och gallring

En arkivansvarig är utsedd och arkivorganisationen kommer att fastställas under 2025. Det är viktigt att arbetet med arkivering utförs inom varje avdelning och enhet, för att få en effektiv och korrekt arkivering. Arkivering innebär också att handlingarna överlämnas till regionarkivet och att ansvaret för personuppgifterna inte längre kommer att ligga på SBF.

Miljö- och byggnämnden har en gallringsplan som är uppdaterad i enlighet med GDPR och som gäller för samtliga handlingar på SBF. Enhetschefen på varje enhet är ansvarig för att gallringsprocessen sker, att den är i enlighet med riktlinjerna och att de personuppgifter som finns antingen raderas eller registreras i ett klassat system.

Informationshanteringsplanen för Region Gotland utgör en grund för arbetet med vad som ska arkiveras och vad som ska gallras.

3.5 Digitalisering

SBF arbetar med att digitalisera hela samhällsbyggnadsprocessen, vilket är positivt ur ett GDPR-perspektiv. Efter många år av pappersbaserat arbete har det funnits stora mängder personuppgifter i arkivmappar i lokalerna. Genom kontinuerligt arbete med digitalisering och gallring av de papper som inte längre ska sparas arbetar SBF med att på sikt ta bort pappersförvaringar i lokalerna. Detta är även viktigt ur ett informationssäkerhetsperspektiv, då det är svårt att styra åtkomst till dessa dokument och spårbarhet på samma sätt som när det gäller handlingar i IT-system.

3.6 Personuppgiftsincidenter

SBF ska ha en tydlig process, med ansvariga som kan hantera personuppgiftsincidenter. Ansvariga avgör om incidenter ska rapporteras till Integritetsskyddsmyndigheten och gör det i så fall inom 72 klocktimmar i enlighet med GDPR. Ansvariga som hanterar incidenterna ska också kunna avgöra om de registrerade behöver delges. En rutin för personuppgiftsincidenter är framtagen för att underlätta och förtydliga hanteringen. Rutinen finns på Insidan samt i Docpoint.

SBF:s sida på Insidan om GDPR, arkiv och informationsbehandling innehåller strategi och handlingsplan för GDPR, rutin för personuppgiftsincidenter, grundutbildning i GDPR, länkar till regiongemensamma GDPR-sidor med mera. På sidan finns även en e-tjänst för rapportering av personuppgiftsincidenter och frågor om GDPR. E-tjänsten skickar frågorna till rätt person direkt, så att ingen e-post riskerar att hamna hos fel mottagare.

4. Avgränsningar i behandlingen av personuppgifter

Personuppgifter förekommer i hela samhällsbyggnadsprocessen och är en förutsättning för att förvaltningens uppdrag och myndighetsutövning kan genomföras. Arbetet styrs av givna lagrum och endast ändamålsenlig hantering av personuppgifter görs. I flera fall behöver lagen tolkas utifrån kontext och nedan finns avgränsningar och förtydligande av förvaltningens arbetssätt.

4.1 Kartor och fastigheter – en balans mellan serviceskyldighet och GDPR

Som en del av den service som Region Gotland erbjuder finns översiktsplaner och detaljplaner på Region Gotlands hemsida och kartor publiceras i en kartportal. Planerna och kartorna, som innehåller fastighetsbeteckningar, efterfrågas och används när någon till exempel ska söka bygglov eller följa utvecklingen på ön.

En fastighetsbeteckning är en personuppgift och omfattas av GDPR. SBF bedömer dock att fastighetsbeteckningarna behöver visas på kartorna, som en del av det allmänna intresset och myndighetsutövningen. Dessutom har förvaltningen en serviceskyldighet som regleras i förvaltningslagen, vilket innebär att myndigheter ska lämna upplysningar, vägledning, råd och annan hjälp till enskilda inom aktuellt verksamhetsområde. Hjälpen ska lämnas i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet (4 § första stycket förvaltningslagen). Serviceskyldigheten gäller oberoende av om den enskilde begär hjälp eller inte. SBF ser kartfunktionen som en viktig del i arbetet med att leva upp till serviceskyldigheten.

4.2 Protokoll och kallelser

Som en del av anpassningen till GDPR rensas alla kallelser och protokoll från personuppgifter (förutom fastighetsbeteckningar och ärendenummer) innan de publiceras eller görs offentliga. När det gäller tjänstepersoner och politiker, är de delaktiga genom sina yrkesroller och personuppgifter som namn, titel och arbetsplats förekommer. Partitillhörighet anges för politiker.

Förvisso kan en publicering ses som viktigt när det gäller allmänt intresse, men enligt offentlighetsprincipen finns det dock ingen skyldighet att publicera den här typen av information på internet – och vi väljer att avstå i de fall vi inte kan säkerställa skydd för personuppgifter.

4.3 Diariet

Region Gotland har ett offentligt diarium där en stor del av den information som visas relaterar till SBF:s ärenden.

Tidigare har samhällsbyggnadsförvaltningen arbetat för att stänga det offentliga diariet, men det har visat sig finnas ett stort allmänt intresse för denna service och vi har valt att istället begränsa vilka ärende som visas och att inte visa äldre ärenden som inte är genomgångna enligt GDPR.

4.4 Bilder

SBF arbetar med bilder på fastigheter och mark och där förekommer det ofta personuppgifter. Alla bilder ska lagras i system som är registrerade och klassade i LISa.

Ansikten, registreringsnummer med mera som kan uttydas på bilderna ska anonymiseras innan de visas offentligt.

4.5 Allmänna handlingar

I enlighet med offentlighetsprincipen har alla rätt att begära handlingar från SBF, men om handlingar begärs utlämnade kommer de att levereras i pappersform om det inte finns en säker digital lösning. SBF har rätt att debitera för utlämnandet om det gäller mer än 9 stycken sidor. En myndighet kan inte välja hur en begäran kommer in, men däremot bestämmer myndigheten själv i vilken form utlämnandet ska ske. Utlämnande av allmän handling handlar endast delvis om GDPR, vilket framgår av rutinen för utlämnande av allmän handling MBN som finns på Insidan och i Docpoint.

5. Uppföljning

Kopplat till strategi GDPR tas årligen en handlingsplan med åtgärder fram. Återrapportering av handlingsplanens genomförda och planerade åtgärder görs årligen till miljö- och byggnämnden.