TJÄNSTESKRIVELSE

Kungsbacka

Datum
2023-02-06

Diarienummer
BN 2021–002091

Konsekvensbedömning e-tjänst Anmäla om tillsyn enligt plan- och bygglagen

Förslag till beslut i byggnadsnämnden

Byggnadsnämnden har tagit del av konsekvensbedömningen för e-tjänst *Anmäla om tillsyn enligt plan- och bygglagen* och godkänner dess personuppgiftsbehandling.

Sammanfattning av ärendet

I e-tjänsten *Anmäla om tillsyn enligt plan-och bygglagen* rör det sig om uppgift om misstänkt lagöverträdelse.

Vid anmälan kan det komma in personuppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden, eftersom det är möjligt att i e-tjänsten bifoga bilagor så som bilder och att i fritext göra en beskrivning.

Ändamålet skulle kunna uppnås genom en mindre omfattande personuppgiftsbehandling. Endast kryssalternativ och karta har diskuterats med tillsynsgruppen. Om endast kryssalternativ och karta används i e-tjänsten finns ingen risk för att personuppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden kan komma in.

Förvaltningen kan också konstatera att ärenden som innehåller känsliga och sekretessbelagda personuppgifter förekommer i mycket liten omfattning i förhållande till inkomna anmälningar via e-tjänsten.

I ärenden som gäller fara för liv och hälsa är det av yttersta vikt att ärendet handläggs omgående. När anmälan innehåller tydlig information med bilagor och fritext kan handläggaren agera snabbare, vilket kan vara svårare om ärendet initialt inte visar fara för liv och hälsa.

Förvaltningen anser att risken att någon kan komma till skada väger tyngre gentemot de personers integritet som kan beröras av e-tjänstens behandling.

Inhämtning av synpunkter från invånare inom kommunens tillsynsområde genomförs regelbundet för de som använder e-tjänsten för att anmäla. Övrig inhämtning har inte genomförts på grund av behandlingens art alltid kan innebära ett intrång i den personliga integriteten, vilken behöver vägas mot risken att någon kan komma till skada på grund av olovligheten.

En informationstext rekommenderas att läggas in för att minska risken för att det ska komma in bilder där det förekommer personer eller privat information i fritextfält. Informationstexten ska upplysa anmälaren om att anmälan och eventuella bilagor kommer att bli allmän handling.

e-tjänsten förväntas medföra att hanteringen av känsliga och sekretessbelagda personuppgifter kommer att behandlas säkrare än när anmälan kommer in på annat sätt.

Förhandssamråd med dataskyddsombud

Förvaltningens bedömning avviker från dataskyddsombudets yttrande i fråga om möjligheten för anmälaren att i e-tjänsten kunna bifoga filer så som bilder samt ifråga om att de registrerades inställning till behandlingen inte fullt ut har inhämtats.

Dataskyddsombudet är tveksam till att det kan anses nödvändigt och proportionerligt att ta in bilder redan vid den initiala anmälan, med tanke på den integritetsrisk det kan innebära för den som blir anmäld. Eftersom det är tillsynsmyndigheten som ska säkerställa empirin innebär det att bevisvärdet på bilderna som inges av anmälare många gånger är lågt eftersom bilder både kan förvanskas och manipuleras. Dataskyddsombudet kan inte se att en snabbare handläggning kan ha företräde framför en mer korrekt och rättssäker när det handlar om enskildas integritet i den privata sfären.

Dataskyddsombudet rekommenderar att de registrerades inställning till behandlingen inhämtas för att få en förståelse för de registrerades perspektiv på en behandling av integritetskänslig karaktär.

Beslutsunderlag

Dataskyddsombudets yttrande, 2022-06-29

Konsekvensbedömning *Anmäla om tillsyn enligt plan- och bygglagen*, 2023-01-12

Förvaltningens tjänsteskrivelse, 2023-02-06

Beslutet skickas till

Kommunstyrelsens förvaltning, dataskyddsombud, Kungsbacka kommun

Veronica Kinn

Arkivarie

Kungsbacka

Datum: 2023-01-12

Diarienummer: BN 2021–002091
Ärende: Konsekvensbedömning

Konsekvensbedömning

Bedömning av risk och konsekvens i samband med personuppgiftsbehandling enligt dataskyddsförordningen 35 art.[1]

Översikt över behandlingen

Personuppgiftsansvarig nämnd
Byggnadsnämnden

Behandlingens namn
Anmäla om tillsyn enligt plan- och bygglagen.

Syfte med behandlingen
Att komma in med anmälan om tillsyn så som olovligt byggande, ovårdad fastighet, enkelt avhjälpta hinder, obligatorisk ventilationskontroll, hissar och andra motordrivna anordningar enligt plan- och bygglagen.

Laglig grund
Behandlingen lutar sig mot **allmänt intresse** som bygger på rättsstöd för digitalisering av den offentliga förvaltningen. Det bygger på förvaltningslagens 6–9 §§ principer om service, tillgänglighet och samverkan samt effektivitet i handläggning (Förvaltningslagen 2017:900). I regeringens *Digitaliseringsstrategi för ett hållbart digitaliserat Sverige* (Näringsdepartementet, 2017) beskrivs satsningar som behövs för att nå det övergripande målet att Sverige ska bli bäst i världen när det handlar om att använda digitalisering för att skapa nytta för medborgare och effektivisera offentlig förvaltning.

Strategin innehåller fem delmål som förklarar hur digitalisering ska kunna bidra till en positiv samhällsutveckling. Det handlar bland annat om målområdena *Digital innovation* och *Digital infrastruktur* som omfattar digitalt tillgängliggörande av offentlig förvaltnings service för medborgare och företagare. I regeringens strategi *Medborgaren i centrum* (Näringsdepartementet, 2012) beskrivs regeringens målsättningar för arbetet med att förstärka myndigheternas förmåga att tillhandahålla en sammantagen digital service till medborgare. I Sveriges Kommuner och Regioners strategi för digital utveckling för kommuner; *Utveckling i en digital tid* (Sveriges Kommuner och Regioner, 2019), beskrivs fyra målområden. Två av dessa målområden är *Informationsförsörjning och digital*

[1] Allmänna dataskyddsförordningen EU 2016/679

infrastruktur, samt *Sammanhållen digital service*. Där beskrivs den nationella målsättningen med att skapa förutsättningar för kommuner att tillgängliggöra digitala tjänster och service till sina invånare, företagare, besökare och föreningar.

Då tjänsten avser att användas för att hantera anmälan om tillsyn, vilar behandlingen även på den lagliga grunden **myndighetsutövning**. Det som kännetecknar myndighetsutövning mot enskild är att det rör sig om beslut eller andra åtgärder som ytterst är ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Byggnadsnämnden har en skyldighet att handlägga tillsynsärenden och besluta om påföljder enligt Plan- och bygglagen 11 kap. 5 §.

Kontaktperson för behandlingen, informationsansvarig
Camilla Cangren, byggnadsinspektör, Bygg- och miljöförvaltningen

Kontaktperson för behandlingen, e-tjänstesamordnare
Nader Al-Tayyar, systemförvaltare, Bygg- och miljöförvaltningen

Dataskyddskontakt
Veronica Kinn, Bygg- och miljöförvaltningen, Byggnadsnämnden

Dataskyddsombud
Karin Malmsten dataskyddsombud@kungsbacka.se

Personuppgiftsbiträde
Nordic Peak AB, organisationsnummer 556815 – 1889

Kvalitetssäkring
Johanna Sjöström, utvecklare, Bygg- och miljöförvaltningen

Datum för konsekvensanalys
2023-01-12 Version 1.1.

Tidigare gjord eller ny konsekvensbedömning

Open ePlatform är en tjänsteplattform hos Kungsbacka kommun. Det har gjorts en kommunövergripande konsekvensbedömning av den grundläggande behandlingen, insamling av personuppgifter för digital service och handläggning, KS 2021-06-22, § 189.

Dess sammantagna bedömning är att behovet av behandlingen av personuppgifter står i proportion till syftet att tillhandahålla digital service till kommunens invånare, företagare, föreningar och besökare samt att förutsättningarna kring behandlingen är tillräckliga för att uppfylla dataskyddsförordningens

krav. Kommunstyrelsens dataskyddsombud ställer sig bakom bedömningen.

Varje nämnd ska därtill göra egna tröskelanalyser för respektive e-tjänst för att avgöra om en konsekvensbedömning behöver göras.

Tröskelanalys

I tabellen nedan framgår ett antal kriterier. De fungerar som stöd för att avgöra behovet av en särskild konsekvensbedömning för den tilltänkta behandlingen. Sannolikheten för att behandlingen medför en hög risk för de registrerades fri- och rättigheter ökar ju fler kriterier som uppfylls. En hög risk innebär också ett ökat behov av en konsekvensbedömning.

Kriterier	Ja	Nej
Personuppgiftsbehandlingen innebär **utvärdering** eller **poängtilldelning**, inklusive profilering och förutsägelse av beteende.	☐	☒
Personuppgiftsbehandlingen innebär **automatiserat beslutsfattande** med *juridisk*, *ekonomisk* eller *annan betydande effekt* för den registrerade.	☐	☒
Personuppgiftsbehandlingen innebär att **systematisk övervakning** används för att *observera*, *övervaka* eller *kontrollera* den registrerade.	☐	☒
Behandling av **extra skyddsvärda personuppgifter** eller **känsliga personuppgifter** ***Kommentar:*** *Det rör sig här om uppgift om misstänkt lagöverträdelse och vid anmälan kan det komma in uppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden då det är möjligt att bifoga bilagor så som bilder och i fritext göra en beskrivning.* *Den som anmäler behöver e-identifiera sig, men kan välja att vara anonym. Personnummer förekommer vid inloggning med e-identifiering. e-identifiering med skyddad identitet är inte möjlig. En text om att det inte är möjligt att e-identifiera sig vid skyddad identitet rekommenderas.*	☒	☐
Personuppgiftsbehandlingen sker i **stor skala** avseende *antalet berörda* personer i registret, *volymen av data* som behandlas, *varaktighet* för behandlingsaktiviteten och/eller den *geografiska omfattningen* av behandlingsaktiviteten.	☐	☒
Personuppgiftsbehandlingen omfattar uppgifter om **utsatta personer,** t ex barn, anställda, asylsökande, äldre, patienter ***Kommentar****: Anmälaren kan skicka in bilder och lägga in fritext och det kan komma in bilder och information om den som utsätts för tillsyn och familjemedlemmar så som barn.*	☒	☐
Personuppgiftsbehandlingen sker med hjälp av **innovativ användning** eller tillämpning av tekniska eller organisatoriska lösningar, exempelvis Internet of things och bodies (IoT och IoB)	☐	☒
Personuppgiftsbehandlingen innebär att **personuppgifter från två eller flera behandlingar kombineras** på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig.	☐	☒

Kommentar: *Personuppgifter från två eller flera behandlingar kan komma att ske om det är nödvändigt för utredningen.*		
Behandlingen innebär att personuppgifter behandlas i syfte att **hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal**	☐	☒
Dataöverföring sker till **länder utanför EU/EES** (tredjeland).	☐	☒

Resultat av tröskelanalys

☐ Det föreligger sannolikt inte en hög risk för den registrerades fri- och rättigheter. Konsekvensbedömning behöver därför inte genomföras.

☒ Förutsättningarna för den tilltänkta behandlingen innebär att kraven för konsekvensbedömning är uppfyllda. En konsekvensbedömning ska därför göras.

Kommentar: Tröskelanalys gjord 2022-06-22.

Kungsbacka

KONSEKVENSBEDÖMNING

Syfte med behandlingen

Syftet med behandlingen är att ge allmänheten en möjlighet att komma in med anmälan via e-tjänst om tillsyn enligt plan- och bygglagen så som olovligt byggande, ovårdad fastighet, enkelt avhjälpta hinder, obligatorisk ventilationskontroll, hissar och andra motordrivna anordningar.

Behandlingens förtjänster

E-tjänsten förenklar förfarandet för den som anmäler och möjliggör att rätt uppgifter lämnas in vid första anmälningstillfället, eftersom e-tjänsten talar om för anmälaren vad som ska fyllas i.

Risken är annars att personen låter bli att anmäla och det kan leda till att personer kan komma till skada om en byggnad inte uppfyller de tekniska egenskapskraven, vid trasiga hissar, saknade stängsel, höga murar som utgör en trafikfara med mera.

Bilder och beskrivning i fritext ger snabbt handläggaren en tydlig uppfattning om vad anmälan berör och handläggaren kan därmed skyndsamt agera utifrån anmälan och vidta eventuella åtgärder än om handläggaren hade behövt inleda med att göra ett platsbesök och undersöka vad som anmälts. Med bilder och beskrivning i fritext kan handläggaren avgöra om det finns fara för liv och hälsa och om ärendet behöver prioriteras. Det är också lättare för handläggaren att avsluta en anmälan som visar sig inte vara befogad, vilket för den som blir anmäld innebär ett snabbt avslut.

Behandlingens lagliga grund

Den specifika behandlingen Anmäla tillsyn enligt plan- och bygglagen grundar sig på **myndighetsutövning**, skyldighet enligt plan- och bygglagen 11 kap. 5 §:

En tillsynsmyndighet ska pröva förutsättningarna för och behovet av att ingripa eller besluta om en påföljd enligt detta kapitel, så snart det finns anledning att anta att någon inte har följt en bestämmelse i denna lag, i föreskrifter, domar eller andra beslut som har meddelats med stöd av lagen eller i EU-förordningar som rör frågor inom lagens tillämpningsområde.

Behandlingen grundar sig också på ett **allmänt intresse** enligt förvaltningslagen 6 och 9 §§:

En myndighet ska se till att kontakterna med enskilda blir smidiga och enkla. Myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Den ska ges utan onödigt dröjsmål.

Ett ärende ska handläggas så enkelt, snabbt och kostnadseffektivt som möjligt utan att rättssäkerheten eftersätts.

Kungsbacka

Behandlingens art

Anmälan initierar endast ett tillsynsärende och handläggaren utreder först utifrån anmälarens information och därefter utifrån egen insamlad information.

Den som anmäler behöver e-identifiera sig, men kan i e-tjänsten välja att vara anonym. Personnummer förekommer vid inloggning med e-identifiering. E-identifiering med skyddad identitet är inte möjlig.

E-identifiering behövs för att någon inte ska kunna göra anmälan i någon annans namn.

En text om att det inte är möjligt att e-identifiera sig vid skyddad identitet rekommenderas.

Om anmälaren inte valt att vara anonym och lämnat sin e-postadress, så genereras ett bekräftelsemejl till anmälaren. I bekräftelsemejlet framgår inga personuppgifter, utan enbart information om att en anmälan tagits emot.

Personuppgifter som behandlas i e-tjänsten är:

- Fastighetsbeteckning (obligatorisk)
- Namn på fastighetsägare eller den som begått överträdelsen (ej obligatorisk)
- Adress till fastighetsägare eller den som begått överträdelsen (ej obligatorisk)
- Namn på anmälare om denna inte valt att vara anonym (obligatorisk)
- Adress till anmälare om denna inte valt att vara anonym (obligatorisk)
- e-postadress till anmälare om denna inte valt att vara anonym (ej obligatorisk)
- Telefonnummer till anmälare om denna inte valt att vara anonym (ej obligatorisk)

I e-tjänsten finns det fritextfält där anmälaren kan lämna information som berör någons privata sfär och uppgifter om sociala förhållanden, men dessa uppgifter är inget som e-tjänsten begär in och förekommer sällan. En karta finns för att markera var olovligheten finns. Därtill kan anmälaren bifoga bilder på fastighet/eventuell lagöverträdelse. Kategorier av registrerade som kan förekomma på bilder eller i fritextalternativen ”annat” och ”beskrivning” är fastighetsägare, byggnadsägare, anmälare, boende och barn.

Antalet anmälda tillsynsärenden är ca 400 per år. Spridningen av uppgifter begränsas till de personer som handläggaren har behov av att involvera vid sin utredning samt om någon begär ut allmän handling.

Behandlingen av personuppgifter i e-tjänsten Anmäla tillsyn enligt plan- och bygglagen är tillfällig då det inte finns behov av eller lagligt stöd för långvarig lagring i e-tjänstens plattform. Information från e-tjänsten flyttas automatiskt över till avsett verksamhetssystem. Personuppgifterna lagras inte längre än nödvändigt i plattformen.

Anmälan kommer in automatiskt via en integration till verksamhetssystemet och registratorerna meddelas via mejl till funktionsbrevlådan - förvaltningens e-brevlåda om att det skapats ett nytt

ärende med dnr i verksamhetssystemet. Funktionsbrevlådan bevakas dagligen på vardagar.

Användare av uppgifterna

De som kommer att använda uppgifterna är:

- Bygg- och miljöförvaltningens anställda.

- Den person som anmäler olovligheten.
- Den anmälde som utsätts för tillsyn.

- De invånare som begär ut allmän handling.
- Andra myndigheter vid exempelvis överklagan av beslut.

Informationssäkerhet

Informationssäkerhet
För att säkerställa rätt nivå av informationssäkerhet har informationsklassificering enligt SKR:s klassningsmodell KLASSA med tillhörande riskanalys genomförts av kommunens specialister inom informationssäkerhet.

Modellen klassificerar information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet kan leda till. Konsekvenserna värderas i grader av oönskad påverkan på verksamheten eller annan part, såsom invånare eller företagare. Detta till följd av otillräcklig konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Om exempelvis invånaren lider allvarlig skada av att viktig information för verksamheten blir tillgänglig för obehöriga, ska informationen placeras i en klass med hög konsekvensnivå gällande konfidentialitet.

Informationsklassificeringen resulterar i en skala som går från Försumbar skada (0), Måttlig skada (1), Betydande skada (2), Allvarlig skada (3) och Synnerligen allvarlig skada (4). Klassificeringen ger ett stöd för att bedöma hur informationen ska värderas och ger på så sätt en vägledning angående vilka hanteringskrav som ska appliceras.

Både Open ePlattform och verksamhetssystemet ByggR klassades gällande Konfidentialitet, Riktighet, Tillgänglighet och Spårbarhet enligt nivå 3, det vill säga Allvarlig skada. Att Open ePlattform klassas enligt nivå 3 på samtliga punkter innebär alltså att konsekvenser av oönskad påverkan på informationens kvalitet kan leda till allvarlig skada för verksamheten eller externa målgrupper.

Resultatet av informationsklassificeringen ligger till grund för informationssäkerhetskraven som inkluderas i avtalet med leverantör av drift, support och förvaltning av plattformen. Dessa krav handlar om tekniska åtgärder såsom brandväggar, krypteringsfunktioner och antivirus eller organisatoriska åtgärder såsom säkerhetsarbetets organisation och rutiner, instruktioner och uppföljning. Kraven

omfattar ett servicenivåavtal och krav på rapportering av leverantörens arbete med informationssäkerhet.

Kommunen har enligt avtalet också rätt till insyn i leverantörens testarbete och rätt att följa upp och övervaka leverantörens efterlevnad gällande kommunens informationssäkerhetskrav, samt krav på hantering av personuppgifter.

Plattformen är baserad på öppen källkod och är byggd utifrån att det ska vara enkelt att både utveckla och använda e-tjänster, samt att det ska finnas möjlighet att få översikt över och enkelt kunna följa de ärenden som e-tjänsterna genererar. Samtliga funktioner och gränssnitt, inklusive funktion för att bygga e-tjänster, är helt webbaserade och använder webstandarden HTML5. Utdata från Open ePlattform skickas i öppna dataformat (XML) med tillhörande dataschema (XSD). Plattformen bygger på ramverket Open Hierarchy som är ett generiskt ramverk för öppen källkod. Open ePlattform kan både skicka och ta emot data via öppna integrationsgränssnitt. Detta innebär att plattformen kan skicka vidare ansökningar, anmälningar och beställningar till externa system, men även att externa system kan skicka exempelvis statusuppdateringar till plattformens funktion Mina sidor.

Om man som privatperson anmäler tillsyn enligt plan- och bygglagen, krävs e-legitimering, men denna kan välja att vara anonym. Då registreras varken informationen om anmälaren i ärendet eller IP-adress från den dator som anmälan kommer i plattformen. Anonymt inskickade ärenden går inte heller att följa via Mina sidor.

Lagring av uppgifterna
Personuppgifter som behandlas i Open ePlattform kan delas upp i följande grupper:

- Uppgifter om interna användare hanteras när en användare skapas och tas bort.
- Uppgifter om externa användare skapas vid första inloggning i plattformen.
- Uppgifter om externa användare via inskickade ärenden registreras vid användning en e-tjänst.

Personuppgifterna lagras hos drift- och supportleverantören Nordic Peak AB i Sundsvall på en avgränsad serveryta som nyttjas endast av Kungsbacka kommun. Leverantörens serverhall är en konstruktion från 2016 och utformad enligt gällande riktlinjer från Myndigheten för samhällsskydd och beredskap. Riktlinjerna syftar till att ge bästa möjliga säkerhet, tillgänglighet och energieffektivitet, exempelvis gällande brandskydd och redundans av lagrad information.

Vid avveckling av hårdvara lämnar ingen lagringsmedia serverhallen innan den destrueras. Endast ett utpekat antal personer inom leverantörens organisation har åtkomst till serverhallen. All inpassering loggas via inpasseringssystem.

Kungsbacka

Personuppgifter kan gallras automatiskt eller manuellt från plattformen via systemets gallringsfunktion. Hur och när gallring av uppgifter om externa användare via inskickade ärenden ska ske specificeras vid framtagande av ny e-tjänst.

Förvaltningen som tar emot ärendet bestämmer när automatisk gallring ska ske i Open ePlattform och tillser att rutiner för gallring finns.

För den avsedda tjänsten Anmäla om tillsyn enligt plan- och bygglagen kommer gallring ske automatiskt i Open ePlattform 3 månader inkommit.

Omständigheter kring eventuellt utlämnande till tredjeland

Ingen överföring av personuppgifter till tredje land förekommer. Leverantören för drift, support och förvaltning, Nordic Peak AB, har sitt säte i Sundsvall, Sverige. Lagringen av personuppgifter sker på en serveryta hos leverantören dedikerad enbart till Kungsbacka. Leverantören har inga underbiträden.

I personuppgiftsbiträdesavtalet med Nordic Peak ställs följande krav gällande lokalisering och överföring av personuppgifter till Tredje land: All data som behandlas ska lagras på biträdets egen server belägen i Sverige. Ingen överföring till tredje land får ske i samband med den behandling som detta avtal berör.

I kravspecifikationen gentemot leverantören ställs följande krav gällande tredje land: All data ska lagras/behandlas inom EU eller i tredje land där EU-kommissionen har fastslagit att landet har en adekvat skyddsnivå för personuppgifter.

I de fall Leverantören erbjuder tjänster utanför EU/EES ska det finnas färdiga och prövade juridiska avtal för det område som behandlingen av informationen avser. Om Leverantören vill placera data i ett tredje land, eller på annat sätt behandla personuppgifter i tredje land och där landet inte svarar mot detta åligger det Leverantören att visa att behandlingen uppfyller kraven i dataskyddsförordningen artikel 46.

Potentiella risker

Obehörig åtkomst

Obehöriga skulle kunna få åtkomst till personuppgifter i Open ePlattform genom att komma över en användares e-legitimation och på så sätt komma in i *Mina sidor*. Personen skulle då endast komma åt uppgifter i ärenden som den berörda användaren har skickat in eller påbörjat. Åtkomst skulle även finnas till grundinformation i form av namn och kontaktuppgifter vilka finns under *Mina sidor*.

Under mina sidor syns dock inte tillsynsärenden därför finns det ingen risk kopplad till den här e-tjänsten.

Kungsbacka

Obehöriga skulle kunna få åtkomst till personuppgifter i Open ePlattform genom att komma över en anställds inloggningsuppgifter och/eller e-legitimation (personalkonto) och på så sätt komma in i plattformen. Vilken omfattning av personuppgifter den obehörige får tillgång till beror på vilken behörighet den anställde har i Open ePlattform. Ett fåtal anställda inom kommunen kommer ha behörighet att ändra behörighet för andra anställda. Risken att ge fel anställd behörighet och därmed åtkomst till personuppgifter de inte bör ha tillgång till finns om rutiner för behörighetstilldelning inte följs.

Risk för missbruk av anställdas egna behörigheter finns. Vilken åtkomst det innebär beror på den anställdes behörighet. Anställda med handläggarbehörighet (handläggare och registratorer) har tillgång till personuppgifter som lämnats via användare av en e-tjänst även om anmälan numera kommer in automatiskt till verksamhetssystemet. Handläggares och registratorers behörighet är kopplad till specifik e-tjänst och de har endast behörighet till de ärenden som är inskickade via den specifika e-tjänsten.

Personal som är behörig till anmälningarna verifierar sin identitet genom inloggningsuppgifter till verksamhetssystemet.

Obehörig ändring

Den som skickat in en anmälan via en e-tjänst kan inte gå in i efterhand via *Mina sidor* och ändra uppgifterna eller komplettera sitt ärende om förvaltningen väljer att ställa in så att det kan göras. Det är då spårbart, både originalärendet och det nya sparas. Informationen om ärendehistorik finns i handläggarverktyget.

En anställd med behörighet som ger tillgång till uppgifter i inskickad anmälan har möjlighet till att ändra denna i supportsyfte om förvaltningen väljer att ställa in så att det kan göras. Den anställde skulle obehörigt kunna ändra eller ta bort personuppgifter i inskickade ärenden. Det är då spårbart, både originalärendet och det nya sparas. Informationen om ärendehistorik finns i handläggarverktyget.

Förlust av uppgifter

Personuppgifterna i Open ePlattform lagras på en serveryta dedikerad till Kungsbacka kommun hos drift- och supportleverantören Nordic Peak AB i Sundsvall. Om serverhallen skulle drabbas av till exempel brand eller stöld kan uppgifter gå förlorade.

All data säkerhetskopieras 1 gång per dygn och lagras som standard i 12 månader bakåt i tiden. Återläsning av backup sker automatiskt i samband med varje backup. Detta innebär att den information som har gallrats i Open-e plattformen ligger kvar i backupen 12 månader bakåt i tiden, men endast de med behörighet till backup kan ta fram denna information.

En användare kommer inte att kunna ta bort information i ett inskickat ärende i Open ePlattform och därmed finns ingen risk för informationsförlust avsiktligt eller oavsiktligt av information hos den egna användaren.

Informationen skulle kunna vara tillfälligt otillgänglig vid exempelvis avbrott, men Open ePlattform är kravställt utifrån en viss servicenivå vilken framgår i avtalet. Enligt avtal ska leverantören ha reservrutiner, reservlösningar och återstartsplaner som uppfyller kommunens krav på tillgänglighet.

Övriga risker kopplat till de registrerades friheter och rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskydds-förordningen. Dessa rättigheter innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller att få ut sina uppgifter.

Den registrerade har rätt att få information när hens personuppgifter behandlas. I Open ePlattform finns det inställningar för information om behandlingen av personuppgifter kopplat till varje e-tjänst. Informationen framgår innan e-tjänsten startas. Om rutiner för personuppgiftsinställningarna inte följs eller felaktig information fylls i riskeras rätten till information.

Den registrerade har rätt att vända sig till en myndighet för att få veta vilka personuppgifter myndigheten behandlar om personen och på vilket sätt uppgifterna behandlas, genom ett så kallat registerutdrag.

Varje person har rätt att vända sig till en myndighet som behandlar personuppgifter och be att få felaktiga uppgifter rättade. Rutiner eller arbetssätt för hur begäran om rättelse kopplat till Open ePlattform ska hanteras måste upprättas för att kunna tillgodose denna rättighet.

Varje person har rätt att vända sig till en myndighet som behandlar personuppgifter och be om att uppgifterna som avser honom eller henne raderas.

Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Integritetsskyddsmyndigheten. Information om rätten till och hur den registrerade kan lämna klagomål ska finnas i början av varje e-tjänst. Om rutinen för att tillse att dessa uppgifter finns på plats inte följs finns risk att information om hur att lämna klagomål inte framkommer.

På kommunens hemsida finns rutiner för utövandet av rättigheter. Förvaltningen har också etablerade rutiner i händelse av personuppgiftsincident.

Parter som gynnas av behandlingen

Bygg- och miljöförvaltningens anställda sparar arbetstid på att få in anmälan via e-tjänst då den möjliggör att rätt uppgifter lämnas in vid första anmälningstillfället, eftersom e-tjänsten talar om för

anmälaren vad som ska fyllas i och ger ökat utrymme för att beskriva olovligheten genom fritextfält och möjlighet att lämna in bilagor så som bilder.

Anmälaren kan snabbt och enkelt anmäla. Invånare gynnas på så sätt att farliga olovligheter snabbare kommer till Bygg- och miljöförvaltningens kännedom.

Den som blivit anmäld kan snabbare få ärendet prövat.

Konsekvenser av att personuppgiftsbehandlingen inte kan utföras

Förvaltningen vill komma bort från hantering av känsliga och sekretessbelagda personuppgifter via e-post/Office 365. Idag landar en del anmälningar och information om tillsynsärenden i e-posten.

Konsekvenserna blir att förvaltningen kan komma att fortsätta behöva hantera känsliga och sekretessbelagda personuppgifter som kräver extra skydd i en tekniskt osäker miljö om föreslagen behandling inte kan utföras.

Kan ändamålet uppnås utan eller genom en mindre omfattande personuppgiftsbehandling

Ändamålet skulle kunna uppnås genom en mindre omfattande personuppgiftsbehandling.

I e-tjänsten Anmälan enligt plan- och bygglagen rör det sig om uppgift om misstänkt lagöverträdelse. Vid anmälan kan det komma in uppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden, eftersom det är möjligt att bifoga bilagor så som bilder och i fritext göra en beskrivning. Endast kryssalternativ och karta i e-tjänsten har diskuterats med tillsynsgruppen.

Om endast kryssalternativ och karta används i e-tjänsten finns ingen risk för att känsliga och sekretessbelagda personuppgifter som kan beröra någons privata sfär, uppgifter om sociala förhållanden och bilder kan komma in via e-tjänsten.

Då dessa känsliga och sekretessbelagda personuppgifter kommer in i mycket liten omfattning och därtill inte är uppgifter som begärs in utan lämnas av anmälaren bedöms risken att någon kan komma till skada väga tyngre gentemot de personer som kan beröras av e-tjänstens behandling.

En intern rutin för att ta emot känsliga och sekretessbelagda personuppgifter ska upprättas för att fånga upp dessa när de kommit in till e-tjänsten och därefter automatiskt till verksamhetssystemet.

De registrerades förväntningar

Internetstiftelsen gör årligen undersökningen *Svenskarna och internet* som är Sveriges mest omfattande och etablerade undersökning av svenskarnas digitala vanor. I de senaste årens undersökningar framgår

att invånares förväntningar på kommuner gällande digital service ökar kraftigt. Den senaste undersökningen, som lanserades december 2020, visar att förväntningarna på att kommunen ska tillhandahålla en på alla sätt tillgänglig och heltäckande digital service av samtliga tjänster har ytterligare snabbats på av Coronapandemin. Resultaten av undersökningen visar att det på många sätt har skett en snabb och omfattande digitalisering i samhället där många invånare börjat använda digitala tjänster mer frekvent än tidigare eller testat dem för första gången. Framför allt äldre har tagit klivet ut på internet och börjat använda digitala tjänster mer än tidigare, och det gäller särskilt de allra äldsta.

I denna e-tjänst rekommenderas att en informationstext läggas in för att minska risken för att det ska komma in bilder där det förekommer personer eller annan privat information i fritextfält. Informationstexten ska upplysa anmälaren om att anmälan och eventuella bilagor så som bilder kommer att bli allmän handling.

Den registrerade kan förvänta sig att en jämförelse med tidigare ärendens handlingar, flygfoton och kartor kan komma att behöva göras då det är viktigt för att utreda anmäld olovlighet.

Ärenden kan också komma att lämnas ut till den som begär ut en allmän handling eller andra myndigheter vid överklagan.

Samråd med registrerade behöver inte genomföras om det är oproportionerligt eller ogenomförbart. I detta fall rör det sig om tillsyn och både de som anmäler och den som anmäls är svåra att identifiera före en olovlighet har anmälts.

Inhämtning av synpunkter från invånare inom kommunens tillsynsområde genomförs regelbundet för de som använder e-tjänsten för att anmäla. Övrig inhämtning har inte genomförts på grund av behandlingens art alltid kan innebära ett intrång i den personliga integriteten, vilken behöver vägas mot risken att någon kan komma till skada på grund av olovligheten.

Den personuppgiftsansvariges ställning

Byggnadsnämnden upprätthåller en offentlig verksamhet med tillsynsansvar som inbegriper myndighetsutövning. Därför har den personuppgiftsansvarige i detta fall en ställning som är mer dominant i förhållande till den registrerades ställning, vilket är viktigt att beakta gällande den tilltänkta behandlingen.

I e-tjänsten har den som blir anmäld för olovlighet en utsatt ställning gentemot den personuppgiftsansvarige.

Den tilltänkta behandlingen av personuppgifter underlättar för den personuppgiftsansvarige att utföra sitt tillsynsansvar och uppfylla de förväntningar som finns från invånare, företagare, föreningar och besökare om att tillhandahålla en god digital service.

Kungsbacka

Tiden från att anmälan kommer in till att ett beslut kan tas i ärendet minskar när anmälan innehåller tydlig information om vad ärendet gäller. Handläggaren kan även tidigt avgöra om det anmälan gäller strider mot plan- och bygglagen och dess föreskrifter och kan även på så sätt minska handläggnings-tiden En kort handläggningstid är fördelaktigt i ärenden med risk för att människor kommer till skada. En kort handläggningstid är även att föredra för den som blir anmäld men även att det finns tydligt underlag så att rättssäkra beslut tas. Sammantaget uppväger ovan nämnda den personuppgiftsansvariges ställning i förhållande till den som anmäls i tillsynsärenden.

Sammanfattande bedömning

I e-tjänsten *Anmäla om tillsyn enligt plan-och bygglagen* rör det sig om uppgift om misstänkt lagöverträdelse.

Vid anmälan kan det komma in personuppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden, eftersom det är möjligt att i e-tjänsten bifoga bilagor så som bilder och att i fritext göra en beskrivning.

Ändamålet skulle kunna uppnås genom en mindre omfattande personuppgiftsbehandling. Endast kryssalternativ och karta har diskuterats med tillsynsgruppen. Om endast kryssalternativ och karta används i e-tjänsten finns ingen risk för att personuppgifter som berör någons privata sfär och som handlar om någons sociala förhållanden kan komma in.

Förvaltningen kan också konstatera att ärenden som innehåller känsliga och sekretessbelagda personuppgifter förekommer i mycket liten omfattning i förhållande till inkomna anmälningar via e-tjänsten.

I ärenden som gäller fara för liv och hälsa är det av yttersta vikt att ärendet handläggs omgående. När anmälan innehåller tydlig information med bilagor och fritext kan handläggaren agera snabbare, vilket kan vara svårare om ärendet initialt inte visar fara för liv och hälsa.

Förvaltningen anser att risken att någon kan komma till skada väger tyngre gentemot de personers integritet som kan beröras av e-tjänstens behandling.

Inhämtning av synpunkter från invånare inom kommunens tillsynsområde genomförs regelbundet för de som använder e-tjänsten för att anmäla. Övrig inhämtning har inte genomförts på grund av behandlingens art alltid kan innebära ett intrång i den personliga integriteten, vilken behöver vägas mot risken att någon kan komma till skada på grund av olovligheten.

En informationstext rekommenderas att läggas in för att minska risken för att det ska komma in bilder där det förekommer personer eller privat information i fritextfält. Informationstexten ska upplysa anmälaren om att anmälan och eventuella bilagor kommer att bli allmän handling.

Kommunens informationssäkerhetsspecialist bedömer informationssäkerheten som mycket bra och inga uppgifter förvaras i tredje land utan på en avgränsad serveryta som endast nyttjas av Kungsbacka kommun.

e-tjänsten förväntas medföra att hanteringen av känsliga och sekretessbelagda personuppgifter kommer att behandlas säkrare än när anmälan kommer in på annat sätt.

Den automatiska gallringstiden i plattformen rekommenderas att utföras 3 månader efter att ärendet har avslutats i e-tjänsten. Om det skulle uppkomma ett problem med integrationen så behövs en gallringstid på 3 månader för att säkerhetsställa att anmälan kommit in och registrerats riktigt. En rutin ska upprättas för prövning, registrering och gallring.

Villkor för behandling

Angående villkor för behandling rörande tekniska och organisatoriska skyddsåtgärder, information till de registrerade samt följder för avtal och övriga följder, se övergripande konsekvensbedömning för Open ePlatform KS 2021-06-22, § 189.

Bedöm sannolikhet för risker och planera åtgärder

I tabellen nedan specificeras möjliga värden för konsekvens.

Konsekvensnivåer	Förklaring
1	Försumbar: Den registrerade har inga svårigheter att utöva sina fri- och rättigheter. Ingen eller endast försumbar ekonomisk eller social påverkan.
2	Måttlig: Den registrerades fri- och rättigheter kan inte garanteras. Den registrerade kan uppleva lindriga besvär men endast måttlig ekonomisk eller social påverkan.
3	Betydande: Den registrerades fri- och rättigheter kränks. Ekonomisk eller social påverkan för den registrerade. Kan också vara en situation där synnerligen många personers uppgifter inom konsekvensnivå 2 sprids.
4	Allvarlig: Skapar stora besvär för den registrerade genom exempelvis diskriminering, identitetsstöld eller identitetsbedrägeri, stor ekonomisk förlust, skadat anseende eller annan betydande ekonomiskt eller social nackdel. Kan även innebära fara för liv och hälsa.

I tabellen nedan specificeras möjliga värden för sannolikhet.

Sannolikhet	Förklaring	Frekvens
1	Skadan har inte inträffat eller sker mycket sällan. Ytterst liten sannolikhet att skadan kommer att inträffa under behandlingens livstid.	Mer sällan än vart 10:e år.
2	Skadan kommer sannolikt att inträffa någon gång.	Mellan vart 10:e och varje år.
3	Skadan kan inträffa regelbundet. Sannolikt att skadan kommer att inträffa.	En gång per år.
4	Skadan kan inträffa ofta.	Flera gånger per år.

I tabellen nedan redogörs för risker för de registrerades fri- och rättigheter i samband med e-tjänstens behandling samt konsekvens och sannolikhet för om dessa risker realiseras.

Risk	Konsekvens, beskriv i ord samt ange siffra (1–4)	Sannolikhet (1–4)	Åtgärd, inklusive ansvarig för genomförande
Obehörig åtkomst till e-tjänsten genom stöld av extern användares e-legitimation	1. Försumbar	1. Ytterst liten sannolikhet att skadan kommer att inträffa under behandlingens tid då det inte finns möjlighet att se tillsynsärenden under *Mina sidor*	
Obehörig åtkomst till e-tjänsten genom stöld av anställds e-legitimation och/eller inloggnings-uppgifter	2. Måttlig, eftersom det endast går att se anmälan men inte göra ändringar i anmälan, eftersom det automatiskt redan är inlämnat och registrerat i ärendehanteringssystemet ByggR	1. Ytterst liten sannolikhet att skadan kommer att inträffa under behandlingen	Uppföljning av att behörighetsrutiner följs Ansvarig för genomförande: Tjänsteutvecklare
Obehörig åtkomst till e-tjänsten genom fel tilldelad behörighet	1. Försumbar	2. Kommer sannolikt att inträffa någon gång	Uppföljning av att behörighetsrutiner följs Ansvarig för genomförande: Tjänsteutvecklare

Obehörig åtkomst till e-tjänsten genom missbruk av egen behörighet	1. Försumbar	1. Inträffar mycket sällan	Uppföljning av att behörighetsrutiner följs Ansvarig för genomförande: Tjänsteutvecklare
Obehörig ändring genom stöld av extern användares e-legitimation	1. Försumbar	1. Ytterst liten sannolikhet att skadan kommer att inträffa under behandlingens tid då det inte finns möjlighet att se tillsynsärenden under *Mina sidor*	
Obehörig ändring av användare med behörighet att göra ändringar i inskickade ärenden	1. Försumbar	2. Skadan kommer sannolikt inträffa någon gång.	Uppföljning och utbildning kring behörigheter i verksamhetssystemet ByggR Ansvarig för genomförande: Tjänsteutvecklare
Förlust av uppgift vid brand eller stöld av server	3. Betydande, men beror på hur stor förlusten blir	1. Inträffar mycket sällan	Uppföljning av krav på leverantören angående säkerhet. Ansvarig för genomförande: Tjänsteutvecklare plattform
Otillgängliga uppgifter vid t.ex. avbrott	1. Försumbar, men är beroende på omfattning av t.ex. avbrott	1. Inträffar mycket sällan	Informationsinsatser angående eventuella planerade och oplanerade driftstopp. Ansvarig för genomförande: Tjänsteutvecklare plattform

Förhandssamråd

Förhandssamråd med dataskyddsombud (DSO)

Yttrande från dataskyddsombudet inkom 2022-06-29. Förvaltningens bedömning avviker från dataskyddsombudets yttrande i fråga om möjligheten för anmälaren att i e-tjänsten kunna bifoga filer så som bilder samt ifråga om att de registrerades inställning till behandlingen inte fullt ut har inhämtats. Dataskyddsombudet är tveksam till att det kan anses nödvändigt och proportionerligt att ta in bilder redan vid den initiala anmälan, med tanke på den integritetsrisk det kan innebära för den som blir anmäld. Eftersom det är tillsynsmyndigheten som ska säkerställa empirin innebär det att bevisvärdet på bilderna som inges av anmälare många gånger är lågt eftersom bilder både kan förvanskas och manipuleras. Dataskyddsombudet kan inte se att en snabbare handläggning kan ha

företräde framför en mer korrekt och rättssäker när det handlar om enskildas integritet i den privata sfären.
Dataskyddsombudet rekommenderar att de registrerades inställning till behandlingen inhämtas för att få en förståelse för de registrerades perspektiv på en behandling av integritetskänslig karaktär.

Förhandssamråd med integritetsskyddsmyndigheten

Riskerna vid behandlingen har kunnat sänkas till en låg nivå och förhandssamråd med IMY behövs därmed inte.

Uppföljning

Plan för löpande uppföljning

Förvaltningsmodellen för Open-e plattformen är utformad för att skapa samsyn i arbetet med att utveckla och förvalta e-tjänster, varav hantering av personuppgifter är en viktig del.

Ansvar, roller och forum i arbetet med förvaltning är tydligt definierade i modellen. I förvaltnings-modellen beskrivs vilka roller som ska ansvara för att behandlingen av personuppgifter följs upp, utvärderas och upprätthålls kontinuerligt. Det finns även beskrivningar av de arbetssätt, rutiner och forum som tagits fram för att stödja arbetet med att kontrollera att skyddet av personuppgifter upprätthålls över tid i samband med förvaltning av plattformen.

Kommunens e-tjänsteplattform Open-e Plattform har en utsedd ägare som kan delegera uppgifter inom verksamheten men inte kan frånsäga sig ansvar. I ansvaret ingår bland annat att upprätta personuppgifts-biträdesavtal. Det operativa arbetet leds av en central e-tjänstesamordnare och där ingår ansvar för att upprätthålla, följa upp och utvärdera personuppgiftshanteringen i förhållande till de villkor som satts upp i konsekvensbedömningen. Gruppen Stöd och samordning har en viktig roll i arbetet och ansvarar för kontakter kring tekniska frågor kopplat till behandlingen av personuppgifter. Det kan handla om att genomföra och följa upp tekniska åtgärder som påverkar hantering av personuppgifter.

Bygg- och miljöförvaltningen har en e-tjänstesamordnare som har kunskap om plattformens funktioner och möjligheter, vilket innefattar hantering av personuppgifter inom sin verksamhet och respektive e-tjänster. E-tjänstesamordnaren är samordnande för verksamheten och har ansvaret att informera övriga roller inom sin förvaltning gällande bland annat hantering av personuppgifter i Open- e Plattform samt att delta i interna forum och nätverk kring förvaltning av plattformen. E-tjänstsamordnaren har ett nära samarbete med nämndens dataskyddskontakt.

Arbetet med kommunens e-tjänster drivs framåt i olika forum med olika inriktningar och syften. Forumet Stöd och samordning stöttar e-tjänstesamordnare och e-tjänsteutvecklare och har det övergripande ansvaret för att genomföra utbildning inom organisationen gällande bland annat hantering av personuppgifter kopplat till förvaltning av Open-e plattformen.

Kungsbacka

Den tilltänkta e-tjänsten *Anmälan om tillsyn enligt plan- och bygglagen* kommer att följas upp genom ett nära samarbete kommunens samordnare för e-tjänster, nämndens e-tjänstsamordnare samt nämndens dataskyddskontakt.

För att motverka obehörig åtkomst behöver behandlingen följas upp utifrån följande kritiska punkter:

- Rätt tilldelning av behörigheter.
- Tydlig information om behörigheter.

För att motverka obehörig ändring behöver behandlingen följas upp utifrån följande kritiska punkter:

- Säkerställande av loggning/tydlig loggningsrutin
- Utbildning om behörigheter för användare med behörighet att göra ändringar i inskickade ärenden.

Bilaga 1: Checklista för konsekvensbedömning (art. 35)

Kontrollera att konsekvensbedömningen åtminstone innehåller följande information. Kommentera om någon punkt inte har berörts.

☒ En **systematisk beskrivning** av den planerade behandlingen och dess syften (samt skälet till varför syftet anses berättigat)

☒ En **bedömning** av behovet av och **proportionaliteten** hos behandlingen i förhållande till dess syfte/n och riskerna.

☒ En **bedömning** av **riskerna för de registrerades rättigheter och friheter.**

☒ De **åtgärder** som behövs och planeras för att hantera riskerna (inbegripet *skyddsåtgärder*, *säkerhetsåtgärder* och *rutiner för att säkerställa skyddet* och för att *visa* att förordningen efterlevs, med hänsyn både till de registrerades och andra berörda personers rättigheter och berättigade intressen).

☒ **Dataskyddsombudets bedömning** av den aktuella behandlingen.
Kommentar: Samråd har skett med dataskyddsombudet, som lämnat yttrande 2022-06-29.

☒ **Beaktande** av de berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas **efterlevnad av godkända uppförandekoder** enligt GDPR artikel 40, framför allt vad gäller rutiner för konsekvensbedömning.

Bilaga 2: Om konsekvensbedömning (art. 35)

Den personuppgiftsansvariga ska säkerställa och visa att dess personuppgiftsbehandling följer dataskyddsförordningen. En konsekvensbedömning enligt dataskyddsförordningen är ett analysverktyg som används för att pröva om en behandling är laglig och berättigad, identifiera risker, vidta lämpliga åtgärder samt upprätthålla en säker personuppgiftshantering.

En konsekvensbedömning ska göras om personuppgifter behandlas på ett sätt som sannolikt leder till hög risk för de registrerades fri- och rättigheter (artikel 35.1, skäl 84). När är då det?

Integritetsskyddsmyndigheten (IMY) har publicerat en förteckning över när en konsekvensbedömning måste göras. Till exempel kräver följande behandlingar att en konsekvensbedömning utförs:

- ✓ Behandling av känsliga eller särskilt skyddsvärda personuppgifter
- ✓ Systematisk och omfattande övervakning eller profilering, t ex användande av kunders lokaliseringsuppgifter eller inrättande av kandidat- eller kompetensdatabaser
- ✓ Behandling som rör ett stort antal registrerade.

Integritetsskyddsmyndighetens förteckning är inte uttömmande, utan det är den personuppgifts-ansvariges ansvar att se till att konsekvensbedömning görs om det behövs. Ju mer komplex en behandling är desto större är risken för felaktig behandling. Syftet är att förebygga att så sker.

I tveksamma fall bör en konsekvensbedömning göras, även om två kriterier inte uppfylls. Det är inte fel att göra en konsekvensbedömning i ”onödan”.

Konsekvensbedömningen ska göras före dess att behandlingen påbörjas[2], och aktualiseras regelbundet.

Bedömningen görs behandling för behandling. Flera snarlika eller närliggande behandlingar kan dock ingå i en och samma konsekvensbedömning.

[2] Detta är förenligt med principerna om inbyggt dataskydd och dataskydd som standard (artikel 25 och skäl 78).

YTTRANDE

Dnr
BN 2021–002091

Datum
2022-06-29

Kungsbacka

Samråd med DSO

Yttrande om konsekvensbedömning för behandling av personuppgifter i samband med anmälan av tillsyn (ver.1.1, 2022-06-20)

Personuppgiftsansvarig nämnd: Byggnadsnämnden

Kontaktperson för konsekvensbedömningen: Camilla Cangren, byggnadsinspektör samt Nader Al-Tayyar, systemförvaltare

Dataskyddskontakt: Veronica Kinn

Jag har tagit del av er konsekvensbedömning avseende dataskydd vid behandling av personuppgifter i samband med anmälan av tillsyn enligt plan- och bygglagen och lämnar följande yttrande. Yttrandet ska diarieföras i det angivna ärendet.

Bedömning och rekommendationer

Metod

Jag ser inget annat än att ni för konsekvensbedömningen följt en ändamålsenlig metod där relevanta kompetenser och aktörer medverkat för att identifiera och sänka flera integritetsrisker som är förknippade med den aktuella personuppgiftsbehandlingen.

Det framgår exempelvis *vilka omständigheter som föranlett* att ni gjort en konsekvensbedömning. Konsekvensbedömningen innehåller också en *systematisk och funktionell beskrivning* av den planerade behandlingen och *dess syfte samt lagliga grund*, inbegripet identifiering av de rättskällor som den lagliga grunden vilar på. Det ges även en *beskrivning av behandlingens art, omfattning* och *sammanhang* samt en *beskrivning av de behandlade personuppgifterna*, *kategorierna av registrerade* och *användare* samt *perioden* som *personuppgifterna kommer att lagras*.

Det finns dessutom en *beskrivning av tillgångarna* som är nödvändiga för att behandla personuppgifterna (såsom programvara, personer). Vidare har en *bedömning gjorts av proportionaliteten i behandlingen i förhållande till syftet och principerna* om laglighet, lagrings- och uppgiftsminimiering samt uppgifternas relevans, samt en *bedömning av potentiella risker för de registrerades rättigheter och friheter*. ***De registrerades inställning*** **till behandlingen har dock inte inhämtats även om det ha beaktats. Jag rekommenderar därför att det görs**. Det behöver inte ske med personer som inkommit med eller varit föremål för anmälan, utan kan vara med invånare som bor i kommunen. Det kan inte anses oproportionerligt eller ogenomförbart utan snarare nödvändigt för att få en förståelse för de registrerades perspektiv på en behandling av integritetskänslig karaktär.

Vidare har en analys gjorts över *potentiella konsekvenser för de registrerades rättigheter och friheter i händelse av obehörig åtkomst, oönskad ändring* och *förlust av uppgifter*, inbegripet *en uppskattning av riskernas sannolikhetsgrad och allvar*. De *åtgärder* som planeras för att sänka behandlingens risker, inbegripet *både tekniska och organisatoriska skydds- och säkerhetsåtgärder*, framgår också och får anses adekvata och rimliga i förhållande till behandlingens risker. *Åtgärder som stärker de registrerades rättigheter i förhållande till artiklarna 15-21* har också beaktats, även i förhållande till biträdet. **Dock har biträdets eventuella anslutning till en *godkänd uppförandekod inte beaktats*. Jag rekommenderar er därför att göra det**. Detta med tanke på att det handlar om en molntjänst där en uppförandekod enligt artikel 40 finns i form av *EU Cloud Code of Conduct*. Ett biträde som är ansluten till en uppförandekod innebär ett bra skydd och kontroll på biträdets dataskyddsförmåga, vilket starkt rekommenderas för att uppfylla omsorgsplikten.

Slutligen har en *planering* gjorts för att kontinuerligt följa upp behandlingens skyddsnivå.

Mot bakgrund av ovan bedömer jag inget annat än att konsekvensbedömningen motsvarar dataskyddsförordningens krav i metod- och innehållshänseende[1].

Åtgärder

Trots att ni identifierat och omhändertagit flera risker som är förknippade med den aktuella behandlingen, vill jag lämna nedanstående kommentarer och rekommendationer för ert fortsatta arbete.

a) Förklara i konsekvensbedömningen varför man behöver verifiera sin identitet med BankId om man valt att vara anonym. Är det för att säkerställa att undvika att anmälan görs av en robot? I så fall – finns andra metoder som kan lösa det? Om BankId är en nödvändig metod– hur säkerställs anonymiteten?

b) Förtydliga hur personal som är behörig till anmälningarna verifierar sin identitet. Eftersom det rör sig om integritetskänsliga uppgifter bör personalens autenticiering vara stark för att uppnå erforderlig säkerhetsnivå enligt artikel 32 i GDPR.

c) Är det nödvändigt med gallringsfrist på 3 månader i plattformen när ärendet ändå direkt överförs till verksamhetssystemet för handläggning? Om ja, utveckla varför och hur det är förenligt med principen om lagringsminimering i artikel 5.1 (e) i GDPR. Tillsynsärenden verkar ju inte synas under *Mina ärenden* ändå? Eller är det bara för dem som anmälan gäller?

d) Klargör vad det betyder för de satta gallringsfristerna att information i Open E lagras som standard i 12 månader bakåt i tiden för backup. Innebär det att information som gallrats dessförinnan ligger kvar som back up? Om det är så, hur ska ni möta principen om lagringsminimering i artikel 5.1 (e) (i GDPR)?

e) Utveckla hur rätten till privatliv balanseras med nyttan av att olovligheter kommer kommunen till känna när möjligheten att anmäla underlättas. Det kan finnas risker att enskildas rätt till privatliv äventyras om grannar och allmänhet inte vet vad man kan klaga på, det vill säga vad som är olovligt. Jag rekommenderar er att utveckla er konsekvensbedömning med en analys av detta och att kompensera med tydlig information om vad anmälan kan användas för så att just *olovligheter* signaleras i e-tjänsten.

[1] Artikel 35.1, 35.3 a-c i GDPR samt IMY:s förteckning enligt artikel 35.4 (DI-2018-13200, 2019-01-16), artikel 35.7 a, 35.8, 35.7 b, 35.7 c, 35.7 d, 35.9, 35.11, skäl 84 och 90 i GDPR samt Artikel 29-gruppens riktlinjer för konsekvensbedömning (WP260 rev.01, 2017-11-29)

f) Jag rekommenderar er att inhämta registrerades inställning till behandlingen, alltså invånare i kommunens tillsynsområde. Det saknar betydelse om dessa invånare har anmält eller blivit föremål för anmälan. Det hindrar inte att be anställda i kommunen som också är invånare bistå med sina synpunkter på behandlingen, om det skulle underlätta för att få fångst på detta perspektiv. Att inhämta de registrerades perspektiv följer dels av artikel 35.8 i GDPR, dels vidgar det er förståelse för vad som är viktigt ur de registrerades synvinkel och hjälper er att utforma behandlingen utifrån det.

g) När det gäller inhämtning av bilder är jag tveksam till att det kan anses nödvändigt och proportionerligt att ta in det redan vid den initiala anmälan, med tanke på den integritetsrisk det kan innebära för den som blir anmäld. Eftersom det är tillsynsmyndigheten som ska säkerställa empirin innebär det att bevisvärdet på bilderna som inges av anmälare många gånger är lågt eftersom bilder både kan förvanskas och manipuleras. Jag kan inte se att en snabbare handläggning kan ha företräde framför en mer korrekt och rättssäker när det handlar om enskildas integritet i den privata sfären. Särskilt eftersom de situationer där detta bedöms vara aktuellt är uppskattade till att vara få och e-tjänsten inte är tänkt för akuta situationer.

   Jag rekommenderar av den anledningen att inte möjliggöra uppladdning av bilder utan i stället upplysa om att eventuella bilder som anmälaren har tagit hämtas in i senare skede. Ett fritextfält där anmälaren i egna ord beskriver sin uppfattning bör däremot vara motiverat ur ett rättssäkerhetsperspektiv, tillsammans med en upplysande text om betydelsen att vid anmälan lämna en saklig och objektiv beskrivning av den befarade olovligheten.

h) Ni anger i konsekvensbedömningen att ”En text om att det inte är möjligt att e-identifiera sig vid skyddad identitet rekommenderas”. Ni anger även att ”En intern rutin för att ta emot extra skyddsvärda personuppgifter och känsliga sekretessbelagda uppgifter ska […] upprättas för att fånga upp dessa uppgifter när de kommit in till e-tjänsten och därefter automatiskt till verksamhetssystemet.” samt att ”En rutin ska upprättas för prövning, registrering och gallring vid avslutande [av anmälan]”. Dessa åtgärder finns dock inte med i den lista som sammanfattar behandlingens riskminimerande åtgärder. Jag rekommenderar er att göra det så att det blir tydligt vilka skyddsåtgärder, både organisatoriska och tekniska, som vidtas för att sänka riskerna som är förenade med den aktuella behandlingen.

i) Att rutiner för utövandet av rättigheterna via kommunens hemsida finns kan med fördel tydliggöras i konsekvensbedömningen. Det kan även tydliggöras att förvaltningen har etablerade rutiner i händelse av personuppgiftsincident. Det stärker motiveringen av behandlingens organisatoriska skyddsnivå.

j) Det finns flera upprepningar i konsekvensbedömningen. Samma textstycke kan förekomma uppemot tre gånger på olika ställen. Det finns även en del korrektur i den löpande texten. För att göra konsekvensbedömningen läsvänlig och begriplig rekommenderar jag er att gå igenom den i sin helhet så att analysen blir sammanhängande och så enkel att förstå som det går.

Sammantagen bedömning

Under förutsättning att ni genomför de åtgärder som ni kommit fram till i konsekvensbedömningen och beaktar mina kommentarer och rekommendationer ovan kan jag inte se annat än att ni bör kunna komma till ett beslut om att den aktuella behandlingen är i linje med intentionerna i GDPR.

Karin Malmsten
Dataskyddsombud

Bilaga: Information om konsekvensbedömning

Krav på att genomföra konsekvensbedömning finns i artikel 35 i GDPR. Om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker. Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter såsom yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet och religionsfrihet.

En konsekvensbedömning ska åtminstone innehålla följande:

1) En **systematisk beskrivning** av den planerade behandlingen och dess syften
2) En **bedömning** av **behovet av** och **proportionaliteten** hos behandlingen i förhållande till dess syfte/n och de risker som finns.
3) En **bedömning** av **riskerna för de registrerades rättigheter och friheter.**
4) De **åtgärder** som behövs och planeras för att hantera riskerna (inbegripet *skyddsåtgärder*, *säkerhetsåtgärder* och *rutiner för att säkerställa skyddet* och för att *visa* att förordningen efterlevs)

Syftet med en konsekvensbedömning enligt artikel 35 är att utreda och påvisa efterlevnad av dataskyddsförordningen i samband med personuppgiftsbehandling som på ett eller annat sätt är riskfylld. Vid genomförandet av en konsekvensbedömning är det viktigt att alla relevanta och kända omständigheter för behandlingen lyfts in, analyseras och utvärderas samt att lämpliga skyddsåtgärder för den tilltänkta behandlingen beskrivs och genomförs. Arbetet med konsekvensbedömning är en iterativ process som handlar om att sänka riskerna som behandlingen är förknippad med. Konsekvensbedömningen har dels har ett internt syfte där organisationen för egen nytta analyserar och bedömer behandlingen med hänsyn till de registrerades rättigheter och friheter, dels ett externt syfte för att gentemot tillsynsmyndighet och andra intressenter visa på hur organisationen lever upp till dataskyddsförordningen.

Dataskyddsombudets roll i en konsekvensbedömning är att ha uppsikt över processen och ge råd utifrån aktuell lagstiftning och rättsläge[2]. Den personuppgiftsansvarige ska diarieföra dataskyddsombudets yttrande tillsammans med konsekvensbedömningen. Vid förnyad konsekvensbedömning kan dataskyddsombudet lämna förnyat yttrande.

Om åtgärder inte kan vidtas för att i tillräcklig utsträckning sänka de identifierade riskerna som framkommit av konsekvensbedömningen bör den personuppgiftsansvarige överväga att anmäla frågan till förhandssamråd med Integritetsskyddsmyndigheten (IMY). Följ då instruktionerna på IMY:s hemsida.

[2] Artikel 39.1 (c) GDPR