Dataskyddsombudets information och rådgivning

Kring hantering av personuppgifter som samlas in genom formulär på webbplatser

Handläggare: Veronica L Rasmussen, dataskyddsombud
Verksamhet: Informationssäkerhetsenheten, Katastrofmedicinskt centrum, Regionledningskontoret

Datum: 2023-08-28, v 2.0

www.regionostergotland.se

Region Östergötland

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Region Östergötland har idag ett antal webbplatser med koppling till regionen i någon form. Kommunikationsenheten arbetar med att samla alla webbplatser till en ny webbplats. På de befintliga webbplatserna förekommer det att olika typer av formulär används. Bland annat formulär för att ta emot beställningar, avbokningar och anmälningar till olika priser och evenemang som ordnas av verksamheter i Region Östergötland. Syftet är att underlätta för invånare, samarbetspartners och anställda att kontakta Region Östergötlands verksamheter i olika ärenden. I många av de formulär som används samlas personuppgifter in och det har uppkommit funderingar avseende hanteringen av personuppgifterna.

I dialog med Kommunikationsenheten har det konstaterats att Kommunikationsenheten erbjuder en tjänst till regionens verksamheter; att tillhandahålla en formulärfunktion via webbplatsen. Kommunikationsenheten förvaltar (här ingår bland annat informationsklassificering och kravställning) det IT-stöd som ligger till grund för webbplatsen och vad avser tjänsten formulär är Kommunikationsenhetens uppdrag och ansvar att ge stöd till regionens verksamheter dels med att upprätta formulär, dels med att bidra till att verksamhetens behandling av personuppgifter är i linje med det skydd som kan ges vid användandet av IT-stödet som Kommunikationsenheten erbjuder.

Den behandling av personuppgifter som genomförs vid användandet av ett formulär är däremot respektive verksamhet ansvarig för att den sker på ett korrekt sätt. Det är utifrån verksamhetens uppdrag som behandlingen av personuppgifter genomförs. Det är viktigt att ett samarbete i frågan om personuppgiftsbehandling sker mellan Kommunikationsenheten och aktuell verksamhet eftersom kunskap om behandlingen i sig och IT-stödet finns hos olika parter.

Det IT-stöd som Kommunikationsenheten förvaltar är Sitevision. Kommunikationsenheten erbjuder två typer av formulär dels frågeformulär som lagras i IT-stödet, dels e-postformulär som lagras i funktionsbrevlåda hos verksamhet eller anställds inkorg (e-postmiljön).

Dataskyddsombudet för Region Östergötland har till uppgift att informera och ge råd till Region Östergötland om dess skyldigheter enligt dataskyddsförordningen[1] och annan tillämplig dataskyddslagstiftning.

1.2 Uppdrag/beställning

Följande uppdrag har getts till dataskyddsombudet:

- Ge råd avseende vad Kommunikationsenheten behöver ta höjd för avseende personuppgiftsbehandling i dialog med verksamhet vid upprättande av ett formulär för att uppnå en god efterlevnad av dataskyddet.
- Ge generella råd avseende vanligt förekommande personuppgifter i formulär samt personuppgifter som inte lämpar sig att behandla i formulär.

1.3 Avgränsning

I denna rådgivning kommer inte befintliga formulär att granskas. Höjd tas inte i denna rådgivning för vilka skyddsåtgärder som finns på plats i IT-stöd/e-postmiljön. Rådgivning som ges är tänkt ska kunna appliceras generellt när en verksamhet beställer/önskar ett formulär av Kommunikationsenheten.

[1] Dataskyddsförordningen (EU) 2016/679.

2 Information och rådgivning

2.1 Inledning

Rådgivning avseende punkterna som anges under uppdrag/beställning ovan ges i avsnitt 2.2 och 2.3. Avsnitt 2.4 innehåller information som är av vikt att känna till med koppling till råd som ges.

Tanken är att nedan råd ska kunna vara ett stöd för er att få till ett arbetssätt som hjälper både Kommunikationsenheten och aktuella verksamheter vid utformande av ett formulär. Hur ni vill ta in nedan i era arbetsprocesser är upp till er. Tanken är att nedan råd kan kompletteras över tid, utifrån behov som uppstår.

2.2 Stöd inför upprättande av formulär med personuppgiftsbehandling

Nedan checklista är framtagen utifrån identifierat behov av stöd som Kommunikationsenheten i samarbete med aktuell verksamhet behöver när verksamhet önskar upprätta ett formulär på webbplatsen som medför en behandling av personuppgifter. Checklistan är till för att säkerställa att personuppgiftsbehandling som är tänkt att ske ska leva upp till de skyldigheter som Region Östergötland har avseende dataskydd. Punkterna hanteras förslagsvis i den ordning som de kommer, men de går att genomföra dem i annan ordning och även parallellt med varandra.

VAD	**HUR**	**STATUS**
Fastställ om önskemål finns att personuppgifter behandlas. Om personuppgifter inte ska behandlas behöver denna checklista inte användas.	Kommunikationsenheten kontrollerar om personuppgifter ska användas i formuläret. Ta hjälp av informationen nedan vad som utgör en personuppgift.	☐ Påbörjat ☐ Klart
Gå igenom uppdrag och ansvarsfördelning	Kommunikationsenheten håller i denna punkt vid ett samtal med verksamheten. Förslag på information att ta upp; Kommunikationsenheten: • Använder det IT-stöd som ligger till grund för webbplatsen där formulär finns. • Tillhandahåller tjänsten formulär där det ingår att ge stöd till regionens verksamheter dels med att upprätta formulär, dels med att bidra till att verksamhetens behandling av personuppgifter är i linje med det skydd som kan ges vid användandet av IT-stödet som Kommunikationsenheten erbjuder. Verksamhet: • Den behandling av personuppgifter som genomförs vid användandet av ett formulär är respektive verksamhet ansvarig för och att den sker på ett korrekt sätt. • Det är utifrån verksamhetens uppdrag som behandlingen av personuppgifter genomförs.	☐ Påbörjat ☐ Klart
Kontrollera tänkt personuppgiftsbehandling	Det är viktigt att den tänkta personuppgiftsbehandlingen har stöd i verksamhetens	☐ Påbörjat

gentemot verksamhetens uppdrag.	uppdrag. Förslagsvis äger verksamhet denna aktivitet, och verksamhet ska kunna visa/bekräfta till er att behandling omfattas av deras uppdrag.	☐ Klart
Identifiera och utvärdera verksamhetens personuppgiftsbehandling gentemot förvaltning av IT-stöd.	Förslagsvis genomförs denna aktivitet tillsammans mellan Kommunikationsenheten och verksamhet. Följande behöver genomföras: 1. Identifiera vilka personuppgifter som önskas samlas in. 2. Identifiera vilket formulär som ska användas. 3. Utvärdera om personuppgifterna behövs för att genomföra verksamhetens uppdrag? Kan några personuppgifter tas bort (uppgiftsminimering)? 4. Gå igenom kvarstående personuppgifter och diskutera om någon personuppgift är olämplig att använda (använd den generella rådgivning som getts avseende personuppgifter i formulär). 5. Genomför en informationsklassificering för att få fram vilket skydd uppgifterna bör ha. 6. Jämför identifierat krav på skydd med det skydd som IT-stödet eller e-posten ger? Är det tillräckligt? 7. Undersök om personuppgiftsbehandlingen omfattas av befintligt personuppgiftsbiträdesavtal med Sitevision. Om inte så behöver en komplettering genomföras.	☐ Påbörjat ☐ Klart
Kontrollera att information om personuppgiftsbehandlingen ges till de registrerade och ta vid behov fram information.	I varje formulär ska det finnas information om hur Region Östergötland behandlar personuppgifter som samlas in via formuläret. Informationssäkerhetsenheten har tagit fram tre övergripande informationsbrev om behandlingen av personuppgifter. Använd det som är lämpligt för ändamålet. • Invånare • Anställda • Patienter Informationen ska finnas med eller nås via en länk i formuläret. Använd det informationsbrev som är relevant för personuppgiftsbehandlingen. Om mail skickas till registrerade ska Region Östergötlands beslutade grafiska profil för e-postsignaturer användas, se här: https://intranat.regionostergotland.se/stod-i-arbetet/administrativt-stod/kommunikation/grafisk-profil-och-mallar. I signaturen står det information med koppling till dataskydd.	☐ Påbörjat ☐ Klart

2.3 Råd avseende användning av personuppgifter i formulär

Önskemål finns om att ge generella råd avseende vilka personuppgifter som kan respektive inte bör behandlas i formulär. Det är till en början av vikt att förklara att även om generell rådgivning ges, behöver varje fall bedömas enskilt utifrån dess omständigheter. Nedan ges således generell information och råd, vilket kan vara ett stöd i arbetet.

Till en början är det viktigt att känna till att det i dataskyddsförordningen inte finns nedskrivet vilka typer av personuppgifter som får användas på vilket sätt. Grundläggande för en bedömning av lämpligheten av att behandla personuppgiften är ett antal principer (nedan nämns de principer som är mest relevanta i detta sammanhang);

- **Ändamålsbegränsning** – Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål (uppdrag som regionen och dess verksamheter har styr vilka ändamål som är relevanta och således vilka personuppgifter som får behandlas). Ändamålet sätter ramarna för vilka personuppgifter samt vilka behandlingar av personuppgifterna som får och inte får ske.
- **Uppgiftsminimering** – Endast de personuppgifter som är nödvändiga för att uppnå ändamålet med behandlingen får behandlas, det är således inte tillåtet att samla in och behandla för många personuppgifter. De personuppgifter som samlas in och behandlas ska vara adekvata och relevanta. Det bör övervägas om ändamålet kan uppnås genom att andra medel/annan information används istället för personuppgifterna.
- **Integritet och konfidentialitet** – Personuppgifter som behandlas ska skyddas så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt. Lämpliga tekniska och organisatoriska åtgärder ska därför vidtas för att skydda personuppgifterna, ett adekvat skydd ska finnas.

2.3.1 Känsliga personuppgifter

I dataskyddsförordningen och dataskyddslagen finns det vägledning vad avser känsliga och integritetskänsliga (se avsnitt 2.3.3) personuppgifter;

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd, de kallas för känsliga personuppgifter och utgör uppgifter om:

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- hälsa (personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus),
- en persons sexualliv eller sexuella läggning,
- genetiska uppgifter, exempelvis kromosom-, DNA- och RNA-analys och
- biometriska uppgifter, exempelvis ansiktsbilder eller fingeravtrycksuppgifter.

Det är som huvudregel förbjudet att behandla känsliga personuppgifter, men det finns undantag. Undantagen handlar i grunden om att det ska finnas en rätt att behandla just dessa kategorier av personuppgifter och att det finns ett särskilt skydd för dem. I denna rådgivning kommer undantagen inte att gås igenom utan generellt avråds behandling av känsliga personuppgifter via formulär.

2.3.2 Använd inte patientuppgifter i formulär

Vad avser uppgift om hälsa omfattas patientuppgifter av detta begrepp. För behandling av personuppgifter inom hälso- och sjukvården, inklusive tandvården, finns en speciallagstiftning; patientdatalagen. I denna lag beskrivs för vilka ändamål patientuppgifter får behandlas samt även vissa specifika säkerhetskrav som måste vara uppfyllda vid behandlingen. I denna rådgivning kommer säkerhetskraven inte att gås igenom utan generellt avråds behandling av patientuppgifter via formulär.

Om det mot förmodan skulle finnas ett absolut behov av att behandla känsliga personuppgifter rekommenderar jag att ett ärende läggs till Informationssäkerhetsenheten för stöd i utredning avseende undantag. I en sådan utredning behöver även Kommunikationsenheten ta höjd för om IT-stödet/e-

postmiljön ger den säkerhet som denna typ av uppgifter behöver. Det kan även finnas andra kommunikationslösningar inom regionen som ev. kan användas för att hantera behovet, exempelvis 1177. Huruvida andra kommunikationslösningar kan användas eller inte behöver lyftas till den förvaltning som äger kommunikationslösningen.

2.3.3 Integritetskänsliga personuppgifter

Vissa personuppgifter är mer känsliga än andra, men utgör inte så kallade känsliga personuppgifter där krav som beskrivs ovan är tillämpliga. Personuppgifter som är mer integritetskänsliga kan exempelvis behöva ett mer omfattande skydd än uppgifter som inte är känsliga. Vilka personuppgifter som är integritetskänsliga kan exempelvis framgå av lag, men det kan även vara så att en verksamhet (utifrån sitt perspektiv) bedömer att en uppgift är integritetskänslig.

Några uppgifter som anses vara integritetskänsliga:

- Personnummer och samordningsnummer
- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

Generellt rekommenderas att integritetskänsliga personuppgifter om möjligt inte behandlas i formulär, men om så ändå vill genomföras behöver en analys göras av användandet och särskilt om ett tillräckligt skydd ges.

2.3.4 Särskilt om personnummer och samordningsnummer

Huvudregeln är att den registrerades samtycke måste inhämtas för att få behandla personnummer eller samordningsnummer. Det finns dock undantag till att personnummer och samordningsnummer får behandlas utan en registrerads samtycke, men detta ska användas restriktivt och i första hand ska det ses över om behandlingen kan genomförs utan att personnummer eller samordningsnummer behandlas. Behandling av personnummer/samordningsnummer får ske om det är klart motiverat med hänsyn till:

- Ändamålet med behandlingen,
- Vikten av en säker identifiering eller
- Något annat beaktansvärt skäl.

En intresseavvägning mellan behovet av behandlingen och de integritetsrisker som behandlingen skulle innebära ska göras. Hänsyn bör vid denna bedömning tas till om syftet kan uppnås på något annat sätt där personnummer och/eller samordningsnummer inte behövs, behandlingens omfattning och om behandlingen förutsätter samkörning av register.

2.3.5 Vanligt förekommande personuppgifter i formulär

I de formulär som idag används på webbplatserna har det identifierats ett antal vanligt förekommande personuppgifter. Nedan ges generell rådgivning avseende dess lämplighet att användas i formulär. I nedan rådgivning har det inte tagits höjd för vilket skydd IT-stödet ger eller det skydd som finns i e-postmiljön (detta måste självklart beaktas), utan råd ges utifrån antagandet att ett tillräckligt skydd är på plats.

Personuppgift/er	**Särskilt krav/information**	**Generellt råd**
För- och efternamn, Telefon E-post	Generellt harmlösa personuppgifter.	Kan generellt användas, men höjd behöver tas till följande: • Behövs uppgifterna för ändamålet? • Finns det en koppling till känsliga eller integritetskänsliga personuppgifter?

Adress Plats Arbetsplats	Generellt harmlös personuppgift. OBS! Kan vara skyddsvärd om person har skyddade personuppgifter. Läs mer här.	Kan generellt användas, men höjd behöver tas till följande: • Behövs uppgiften för ändamålet? • Hur minimeras risken för angivande om skyddade personuppgifter och hur kan det hanteras?
HSA-id	Generellt harmlösa personuppgifter. Utgör en pseudonymiserad personuppgift.	Kan generellt användas, men höjd behöver tas till följande: • Behövs uppgiften för ändamålet?

Personnummer/ samordningsnummer	Integritetskänslig personuppgift.	Kan inte användas generellt. Innan användning behöver ställning tas till följande:
		
		• Behövs uppgiften för ändamålet?
		• Hur skyddas uppgiften?
		• Har RÖ rätt att behandla pnr? Om ja, utifrån vilken grund:
		  ○ Samtycke
		  ○ Motiverat utifrån ändamålet med behandlingen,
		  ○ Motiverat utifrån vikten av en säker identifiering eller
		  ○ Motiverat utifrån något annat beaktansvärt skäl.

Diarienummer	Generellt harmlösa personuppgifter (i vissa fall är det kanske inte en personuppgift).	Kan generellt användas, men höjd behöver tas till följande: Behövs uppgiften för ändamålet?
Meddelandefält	Fritextfält utgör alltid en risk för att person skriver in personuppgifter som regionen inte vill eller har rätt att samla in.	Ställ er alltid frågan om det behöver finnas ett fritextfält? Om ja, lägg till en text som ger råd om att inte ange personuppgifter.

2.4 Information om skyldigheter inom dataskydd

2.4.1 Personuppgift

Nedan ges information som är tänkt att ge kunskap i vad som utgör en personuppgift eller inte.

Personuppgift
Personuppgifter utgör varje upplysning som avser en identifierad eller identifierbar fysisk person (även benämnd som registrerad i dataskyddsförordningen), som direkt eller indirekt identifierar personen.

Personuppgifter är således all slags information som kan knytas till en levande person. Det kan röra sig om namn, identifikationsnummer, adress, personnummer och IP-adress eller faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Även bilder på personer klassas som personuppgifter, till och med ljudinspelningar som lagras digitalt kan vara personuppgifter även om det inte nämns några namn i inspelningen.

Pseudonymiserad uppgift
Personuppgifter kan vara pseudonymiserade. Pseudonymisering är en säkerhetsåtgärd som kan vidtas för att minska riskerna för de registrerade samt att hjälpa personuppgiftsansvarig och personuppgiftsbiträde att fullgöra sina skyldigheter avseende dataskydd. Pseudonymisering innebär att personuppgifter inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. En förutsättning är att de kompletterande uppgifterna förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Om uppgifter är pseudonymiserade är de fortfarande personuppgifter.

Anonym uppgift
En anonym uppgift är en uppgift som inte har en koppling till en identifierad eller identifierbar fysisk person, eller personuppgifter som har anonymiserats på ett sätt som medför att den registrerade inte är identifierad eller identifierbar. Om uppgiften är anonym är dataskyddsbestämmelser (exempelvis dataskyddsförordningen) inte tillämplig på den behandlingen.

2.4.2 Informationsplikt

Utifrån dataskyddsförordningen ställs det krav på att information ska ges till registrerade när deras personuppgifter behandlas av Region Östergötland. Nedan följer en beskrivning av de krav som finns med koppling till informationsplikten.

Tidsaspekter och formkrav
Beroende på hur personuppgifterna samlas in finns det olika tidsaspekter för när Region Östergötland ska lämna informationen;

- Om personuppgifterna **samlas in från den registrerade** ska information lämnas när personuppgifterna erhålls (det vill säga direkt).
- Om personuppgifterna **samlas in från annan än den registrerade** ska information lämnas enligt följande:
    - inom en rimlig period efter att personuppgifterna har erhållits, dock senast inom en månad. Hänsyn ska tas till särskilda omständigheter som personuppgifterna behandlas,
    - senast vid tidpunkten för första kommunikationen med den registrerade om det är så att personuppgifterna ska användas för kommunikation med den registrerade eller
    - senast när personuppgifterna lämnas ut för första gången om ett utlämnande till en annan mottagare förutses.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk.

Innehåll
Beroende på hur personuppgifterna samlas in ska olika typer av information ges. Nedan tabell ger information om vilken information som ska ges när personuppgifter samlas in från den registrerade respektive från annan än den registrerade.

Information som ska ges	**Insamling från registrerad**	**Insamling från annan än registrerad**
Identitet och kontaktuppgifter för personuppgiftsansvarig (inkl. ev. företrädare)	x	x
Kontaktuppgifter till dataskyddsombud	x	x
Ändamål med behandling	x	x
Rättslig grund för behandling	x	x
Berättigade intressen vid en ev. intresseavvägning som rättslig grund	x	x
Kategorier av personuppgifter		x

Mottagare/kategorier av mottagare av personuppgifter	x	x
Om överföring av uppgifter till tredje land sker, samt: • Om beslut från kommissionen finns för adekvat skyddsnivå eller lämpliga/passande skyddsåtgärder som vidtagits och • Hur en kopia av skyddsåtgärderna kan erhållas eller gjorts tillgängliga	x	x
Lagringstid eller kriterier för fastställande av lagringstid	x	x
De registrerades rättigheter, särskilt rätten till: • Registerutdrag • Rättelse • Radering • Begränsning • Invändning • Dataportabilitet • Att inge klagomål till tillsynsmyndigheten	x	x
Rätten att återkalla ett samtycke (enbart om samtycke används som rättslig grund eller för behandling av känsliga personuppgifter)	x	x
Om insamlandet av uppgifter sker utifrån uppgiftsskyldighet enligt lag eller avtal avseende tillhandahållande av personuppgifter eller om det är nödvändigt för att kunna ingå ett avtal samt eventuella följder om registrerad inte lämnar uppgifter	x	
Källa varifrån personuppgifter har hämtats och om de kommer från allmänt tillgängliga källor		x
Om automatiserat beslutsfattande (inklusive profilering) sker och logiken bakom samt betydelsen och förutsedda följder av behandlingen	x	x