Datainspektionen informerar

Nr 5/2018

Allmänna råd

Datainspektionen ger ut allmänna råd i syfte:

1) att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt EU:s dataskyddsförordning samt

2) att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

De allmänna råden är inte bindande, utan innehåller rekommendationer om hur de bindande kraven i dataskyddsförordningen kan uppnås. Detta dokument är en **allmän vägledning om myndigheternas behandling av personuppgifter.**

Datainspektionen

Den 4 maj 2018

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

1. Allmänt

Inom landskapsförvaltningen och den kommunala förvaltningen förekommer många olika typer av administrativa system, både beträffande den egna personalen och beträffande allmänheten.

Från och med den 25 maj 2018 ställer dataskyddsförordningen[1] stora krav på behandlingen av personuppgifter i de administrativa systemen. När personuppgifter behandlas är det av grundläggande betydelse att personuppgifterna ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och att inte fler person-uppgifter behandlas än nödvändigt. En viktig aspekt är också att lämpliga säkerhets-åtgärder vidtas.

Sammanfattningsvis bör den personuppgiftsansvariga myndigheten tänka på följande:

- Personregister måste ha en hög kvalitet.
- Det är nödvändigt att skaffa den utrustning som behövs och att använda den rätt.
- Ändamålet med varje behandling av personuppgifter behöver vara klart definierat, så att det är lätt att urskilja om behandlingen överensstämmer med ändamålet.
- Användningen av personregister måste vara i samklang med personregistrets ändamål.
- Den registrerade personen har rätt att få information.
- Förekomsten av personregister hos myndigheten behöver kartläggas.
- Ett register över all förekommande behandling av personuppgifter ska föras.
- Personuppgifterna måste skyddas.
- Regler och rutiner beträffande behandling av personuppgifter bör upprättas.
- Information och utbildning behöver bedrivas kontinuerligt.
- Uppföljning behöver ske över att regler och rutiner följs och respekteras.
- Den personuppgiftsansvariga myndigheten har ansvar för att instruera, utbilda och övervaka.
- En fungerande organisation för säkerhet behöver skapas.
- Eventuella hotbilder bör kartläggas.
- Säkerheten måste testas regelbundet.

2. Personuppgiftsansvar

Innebörden av personuppgiftsansvaret

En myndighet som behandlar personuppgifter har personuppgiftsansvar, d.v.s. ett stort antal skyldigheter som hör ihop med behandlingen av personuppgifterna. Det åligger den personuppgiftsansvarige att säkerställa att personuppgifter ska behandlas på ett korrekt och lagligt sätt. Bestämmelserna om den registrerades rätt till information, tillgång, rättning, utplåning eller blockering samt rätt att göra invändningar mot behandlingen av

[1] Härmed avses Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

personuppgifter har utformats på ett sätt som skapar skyldigheter för den personuppgiftsansvarige. Den personuppgiftsansvarige är ansvarig för eventuella skador till följd av otillåten behandling. Se även Datainspektionens allmänna råd angående personuppgiftsansvar.

Gemensamt personuppgiftsansvar
Bestämmelser beträffande gemensamt personuppgiftsansvar finns i artikel 26 i dataskyddsförordningen. Myndigheter eller andra organ som agerar tillsammans har en viss flexibilitet när det gäller att fördela skyldigheter och ansvar sinsemellan, så länge de garanterar en fullständig efterlevnad av dataskyddsförordningens bestämmelser. Det är dock viktigt att se till att efterlevnaden av dataskyddsbestämmelserna och ansvaret för eventuella brott mot dataskyddsbestämmelserna är tydligt fördelade. I synnerhet gäller detta i komplexa behandlingsmiljöer där olika personuppgiftsansvariga har del i behandlingen av personuppgifter. Det är av stor betydelse att de registrerade personerna får tydlig information som förklarar de olika steg och aktörer som ingår i behandlingen. Dessutom bör det tydligt framgå om varje personuppgiftsansvarig har befogenhet att tillgodose alla rättigheter för registrerade, eller vilken personuppgifts-ansvarig som är behörig för vilken rättighet.

3. Personuppgiftsbiträde

Av effektivitetsskäl kan det vara lämpligt att en myndighet väljer att lägga över viss hantering av personuppgifter på ett annat organ, som då fungerar som personuppgifts-biträde. Ett personuppgiftsbiträde har en viktig funktion vid tillämpningen av bestäm-melserna gällande sekretess och säkerhet vid behandlingen. Personuppgiftsbiträdet agerar för den personuppgiftsansvariges räkning och ska följa instruktionerna från personuppgiftsansvarig. Se även Datainspektionens allmänna råd angående personuppgiftsbiträdens behandling av personuppgifter för personuppgiftsansvariga myndigheters räkning.

4. Vad är en personuppgift?

Personuppgifter är ”varje upplysning som avser en identifierad eller identifierbar fysisk person. ”En identifierbar fysisk person” är därvid en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikations-nummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet” (artikel 4.1 i EU:s dataskyddsförordning).

Varje upplysning
Formuleringen ”varje upplysning” i dataskyddsförordningen gör att begreppet ”person-uppgifter” omfattar väldigt många olika saker. I stort sett allt kan tolkas in under ”varje upplysning”.

Som avser en
En upplysning kan anses avse en person när upplysningen handlar om den personen. Sådana upplysningar uppkommer exempelvis när uppgifter, som avser personens situation som anställd, registreras i hans eller hennes akt på ett personalkontor. Upplysningar som avser en person uppkommer även när en person filmas av en övervakningskamera eller när resultatet av en patients medicinska test förs in i hans eller hennes patientjournal.

I vissa fall gäller informationen föremål och inte enskilda personer. Dessa föremål tillhör vanligtvis någon, eller har ett särskilt inflytande eller påverkas av personer, eller har en sorts fysisk eller geografisk närhet till personer eller andra föremål. Uppgifter om värdet på ett hus är information om ett föremål. Under vissa omständigheter kan information om föremål också betraktas som personuppgifter. Huset som sådant utgör ju en ägares tillgångar, och följaktligen kommer informationen om värdet att användas för att t.ex. avgöra ägarens skyldighet att betala skatt. Följden blir att sådan information kan betraktas som personuppgifter. (Däremot är det klart att bestämmelserna om personuppgifter inte är tillämpliga om information om värdet på olika hus endast kommer att användas som illustration för fastighetspriserna i ett visst område.)

Identifierad eller identifierbar fysisk person
Med fysiska personer menas människor.

Personer kan identifieras exempelvis genom telefonnummer, registreringsnummer, personbeteckning och passnummer. Vidare kan en person identifieras indirekt genom s.k. unika kombinationer vilket avser en eller flera faktorer som är specifika för personens fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet (ålder, yrkesverksamhet, bostadsort etc.). En kombination av väsentliga kriterier gör att en person känns igen genom att den grupp som han eller hon tillhör ringas in. Vissa utmärkande egenskaper är så unika att en person lätt kan identifieras (”den nuvarande stadsdirektören”), men en kombination av upplysningar på kategorinivå (ålderskategori, regionalt ursprung m.m.) kan också vara tämligen avgörande under vissa omständigheter, särskilt om det finns tillgång till någon form av ytterligare information.

Det bör noteras att även om identifiering genom namnet i praktiken är vanligast så är ett namn i sig inte alltid nödvändigt för att identifiera en individ. T.ex. i datafiler för registrering av personuppgifter ges de registrerade vanligen en unik identifierare för att undvika sammanblandning mellan två personer i filen. Även på nätet ger verktygen för övervakning av internettrafiken möjlighet att på ett enkelt sätt identifiera en dators beteende och bakom den datoranvändaren. På detta vis pusslar man ihop individens

personlighet för att tillskriva individen vissa beslut. Utan att ens ta reda på en individs namn och adress är det möjligt att kategorisera personen på grundval av socio-ekonomiska, psykologiska, filosofiska och andra kriterier och att tillskriva honom eller henne vissa beslut. Individens kontaktpunkt (en dator) kräver nödvändigtvis inte längre att individens identitet i snäv bemärkelse avslöjas. Således kan en individ identifieras utan att hans eller hennes namn är känt.

I själva verket är den personuppgiftsansvariges syfte med databehandlingen en relevant faktor för att bedöma vilka hjälpmedel som kan komma att användas för att identifiera personer. I de fall där syftet med databehandlingen innebär identifiering av individer kan man förutsätta att den personuppgiftsansvarige eller någon annan delaktig person har eller kommer att ha hjälpmedel som rimligen kan komma att användas för att identifiera den registrerade. Därför bör informationen anses avse identifierbara individer och behandlingen omfattas av uppgiftsskyddsbestämmelserna. IP-adresser har ansetts vara uppgifter som avser en identifierbar person[2].

5. Behandling av personuppgifter

Vid alla myndigheter förekommer flera olika sorters behandling av personuppgifter i flera olika register.

Behandling av personuppgifter avser, enligt artikel 4.2 i dataskyddsförordningen, varje åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Exempel på sådan behandling är insamling, registrering, organisering, lagring, bearbetning eller sammanställning.

Enligt artikel 4.6 i dataskyddsförordningen är definitionen av ett register en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

En systeminventering bör göras, så att myndigheten vet var det finns personuppgifter och kan fastställa ändamålen med dem. Exempel på personregister kan vara kund- och personalregister, beskrivningar av fastighetsskötsel såsom dörrlås och fysisk säkerhet, schema, betyg m.m. Även insamling av information via internet såsom kundförfrågningar, arbetsplatsansökningar, anmälningsblanketter och insamling av besökarrespons är exempel på behandling av personuppgifter.

[2] Enligt Artikel 29-arbetsgruppen för skydd av personuppgifter kan nätleverantörer och förvaltare av lokala nätverk (LAN) med rimliga medel identifiera de internet-användare som de har tilldelat IP-adresser eftersom de i allmänhet i en fil bokför datum, tidpunkt, varaktighet och den dynamiska IP-adress som internet-användaren har fått. Samma sak gäller för internet-leverantörer som för en loggbok på http-servern.

Följande omständigheter bör beaktas i samband med att personuppgifter behandlas i myndigheternas register:

5.1 Några av de grundläggande skyldigheterna enligt dataskyddsförordningen

Information till de registrerade personerna
Se Datainspektionens allmänna råd angående hur myndigheterna ska informera personer vars personuppgifter registreras.

Utförande av åtgärder på begäran av de registrerade personerna
Personer, vars personuppgifter har registrerats, har enligt dataskyddsförordningen rätt att få olika åtgärder utförda beträffande dessa personuppgifter. Bland annat har de rätt till:

- rättelse av personuppgifter (artikel 16),
- radering av personuppgifter under vissa förutsättningar (artikel 17).

Bedömning av hur länge personuppgifterna får bevaras
Det föreskrivs i artikel 5.1 i dataskyddsförordningen att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifterna ska således inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Därför är det nödvändigt att analysera och ta ställning till behovet av bevarande och gallring.

Regler om arkivering, förvaring och gallring finns i arkivlagen (2004:13) för landskapet Åland. Enligt 6 § ska varje arkivbildare ha en arkivplan där handlingarnas förvarings-tider, förvaringssätt och utgallring framgår.

Samarbete med tillsynsmyndigheten
Enligt artikel 31 i dataskyddsförordningen ska personuppgiftsansvariga och personuppgiftsbiträden samarbeta med tillsynsmyndigheten vid utförandet av tillsynsmyndighetens uppgifter.

5.2 Rutiner för god säkerhet

IT-säkerhetsåtgärder
Den personuppgiftsansvariga myndigheten ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

A) De tekniska möjligheter som finns,
B) Vad det skulle kosta att genomföra åtgärderna,

C) De särskilda risker som finns med behandlingen av personuppgifterna, och hur pass känsliga de behandlade personuppgifterna är.

När den personuppgiftsansvariga myndigheten anlitar ett personuppgiftsbiträde, ska den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Säkerhet i datatrafiken

Myndigheterna behöver kontrollera att deras IT-system inte kan användas utan befogenhet via dataöverföringsutrustning eller nätförbindelser.

Säkerheten gällande utrustning och programvara

Det behöver finnas rutiner som begränsar obehöriga personers tillgång till utrymmen där det finns IT-utrustning eller där personuppgifter behandlas på andra sätt. Person-uppgifter ska inte kunna tillföras, överföras, ändras eller avlägsnas av andra än sådan personal som har anförtrotts uppgiften att göra det.

För att hindra obehöriga från att få tillgång till personuppgifter bör användarrättigheter, d.v.s. inloggningsrättigheter och behörigheter. vara så begränsade som möjligt. Behovet av att kunna utföra en viss arbetsuppgift ska styra behörigheten.

Det är önskvärt att det i efterskott ska kunna gå att granska och verifiera vilka uppgifter som lagts till eller avlägsnats samt när det skett och av vem. Det bör gå att identifiera användare, exempelvis genom personliga lösenord.

Datamediers säkerhet

CD-ROM-skivor, magnetband, disketter, minnesstickor m.m, som innehåller personuppgifter, behöver förvaras på ett sådant sätt att de inte kan läsas, kopieras, ändras eller bortföras av obehöriga.

Fria textfält

En av principerna för behandling av personuppgifter är, enligt artikel 5.1 i dataskyddsförordningen, uppgiftsminimering, vilket innebär att personuppgifterna ska vara adekvata, relevanta och inte allt för omfattande. En viktig sak att tänka på vid behandling av personuppgifter är således att tillförseln av onödiga omdömen och uppgifter bör begränsas. När det förekommer fria textfält (d.v.s. där det är fritt att skriva vad man vill) behöver det finnas rutiner och riktlinjer till personalen. Det behövs tydliga instruktioner till användarna om vilken information som får skrivas i fritextfältet. Instruktionerna bör exempelvis ange hur värderande omdömen om personal eller elever ska formuleras och att kränkande uttalanden inte är tillåtna.

Hemliga personuppgifter
I vissa fall förekommer skyddade personuppgifter såsom namn och adress. I sådana fall ska åtkomsten begränsas och spridning av uppgifterna begränsas. Rutinerna behöver regelbundet följas upp.

Straffbestämmelser

Den som gör intrång i någon persons integritetsskydd genom att skaffa personuppgifter på ett sätt som inte är förenligt med ändamålet eller att lämna ut personuppgifter på otillåtet sätt kan göra sig skyldig till dataskyddsbrott.

Den som avslöjar vad han eller hon har fått kännedom om, vid behandling av personuppgifter, beträffande enskild persons egenskaper, personliga förhållanden, ekonomiska ställning eller affärs- eller yrkeshemlighet kan göra sig skyldig till brott mot tystnadsplikt.

6. Sökmotorer

Google och andra sökmotorer har inte personuppgiftsansvar för information som erhålles vid en sökning. Det är den webbplats där informationen ursprungligen publicerades som är personuppgiftsansvarig för informationen. Sökmotorn är bara ansvarig för sådan information som sparas trots att den ursprungliga webbplatsen raderats t.ex. vid cachning.

Tillvägagångssättet för att förhindra att viss information erhålls genom sökning med sökmotor är att ta bort informationen från webbplatsen eller att vidta åtgärder för att webbsidan eller delar av den inte ska indexeras (d.v.s. att sökmotorn inte ska katalogisera ord och fraser på webbsidan).

7. Personuppgifter i sociala media

Användningen av Facebook, Twitter, bloggar och andra typer av sociala medier kan innebära att personuppgifter behandlas. Det innebär i så fall att dataskydds-förordningen är tillämplig.

Ansvaret för personuppgifter som publiceras via sociala media är beroende av utformningen av den sociala medietjänst som används. Samtidigt är de sociala medierna under ständig förändring och utveckling.

Vad beträffar Facebook och bloggar så är myndigheten ansvarig för personuppgifter som publiceras på myndighetens Facebook-sida och/eller blogg. Ansvaret omfattar både personuppgifter som myndigheten själv publicerar och personuppgifter som publiceras av andra i till exempel en kommentar på sidan. Även den besökare som skrivit en kommentar kan ha ett ansvar för vad den själv skrivit. Vad beträffar Twitter så ansvarar myndigheten endast för personuppgifter som myndigheten själv publicerar, inte personuppgifter som andra twittrande lämnat. Orsaken till det begränsade ansvaret är att myndigheten inte kan påverka andras Twitter-inlägg.

Myndigheten har ett ansvar för att personuppgifter på dess Facebook-sida, blogg, Twitterkonto och liknande inte behandlas på ett sådant sätt att de kränker enskildas personliga integritet. Det innebär att myndigheten även ska hålla uppsikt över besökares kommentarer för att upptäcka kränkande personuppgifter. Kränkande personuppgifter ska avlägsnas. Myndigheten kan bli skadeståndsskyldig för kränkande personuppgifter.

För att minska risken för kränkningar av enskildas personliga integritet och för att minska risken för skadeståndsansvar bör myndigheten vidta åtgärder i förebyggande syfte. Dessa åtgärder kan bland annat vara att informera om syftet med Facebook-sidan, bloggen eller liknande samt för vilket ändamål kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och vad som kan hända om enskilda inte följer anvisningarna. Vidare kan besökare ombes att rapportera kränkande innehåll. Myndigheten bör ha rutiner för att hantera klagomål. Det är viktigt att utforma sidan så att det tydligt framgår att det är en myndighet som står bakom den.

8. Datainspektionens roll

Datainspektionen är en myndighet som arbetar för att medborgarnas personliga integritet inte kränks när personuppgifter behandlas. Myndigheten finns till för medborgarna.

Vi arbetar också proaktivt genom att informera myndigheterna om deras skyldighet att hantera personuppgifter på ett korrekt sätt. Bland annat ska myndigheterna informera om hur de behandlar personuppgifter. I vårt arbete ingår också att ge allmänna råd. Vi utbildar och informerar myndigheterna om användningen av personuppgifter.