Pontus Lilja, 0322-60 06 24
pontus.lilja@vargarda.se

Godkänd/ansvarig

Utgåva

Riktlinjer för personuppgiftshantering

Innehåll

Inledning

Vårgårda kommuns riktlinjer för personuppgiftshantering är ett övergripande dokument som redovisar kommunens arbetssätt och inriktning med personuppgiftshantering. Detta dokument konkretiserar och förklarar hur Vårgårda kommun ska arbeta med personuppgifter utifrån gällande Dataskyddsförordning och kompletterande nationell lagstiftning.

Riktlinjernas omfattning

Dessa riktlinjer innehåller information och vägledning gällande hantering av personuppgifter i Vårgårda kommun.

Riktlinjerna gäller för alla verksamheter i Vårgårda kommun, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa.

Riktlinjerna gäller inte för kommunens bolag, utan dessa beslutar om hur de ska arbeta med personuppgiftshantering inom egen verksamhet.

Dessa riktlinjer utgår från och ska följa Dataskyddsförordningen. Riktlinjerna anger hur verksamheten ska förhålla sig till Dataskyddsförordningen och hur den ska tillämpas för att säkerställa följdriktigheten av dess innehåll.

Struktur och läsanvisningar

För att ge god läsbarhet är dokumentet uppdelat i block som förklarar hur kommunen ska förhålla sig till och arbeta utifrån gällande lagstiftning. Varje central del av Datasskyddsförordningen är ett eget block som redogör för hur Vårgårda kommun ska arbeta inom just det området.

Block		Innehåll	Sidor
A	Personuppgifter, behandling, principer för behandling och register	Vad är en behandling? Vad är en personuppgift? Vad är register? Vilka principer ska gälla för behandling?	8-19
B	Ansvar och fördelning av ansvar	Vem ansvarar för personuppgifter i Vårgårda kommun?	20-22
C	Ändamål och rättslig grund för behandling samt undantag och kompletterande ändamål.	Centrala delar om varför vi hanterar personuppgifter och de krav som ställs.	23-30
D	Informationskrav	Vad ska vi förmedla och vad ska de registrerade känna till inför, under och efter personuppgiftsbehandling?	31-35
E	Personuppgiftsincident, hantering och rapportering	Hur agerar vi om något sker med våra uppgifter p g a misstag eller medvetenhet.	36-42
F	Biträden, underleverantör, tredje part, utanför EU/EES	Vilka utanför organisationen hanterar/tar del av våra personuppgifter och vad krävs.	43-49
G	Risk- och sårbarhetsanalys, konsekvensanalys - Privacy impact Assessment (PIA) och förhandssamråd	Om att skapa en teknisk och organisatorisk säkerhet. Hantera risker, se konsekvenser, begära samråd med tillsynsmyndighet.	50-56
H	Tillsyn, Dataskyddsombud, tillsynsmyndighet	Om kontrollfunktionerna för att vi följer Dataskyddsförordningen	57-63
I	Registrerades rättigheter	Vilka grundläggande rättigheter har de registrerade när vi behandlar deras personuppgifter.	64-69

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska. En förutsättning för att tillämpa riktlinjer för personuppgiftshantering är att ha en grundläggande kunskap om begrepp och förståelse för vad de innebär. Riktlinjerna är utformade som ett stöd för att erhålla kunskap och förståelse. Samtliga riktlinjer är numrerade och i tabellform med blått huvud.

Dataskyddsförordningen omfattar all hantering av personuppgifter. Dessa riktlinjer anger hur Vårgårda kommun ska arbeta för att följa förordningen och vad som bör tas hänsyn till i befintlig hantering såväl som ny hantering av personuppgifter.

De främsta skälen för Dataskyddsförordningen är framför allt hänsyn till medborgarens friheter och rättigheter. Det är två värden som alltid ska beaktas utifrån riktlinjerna. Det innebär att det ska finnas en riskmedvetenhet när all behandling sker. Finns det risker eller sårbarhet för att en behandling innebär skada för en persons friheter eller rättigheter enligt Europakonventionen ska det tas särskild hänsyn till och särskild vård enligt förordningen och dessa riktlinjer.

Bedömning om behandling

Om det finns osäkerhet gällande hantering av personuppgifter, behov av stöd, behov av att genomföra åtgärder andra än det som rutiner och dokumentation anger ska frågan ställas till ansvarig chef som ska rådgöra med kommunens Dataskyddsombud.

Introduktion till Dataskyddsförordningen och personuppgiftshantering

Namnet på förordningen är Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG. Ofta talar man om den som Dataskyddsförordningen eller GDPR(som är en förkortning av General Data Protection Regulation).

Dataskyddsförordningens syfte

Förordningen fastställer bestämmelser om skydd för fysiska personer när det gäller behandlingen av personuppgifter och det fria flödet av personuppgifter. Förordningen skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

Vanliga begrepp och definitioner

Begrepp	Definition
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, där en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Direkta personuppgifter	Direkta personuppgifter är framför allt namn och personnummer, alltså sådan information som direkt pekar ut en individ utan att man behöver tillföra ytterligare information. Det är lätt att förstå att de är personuppgifter.
Indirekta personuppgifter	De indirekta personuppgifterna är lite mer komplicerade. Det rör sig om uppgifter som pekar ut en individ om man kompletterar dem med annan information. Ett kundnummer i sig ger exempelvis ingen information om vem en individ är, men det går lätt att ta reda på vem kunden är genom att titta i kundregistret. Således är kundnumret en personuppgift även utanför kundregistret.
Behandling	En åtgärd eller kombination av åtgärder för personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte.
Profilering	Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Pseudonymisering	Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person
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.
Personuppgiftsansvarig:	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandling av personuppgifter.
Personuppgiftsbiträde	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Mottagare	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare.
Tredje part	En fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.
Företrädare	En i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning.
Bindande företagsbestämmelser	Strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp företag som deltar i gemensam ekonomisk verksamhet.
Tillsynsmyndighet	En oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51, i Sverige Integritetsskyddsmyndigheten
Gränsöverskridande behandling	a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda

	verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat.

Block A: Behandling, personuppgifter, principer för behandling, register, medvetenhet, utbildning och kunskap

A.1 Behandling

För att förstå och inse vad som menas med behandling behöver begreppet vidgas och förtydligas för att skapa förståelse för den omfattande och diversifierade behandling en kommun ansvarar för. Behandling där personuppgifter ingår innebär att Dataskyddsförordningen gäller. Därför behöver det redogöras för olika behandlingar eftersom dessa endast får göras med angivet och informerat ändamål och en gällande rättslig grund (Se block C).

Vad är en behandling?

En åtgärd eller kombination av åtgärder för personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat, delvis automatiserat eller om de hanteras manuellt genom flera variabler av uppgifter.

- Insamling
- Registrering
- Organisering
- Strukturering
- Lagring
- Bearbetning eller ändring
- Framtagning
- Läsning
- Användning
- Utlämning genom överföring
- Spridning eller tillhandahållande på annat sätt
- Justering eller sammanförande
- Begränsning
- Radering eller förstöring.

Ny behandling
När du för ett ändamål samlar in personuppgifter följer en del skyldigheter. Informationsskyldighet innebär att vid varje ny behandling, registrering av personuppgifter ska grundläggande information ges.

Befintlig behandling
Enligt Förordningen är vi skyldiga att veta vilka behandlingar vi utför och varför. Det ska ingå i en registerförteckning. Samtliga behandlingar som innehåller personuppgifter ska föras till ett sådant register.

Avslutad behandling
Det är viktigt att känna till hur länge personuppgifter ska bevaras eller om de ska gallras, arkiveras eller användas för annat berättigat ändamål. Läs om det i Block I.

Riktlinjer för behandling	
A.1.1	Vid ny behandling ska följande information ges: • Vilka personuppgifter som ska behandlas

	• Ändamål med behandlingen (Block C) • Varifrån och/eller hur uppgifterna samlas in • Rättslig grund (Block C) • Hur länge uppgifterna kommer att sparas • Vilka vi delar information med (Block F) • Om vi för över uppgifter till tredje land • Vem som är personuppgiftsansvarig och kontaktinformation (Block B) • Kontaktuppgifter för registerutdrag, radering, rättelse, överföring, begränsning m. m. • Kontaktuppgifter till dataskyddsombud
A.1.2	Befintliga behandlingar av personuppgifter ska vara inventerade och registrerade i kommunens registerförteckning för personuppgiftsbehandlingar
A.1.3	Personuppgifter ska raderas (gallras) när ändamålet/anledningen till behandlingen upphör såvida de inte ska bevaras av andra skäl som anges i gällande nationell eller Europeisk lagstiftning (Block I)

A.2 Personuppgifter

Förordningen ska gälla för behandling av personuppgifter som helt eller delvis görs på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Vad är en personuppgift?

Personuppgifter är all information som direkt eller indirekt kan knytas till en person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter.
Ett organisationsnummer är en personuppgift om det handlar om en enskild firma. Registreringsnumret på en bil är en personuppgift om det går att knyta till en person, medan registreringsnumret på en firmabil som används av flera anställda, inte är en personuppgift.
I vissa fall räknas även olika slags elektroniska identiteter, som exempelvis IP-nummer, som personuppgifter om de kan kopplas till en viss person.

Känsliga personuppgifter

I dataskyddsförordningen skiljer man mellan vanliga personuppgifter och känsliga personuppgifter. Med känsliga personuppgifter menas:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar en person.

Känsliga uppgifter är förbjudet att registrera såvida de inte omfattas av undantag för sådan registrering.

Undantag för känsliga personuppgifter
Förbudet ska inte tillämpas om något av följande gäller:

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet inte kan upphävas av den registrerade.

b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet.

i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder

för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Känsliga personuppgifter som anges ovan får behandlas för de ändamål som avses i punkt h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.

Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Skyddsvärda personuppgifter.

Det finns även en ytterligare bedömning och det är särskilt skyddsvärda personuppgifter. För behandling av skyddsvärda personuppgifter behöver de ha utökat tekniskt skydd och motivering för att registrera. Det kan vara omdömen, värderande information så som kamratrelationer, inlärningsförmåga, social utveckling, provresultat m.m. Sekretessbelagd information, personnummer, viss ekonomisk information eller annat som ligger nära privatlivet.

Direkta personuppgifter

Direkta personuppgifter är framför allt namn och personnummer, alltså sådan information som direkt pekar ut en individ utan att man behöver tillföra ytterligare information. Det är lätt att förstå att de är personuppgifter.

Indirekta personuppgifter

De indirekta personuppgifterna är lite mer komplicerade. Det rör sig om uppgifter som pekar ut en individ om man kompletterar dem med annan information. Ett kundnummer i sig ger exempelvis ingen information om vem en individ är, men det går lätt att ta reda på vem kunden är genom att titta i kundregistret. Således är kundnumret en personuppgift även utanför kundregistret.

Riktlinjer för personuppgifter	
A.2.1	Varje verksamhet ska känna till vilka personuppgifter de hanterar var
A.2.2	Det ska vara identifierat vilken typ av personuppgifter det är. Är det ”vanliga” personuppgifter, känsliga personuppgifter eller skyddsvärda personuppgifter
A.2.3	Känsliga uppgifter ska identifieras och motiveras enligt undantagen för behandling av känsliga personuppgifter
A.2.4	Särskilt skyddsvärda uppgifter ska identifieras och de ska motiveras för behandling

A.2.5	Vid behandling av känsliga personuppgifter ska lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställas. PIA, läs mer Block G

A.3 Principer för behandling i Dataskyddsförordningen

Vid behandling av personuppgifter ska följande gälla:

Laglighet, korrekthet och öppenhet

Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Personuppgifter ska alltid hanteras på ett sådant sätt att de registrerade förstår hur deras uppgifter behandlas och varför. Att en behandling ska vara laglig och korrekt betyder att den inte får strida mot andra bestämmelser i förordningen, och då framförallt gällande rättslig grund. Att behandlingen ska vara öppen betyder att det ställs krav på att man tillhandahåller information om all personuppgiftsbehandling samt att all kommunikation ska vara lättillgänglig och begriplig.

Ändamålsbegränsning

Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska anses inte vara oförenligt med de ursprungliga ändamålen.

Man får bara behandla personuppgifter för specifika ändamål som är väl förankrade i verksamheten. Man kan inte utan vidare övergå till att behandla personuppgifterna för något annat syfte i ett senare skede.

Uppgiftsminimering

Alla personuppgifter som behandlas ska vara relevanta i förhållande till ändamålet med behandlingen, det vill säga det ska finnas en direkt poäng med att man samlar in dem. Man får inte registrera fler personuppgifter än vad som är nödvändigt. Att samla in och spara uppgifter "för att de kan vara bra att ha" eller "ifall vi behöver dem senare" är inte förenligt med lagstiftningen. Personuppgifterna ska vara relevanta i sammanhanget och inte onödigt många.

Korrekthet

Uppgifterna ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. Värt att notera är att korrekthet också nämns i första punkten *Laglighet, korrekthet och öppenhet* men då handlar det främst om att behandlingen ska vara korrekt, medan man med denna punkt syftar på att personuppgifterna i sig ska vara korrekta.

Lagringsminimering

Uppgifterna får inte förvaras i en form som gör det möjligt att identifiera den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska

forskningsändamål eller statistiska ändamål under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enlig förordningen genomförs för att säkerställa den registrerades rättigheter och friheter. Personuppgifter ska typiskt sett tas bort när de inte längre behövs med hänsyn till det ändamål som de samlades in för. Det finns undantag från denna princip för bland annat arkivändamål och statistiska ändamål, och man kan också tänka sig att uppgifter sparas i en form där de helt har avidentifierats och alltså inte längre är personuppgifter i lagens mening, men grundregeln är att ingenting får sparas i onödan.

Integritet och konfidentialitet

Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inräknat skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Ansvarsskyldighet

Den personuppgiftsansvarige ska ansvara för och kunna visa att laglighet, korrekthet och öppenhet efterlevs. Alla organisationer som behandlar personuppgifter ska kunna visa att de följer dataskyddslagstiftningen och hur de förhåller sig till alla de ovan nämnda principerna. Detta kräver bl.a. internkontroll, dokumentation, analyser, avtal, strategidokument och styrande dokument.

Riktlinjer för Dataskyddsförordningens principer	
A.3.1	Chef ska säkerställa att Dataskyddsförordningens principer följs inom sitt ansvarsområde
A.3.2	Personuppgiftsbehandlingar som sker utan stöd, utanför verksamhetens kontroll och därmed inte följer Dataskyddsförordningen är inte tillåtet
A.3.3	Finns det osäkerhet med vad det innebär att följa Dataskyddsförordningen ska man söka stöd av verksamhet, IT eller Dataskyddsombud
A.3.4	Varje medarbetare och chef ska ha klart för sig varför (vilket ändamål) personuppgifter behandlas i arbetet. (Se Block B)

A.4 Register

Ett register och därmed föremål för behandling av personuppgifter måste följa Dataskyddsförordningen bestämmelser. Vårgårda kommun använder begreppet register även över den sammanställning av behandlingar som enligt förordningen måste finnas.

Vad är ett register?

Dataskyddsförordningen gäller för helt eller delvis automatiserad behandling av personuppgifter. Det är varje enskild uppgift som behandlas eller har behandlats genom någon form av teknisk lösning, t ex system, applikationer, program, databaser, webbsida, mobil, dator, kamera, med mera.

Det gäller också för manuell behandling av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett manuellt register som är sökbart enligt särskilda kriterier. Enskilda uppgifter som inte vid något tillfälle har varit innehåll i en teknisk lösning anses inte vara ett register. Men om det finns två faktorer (uppgifter) om en individ ska det anses vara ett register även i enbart manuell behandling.

Ex. 1. För en E-tjänst där det förekommer personuppgifter gäller Dataskyddsförordningen.

Ex. 2: En excelfil som man skrivit ut är ett register, en personuppgiftsbehandling där Dataskyddsförordningen gäller.

Ex 3: Nedskriven information i ett kollegieblock är inte ett register om det endast förekommer en uppgift om person (namn). Men om man skriver namn och personnummer är det två faktorer och blir därmed ett register och då gäller Dataskyddsförordningen.

Register över behandlingar

Både personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register eller en förteckning över behandlingar av personuppgifter. Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Dataskyddsombudet och tillsynsmyndigheten.

Vad som ska finnas med i förteckningen

- Namn och kontaktuppgifter för den personuppgiftsansvarige
- I tillämpliga fall gemensamt personuppgiftsansvariga
- Dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen.
- Dokumentation av lämpliga skyddsåtgärder.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare göra registret tillgängligt för tillsynsmyndighet.

Riktlinjer för register	
A.4.1	Varje verksamhet ska ha en registeransvarig för det centrala registret.
A.4.2	Varje medarbetare ska känna till sina egna behandlingar och därmed register.
A.4.2	Varje register ska godkännas av chef.
A.4.3	Varje register ska registreras i en förteckning (centralt register). Detta anmäls till verksamhetens registeransvarige.

A.4.4	Som anställd och chef ska du löpande inventera om det finns objekt som inte finns med i centrala registret. Nya objekt ska anmälas till registeransvarige för verksamheten
A.4.5	Registeransvarige ska stötta och hjälpa verksamheten med att registrera befintliga och nya behandlingar (register)
A.4.6	Registeransvarige ska bistå Dataskyddsombudet och tillsynsmyndigheten i deras arbete och tillsyn
A.4.7	Begäran om att föra in en behandling (register) till det centrala registret ska prioriteras i det löpande arbetet
A.4.8	Att vara registeransvarig innebär: • Ansvar för att hantera och uppdatera register/förteckning med de informationsobjekt som behandlar personuppgifter. Till exempel, hålla register uppdaterade så att informationen är riktig och tillgänglig • Kommunicera åtgärdsförslag för respektive register • Medarbetaren får en licens i Draft IT "Dataskydd" vilket innebär tillgång till en kunskapsbank och juridiskt stöd i systemet

A.5. Registerutdrag

Rätten till tillgång handlar om att de registrerade själva ska ha rätt att få ta del av den information om dem som finns sparad I Vårgårda kommun. En person kan be att få ut ett så kallat registerutdrag, det vill säga en kopia på alla de uppgifter som Vårgårda kommun har samlat på sig om hen. En begäran om registerutdrag kan komma in till kommunen när som helst. Det är därför viktigt att ha en klar process för hur det ska gå till när man tar fram information om en registrerad och lämnar ut den.

Innehållet i ett registerutdrag

Att göra ett registerutdrag handlar om att plocka ut de faktiska uppgifterna, inte bara information om dem, och leverera dem till den registrerade. Det är viktigt att registerutdragen blir korrekta. Att lämna felaktiga uppgifter till en person som begär ut information kan leda till sanktionsavgifter på den högre skalan.

Utdraget ska lämnas inom en månad

All information om en person ska kunna plockas fram och lämnas ut så snabbt det bara går. Man har enligt dataskyddsförordningen högst en månad (30 dagar) på sig att lämna ut ett registerutdrag när en förfrågan kommit in. Det finns dock möjlighet att förlänga den tiden med ytterligare två månader under vissa omständigheter.

Det kan vara svårt att förutse hur många förfrågningar som kommer att komma, och likaså när. Arbetsbelastningen kan plötsligt bli ovanligt hög, om organisationen exempelvis av någon anledning får extra uppmärksamhet riktad mot sig.

Utdraget ska lämnas kostnadsfritt

Ett registerutdrag ska vara kostnadsfritt. Organisationen får alltså inte ta ut en avgift från de registrerade som begär att få ta del av sina egna personuppgifter. Skulle en person återkomma med samma begäran flera gånger på ett sätt som kan uppfattas som oskäligt, kan den personuppgiftsansvarige dock ta ut en administrativ avgift eller vägra att lämna fler utdrag.

Utdraget kan behöva skickas elektroniskt

De registrerade har också rätt att få registerutdraget i digitalt format om begäran skickades in digitalt, exempelvis via en webbportal med en stark autentisering vid inloggningen så att man vet att registerutdraget verkligen når rätt person.

Viktigt att säkerställa mottagarens identitet

Tänk på att det är mycket viktigt att säkerställa mottagarens identitet, särskilt om informationen skickas elektroniskt. En enskild individs personuppgifter ska absolut inte skickas till fel person. Det är också viktigt att den information som skickas ut bara innehåller uppgifter om just den person som efterfrågar registerutdraget, alltså inga personuppgifter om några andra registrerade personer.

Vårdnadshavare eller förvaltare kan begära ut vissa uppgifter

Det finns en möjlighet för vårdnadshavare och förvaltare/god man att begära registerutdrag. Men det kan bero på vilket slags information det rör sig om och vilket uppdrag den gode mannen har. Om man får en sådan förfrågan måste man som personuppgiftsansvarig vara mycket noga med att kontrollera att de påstådda förhållandena är korrekta och att absolut inte lämna ut någon information som kan vara sekretessbelagd till exempel mellan förälder och tonåring.

Blanda inte ihop registerutdrag med offentlighetsprincipen

Blanda inte ihop skyldigheten enligt dataskyddslagstiftningen att lämna registerutdrag, med skyldigheten enligt offentlighetsprincipen att lämna ut allmänna och offentliga handlingar. En handling behöver inte vara vare sig offentlig eller allmän för att den ska ingå i ett registerutdrag.

Innehåll i registerutdraget

Utdraget kan levereras i form av utskrifter, textfiler, skärmdumpar eller annat, beroende på vad som passar i det aktuella fallet.

All information ska vara begriplig på så sätt att koder och liknande förklaras eller skrivs ut i klartext. Däremot behöver man inte göra översättningar till andra språk eller förklara vedertagna facktermer.

Hur mycket måste man leta?

Det kan krävas stora ansträngningar, särskilt av en organisation som behandlar många personuppgifter i många olika sammanhang. Som personuppgiftsansvarig förväntas man använda alla möjligheter som finns till sökning och sammanställning. Den som samlar på sig stora mängder personuppgifter får som regel finna sig i att också behöva göra stora ansträngningar för att kunna tillgodose de registrerades grundläggande rättigheter.

Rätten till tillgång även omfattar sådan information som finns i fritextfält och i löpande text, exempelvis i dokument. En text ska till exempel tas med i registerutdraget om det framgår, till exempel av rubriken, att texten handlar om den person som begärt utdraget. Men om det däremot är omöjligt söka reda på uppgifterna så kan de normalt sett inte användas för att identifiera en person, och då behöver de inte heller ingå i registerutdraget.

Information i följebrev

Dataskyddsförordningen ställer dessutom krav på klar och tydlig information också i samband med registerutdrag. Den personuppgiftsansvariga ska i ett följebrev ange följande:

- varför personuppgifterna behandlas (ändamålen)
- vilka kategorier av personuppgifter man har behandlat
- om man har lämnat ut personuppgifterna och i sådana fall till vilka kategorier av mottagare
- hur länge man avser att behandla uppgifterna
- om uppgifterna förs över till tredjeland eller en internationell organisation, i sådana fall vart och vilka skyddsåtgärder som vidtagits med anledning av det
- att individen kan ha rätt att rätta, begränsa eller invända mot behandlingen av dennes personuppgifter samt rätt att radera sina personuppgifter och inge klagomål till tillsynsmyndigheten
- källan som uppgifterna hämtats ifrån (om man inte har samlat in informationen själv)
- om man använder sig av automatisk beslutfattande som har rättslig konsekvens eller likande

Riktlinjer för registerutdrag	
A.5.1	Använd framtagna rutiner för att tillgodose begäran om registerutdrag
A.5.2	En begäran om registerutdrag ska prioriteras i arbetet
A.5.2	Verksamheten ska registrera sina register i det centrala registret för att underlätta framtagandet av registerutdrag
A.5.3	Säkerställ att det är den registrerade som begär utdrag genom någon form av identifikation
A.5.4	Kontakta din chef eller registeransvarig vid begäran av registerutdrag
A.5.5	Fråga den som begär utdrag om det är en specifik uppgift eller alla uppgifter som personuppgiftsansvarig ansvarar för som eftersöks. Begär alltså specificering om det räcker (för att underlätta för den registrerade och för hanteringen av begäran)

A.6. Medvetenhet, utbildning och kunskap

För att ha möjlighet att följa förordningen är det avgörande att Dataskyddsförordningens bestämmelser, kompletterande lagstiftning, praxis och rättsliga prejudikat är kända i organisationen.

Medvetenhet

För de som arbetar i verksamheter där det förekommer personuppgiftsbehandlingar ska alla vara medvetna om grunderna i Dataskyddsförordningen. Det innebär att känna till vad som rör sig i samtiden. Att ta ett medvetet beslut betyder att man tänkt igenom vad beslutet innebär och vilka konsekvenser det kan ha.

Riktlinjer medvetenhet	
A.6.1	Chef ska regelbundet informera personal om Dataskyddsförordningen utifrån policy, riktlinjer och lagstiftning
A.6.2	Medarbetare ska vara medvetna om vad som gäller för deras område i relation till Dataskyddsförordningen

A.6.3	Vårgårda kommun ska bevaka utvecklingen i området och tillämpa och anpassa styrande dokument, arbetssätt och rutiner om nödvändigt

Utbildning

Utbildning innebär att vi utvecklas och skaffar oss kunskap, bildning och färdighet. Det är viktigt att chefer och nyckelroller får möjlighet till utbildning i Dataskyddsförordningen för att kunna säkra kompetensen inom området i den egna organisationen.

Riktlinjer för utbildning	
A.6.4	Informationssäkerhetsansvarig och Dataskyddsombud ansvarar för att verksamheten får nödvändig utbildning, råd och stöd
A.6.5	En gång varje år ska chefer ges möjlighet till utbildning i personuppgiftshantering
A.6.6	Personuppgiftshantering ska ingå i introduktion av nyanställda

Block B: Ansvar och fördelning av ansvar

Inledning

Detta block beskriver hur ansvarsfördelningen ser ut i stort.

Den primära målgruppen för detta kapitel är chefer samt de som leder arbete där personuppgiftshantering är betydande.

Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med personuppgifter bedrivs i Vårgårda kommun.

B. 1. Personuppgiftsansvar

Ansvaret för personuppgiftshantering är alltid personuppgiftsansvarig. I en kommun är normalt både kommunstyrelsen och de kommunala nämnderna om de är så självständiga att de är förvaltningsmyndigheter – personuppgiftsansvariga, var och en i sin verksamhet. Vilket organ i kommunen som är personuppgiftsansvarig kan variera; de faktiska omständigheterna måste prövas i varje enskilt fall, till exempel om nämnden självständigt förfogar över de personuppgifter som behandlas.

Det finns alltid någon som är personuppgiftsansvarig för en behandling av personuppgifter. Enligt dataskyddsförordningen är den organisation personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Det går inte att delegera personuppgiftsansvaret till en fysisk person. Chef eller andra enskilda tjänstepersoner är aldrig personuppgiftsansvariga.

Den personuppgiftsansvariges ansvar

Personuppgiftsansvaret innebär att man bestämmer över och därmed också ansvarar för all behandling av personuppgifter som sker inom ramen för en viss verksamhet. Den personuppgiftsansvariga organisationen har en direkt skyldighet att vidta åtgärder för att skydda de registrerades personliga integritet, och att kunna visa att man har gjort så.

Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att lagen följs och att de registrerade behandlas korrekt.

Verkställdhet av kommunens tjänster följer verksamhetsansvaret, från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en verkställdhet också följer lagen för korrekt personuppgiftshantering.

Den personuppgiftsansvarige har ansvar för all behandling av personuppgifter som sker inom verksamheten. Observera att detta inkluderar sådant som enskilda individer registrerar i sin yrkesroll. Även om organisationen som sådan inte har bett om en viss behandling av personuppgifter eller inte känner till en behandling som någon utför, så är man som personuppgiftsansvarig ansvarig för den, så länge den inte sker för helt privat bruk. Är det exempelvis någon anställd som på eget initiativ samlar in eller lämnar ut information i strid med lagstiftningen, så är det den personuppgiftsansvariges ansvar.

Riktlinjer för personuppgiftsansvariga	
B.1.1	Kommunstyrelsen/nämnder ska utse dataskyddsombud.

B.1.2	Kommunstyrelsen/nämnder ska ange det operativa ansvaret i delegationsordning och/eller reglemente

Riktlinjer för kommunchef	
B.1.2	Har det yttersta förvaltningsansvaret för att personuppgiftshantering bedrivs i linje med Dataskyddsförordningen och den av kommunfullmäktiges fastställda policy för informationssäkerhet och personuppgiftshantering samt kompletterande styrdokument
B.1.3	Ska utse centralt registeransvarig

Riktlinjer för chef	
B.1.4	Ansvarar för att personuppgiftshantering inom verksamheten följer Dataskyddsförordningen
B.1.5	Ansvarar för att medarbetare inom den egna verksamheten har tillräcklig kunskap, medvetenhet och förståelse för att erforderlig personuppgiftshantering i verksamheten uppnås

Riktlinjer för medarbetare	
B.1.6	Ansvarar för att följa Dataskyddsförordningen samt Vårgårda kommuns policy för informationssäkerhet och personuppgiftshantering, riktlinjer personuppgiftshantering samt övriga styrdokument

Riktlinjer för Centralt registeransvarig	
B.1.7	Ansvarar för kommunens centrala register över personuppgiftsbehandlingar
B.1.8	Är kontaktperson gentemot tillsynsmyndighet och Dataskyddsombud
B.1.9	Ansvarar för att utbilda organisationen, samordna och administrera hanteringen av den centrala registerförteckningen

Riktlinjer för registeransvarig	
B.1.10	Ansvarar för att hantera, förvalta och uppdatera register/förteckning med förvaltningens/verksamhetens samlade informationsobjekt som behandlar personuppgifter
B.1.11	Sköter kontakten med verksamhetens objektsägare, säkerställer att registrerade objekt är fullständigt ifyllda
Riktlinjer för objektsägare	
B.1.12	Ansvarar för att objekt som innehåller personuppgifter följer Dataskyddsförordningen
B.1.13	Registrera behandlingar av personuppgifter i centrala registret

Block C: Ändamål och rättslig grund för behandling samt undantag och kompletterande ändamål.

Inledning

Detta block beskriver ändamål, rättslig grund, undantagsbestämmelser och kompletterande ändamål.

C. 1. Ändamål

Personuppgifter ska bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det gäller att ha klart för sig varför personuppgifterna behövs. Det innebär att den som ska behandla personuppgifter måste ha ändamålen klara för sig redan innan insamlingen av personuppgifter börjar. Personuppgifterna får sedan inte behandlas på ett sätt som är oförenligt med dessa ändamål. De på förhand fastställda ändamålen är med andra ord det som sätter ramarna för behandlingen. Ändamålen ska dokumenteras skriftligt i den centrala registerförteckningen och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är oförenliga med de ursprungliga ändamålen måste de registrerade informeras om detta.

Ändamålet för att behandla en personuppgift kan till exempel vara:

- Fakturering barnomsorg
- Tillsyn av enskilda avlopp
- Bedömning om utbetalning av ekonomiskt bistånd
- Närvarokontroll av elever i skolan
- Tillagning av specialkost

Riktlinjer för ändamål	
C.1.1	Ändamålen ska dokumenteras skriftligt i den centrala registerförteckningen och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det
C.1.2	En personuppgift får inte användas för annat ändamål än det som dokumenterats och informerats
C.1.3	När objekt/system innehåller flera olika ändamål ska dessa separeras och förtydligas

De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen om det finns lämpliga skyddsåtgärder för de registrerades rättigheter (se block I).

C. 2. Rättslig grund

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad rättslig grund. De rättsliga grunderna är:

- Nödvändig för att fullgöra ett **Avtal**
- Fullgöra en **rättslig förpliktelse**
- Skydda den registrerades **grundläggande intressen**
- Fullgöra en uppgift av **allmänt intresse**

- För **myndighetsutövning**
- **Samtycke** från den registrerade
- Samt efter en **intresseavvägning**. Obs! Gäller inte för offentlig verksamhet!

Förutom kravet på rättslig grund måste behandlingen också uppfylla övriga bestämmelser i förordningen. Kom ihåg att möjligheten att behandla personuppgifter begränsas av de grundläggande principerna (Se block A.3) för behandling av personuppgifter och de ytterligare krav som tillkommer för vissa typer av personuppgifter, till exempel känsliga personuppgifter och uppgifter om lagöverträdelser.

Riktlinjer för rättslig grund	
C.2.1	För att behandla en personuppgift ska det finnas en giltig rättslig grund
C.2.2	Rättslig grund ska anges i centrala registret tillsammans med ändamålet
C.2.3	Rättslig grund ska alltid informeras om till den registrerade

C. 2. 1. Avtal som rättslig grund

Att ha avtal som rättslig grund innebär att behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Det gäller bara sådana avtal i vilka den registrerade är eller avser att bli part.

Grunderna i ett avtal är:
När två parter är bundna av ett avtal har de ett inomobligatoriskt förhållande (*obligatorium* = skyldighet, avtalet gör att parterna har skyldigheter gentemot varandra).

Den allmänna avtalsrätten omfattar:

- Avtals uppkomst
- Bestämmande av avtalets innehåll
- Förändringar av avtalets innehåll
- Regler för om inte avtalet följs

Viktiga frågor inom den allmänna avtalsrätten:

- Har det ingåtts ett avtal?
- Har part varit beträdd av behörig?
- Hur ska avtalet tolkas?
- Oförutsedda omständigheter

I Sverige är ett muntligt avtal lika giltigt som ett skriftligt. Det viktigaste är att ni kan säkerställa att personen fått ta del av villkoren innan avtalet ingås. Då gäller även alla obligatoriska delar som följer av Dataskyddsförordningen. Se Block D om informationskrav.

Riktlinjer för avtal	
C.2.1.1	Varje verksamhet ska känna till vilka personuppgiftsbehandlingar som använder avtal som rättslig grund och det ska anges i centrala registret
C.2.1.2	Vid avtal som rättslig grund ska inte fler personuppgifter behandlas än vad som krävs för fullgörandet av avtalet

C. 2. 2. Rättslig förpliktelse som rättslig grund

Personuppgifter får behandlas om det är nödvändigt för att uppfylla en rättslig förpliktelse. Den rättsliga förpliktelsen ska åligga den personuppgiftsansvarige och följa av EU-rätt eller svensk rätt. Exempel på en rättslig förpliktelse är bland andra bokföringslagen, arkivlagen, skollagen, rapporteringar enligt skatteregler, registreringsskyldighet m.m.

Det är viktigt att ha kännedom om speciallagstiftning (andra lagar som anger att personuppgifter ska behandlas) för respektive verksamheter för att identifiera behandlingar som har rättslig förpliktelse som grund. För offentlig verksamhet och myndighetsutövning kan de vara många.

Riktlinjer för rättslig förpliktelse	
C.2.2.1.	Varje verksamhet ska känna till vilka personuppgiftsbehandlingar som använder rättslig förpliktelse som rättslig grund och det ska anges i centrala registret
C.2.2.2	Använd rättslig förpliktelse som rättslig grund om det framgår krav på personuppgiftsbehandlingar i annan lagstiftning

C. 2. 3. Allmänt intresse/myndighetsutövning som rättslig grund

Med allmänt intresse/myndighetsutövning menas att personuppgiftsbehandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Det betyder inte att det är tillåtet att behandla personuppgifter i en verksamhet som många är intresserade av, utan det ska vara en verksamhet som är viktig för samhället, det vill säga i det allmännas intresse. Det är alltså syftet med verksamheten som är det väsentliga.

Försiktighet ska råda innan man använder sig av den här bestämmelsen som grund för att en behandling av personuppgifter. Det ställs stora krav på verksamheten innan den kan anses vara av allmänt intresse (eller mer logiskt uttryckt; i det allmännas intresse). För att det ska vara fråga om allmänt intresse ska det allmänna intresset följa av lag eller annan författning (till exempel förordning), av kollektivavtal eller av beslut som har meddelats med stöd av lag (till exempel myndigheters föreskrifter).

Riktlinjer för rättslig förpliktelse	
C.2.3.1	Varje verksamhet ska känna till vilka personuppgiftsbehandlingar som använder allmänt intresse/myndighetsutövning som rättslig grund och det ska anges i centrala registret
C.2.3.2	Om personuppgiftsbehandling använder sig av allmänt intresse som rättslig grund ska det baseras på objektiv bedömning utifrån vad som är det allmännas intresse. Det ska finnas stöd i lag, praxis eller utlåtande av tillsynsmyndighet

C. 2. 4. Samtycke som rättslig grund.

I princip alla behandlingar av personuppgifter är tillåtna med den registrerades samtycke. Samtycke används när en behandling inte kan användas av de andra skälen, till exempel att uppfylla avtal eller följa andra lagar.

Ett samtycke ska enligt dataskyddsförordningen vara en frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör hen. En förutsättning för ett

giltigt samtycke är med andra ord att man som personuppgiftsansvarig kan visa att den registrerade har fått tydlig information och har gjort ett fritt, aktivt val att samtycka.

Samtyckestexten ska vara lätt att förstå och lätt att hitta
Den registrerade har rätt till information i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Denna öppenhetsprincip innebär i praktiken att texten ska vara skriven på ett sätt som gör att de registrerade förstår innebörden av sitt samtycke, alltså att det inte är beskrivet i för generella termer.

Öppenhetsprincipen innebär också att samtyckestexten ska vara lätt att hitta. Man ska förstå att man har samtyckt till någonting, och vad man har samtyckt till. Den personuppgiftsansvarige ska inte kunna gömma samtycken i långa villkorstexter.

När går det inte att använda samtycke som rättslig grund
Det finns situationer där det inte går att lämna ett giltigt samtycke, på grund av förhållandet mellan den personuppgiftsansvarige och den registrerade. Om det föreligger en betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, så kan samtycket bedömas som ogiltigt. Detta eftersom det kan hända att den registrerade trots allt inte har upplevt situationen som frivillig.

Det är inte omöjligt för en myndighet eller en arbetsgivare att använda samtycke, men det måste stå helt klart för den registrerade att valet är fritt och att det inte kommer att få framtida konsekvenser vad gäller hens förhållande till myndigheten/arbetsgivaren.

Den registrerade ska få valmöjligheter
För att samtycket ska vara giltigt, ska den registrerade ha fått valmöjligheter om så behövs. Om det är flera ändamål som den personuppgiftsansvarige ber om samtycke för, ska det finnas möjlighet att ge separata samtycken för de olika behandlingarna. Det ska alltså vara möjligt att acceptera vissa ändamål men inte andra. Detta gäller inte i alla situationer, men när det är lämpligt.

Uppgifter för att kunna inhämta samtycke
Ofta behöver den personuppgiftsansvarige inledningsvis registrera personuppgifter för att över huvud taget kunna ta kontakt för att inhämta samtycke. Denna speciella behandling av uppgifter är oftast tillåten med stöd av ett berättigat intresse under förutsättning att uppgifterna sedan tas bort för personer som inte lämnar sitt samtycke.

Information ska alltid lämnas
Observera att man som registrerad normalt sett alltid har rätt till information om behandling av personuppgifter som rör en själv. Detta gäller även när behandlingen inte grundar sig på samtycke.

Exempel på när samtycke ska inhämtas:

- När du vill använda bilder där man kan identifiera personen på bilden (om det inte är bilder med avtal).
- Om du vill spara platsangivelser från användare för att kunna anpassa innehåll eller marknadsföring
- Om vårdgivare vill skicka en patientjournal till en annan vårdgivare

- Befintliga e-postlistor för nyhetsbrev och liknande
- När du vill spara uppgifter om webbplatsbesökare för att kunna personalisera innehållet
- När du vill spara uppgifter om tidigare köp för att kunna erbjuda riktade erbjudanden
- När du ber om fler uppgifter än direkt nödvändigt, till exempel namn och företag när någon ska prenumerera på nyhetsbrev
- När du vill spara uppgifter om tidigare deltagare på kurser eller evenemang för att kunna skicka nyheter eller liknande till dem

Rätten att dra tillbaka samtycke
Den registrerade har rätt att återkalla sitt samtycke. Däremot kan man inte återkalla samtycket retroaktivt, utan det påverkar bara framtida behandlingar. Den registrerade ska informeras om sin rätt att återkalla samtycket i den text som föregår samtycket. Det ska vara lika lätt att återkalla samtycket som att ge det.

Riktlinjer för samtycke	
C.2.4.1	Varje verksamhet ska känna till vilka personuppgiftsbehandlingar som använder samtycke som rättslig grund och det ska anges i centrala registret
C.2.4.2	Värdera i alla situationer om samtycke ska användas som rättslig grund
C.2.4.3	Särskilj mellan olika ändamål vid inhämtande av samtycke
C.2.4.4	Vid inhämtande av samtycke ska den registrerade alltid få möjligheten att svara nej (framför allt i formulär eller e-tjänster)
C.2.4.5	Dokumentera alltid samtycken, följ de rutiner som finns för detta
C.2.4.6	Ett samtycke ska kunna dras tillbaka lika enkelt och helst på samma sätt som det gavs

C. 3 Undantag och kompletterande ändamål

Det är bra att känna till några områden där det finns undantag för hanteringen av personuppgifter enligt dataskyddsförordningen. Undantagen innebär att viss hantering kan ske utifrån annan hänsyn där således kraven i dataskyddsförordningen inte gäller. Det är ändå viktigt att sådan hantering finns med i kommunens dokumenthanteringsplan eller liknande, framför allt när det gäller bevarande och gallring(arkiv) eller statistik och forskning.

Privat behandling

Fysiska personers behandling av personuppgifter som görs i ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll omfattas inte av förordningens regler. Det handlar således om behandling som är helt och hållet privat, utan koppling till yrkes- eller affärsmässig verksamhet.

Yttrande- eller informationsfrihet

Dataskyddsförordningen gäller inte då någon behandlar personuppgifter i samband med utövande av sin yttrande- eller informationsfrihet. Enligt förordningen ska undantag för yttrande- och informationsfrihet göras i nationell rätt. I Sverige innebär det bland annat att sådan personuppgiftsbehandling som omfattas av grundlagsskyddet i

tryckfrihetsförordningen och yttrandefrihetsgrundlagen undantas om tillämpningen av förordningen skulle komma i konflikt med grundlagarna.

Journalistiska, akademiska, konstnärliga eller litterärt skapande ändamål

Behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande undantas från de flesta av bestämmelserna i dataskyddsförordningen.

Offentlighetsprincipen

Dataskyddsförordningen hindrar inte myndigheter och andra organ att lämna ut allmänna handlingar enligt offentlighetsprincipen. Skyldigheten att lämna ut allmänna handlingar omfattar dock inte elektronisk utlämning varför dataskyddsförordningen gäller för sådant utlämnade via till exempel epost eller via internet.

Arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från vissa av registrerades rättigheter; rätt till tillgång, rätt till rättelse, rätt till begräsning av handling, rätt att göra invändningar (Block I). Undantag för den registrerades rättigheter finns även för arkivändamål av allmänt intresse.

Brott

Dataskyddsförordningen gäller inte för personuppgiftsbehandling som myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. I det ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Dataskyddsförordningen gäller inte heller personuppgiftsbehandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten, till exempel verksamhet som rör nationell säkerhet. Sådan personuppgiftsbehandling regleras i stället av nationella bestämmelser.

Endast levande personer

Uppgifter om avlidna personer är inte personuppgifter i dataskyddslagstiftningens mening. Man kan alltså registrera uppgifter om sådana personer utan att dataskyddslagstiftningen blir tillämplig. Men uppgifter om levande släktingar till den avlidne/ofödde är förstås personuppgifter.

Riktlinjer för undantag	
C.3.1	Vårgårda kommun ska följa rutiner för bedömning utifrån undantagen
C.3.2	Används behandling utifrån undantagen ska dataminimering alltid beaktas; pseudonymisering, anonymisering osv.
C.3.5	Beakta sammansatt information när det gäller personer som är i livet samt är avlidna. Genomför åtgärder för att bibehålla de som ska finnas kvar i register, i övrigt ska de följa rutiner för bevarande och gallring
C.3.6	Används undantag ska hanteringen ändras, ändamål korrigeras och därefter följa de nya ändamålen såsom arkivändamål osv.

D

Block D: Informationskrav

D.1 Inledning

Den som vill använda sig av personuppgifter i sin verksamhet är skyldig att informera de registrerade om det. Detta gäller oavsett om man måste invänta ett samtycke eller inte. De registrerade har alltid rätt att veta om att de är registrerade, varför och under vilka förutsättningar. Informationen ska vara uttömmande och förmedlas på ett lättbegripligt sätt.

Grunden i dataskyddsförordningen är att uppgifterna om en individ endast kan lånas av organisationer. Personuppgifterna ses som en del av en individs privatliv, och skyddas därmed av den europeiska konventionen om de mänskliga rättigheterna. Denna rättighet kombinerad med principen om öppenhet gör att man som organisation tydligt måste informera registrerade personer om vad man avser att göra med personuppgifterna som man samlar in. Om man som organisation behandlar personuppgifter på sätt som de registrerade inte är medvetna om, kan det vara skäl till att man tilldöms en sanktionsavgift på den högre skalan.

Tanken är att den registrerade ska känna till alla behandlingar av personuppgifter som innehåller information om hen, för att kunna ta ställning till om man vill vara registrerad, veta att och hur man kan begära registerutdrag och så vidare. Ingenting ska ske utan den registrerades vetskap (med undantag för eventuella polisutredningar och liknande).

Riktlinjer för informationsplikt	
D.1.1	Används personuppgifter i en verksamhet ska den registrerade informeras om det

D.2. Vilken information ska man lämna?

I dataskyddsförordningen skiljer man på om information samlas in direkt från en individ eller om den kommer från tredje part. Skillnaden är att om informationen kommer från tredje part, måste man uppge för den registrerade varifrån uppgifterna är hämtade. Detta måste ske vid första kommunikationstillfället eller inom en månad från att uppgifterna samlades in. Enligt dataskyddsförordningen måste man bland annat informera den registrerade om på vilken rättslig grund man kommer att behandla personuppgifterna.

I artiklarna 13-14 i dataskyddsförordningen listas ett antal saker som man måste informera de personer om vars uppgifter man samlar in.

När personuppgifterna samlas in direkt från den registrerade måste man minst informera om följande:

- Den personuppgiftsansvariges identitet och kontaktuppgifter
- Kontaktuppgifter till dataskyddsombudet
- Ändamålen med behandlingen av personuppgifter
- Den rättsliga grunden för behandlingen av personuppgifter
- Den personuppgiftsansvariges (eller tredje parts) berättigade intresse, om man använder det som rättslig grund
- Vilka som kan komma att ta del av personuppgifterna, antingen inom "koncernen" eller vid överföring till andra externa parter

- Om personuppgifterna ska överföras till tredjeland eller internationell organisation samt information om ifall en adekvat skyddsnivå finns där eller inte
- Kriterierna för hur länge de insamlade uppgifterna kommer att lagras
- Vilka rättigheter den registrerade har, exempelvis rätten till registerutdrag, rätten till radering, rätten att återkalla ett samtycke, rätten att göra invändningar, rätten att klaga till en tillsynsmyndighet etc.
- Om den registrerade är skyldig att tillhandahålla personuppgifterna och vilka följder det kan få att inte göra det
- Om det föreligger något automatiskt beslutsfattande/profilering (i så fall ska logiken bakom den förklaras på ett begripligt sätt).

När personuppgifterna samlas in från någon annan än den registrerade måste man dessutom upplysa om vilka personuppgifter som samlas in och varifrån de kommer, och särskilt ange att de kommer från allmänt tillgängliga källor om så är fallet.

I sektorsspecifika lagstiftningar och branschöverenskommelser/uppförandekoder kan det finnas speciella regler om vilken information som ska lämnas, exempelvis i patientdatalagen.

Riktlinjer för vilken information som ska lämnas den registrerade	
D.2.1	När personuppgifter samlas in direkt från den registrerade ska information lämnas enligt kraven ovan
D.2.2	När personuppgifter samlas in från någon annan än den registrerade ska information lämnas enligt kraven ovan tillsammans med vilka personuppgifter som samlas in och varifrån personuppgifterna kommer ifrån

Skapa en strategi för att informera

Det är viktigt för den personuppgiftsansvarige att ha en strategi för att informera på ett korrekt sätt, men också på ett effektivt sätt som inte är onödigt krångligt eller dyrt.
Rent generellt gäller det förstås att i möjligaste mån använda existerande informationskanaler för att lämna information enligt dataskyddsförordningen.
Att den registrerade får tydlig information om hur hens personuppgifter kommer att hanteras, är en av de grundläggande dataskyddsprinciperna (principen om öppenhet) och är dessutom ett ofta återkommande ämne i dataskyddsmyndigheternas tillsynsverksamhet. Det är mycket väsentligt att kunna visa att man har gjort vad som kan förväntas, när man har informerat de registrerade om sin behandling av deras personuppgifter.

Därför är det extra viktigt att arbeta med texterna så att de verkligen upplevs som tydliga och begripliga. Kommunikationsvägarna är också viktiga att tänka över, alltså hur man når ut med informationen till de som berörs.

D.3.Lättbegripligt innehåll

Samtidigt som det är mycket information som ska förmedlas, så ska informationen vara kort och lättbegriplig. Undvik långa och krångliga meningar och använd ord som folk normalt förstår. Ändamålet med

behandlingen av personuppgifter ska vara presenterat på ett sätt som gör att den registrerade faktiskt förstår vad personuppgifterna ska användas till.

Exempel: Skriv inte "Detta gör vi för att förhöja din upplevelse av vår hemsida", när syftet egentligen är marknadsföring. Det är inte konkret och inte begripligt för allmänheten.

Det är alltså viktigt att anpassa texten så att mottagaren förstår den, speciellt om mottagaren är ett barn (i den mån texten verkligen bör riktas till barnet och inte till vårdnadshavaren) eller har någon funktionsvariation som kan ha betydelse i sammanhanget.

Riktlinjer för lättbegripligt innehåll	
D.3.1	Informationen ska vara kort och lättbegriplig, anpassa texten så att mottagaren förstår den

D.4. Språk som mottagaren förstår

I vissa fall kan man behöva översätta en informationstext till andra språk. Det finns ingenting uttalat om hur många av de registrerade som ska ha svårt att förstå svenska för att man ska vara tvungen att översätta texten, det måste man avgöra själv. Det kan röra sig om många föräldrar på en skola eller många boende i ett bostadsområde, för att detta ska bli aktuellt.

Riktlinjer för språk	
D.4.1	Informationstexter ska skrivas på de språk som bedöms nödvändigt

D.5. Tillgängliggörandet av information

Det är viktigt att informationen presenteras på ett tydligt sätt, alltså att den är lätt att hitta. Det finns däremot inget krav på att den personuppgiftsansvarige ska kunna visa att den registrerade faktiskt har läst texten, utan det räcker med att man har gjort det möjligt på ett enkelt sätt.

Texten får till exempel inte "gömmas" i andra texter så att den blir svår att upptäcka och ta del av. Den kan visserligen vara en del av en avtalstext eller tjänstevillkor, men då ska man på något sätt ha uppmärksammat läsaren särskilt på var i dokumentet just denna text finns att läsa. Det kan man göra i inledningen av avtalet genom en hänvisning till den rubrik som handlar om behandlingen av personuppgifter, eller via en länk som går direkt till den aktuella rubriken. Självklart måste texten vara skriven i en normalt läslig storlek.

Det är en stark rekommendation att alltid se till att informationen lämnas skriftligt, inte bara muntligt. En muntlig informationsinsats är väldigt svår att bevisa i efterhand, både att den faktiskt genomförts men också vilken information som framförts och hur.

Fundera noga på den bästa kommunikationsvägen till de registrerade. Utgångspunkten är att det ofta är fullt tillräckligt att skriva en kortare informationstext i exempelvis en ansökningshandling eller på en blankett, där framförallt ändamålet med behandlingen av personuppgifter framgår tydligt, och sedan hänvisa till en fullständig informationstext på hemsidan. Men det får inte vara några långa krångliga webbadresser utan en tydlig länk direkt synlig på startsidan, i sådana fall. Hur mycket av informationen som ska finnas med omedelbart synlig, beror helt på omständigheterna i det enskilda fallet. Fundera på vad som är det viktigaste att veta, förutom

ändamålet kan det vara att uppgifterna kommer att lämnas vidare till en tredje part, sparas under en lång tid eller hämtas in från offentliga källor.

Det är inte alltid en hänvisning till hemsidan är tillräckligt, utan det beror på kategorin av registrerade. Kan man förutsätta att det kommer att vara äldre personer eller invandrade personer i ganska stor utsträckning, är hemsidan inte den bästa kommunikationsvägen då deras erfarenhet av datorer och internet fortfarande inte sällan är begränsad. Välj då en annan kommunikationsväg, så som att sätta upp anslag i väntrum på en vårdcentral eller på anslagstavlor i bostadshus.

Var alltid beredd att skriva ut eller skicka informationen till den som vill det. Det ska vara enkelt att begära det.

Riktlinjer för tillgängliggörandet av information	
D.5.1	Information ska tillgängliggöras för den registrerade på ett enkelt och tydligt sätt
D.5.2	Utgångspunkten är att all information lämnas skriftligt

Block E: Personuppgiftsincident, hantering och rapportering

Inledning

En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats kallas för personuppgiftsincident. Dataskyddsförordningen ställer särskilda krav på hantering vid en sådan.

Grunden för arbetet är att använda och ha tillgängligt lämpliga tekniska och organisatoriska åtgärder så att personuppgifter är behandlade på ett sätt som säkerställer lämplig säkerhet.

Detta avsnitt gäller personuppgifter. Skilj mellan säkerhetsincident och personuppgiftsincident. Alla personuppgiftsincidenter är säkerhetsincidenter, men inte alla säkerhetsincidenter är personuppgiftsincidenter.

E.1 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Vidare har medarbetare ansvar att uppmärksamma brister och incidenter och rapportera dessa till närmaste chef. Om anställd medvetet eller av betydande oaktsamhet avviker från detta i sitt arbete kan arbetsrättsliga åtgärder vidtas.

En personuppgiftsincident kan få allvarliga konsekvenser för registrerade personer. De kan råka ut för till exempel ekonomisk skada eller kränkning av sina friheter och rättigheter.

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan också påverka tilltron till den organisation som behandlar personuppgifter. Det kan dessutom leda till sanktionsavgifter.

En incident ska anmälas till nationell ansvarig myndighet. Det är obligatoriskt om incidenten ger det sannolikt att det resulterar en risk för frihet och rättigheter för individer.

I vissa fall meddelas berörda registrerade. Vid en anmälan kan man få stöd i bedömningen om registrerade ska informeras.

Dokumentera och rapportera

Tillfälliga brister i olika typer av incidenter bör oavsett tid och påverkan dokumenteras, för senare bedömning. Sedan ska det bedömas från fall till fall om det ska rapporteras till tillsynsmyndigheten.

Om inte en rapportering sker kan tillsynsmyndighet utdöma sanktionsavgift för bristande rapportering. Samt eventuellt en anmälan till för att man inte vidtagit rätt tekniska eller organisatoriska åtgärder för att förhindra att det har skett. Alltså kan en incident innebära två böter om man slarvar med rapporteringen.

Dokumentera

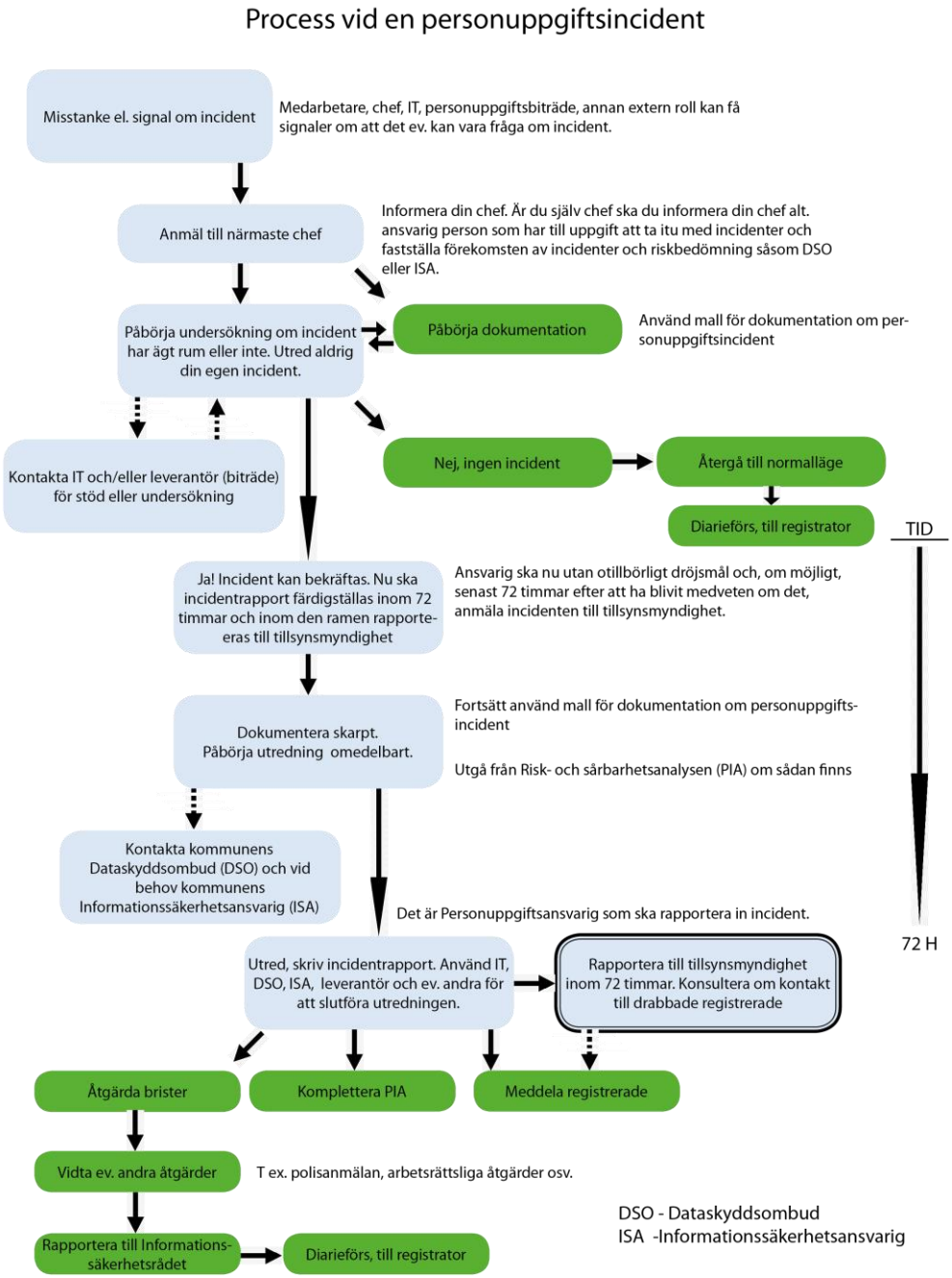
När ansvarig har en rimlig grad av övertygelse att en säkerhetincident har inträffat som har lett till att personuppgifter äventyras ska det dokumenteras. Omständigheterna för den specifika händelsen kan variera och det är inte alltid självklart huruvida det rör sig om en incident. I vissa fall är det relativt klart från början att det handlar om en incident, medan det i andra fall kan det kan ta lite tid att fastställa om personuppgifter har äventyrats. Men betoningen borde ligga vid snabba åtgärder för att utreda en incident för att avgöra om personuppgifter verkligen har påverkats, och i så fall, vidta korrigerande åtgärder och rapportera om det behövs. Påbörja dokumentation så tidigt som möjligt.

Det bör redan finnas nedtecknat i en risk- och sårbarhetsanalys (Privacy Impact Assessment, PIA, Block G) om hur incident kan upptäckas och vad det innebär. Men omständigheter i enskilda incidenter kanske inte alltid överensstämmer med PIA och bör då kompletteras och åtgärdas vid nya erfarenheter.

Åtgärdsprocessen, dokumentation och rapportering hur man ska agera vid incidenter är väsentlig.

Exempel 1.
Ett borttappat USB (Universal Serial Bus) med krypterad information. Vet inte var den är eller om den hamnat i orätta händer, men vi har förlorat kontrollen och då är ansvarig medveten om incident när man inser att den är borta.

Exempel 2.
Efter att först ha informerats om en potentiell incident av en individ, en mediaorganisation eller en annan källa, eller när den själv har upptäckt en säkerhetsincident, kan ansvarig genomföra en kort tids utredning för att fastställa huruvida in incident faktiskt har inträffat eller inte. Under denna period kan kontrollanten inte anses vara "medveten".



Figur 1: Process vid incident

Rapportering till tillsynsmyndighet

Vid personuppgiftsincident ska ansvarig utan otillbörligt dröjsmål och, om möjligt, senast 72 timmar efter att ha blivit medveten om det, anmäla incidenten till tillsynsmyndighet som är behörig, om inte personuppgifterna som bryts är osannolikt att det medför risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndighet inte görs inom 72 timmar, ska den åtföljas av skälen till förseningen.

Ändra eller komplettera

Tillsynsmyndigheten tar hänsyn till att det inte alltid är möjligt att utreda en personuppgiftsincident fullt ut inom 72 timmar. Kommunen har därför rätt att komma in med ändringar, kompletteringar och information om att den

tidigare anmälan var felaktig i efterhand. Det är dock mycket viktigt att kompletteringarna kommer in så fort som möjligt.

Kommunen är själv ansvarig för att skicka in kompletteringar. Utan kompletteringarna kan följden bli att anmälan inte anses vara komplett. Detta kan i så fall vara en anledning till att tillsynsmyndigheten inleder tillsyn.

Vad händer om inte all information finns tillgänglig?
Om kommunen inte kan lämna in all nödvändig information inom 72 timmar bör det förklaras varför i anmälan. Lämna in den information som finns och komplettera i ett senare skede. Informationen kan lämnas i faser så länge detta sker utan otillbörlig försening, dock **senast inom två veckor efter anmälan.**

Ansvar, resurser och prioritet
Tillsynsmyndigheten förväntar sig att ansvariga chefer prioriterar undersökningen av personuppgiftsincidenterna och ger alla som är involverade i undersökningen tillräckliga resurser för att snabbt kunna utreda dessa.

Meddela registrerade

När ska de registrerade informeras?
I vissa fall ska kommunen berätta om personuppgiftsincidenten för de registrerade, alltså för de personer som kan drabbas av händelsen. Detta gäller om personuppgiftsincidenten kan leda till en hög risk för deras rättigheter och friheter.

Enligt förordningen måste de informeras direkt och utan onödigt dröjsmål om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Bedöm risken
Ni måste bedöma både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och sannolikheten för att detta inträffar.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Mildra risken för skador
När risken är hög måste kommunen genast informera de personer som har drabbats, särskilt om det finns ett behov av att mildra en omedelbar risk för skador. En av huvudorsakerna är att kommunen ska kunna hjälpa dem att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

Exempel 1: Informera patienterna
Ett sjukhus drabbas av en personuppgiftsincident som leder till obehörigt röjande av patientjournaler. Personuppgiftsincidenten kan sannolikt få betydande inverkan på individerna, på grund av att uppgifterna är känsliga och att patienternas konfidentiella medicinska detaljer blir kända för andra. Detta kan medföra en hög risk för patienternas rättigheter och friheter. Informera dem därför om personuppgiftsincidenten.

Exempel 2: Informera kunderna
Om en kunddatabas blir stulen bör ni antagligen informera kunderna. Kunddatabasens personuppgifter kan användas för att begå

identitetsbedrägeri, vilket kan leda till ekonomisk förlust eller andra konsekvenser för de drabbade. Personuppgiftsincidenten kan alltså leda till en hög risk för fysiska personers rättigheter och friheter.

Exempel 3: Informera *inte* de anställda
Ett universitet drabbas av en personuppgiftsincident när en anställd av misstag raderar ett register med kontaktuppgifter till de anställda. Detaljerna återskapas senare från en säkerhetskopia. Det är osannolikt att detta medför en hög risk för de anställdas rättigheter och friheter. De behöver därför inte informeras, men dokumentera ändå alltid beslutet.

Exempel 4: Informera *inte* de anställda
Om en telefonlista för personalen har försvunnit, eller om någon har ändrat i den utan tillåtelse, behöver ni normalt sett inte anmäla det till Datainspektionen, och då behöver ni inte heller informera de anställda. Händelsen kommer troligen inte att leda till en hög risk för fysiska personers rättigheter och friheter. Motivera beslutet och dokumentera det.

Obs! Tillsynsmyndighet har befogenhet att tvinga ansvarig att informera berörda personer om den anser att det finns en hög risk. Under alla omständigheter bör beslutsprocessen dokumenteras.

Vilken information ska lämnas till de registrerade?
Följande punkter är ett minimikrav:

- Beskriv orsaken till personuppgiftsincidenten klart och tydligt.
- Ge namn och kontaktuppgifter till dataskyddsombudet, om er organisation har ett, eller till en annan kontakt som är insatt i frågan och kan svara på frågor.
- Beskriv de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskriv vad ni har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- I förkommande fall: Beskriv vad ni har gjort för att mildra eventuella negativa effekter.

Personuppgiftsbiträdets skyldigheter

Personuppgiftsbiträden har eget ansvar och egna skyldigheter när det gäller att anmäla personuppgiftsincidenter.

Den personuppgiftsansvarige har alltid det huvudsakliga ansvaret för att personuppgiftsincidenter anmäls till tillsynsmyndigheten och till de registrerade personer som kan drabbas av händelsen.

Personuppgiftsbiträde är dock skyldigt att rapportera till den personuppgiftsansvarige om denne upptäcker en personuppgiftsincident. Detta för att den personuppgiftsansvarige ska kunna uppfylla sina skyldigheter i förordningen.

Rapportera snarast möjligt
Personuppgiftsbiträde ska rapportera till den personuppgiftsansvarige så snart de fått vetskap om en personuppgiftsincident. Finns inte all information tillgänglig från början kan den lämnas stegvis.

Avtalet ska vara tydligt
Det ska framgå av personuppgiftsbiträdesavtalet hur biträdet ska agera om de upptäcker en personuppgiftsincident och till vem hos den personuppgiftsansvarige ni ska rapportera.

Obs! Det juridiska ansvaret att anmäla personuppgiftsincidenten ligger kvar hos den personuppgiftsansvarige.

Riktlinjer för incidenthantering	
E.1.1	Vidta lämpliga tekniska och organisatoriska åtgärder så att personuppgifter är behandlade på ett sätt som säkerställer lämplig säkerhet.
E.1.2	Meddela drabbade om nödvändigt. Konsultera tillsynsmyndighet om det råder osäkerhet i bedömningen.
E.1.3	Rapportera dokumenterad incident till tillsynsmyndighet
E.1.4	Åtgärda brister som inneburit en incident
E.1.5	Dokumentera alla personuppgiftsincidenter, även dem som inte måste anmälas till Datainspektionen.
E.1.6	Komplettera nya incidenter i Risk- och sårbarhetsanalys (PIA)
E.1.7	Ändra och komplettera till tillsynsmyndighet om det uppkommer ny information, ändrad information eller om första rapporteringen inte är komplett.
E.1.8	Chef ska informera sin personal om incidenthanteringen och hur rutinen ser ut.
E.1.9	Formulera kraven för incidentrapportering i verksamhetens personuppgiftsbiträdesavtal
E.1.10	Rapportera incident till kommunens Informationssäkerhetsråd
E.1.11	Följ processen (figur 1. För incidenthantering)
E.1.12	Använd framtagna dokument för dokumentation av incident
E.1.13	Chef bör aldrig utreda incident som den själv ansvarar för

Block F: Personuppgiftsbiträde, underleverantör, tredje part, utanför EU/EES, personuppgiftsbiträdesavtal

Inledning

Ganska ofta använder Vårgårda kommun externa aktörer för att leverera system, tjänster och/eller verktyg för att administrera och behandla data för våra verksamheter, inte sällan innehåller data personuppgifter. När externa aktörer behandlar personuppgifter gäller Dataskyddsförordningen och Vårgårda kommun är ansvariga för den behandlingen.

F. 1. Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Ofta är det en IT-systemleverantör som är personuppgiftsbiträde, när denna driftar ett system och lagrar personuppgifter åt en kund på sina servrar. Men observera att det inte alls behöver handla om lagring av personuppgifter, utan det är också en biträdessituation när en extern part har åtkomst till den personuppgiftsansvariges data genom sitt uppdrag för service, support, underhåll, utveckling och liknande.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig. Den personuppgiftsansvarige och personuppgiftsbiträdet måste upprätta ett så kallat biträdesavtal. Dataskyddsförordningen räknar upp vad ett sådant biträdesavtal ska innehålla.

Ansvarsförhållande mellan biträde och den ansvarige

Det är alltid den personuppgiftsansvarige som ansvarar för att en behandling av personuppgifter är laglig. Den registrerade kan dessutom bara kräva sina rättigheter av den personuppgiftsansvarige. Man kan till exempel inte begära registerutdrag direkt från ett personuppgiftsbiträde.

Riktlinjer för personuppgiftsbiträde	
F.1.1	Chefer ska identifiera och känna till de personuppgiftsbiträden som de ansvarar för
F.1.2	Personuppgiftsbiträden ska redovisas för i Vårgårda kommuns centrala register
F.1.3	Det ska finnas personuppgiftsbiträdesavtal när så krävs
F.1.4	Det är Vårgårda kommun som är ansvarig och bör som utgångspunkt formulera innehållet i personuppgiftsbiträdesavtalet, inte biträdet
F.1.5	I förekommande fall kan biträdet ge förslag på biträdesavtal. Då ska det göras en ordentlig bedömning om det är tillämpligt för de krav Vårgårda kommun bör ställa vid personuppgiftsbehandlingen

Sanktioner och skadestånd även för biträden
Bestämmelserna om ekonomiska sanktionsavgifter och krav på skadestånd gäller även för personuppgiftsbiträden. Det finns alltså ett starkt incitament för exempelvis IT-systemleverantörer att se till att deras IT-system lever upp till Dataskyddsförordningens krav.

Om ett personuppgiftsbiträde använder kundens personuppgifter på ett sätt som denne inte har fått instruktioner om, och alltså själv bestämmer ändamålet och medlen med behandlingen av personuppgifter, så övergår biträdet till att bli personuppgiftsansvarig för behandlingen med allt vad det innebär i ansvar för att det finns en rättslig grund och så vidare.

Krav på personuppgiftsbiträde

Personuppgiftsbiträdet har en skyldighet att ha kontroll över vilka behandlingar av personuppgifter man utför åt respektive kund. Man är skyldig att upprätta en registerförteckning. För varje kund ska minst fem punkter dokumenteras:

1. Namn och kontaktuppgifter till den organisation som är personuppgiftsbiträde (inom den egna verksamheten)
2. Namn och kontaktuppgifter till den personuppgiftsansvarige (kunden)
3. Information om vilka kategorier av behandlingar som utförs
4. Information om vilka överföringar av personuppgifter som sker till tredjeländer
5. Information om vilka säkerhetsåtgärder som vidtagits

Biträdesavtal och underleverantörer

Personuppgiftsbiträdet har egentligen ingen rättslig skyldighet att se till att det finns ett biträdesavtal. Det är den personuppgiftsansvariges ansvar. Men om det inte finns ett biträdesavtal så har personuppgiftsbiträdet ingen grund för att behandla personuppgifterna. Därför blir avtalet i praktiken ett krav även för personuppgiftsbiträdet.

Fullt ansvar för underleverantörer

Dataskyddsförordningen innehåller också en hel del bestämmelser om hur personuppgiftsbiträdet ska agera när man vill anlita en underleverantör någonstans i leveransen, eller byta en befintlig underleverantör. I princip ska den personuppgiftsansvarige alltid underrättas i god tid och godkänna underleverantören. Personuppgiftsbiträdet har fullt ansvar för hur dess underleverantörer hanterar kundens personuppgifter och att det finns ett avtal som reglerar det.

Tillräckliga garantier

Den personuppgiftsansvarige har bara rätt att anlita ett personuppgiftsbiträde som kan visa att man kommer att genomföra lämpliga tekniska och organisatoriska åtgärder så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. För personuppgiftsbiträdets del innebär det att man måste ta fram dokumentation och rutiner så att man kan ge kunderna tillräckliga garantier för detta.

Incidenthantering

Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter (se Block E) och anmäla de flesta av dem till tillsynsmyndigheten. Om personuppgiftsbiträdet har fått vetskap om en incident, ska denne underrätta den personuppgiftsansvarige så snart som möjligt.

Många incidenter inträffar just hos IT-leverantören/biträdet eller dennes underleverantörer. Det kan handla om brand, obehöriga intrång med mera. Detta innebär att det krävs organisation för incidenthantering hos personuppgiftsbiträdet. Det är viktigt att ha väl utvecklade rutiner för att omedelbart kunna meddela kunderna (de personuppgiftsansvariga) om incidenter som berör deras data. Anmälan till tillsynsmyndigheten ska ske inom 72 timmar, men kan i och för sig göras i etapper om det är svårt att lämna all information så snart. Det är den personuppgiftsansvarige som ansvarar för att göra anmälan, och de vill sannolikt utforma den själva, men det är rimligt att personuppgiftsbiträdet har kompetens att hjälpa till med anmälan och framförallt att ge all nödvändig information så snart som möjligt.

Biträdets samarbete och företrädare

Personuppgiftsbiträdet har också en skyldighet att samarbeta med nationella tillsynsmyndigheter och då kan det bli aktuellt att utse en företrädare för sig. Om personuppgiftsbiträdet inte är etablerad inom EU ska man skriftligen utse en företrädare som är etablerad i någon av de medlemsstater som behandlingen rör. Det är ett krav i dataskyddsförordningen. Men det gäller att ta reda på vad som gäller i det land där kunden är etablerad. Kraven kan se annorlunda ut utanför EU.

Reglerna om ansvarig/ledande tillsynsmyndighet i innebär i praktiken att ett personuppgiftsbiträde kan behöva samarbeta med ett stort antal tillsynsmyndigheter om man exempelvis har råkat ut för en säkerhetsincident i ett IT-system som används i många länder.

Hjälpa den personuppgiftsansvarige

Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige så att de registrerades rättigheter kan fullgöras, så som att ta fram information till registerutdrag eller radera personuppgifter.

Personuppgiftsbiträdet ska bidra till granskningar och inspektioner och ge den personuppgiftsansvarige tillgång till information om säkerhetsarbetet och annat som behövs för att den personuppgiftsansvarige ska kunna kontrollera att dataskyddslagstiftningen följs.

Informera om behandlingen strider mot lagstiftningen

Personuppgiftsbiträdet har en skyldighet att omedelbart informera den personuppgiftsansvarige om man anser att en instruktion om behandlingen av personuppgifter strider mot dataskyddslagstiftningen, men har inte ansvar för regelefterlevnaden i det avseendet.

Avtala om tystnadsplikt

Personer som arbetar för personuppgiftsbiträdet och som har rätt att ta del av personuppgifter, ska skriva på ett tystnadspliktsavtal.

Dokumentation

Fakta kring säkerhet och funktioner ska dokumenteras så att det finns möjlighet att visa kunderna att det finns tillräckliga garantier för att både de som personuppgiftsansvariga och personuppgiftsbiträdet kommer att kunna uppfylla kraven i dataskyddslagstiftningen och säkerställa att de registrerades rättigheter skyddas. Kunden har rätt till sådan information.

Annan dataskyddslagstiftning för biträden

Personuppgiftsbiträden som har en kundkrets utanför EU eller som på annat sätt kan komma att påverkas av dataskyddslagstiftning utanför EU, måste även ta hänsyn till sådan nationell lagstiftning. Samma sak gäller sådan lagstiftning som kompletterar GDPR i respektive EU-medlemsstat, exempelvis den svenska dataskyddslagen.

F. 2. Överföringar till tredjeland

När kundens personuppgifter tillgängliggörs i tredjeland, alltså utanför EU/EES är utgångspunkten att det inte är tillåtet att överföra personuppgifter till tredjeland utan att man vidtar särskilda åtgärder för att säkerställa en tillräckligt hög nivå för skyddet för de registrerades personliga integritet.

Personuppgifterna behöver inte rent faktiskt användas i tredjeland för att bestämmelserna ska vara tillämpliga, utan det räcker med att personer i tredjeland skulle kunna ta del av dem.

Det finns en hel del olika åtgärder som parterna kan vidta för att en överföring av personuppgifter till tredjeland ska bli tillåten. Vissa länder har EU-kommissionen gett en särskild status genom att besluta att de har en adekvat skyddsnivå för behandling av personuppgifter, vilket innebär att det är tillåtet att överföra personuppgifter till dem (naturligtvis under förutsättning att alla övriga krav i dataskyddslagstiftningen uppfylls).

Exempel på åtgärder

- EU-kommissionens olika standardavtal
- Bindande företagsbestämmelser (BCR)
- Uppförandekoder och certifieringar
- Undantag i särskilda situationer efter beslut från berörda dataskyddsmyndigheter

Tredjeland - Var är kundens personuppgifter tillgängliga?

Reglerna om överföring av personuppgifter till tredjeland gäller även för personuppgiftsbiträden. För ett personuppgiftsbiträde är det därför av stor vikt att hålla reda på var någonstans i världen som kundens personuppgifter görs tillgängliga genom biträdet. Det gäller inte bara lagring, utan även åtkomst för exempelvis support, service, underhåll, drift eller utveckling.

Huvudleverantören ska inför den personuppgiftsansvarige redogöra för vilka underleverantörer som anlitas i leveransen och var i världen personuppgifterna är tillgängliga. Det gäller inte bara de egna underleverantörerna utan även underleverantörer i flera led.

Detta kräver inte sällan ett stort kartläggningsarbete och en disciplin vad gäller hur och när underleverantörerna ska meddela planer på förändringar. Alla förändringar kräver nämligen att den personuppgiftsansvarige

underrättas och oftast att denne ska godkänna förändringen på något sätt. Detta är huvudleverantörens ansvar.

Riktlinjer för överföring till tredjeland	
F.2.1	Överväg noga huruvida en tjänst som överför till tredje land är nödvändigt. Välj i huvudsak överföringar till EU/EES och av EU godkända länder. Det uppfyller ett av huvudsyftena med Dataskyddsförordningen.
F.2.2	Om vi överför till tredje land ska särskild utredning genomföras för att säkerställa att säkerhetskraven följer bestämmelserna I Dataskyddsförordningen.
F.2.3	Endast chef beslutar om överföring till tredje land
F.2.4	Chef ansvarar för att all behandling av personuppgifter uppfyller kraven i Dataskyddsförordningen om det beslutas att överföra uppgifter till tredje land.
F.2.5	Chef ska kontrollera befintliga biträdesavtal och säkerställa till var överföringar sker.
F.2.6	Chef ska kontrollera befintliga biträdesavtal och säkerställa till var eventuella underleverantörer överför personuppgifter.
F.2.7	Undvik överföring till tredje land

F. 3. Biträdesavtal

Biträdesavtal är i praktiken ett krav. Hur biträdesavtalet är formulerat är av mycket stor betydelse i många avseenden. Det finns en hel del rättsliga krav på vilka bestämmelser som avtalet ska omfatta.

Ett företag eller myndighet som behandlar personuppgifter för någon annans räkning är att anse som ett personuppgiftsbiträde. En organisation som vill anlita ett sådant biträde (den personuppgiftsansvarige) måste teckna ett skriftligt avtal med biträdet.

I avtalet ska biträdet åta sig att:

- Bara behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige
- Se till att personer som har behörighet att behandla personuppgifter hos biträdet har åtagit sig att iaktta tystnadsplikt eller omfattas av lagstadgad sådan
- Vidta alla tekniska och organisatoriska åtgärder som är nödvändiga för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna med behandlingen
- Respektera kraven på förhandstillstånd och avtal vid anlitande av ett annat biträde (ett underbiträde)
- Vidta lämpliga tekniska och organisatoriska åtgärder så att den personuppgiftsansvarige kan svara på en enskilds begäran om att få utöva sina rättigheter, såsom rätten till information och registerutdrag, rättelse, radering med mera
- Bistå den personuppgiftsansvarige med att se till att skyldigheterna fullgörs ifråga om säkerhetsåtgärder, anmälan av personuppgiftsincidenter och information om sådana incidenter till de registrerade samt konsekvensbedömning och förhandssamråd

- Radera eller återlämna alla personuppgifter till den personuppgiftsansvarige (beroende på vad den personuppgiftsansvarige väljer) när uppdraget avslutas och även radera alla kopior
- Ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att man fullgör alla skyldigheter som man har som biträde samt att möjliggöra och bidra till inspektioner och andra granskningar som den personuppgiftsansvarige vill genomföra.

Eget biträdesavtal eller leverantörens biträdesavtal

I många fall använder sig kommunen av leverantörer med stora system, många lösningar och inte sällan levererar de lösningar för en stor mängd kunder. Det som kan uppstå då är att leverantören själva presenterar färdiga biträdesavtal, schablonavtal som de önskar att kunden skriver på.

Det är då viktigt att utgå från Vårgårda kommuns hanteringskrav, arbetssätt och säkerhetskrav. Det är framtaget en mall för personuppgiftsbiträdesavtal i Vårgårda kommun. Ansvarig för avtal ska alltid utgå från den mallen och utifrån det förhandla om ett personuppgiftsbiträdesavtal med leverantören. Viktigt att komma ihåg är att det alltid är Vårgårda kommun som är personuppgiftsansvarig. Agerar leverantören utanför biträdesavtalet blir de ansvariga. Därför ska avtalen inte vara för generella eller oprecisa i sitt innehåll.

I andra hand är det möjligt att använda leverantörens biträdesavtalsförslag. Men det är bara om det uppfyller samma krav som Vårgårda kommun ställer på ett personuppgiftsbiträde samt dess eventuella underleverantörer.

Riktlinjer för Personuppgiftsbiträdesavtal	
F.3.1	Chef eller systemägare är ansvarig för att upprätta personuppgiftsbiträdesavtal för de tjänster de ansvarar
F.3.2	Det är Vårgårda kommun som är personuppgiftsansvarig. Därför ska biträdesavtalet styras av Vårgårda kommun. Det är inte biträdet som bestämmer krav eller hur de anser att de ska behandla personuppgifter
F.3.3	Använd mall framtagen för biträdesavtal.
F.3.4	När en leverantör/biträde delger eget biträdesavtal ska det användas i andra hand efter vår egen mall. Då ska det kontrolleras att de följer våra krav
F.3.5	Personuppgiftsbiträdesavtal ska vara ett separat avtal. Alltså ska det tydligt skiljas från leveransavtalet eller i innehållet i avtalet för ett system eller objekt
F.3.6	Personuppgiftsbiträdesavtalen ska dokumenteras och finnas med i centrala registret
F.3.7	Personuppgiftsbiträdesavtalet ska ses över vid varje ändring i leveransavtal eller förändringar i leverantörens tjänster

Block G: Risk- och sårbarhetsanalys, konsekvensanalys - Privacy impact Assessment (PIA) och förhandssamråd

Inledning

Att genomföra konsekvensbedömningar är den personuppgiftsansvariges ansvar, ibland går det att få stöd och hjälp av personuppgiftsbiträdet som ofta besitter kompetens för att hjälpa till med det. Även Dataskyddsombudet kan och bör ge råd om när en konsekvensbedömning avseende dataskydd ska göras samt vara delaktig i genomförandet av den. Det är viktigt att skilja mellan en risk- och sårbarhetsanalys och konsekvensbedömning där den senare är ett krav om det finns hög risk för människors fri- och rättigheter. En risk- och sårbarhetsanalys hjälper till att bedöma om så är fallet.

G.1. Konsekvensbedömningar och förhandssamråd

Konsekvensbedömning handlar om att identifiera och förebygga risker innan de uppkommer. Vid behandling av personuppgifter som kan leda till en hög risk för de registrerade måste organisationen göra en så kallad konsekvensbedömning avseende dataskydd. I korthet handlar det om att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter.

Målet är att minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk.

Om konsekvensbedömningar

Syftet med konsekvensbedömning är att förebygga risker innan de uppkommer. Det kan behövas göra en konsekvensbedömning:

- innan påbörjan av en personuppgiftsbehandling
- om risken med en pågående behandling ändras
- för pågående behandlingar om det inte har gjorts tidigare.

Konsekvensbedömningen är en process för att

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att bemöta dessa risker
- visa att man uppfyller dataskyddsförordningens krav.

En konsekvensanalys ska genomföras när en behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det bör i första steget tas reda på genom att bedöma vilka personuppgifter det handlar om och/eller genomföra en risk-och sårbarhetsanalys.

Börja med en risk- och sårbarhetsanalys

Ni ska alltid göra en konsekvensbedömning, om er behandling av personuppgifter sannolikt leder till en hög risk för enskilda personers fri- och rättigheter. Men alla måste inte alltid genomföra en regelrätt konsekvensbedömning:

1. Analysera vilka risker behandlingen av personuppgifter kan innebära och föreslå lämpliga säkerhetsåtgärder. Genomför en risk- och sårbarhetsanalys. Dokumentera resultatet, så att det går att visa att förordningen följs.

2. Utifrån riskanalysen beslutas om organisationen behöver gå vidare och göra en konsekvensbedömning.

Obs! I tveksamma fall bör alltid en konsekvensbedömning göras.

Exempel på kontrollfrågor:

- Är det en behandling av personuppgifter
- Registreras några integritetskänsliga personuppgifter
- Finns det någon lagring eller åtkomst från tredjeland
- Kommuniceras personuppgifter via öppna nätverk

Varför konsekvensbedömning?

En konsekvensbedömning är en pågående process som behöver omprövas och uppdateras kontinuerligt.

Ett krav i vissa fall
Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter ska alltid genomföras en konsekvensbedömning. Den som bryter mot skyldigheten att göra en konsekvensbedömning riskerar att drabbas av en sanktionsavgift.

Konsekvensbedömningen som beslutsunderlag
Den personuppgiftsansvarige kan med fördel göra en konsekvensbedömning även för sådana personuppgiftsbehandlingar som medför en lägre risk. En konsekvensbedömning kan ge organisationen förståelse för personuppgiftsbehandlingens konsekvenser och risker och vara till hjälp när det ska avgöras vilka säkerhetsåtgärder som ska vidtas eller vilka tekniska lösningar som ska väljas.

Konsekvensbedömning för att visa att organisationen följer dataskyddsförordningen
Konsekvensbedömningar är inte bara till hjälp för att uppfylla kraven i dataskyddsförordningen. De är också ett sätt att visa tillsynsmyndigheten att förordningen följs.

En pågående process för integritetens skull
Konsekvensbedömningen kan ses som en pågående process som behöver omprövas och uppdateras kontinuerligt. Då blir det enklare att uppmärksamma och införliva integritetsaspekten i personuppgiftsbehandlingens alla delar.

Vem måste göra en konsekvensbedömning?

Utgå från risk- och sårbarhetsanalysen. Om behandlingen av personuppgifter sannolikt leder till en hög risk för enskilda personers fri- och rättigheter ska det alltid göras en konsekvensbedömning. För att veta om ni måste göra en konsekvensbedömning måste ni alltså först göra en riskanalys.

Att bedöma risk
För att kunna bedöma en risk ska man analysera risken, det vill säga beskriva

- händelsen och varför den är en potentiell risk
- hur sannolikt det är att händelsen inträffar
- hur allvarliga konsekvenserna blir om händelsen inträffar.

Exempel: Hög risk kan det vara om det saknas tillräckliga säkerhetsåtgärder, så att "fel" personer får tillgång till personlig eller känslig information, till exempel uppgifter som kan leda till risk för diskriminering, identitetsstöld, bedrägeri, ekonomisk förlust eller skadat anseende.

Risken som uppkommer vid era personuppgiftsbehandlingar måste bedömas kontinuerligt. Förutom risken för den enskildes personliga integritet ska även risken när det gäller andra grundläggande rättigheter bedömas, till exempel:

- yttrandefrihet
- tankefrihet
- fri rörlighet
- förbud mot diskriminering
- rätt till frihet, samvete och religion.

Exempel på behandlingar som sannolikt leder till hög risk
Dataskyddsförordningen ger tre exempel på behandlingar som sannolikt leder till hög risk:

- När det används automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors personliga aspekter, till exempel profilering.
- När det behandlas uppgifter om lagöverträdelser eller känsliga personuppgifter, till exempel uppgifter om hälsa, religiös tro, politisk uppfattning eller etniskt ursprung, i stor omfattning.
- När det sker systematiskt övervakning på en allmän plats i stor omfattning, genom till exempel kameraövervakning.

Vilka måste göra en konsekvensbedömning?
Om personuppgiftsbehandling faller in under någon av nedanstående kategorier kan det innebära att det behöver göras en konsekvensbedömning.

- utvärderar eller poängsätter människor,
- behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande betydande följder för den registrerade
- systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer
- behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till exempel ett sjukhus som lagrar patientjournaler och liknande
- behandlar personuppgifter i stor omfattning
- kombinerar personuppgifter från två eller flera behandlingar på ett sätt som den registrerade inte förväntar sig, till exempel när man samkör register
- behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, exempelvis barn, anställda, asylsökande, äldre och patienter

- använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)
- behandlar personuppgifter på ett sätt som hindrar de registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel ett registerutdrag från Polis

Konsekvensbedömning är inte alltid nödvändig
Om det redan har gjorts en konsekvensbedömning för en behandling som är mycket lik den planerade behandlingen behöver ni inte göra en ny konsekvensbedömning. Då kan resultatet från den tidigare konsekvensbedömningen användas

En konsekvensbedömning behöver inte heller göras om den planerade personuppgiftsbehandlingen inte sannolikt leder till en hög risk för enskildas fri- och rättigheter.

Så här gör man en konsekvensbedömning

Det är viktigt att påbörja konsekvensbedömningen så tidigt som möjligt och att införliva konsekvensbedömningen i arbetssättet.

Gör konsekvensbedömningen innan personuppgiftsbehandlingen inleds.

Ibland krävs en konsekvensbedömning även för befintliga behandlingar. Riskerna kanske har ökat, till exempel för att det samlas in fler uppgifter än tidigare eller för det införts nya tekniska lösningar. Eller så är det inte gjort någon konsekvensbedömning tidigare.

Grundläggande krav på en konsekvensbedömning

För att kunna bedöma riskerna för enskildas friheter och rättigheter måste ett helhetsgrepp tas om situationen och titta på många olika faktorer i personuppgiftsbehandlingen.

Det finns fyra grundläggande krav på vad en konsekvensbedömning ska innehålla:

- En systematisk beskrivning av den planerade behandlingen och behandlingens syfte
- En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den
- En bedömning av riskerna för de registrerades rättigheter och friheter
- De åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

Dessutom måste
- rådgöras med dataskyddsombudet
- inhämtas synpunkter från de registrerade eller deras företrädare när det är lämpligt

En konsekvensbedömning för flera behandlingar
En enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker.

Obs! Den som gör en gemensam konsekvensbedömning för flera personuppgiftsbehandlingar ska motivera varför en enda konsekvensbedömning har utförts.

Att avhjälpa risker
Överväg i första hand om behandlingen är nödvändig och proportionerlig i förhållande till syftet. Kanske kan syftet med behandlingen uppnås på ett annat sätt så att riskerna inte uppstår.

Exempel på åtgärder som kan användas för att hantera risker är

- autentisering
- kryptering
- rutiner och tydlig information om säkerhet till systemets användare
- logg över vem som använder personuppgifter
- stöd för säkerhetskopiering
- pseudonymisering av personuppgifter
- öppen redovisning av personuppgifternas syfte och behandling
- möjlighet för den registrerade att övervaka uppgiftsbehandlingen.
- minska antalet personer som har tillgång till uppgifterna
- begränsa sökbegrepp så att det inte går att söka på känsliga personuppgifter
- införa automatisk borttagning av personuppgifter som inte längre ska behandlas
- utforma IT-systemen så att inte fler personuppgifter än nödvändigt behandlas, det vill säga inbyggt dataskydd och dataskydd som standard.

Motivera och dokumentera
Motivera och dokumentera de val som görs, till exempel om det bedöms att det inte är lämpligt att inhämta eller följa synpunkter från de registrerade.

Införliva konsekvensbedömningar i arbetssätt
För att se till att det redan från början tas hänsyn till skyddet för personuppgifter i arbetsprocesser bör det införlivas konsekvensbedömningen i arbetssätt. Till exempel att ha med konsekvensbedömningar i arbetsordning eller i projektplaner.

Publicera för öppenhet och ansvarsskyldighet
Även om det inte är ett krav bör det övervägas att publicera hela, eller åtminstone delar av, konsekvensbedömningen. En sådan publicering kan bland annat hjälpa till att uppfylla förordningens principer om öppenhet och ansvarsskyldighet.

Publicering kan vara särskilt bra när behandlingen rör allmänheten, till exempel vid övervakning på allmän plats. Publiceringen kan bestå av en sammanfattning av konsekvensbedömningens huvudsakliga innehåll.

Ompröva riskbedömningen kontinuerligt
Ompröva bedömningen av riskerna flera gånger under utvecklingsprocessen, särskilt när behandlingen förändras på ett sätt som kan påverka risken, till exempel för att det samlas in fler uppgifter än tidigare eller inför nya

tekniska lösningar. Även efter att en behandling har påbörjats kan ni behöva gå tillbaka till den ursprungliga konsekvensbedömningen och ompröva bedömningen av risken.

Riktlinjer för Konsekvensbedömningar och risk- och sårbarhetsanalyser	
G.1.1	Genomför risk- och sårbarhetsanalys vid nya behandlingar av personuppgifter, det är inget krav men underlättar arbetet
G.1.2	Bedöm utifrån risk- och sårbarhetsanalys om en konsekvensbedömning är nödvändig
G.1.3	Genomför konsekvensbedömning för de behandlingar som kräver det, för känsliga personuppgifter är det ett krav
G.1.4	Dokumentera, använd kommunens mallar för analys/bedömning
G.1.5	Använd Dataskyddsombud för stöd i arbetet med konsekvensbedömning
G.1.6	Vid förändringar i teknik eller organisation ska det alltid genomföras en ny analys för att utreda huruvida det innebär nya risker eller sårbarheter

G.2. Förhandssamråd

Om det ändå anses finnas hög risk med personuppgiftsbehandlingen ska verksamheten samråda med Datainspektionen innan ni behandlingen påbörjas.

Obs! Innan begäran om förhandssamråd ska det ha gjorts en gedigen konsekvensbedömning som är väl dokumenterad.

Kontakta tillsynsmyndighet om inte risken kan begränsas

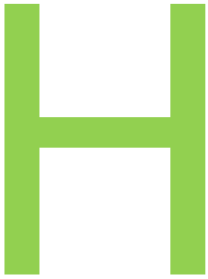
I konsekvensbedömningen ska det tydligt dokumenteras vad som ska göras för att garantera säkerheten i personuppgiftsbehandlingen. Om man i bedömning ändå anser att det finns hög risk med personuppgiftsbehandlingen ska samråd ske med tillsynsmyndighet innan behandlingen får påbörjas. Det kan till exempel vara att riskerna inte kan begränsas tillräckligt genom åtgärder som är rimliga med tanke på tillgänglig teknik och kostnader.

Om tillsynsmyndigheten bedömer att personuppgiftsbehandlingen strider mot förordningen får kommunen råd om hur man ska gå vidare. Tillsynsmyndigheten har även möjlighet att till exempel förbjuda en behandling som strider mot förordningen.

Förbered innan begäran om förhandssamråd

Innan begäran om förhandsråd ska en gedigen konsekvensbedömning genomförts som är väl dokumenterad. Det ska också kunna redogöras för vilka risker som kvarstår och varför inte de kunnat åtgärdas. Dokumentationen av konsekvensbedömningen ska bifogas i begäran om förhandssamråd.

Riktlinjer för förhandssamråd	
G.2.1	Om en behandling är nödvändig men risken är hög bör begäran om förhandssamråd ske
G.2.2	Gör risk- och sårbarhetsanalys och konsekvensbedömning innan begäran om förhandssamråd ställs till tillsynsmyndighet
G.2.3	Begär stöd av Dataskyddsombud om det anses nödvändigt



Block H: Tillsyn, Dataskyddsombud, tillsynsmyndighet

Inledning

En tillsynsmyndighet i varje EU-land ska övervaka att de som behandlar personuppgifter följer dataskyddsförordningen. Tillsynsmyndigheten ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter. Tillsynsmyndighet har möjlighet att bland annat utfärda varningar och reprimander och att förelägga organisationer att vidta åtgärder. Tillsynsmyndigheten kan även besluta om att begränsa eller förbjuda behandling och att påföra administrativa sanktionsavgifter.

Tillsyn

Med tillsyn menas att tillsynsmyndighet genom egna iakttagelser av kommunen kontrollerar att lagar och förordningar följs.

Tillsynen sker antingen på plats eller per brev, telefon eller e-post. Om tillsynen ska genomföras på plats informerar tillsynsmyndigheten normalt tillsynsobjektet i förväg om tid för inspektionen. Oanmälda inspektioner förekommer också.

Skälen till tillsyn kan variera. Ibland kan det bero på att tillsynsmyndigheten mottagit klagomål eller har uppmärksammats på något missförhållande via massmedia. I andra fall kan det bero på att förhållandena i en hel bransch ska granskas.

Tonvikten ligger på breda och djupa granskningar av en bransch eller sektor, till exempel vården, arbetslivet, forskning eller bank/försäkring. En sådan granskning kan innehålla både fältinspektioner och enkäter.

H.1. Tillsynsmyndighet

Tillsynsmyndighetens kanske största uppgift är att ge information, stöd och råd till alla som behandlar personuppgifter i olika verksamheter. Tillsynsmyndigheten har också till uppgift att övervaka att behandlingen av personuppgifter i Sverige går till på rätt sätt. De utför inspektioner och hanterar även frågor och klagomål från enskilda personer.

Datainspektionen utfärdar också föreskrifter och allmänna råd och ger synpunkter på utredningar och lagförslag.

Även om inspektionens kanske största uppgift är att ge stöd och råd, är det också en tillsynsmyndighet som har till uppgift att övervaka att behandlingen av personuppgifter i Sverige går till på rätt sätt.

(Därför måste man tänka sig för lite innan man svarar på deras frågor eller ställer frågor till dem.

Det bästa är om en person i organisationen har det övergripande ansvaret för kontakterna med Datainspektionen, så att det finns någon som kan hålla reda på de frågor och svar som har diskuterats. Finns det ett dataskyddsombud utsett kan det vara den naturliga personen att välja, men måste inte vara det., det beror lite på hur er dataskyddsorganisation ser ut.)

Områden som tillsynsmyndighet ansvarar för och erbjuder:

- Information och rådgivning

- Förhandssamråd (Block G)
- Samråd
- Incidentrapporter (Block E)
- Tillsyn, inspektion och klagomål

Tillsyn, inspektion och klagomål

Det händer att tillsynsmyndigheten öppnar ett så kallat tillsynsärende om de får in ett klagomål eller på något annat sätt blir uppmärksammade på någon behandling av personuppgifter som de vill veta mera om. När en organisation blir kontaktad sker det sannolikt i form av ett brev med en uppmaning om att inom en viss tid (vanligtvis några veckor) beskriva personuppgiftsbehandlingen och svara på några frågor. Det kan också hända att man blir kontaktad via e-post eller telefon, och att inspektionen vill komma och inspektera på plats i lokalerna

Det är alltid bra att tänka efter innan man besvarar frågor från en granskande myndighet. Om man känner sig osäker och inte kan besvara alla frågor från tillsynsmyndigheten med en gång, är det ofta bättre att be att få återkomma.

Observera att det är viktigt att svara noggrant och sanningsenligt. Det går inte att vägra att svara. Det är mycket olämpligt att fara med osanningar eller dölja problem, eftersom det innebär en stor risk för att sanktionsavgifterna blir högre av den anledningen. Det framgår bland annat av Dataskyddsförordningen.

Om Datainspektionens tillsynsärende skulle hitta en eller flera brister i verksamhetens dataskydd, är det viktigt att se till att bristerna blir åtgärdade. Att så snart som möjligt kunna svara att man har gjort något åt saken, eller åtminstone tagit fram en åtgärdsplan, visar att man tagit till sig av tillsynsmyndighetens kritik och anstränger sig för att förändra förhållandena.

Om ett tillsynsärende berör en fråga där organisationen själv anser att man behandlar personuppgifter på ett korrekt sätt, så finns det all anledning att ändå svara och beskriva hur man resonerat. Då slipper man förhoppningsvis vidare skriftväxling och ärendet blir avslutat utan åtgärd från tillsynsmyndighetens sida.

Enkätinspektioner och klagomål

Samma sak gäller så kallade enkätinspektioner. Det är undersökningar där tillsynsmyndigheten ställer samma frågor till ett större antal organisationer om en viss typ av behandling av personuppgifter.

Kommer ett klagomål direkt från en registrerad är det bäst om det kan besvaras på ett sådant sätt att den registrerade nöjer sig med svaret och inte går vidare till tillsynsmyndigheten. Framförallt: svara alltid och svara vänligt och begripligt.

Inspektioner på plats

Tillsynsmyndighet har rätt att komma in i era lokaler, se era IT-system, granska säkerhetsåtgärder och hur personuppgifter behandlas. De har rätt att ta del av all dokumentation om era behandlingar av personuppgifter. De kan

beordra körningar och utskrifter. De kan dock inte ta hjälp av Kronofogden för att bereda sig tillgång till lokaler eller system.

Riktlinjer med beaktande av tillsynsmyndighet	
H.1.1	Prioritera alltid ärenden/förfrågningar som kommer från tillsynsmyndigheten
H.1.2	Råder osäkerhet om hur en verksamhet ska agera, kontakta Dataskyddsombud för råd och stöd
H.1.3	Begär stöd från verksamhetens
H.1.4	Chef bör ansvara för kontakt med Vårgårda kommuns ansvariga för dataskyddsförordningens arbete och med tillsynsmyndighet

H.2. Dataskyddsombud

Ombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Dataskyddsombud kan ha ansvar för flera olika myndigheter. Så är fallet för Vårgårda kommun. Dataskyddsombud (2 st.) delas med övriga kommuner i Sjuhärad. En förutsättning för det är att dataskyddsombudet har tillräckligt med tid och resurser för att utföra uppdraget, och att alla som behöver komma i kontakt med dataskyddsombudet lätt kan göra det.

Vad gör ett dataskyddsombud?

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. Det innebär bland annat att

- samla in information om hur organisationen behandlar personuppgifter
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen.

Dataskyddsombudet ska också

- ge råd om konsekvensbedömningar
- vara kontaktperson för tillsynsmyndigheten
- vara kontaktperson för de registrerade och personalen inom organisationen
- samarbeta med tillsynsmyndighet, till exempel vid inspektioner.

Dataskyddsombudet är inte ansvarigt och får inte bestraffas

Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet. Personuppgiftsansvarig får heller inte bestraffa dataskyddsombudet för att ha utfört sina arbetsuppgifter.

Vara kontaktperson och samarbeta med tillsynsmyndigheten
Dataskyddsombudet ska vara kontaktperson för

- de registrerade, som till exempel vill nå dataskyddsombudet för att få veta vilka uppgifter som finns registrerade om dem
- personalen inom organisationen, som kan vilja veta om de gör rätt när de behandlar personuppgifter
- Tillsynsmyndigheten, som kan vilja inspektera verksamheten.

Myndigheter och offentliga organ måste ha ett dataskyddsombud oavsett vilka uppgifter de behandlar. Ett dataskyddsombud hjälper organisationen i arbetet med dataskydd och fungerar som kontaktpunkt för tillsynsmyndigheten och de registrerade.

Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i lagen.

Konsekvensbedömningar

Dataskyddsombudet ska alltid vara inblandat om en organisation gör, eller överväger att göra, en konsekvensbedömning för behandling av personuppgifter. En konsekvensbedömning behövs om ni ska samla in personuppgifter och det finns hög risk för personers rättigheter och friheter.

Det är den personuppgiftsansvarige, inte dataskyddsombudet, som ska se till att organisationen gör konsekvensbedömningar när det behövs. Men den personuppgiftsansvarige eller personuppgiftsbiträdet ska rådfråga dataskyddsombudet, till exempel för att bedöma

- om det behövs en konsekvensbedömning i ett visst fall
- vilken metod som ska användas för konsekvensbedömningen
- om det är bra att konsekvensbedömningen görs internt eller om en extern part ska göra den
- vilka skyddsåtgärder som behövs för att begränsa eventuella risker för de registrerades rättigheter och intressen
- om en konsekvensbedömning har utförts korrekt och om slutsatserna är korrekta.

Tillgängligt

Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Det är viktigt att dataskyddsombudet är "lättillgängligt". Det innebär till exempel att de registrerade, de som arbetar internt inom organisationen och tillsynsmyndigheten lätt ska kunna hitta kontaktuppgifter till dataskyddsombudet. Det ska också vara lätt att komma i kontakt med dataskyddsombudet, som måste kunna kommunicera effektivt med de registrerade.

De organisationer som ska ha ett dataskyddsombud måste meddela dataskyddsombudets namn och kontaktuppgifter till tillsynsmyndigheten. Dataskyddsombudets kontaktuppgifter måste också offentliggöras så att de registrerade vet vart de kan vända sig.

Dataskyddsombudets ställning

Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet dennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Hen får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå.

Dataskyddsombudets resurser

Dataskyddsombudet måste ha de resurser som krävs för att kunna fullgöra sina uppgifter, till exempel

- aktivt stöd från högsta ledningen för dataskyddsombudets arbete
- aktivt stöd och information från andra avdelningar inom kommunen
- tillräckligt med tid för att kunna fullgöra sina uppgifter
- ekonomiska resurser
- fortbildning
- infrastruktur (lokaler, hjälpmedel, utrustning)
- personal i förekommande fall.

All personal i organisationen ska informeras om att det finns ett dataskyddsombud och om vilka uppgifter dataskyddsombudet har.

Kommunen bör bland annat:

- bjuda in dataskyddsombudet att regelbundet delta i möten på högsta och mellanliggande förvaltningsnivå
- låta dataskyddsombudet delta i beslut som har följder för dataskyddet
- förmedla all relevant information till dataskyddsombudet så att ombudet i god tid kan ge lämpliga råd
- dokumentera sina skäl i de fall dataskyddsombudets råd inte följs
- rådfråga dataskyddsombudet omedelbart när en incident har inträffat
- tydligt ange dataskyddsombudets exakta uppgifter och deras omfattning, särskilt när det gäller konsekvensbedömningar.

Sekretess

För dataskyddsombud i det allmännas verksamhet gäller offentlighets- och sekretesslagens bestämmelser om sekretess. Sekretessen/tystnadsplikten innebär dock inte att det är förbjudet för dataskyddsombudet att kontakta och samråda med tillsynsmyndighet.

Dataskyddsombudet får inte ha andra uppgifter som kan leda till intressekonflikter. Till exempel kan dataskyddsombudet inte vara med och fastställa ändamålen med och medlen för behandlingen av personuppgifter.

Riktlinjer med beaktande av Dataskyddsombud	
H.2.1	Använd Dataskyddsombudet som en viktig resurs för ditt arbete
H.2.2	Följ instruktioner från Dataskyddsombudet
H.2.3	Konsultera Dataskyddsombud vid nya behandlingar som har hög risk
H.2.4	Konsultera Dataskyddsombud vid konsekvensbedömningar och förhandssamråd
H.2.5	Konsultera Dataskyddsombudet i händelse av en personuppgiftsincident (se block E, process))
H.2.6	Vårgårda kommun ansvarar för att Dataskyddsombudet har möjlighet att stödja, råda och att sköta sitt uppdrag. Det är Vårgårda kommun som ska ta initiativ till att använda Dataskyddsombudets kompetens i vårt eget dataskyddsarbete.

Block I: Registrerades rättigheter

Inledning

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen.

Rätt till information

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen. Det står mer om informationsskyldigheten i Block D.

I.1. Rätt till rättelse

Varje person har rätt att vända sig till Vårgårda kommun och be att få felaktiga uppgifter rättade. Det innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen. Att den som behandlar personuppgifter också själv måste se till att uppgifterna är korrekta och uppdaterade framgår redan av de grundläggande principerna (Block A) i dataskyddsförordningen.

Rätten till rättelse går ut på att de registrerade kan kräva att de uppgifter som behandlas är korrekta och i vissa fall även aktuella. Därmed har de registrerade också rätt att få uppgifterna korrigerade eller kompletterade vid behov. Detta ger varje individ möjligheten att anpassa informationen till den situation som han eller hon befinner sig i, exempelvis vad gäller bostadsadress, arbetsplats, civilstatus och så vidare. Framförallt handlar det dock om att korrigera direkta felaktigheter eller komplettera missvisande information.

En önskan om rättelse ska uppfyllas av den personuppgiftsansvarige så snart som möjligt (eller utan onödigt dröjsmål), men självklart behöver man inte rätta information som man själv inte anser är felaktig eller missvisande. I sådana fall får man meddela den registrerade detta, som kan klaga till tillsynsmyndigheten.

Om uppgifter rättas på den enskildes begäran måste Vårgårda kommun också informera dem som de har lämnat ut uppgifter till om att uppgifter rättats. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.

Riktlinjer för rätten till rättelse

I.1.1	Begäran från registrerad om rättelse ska prioriteras i arbetet (hanteras skyndsamt)
I.1.2	Vid varje begäran om rättelse ska uppgifterna kontrolleras mot ändamål och rättslig grund för att bedöma huruvida uppgifterna är korrekta eller felaktiga
I.1.3	Om rättelse inte kan medges ska orsaken tydligt kommuniceras. Informera alltid om rätten att överklaga ett sådant beslut
I.1.4	Rätten till rättelse ska bedömas sakligt och objektivt när en sådan begäran inkommer

I.2. Rätt till radering

Varje person har rätt att vända sig till Vårgårda kommun och be att uppgifterna som avser hen raderas. Uppgifterna måste raderas i följande fall:

- Om uppgifterna inte längre behövs för de ändamål som de samlades in för
- Om behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket
- Om behandlingen sker för direktmarknadsföring och den enskilde motsätter sig att uppgifterna behandlas
- Om personuppgifterna har behandlats olagligt
- Om radering krävs för att uppfylla en rättslig skyldighet
- Om personuppgifterna avser barn och har samlats in i samband med att barnet skapar en profil i ett socialt nätverk

Om uppgifter raderas på den enskildes begäran Vårgårda kommun också informera dem som de har lämnat ut uppgifter till om raderingen. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.

Som individ har man rätt att begära att personuppgifter ska tas bort. Det kallas ofta "rätten att bli glömd". Det rör sig inte om någon absolut rättighet som gäller i alla sammanhang. En anställd har till exempel inte rätt att kräva att uppgifterna i ett löneadministrativt system raderas, och inte heller en kund under ett pågående kundförhållande. Om det inte finns någon annan grund för behandlingen än samtycke eller om grunden är ett avtalsförhållande och det har avslutats, så har man rätt att begära att "bli glömd".

En enskild registrerad kan däremot inte begära att uppgifterna raderas om behandlingen av personuppgifter är nödvändiga för:

1. att kunna utöva rätten till yttrande- och informationsfrihet
2. att kunna uppfylla ett lagkrav (exempelvis bokföringslagens krav på sparande av personuppgifter i sju år för redovisningsändamål) eller det är en del i en myndighetsutövning
3. folkhälsoändamål
4. arkiveringsändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål
5. att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Det är den personuppgiftsansvarige som ska kunna visa på sin rätt att ha kvar uppgifterna om den registrerade begär att de ska tas bort.

Riktlinjer för rätten till radering	
I.2.1	Vid begäran om radering av registrerad ska kontroll utföras om den rätten finns utifrån kommunens ändamål och rättslig grund.
I.2.2	Om uppgifter om registrerad finns i register och rätten till radering önskas ska det göras bedömning om uppgifterna ska hanteras på annat sätt än att raderas. Det är viktigt att utreda om det bör hanteras på annat sätt utifrån annan lagstiftning såsom arkivändamål, statistikändamål osv.
I.2.3	Om radering inte kan medges ska orsaken tydligt kommuniceras. Informera alltid om rätten att överklaga ett sådant beslut.
I.2.4	Rätten till radering ska bedömas sakligt och objektivt utifrån rättslig grund för behandling när en begäran inkommer.
I.2.5	Som myndighet är inte intresseavvägning giltigt för att bedöma huruvida uppgift ska raderas eller inte.

I.3. Rätt till begränsning av behandling

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.

Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och begärt rättelse. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds.

Som personuppgiftsansvarig kan man då tvingas behålla uppgifterna, men utan att ha rätt att använda dem. Detta kan bli aktuellt i följande situationer:

- Om man måste kontrollera personuppgifternas korrekthet
- Om behandlingen av personuppgifter varit olaglig, men den registrerade motsätter sig en radering
- Om den personuppgiftsansvarige inte behöver uppgifterna längre, men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara ett rättsligt anspråk denne har

Om man en gång har begränsat användandet av någons personuppgifter, måste man alltid meddela personen i förväg ifall begränsningen kommer att hävas.

Den personuppgiftsansvarige ska underrätta varje mottagare som man har lämnat ut de aktuella uppgifterna till om behandlingen har begränsats. Detta gäller så länge det inte visar sig vara omöjligt eller en oproportionell ansträngning. Man ska också tala om för den registrerade vilka mottagarna är, om den registrerade efterfrågar den informationen.

Riktlinjer för rätten till begränsning	
I.3.1	En begäran om begränsning är alltid giltig. Ange att det behöver utredas innan verkställighet av någon form ska ske. Begränsa informationen denna tid genom att vidta nödvändiga åtgärder när det gäller distribution, behörigheter osv.
I.3.2	Vissa delar av denna rättighet påverkar andra viktiga mottagare av de personuppgifter som behandlas. Det bör därför finnas rutiner för vilka Vårgårda kommun delger sådana uppgifter och de ska delges

	information om begränsning eller utredning om begränsning då detta kan påverka en registrerads rättigheter och frihet.

I.4. Rätten till dataportabilitet

Rätten till dataportabilitet innebär att en registrerad har rätt att, på begäran, få ut de uppgifter som finns registrerade om hen i syfte att föra över dem och återanvända dem hos en annan part, till exempel en annan leverantör. Det skulle kunna jämföras med att en person kan byta telefonbolag men behålla sitt telefonnummer.

Denna rättighet gäller endast om behandlingen grundar sig på samtycke eller ett avtalsförhållande.

Den information som ska omfattas av dataportabiliteten är dels sådan information som den registrerade själv har lämnat ifrån sig, dels sådan information som har hämtats in automatiskt genom den registrerades aktiviteter, till exempel trafikdata, sökhistorik, hälsodata som skapats i en app., geografisk data med mera.

Som personuppgiftsansvarig måste man tillhandahålla uppgifterna i ett "strukturerat, allmänt använt och maskinläsbart format" som gör det möjligt för den registrerade att skicka informationen vidare. Om det är tekniskt möjligt kan informationen också skickas direkt till en annan organisation om den registrerade efterfrågar det.

Det är för att möta kravet om dataportabilitet viktigt att ta fram standarder och format för Vårgårda kommun som på ett enkelt sätt kan tillmötesgå detta lagkrav.

Riktlinjer för rätten dataportabilitet	
I.4.1	Verksamheten ska så långt som det är möjligt arbeta med öppna standarder och godkända format för att förenkla rätten till dataportabilitet.

I.5 Rätten att göra invändningar

En enskild har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hens personuppgifter.

Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning. Vårgårda kommun som offentlig myndighet/verksamhet kan inte använda intresseavvägning.

Om den enskilde invänder mot behandlingen i sådana fall får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Den enskilde har alltid rätt att invända mot att hens personuppgifter används för direkt marknadsföring. En sådan invändning kan göras när som helst. Görs en invändning mot direkt marknadsföring, får personuppgifterna inte längre behandlas för sådana ändamål.

Särskilda regler gäller för personuppgifter som behandlas för vetenskapliga och historiska forskningsändamål eller statistiska ändamål.

Den personuppgiftsansvarige måste informera de registrerade om rätten att göra invändningar.

De registrerade ska få information om sin rätt att invända senast i samband med det första reklamutskicket, och då på ett tydligt och begripligt sätt. Observera också att det inte finns något skriftlighetskrav i dataskyddsförordningen när det kommer till att invända mot marknadsföring. Man kan alltså inte kräva att den registrerade ska invända genom att skicka ett skriftligt brev med sin begäran.

Riktlinjer för rätten att invända mot behandling	
I.5.1	För att kunna ansvara och svara på rätten till invändning ska ändamål med behandling och rättslig grund för den vara tydligt. Det ska anges i kommunens registerförteckning.
I.5.2	För de fall där kommunen använder sig av marknadsföring, nyhetsbrev, inbjudningar och liknande ska information om denna rätt ges i anslutning till sådana utskick.

I.6. Automatiserat beslutsfattande, inbegripet profilering

Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar hen.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på en kreditansökan på internet eller vid ett nekande besked från e-rekrytering via internet utan personlig kontakt.

Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning.

Den personuppgiftsansvarige måste informera de registrerade om att automatiserat beslutsfattande används enligt den generella informationsskyldigheten i förordningen (Block D).

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut. Profilering innebär varje form av automatisk behandling av personuppgifter då uppgifterna används för att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Profilering utgör en behandling av personuppgifter som måste utföras i enlighet med samtliga bestämmelser i dataskyddsförordningen.

Riktlinjer för Automatiserat beslutsfattande, inbegripet profilering	
I.6.1	För att kunna ansvara och svara på rätten till invändning ska ändamål med behandling och rättslig grund för den vara tydligt. Det ska anges i kommunens registerförteckning.
I.6.2	För de fall där kommunen använder sig av marknadsföring, nyhetsbrev, inbjudningar och liknande ska information om denna rätt ges i anslutning till sådana utskick.