Vägledning för personuppgiftsbiträden

I mitten av 2018 ska den nya dataskyddsförordningen börja tillämpas. Dataskyddsförordningen kommer att gälla som lag i Sverige och ersätta personuppgiftslagen. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU vilket underlättar för företag att verka på hela unionens inre marknad. Dataskyddsförordningen kommer att medföra stora förändringar för de som behandlar personuppgifter.

Datainspektionen har tidigare tagit fram en vägledning för hur **personuppgiftsansvariga** redan idag ska kunna förbereda sig inför de nya reglerna. Vägledningen hittar du på vår webbplats: www.datainspektionen.se/dataskydd-pua

Dataskyddsförordningen kommer dessutom att medföra stora förändringar för er som behandlar personuppgifter för annans räkning. Den här informationen riktar sig därför särskilt till er som är **personuppgiftsbiträden**.

Samma definition men en förändrad roll

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning kommer, i likhet med vad som gäller idag, att vara personuppgiftsbiträde. I den nya dataskyddsförordningen förändras dock denna roll. Personuppgiftsbiträdet kommer att få nya skyldigheter och ett betydligt utökat eget ansvar för personuppgiftsbehandlingen. I ett flertal situationer kommer även personuppgiftsbiträden att omfattas av samma skyldigheter som gäller för personuppgiftsansvariga.

Datainspektionen

Juni 2016

Här är några av de viktigaste förändringarna för personuppgiftsbiträden

Föra register
Ni ska föra ett register över alla kategorier av behandling som utförs för den personuppgiftsansvariges räkning. Registret ska bland annat omfatta namn och kontaktuppgifter för personuppgiftsbiträdet och den personuppgiftsansvarige, vilka kategorier av behandling som utförs för varje personuppgiftsansvariges räkning samt information om tredjelandsöverföring och säkerhetsåtgärder. Det finns vissa undantag från denna skyldighet för mindre företag.

Ansvar vid anlitande av ett underbiträde
Om ni vill anlita ett annat personuppgiftsbiträde måste ni ha ett skriftligt förhandstillstånd från den personuppgiftsansvarige. Har ni fått ett generellt tillstånd att anlita underbiträden måste ni ändå informera den personuppgiftsansvarige om era planer på att anlita ett nytt biträde, så att den ansvarige kan göra invändningar mot detta.

När ni anlitar ett underbiträde måste ni teckna avtal som gör att biträdet omfattas av samma skyldigheter som ni har gentemot den personuppgiftsansvarige. Om det andra biträdet inte fullgör sina skyldigheter kommer ni enligt förordningen att vara fullt ansvarig gentemot den personuppgiftsansvarige för att dessa skyldigheter utförs.

Utse dataskyddsombud
Ni är i vissa fall skyldiga att utse ett dataskyddsombud (motsvarande personuppgiftsombud i personuppgiftslagen). Skyldigheten att utse dataskyddsombud omfattar bland annat offentliga myndigheter och organisationer vars verksamhet involverar särskilt riskfylld behandling, som exempelvis regelbunden och systematisk övervakning av registrerade i stor skala eller omfattande behandling av känsliga personuppgifter. En särskilt integritetskänslig behandling kan därför komma att kräva att dataskyddsombud utses både hos den personuppgiftsansvarige och hos personuppgiftsbiträdet.

Den person som utses måste ha tillräcklig kunskap om dataskydd och få det stöd och de befogenheter som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt.

Samarbeta med tillsynsmyndigheten
Ni har en uttrycklig skyldighet att på begäran samarbeta med tillsynsmyndigheten (Datainspektionen i Sverige).

Ansvar för att vidta säkerhetsåtgärder
Ni har ett eget ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att se till att säkerhetsnivån för er behandling är tillräcklig. Det kan bland annat medföra att ni behöver fundera över frågor som pseudonymisering och kryptering av personuppgifter, hur ni säkerställer att era system är tillräckligt säkra och motståndskraftiga samt hur ni fortlöpande testar och utvärderar systemen.

Vilka åtgärder som är nödvändiga beror på vilka särskilda risker som finns med er behandling. Ni behöver till exempel ha ett starkare skydd om ni behandlar känsliga personuppgifter, såsom uppgifter som rör hälsa eller religiös övertygelse.

Det bör även nämnas att personuppgiftsbiträdets utökade ansvar inte medför att den personuppgiftsansvariges eget ansvar minskar. Ansvaret för att se till att säkerheten kring de personuppgifter som behandlas är tillräcklig kommer att ligga på både den personuppgiftsansvarige och personuppgiftsbiträdet.

Omgående underrätta den personuppgiftsansvarige om personuppgiftsincidenter

Om ni blir utsatta för dataintrång eller på något annat sätt förlorar kontrollen över de uppgifter ni behandlar, en så kallad personuppgiftsincident, måste ni utan onödigt dröjsmål underrätta den personuppgiftsansvarige om detta. Det kan vara bra att bestämma var i er organisation en sådan rapporteringsskyldighet ska ligga eftersom ni, om en personuppgiftsincident inträffar, måste agera skyndsamt.

Bistå den personuppgiftsansvarige

Ni har även en mer allmän skyldighet att bistå den personuppgiftsansvarige när denne ska fullgöra sina skyldigheter enligt förordningen. Ni ska bland annat hjälpa till med att svara på begäranden om elektroniska registerutdrag, och att bistå den personuppgiftsansvarige för att se till att säkerheten för behandlingen är tillräcklig.

Risk för sanktioner

Tillsynsmyndigheten kommer att ges möjlighet att döma ut en administrativ sanktionsavgift på upp till 20 miljoner euro eller 4 procent av organisationens omsättning. Ni kommer, i likhet med vad som gäller för personuppgiftsansvariga, riskera att drabbas av sådana administrativa sanktionsavgifter om ni inte uppfyller de skyldigheter som finns i förordningen.

Hur ska ni förbereda er?

Dataskyddsförordningen kommer att ställa större krav på er att kontrollera att personuppgiftsbehandlingen uppfyller de krav som ställs i förordningen. De personuppgiftsansvariga får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att skyldigheterna i förordningen kommer att uppfyllas och att de registrerades rättigheter skyddas.

Ni måste därför redan nu börja förbereda er på de kommande förändringarna och anpassa er verksamhet till de nya kraven. Ni kan behöva gå igenom vilka uppgifter ni behandlar och för vem behandlingen görs. Ni kan även behöva se över säkerheten i era system och era interna rutiner och instruktioner. Hur omfattande förberedelser som behövs beror på hur er verksamhet ser ut idag och vilka risker som finns med er personuppgiftsbehandling.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

Datainspektionen