

Lagstadgat krav på att upprätta skriftliga personuppgiftsbiträdesavtal

Den 25 maj 2018 infördes EU:s dataskyddsförordning, General Data Protection Regulation ("GDPR") som lag i Sverige. Förordningen medförde ett skärpt och i vissa delar ett nytt regelverk för behandling av personuppgifter.

Definitioner

Med *personuppgifter* avses varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en *registrerad*). Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande fysisk person.

Med *behandling* (av personuppgifter) menas i princip allting som går att göra med personuppgifterna. Det kan vara åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom 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.

Den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandling av personuppgifter, är *personuppgiftsansvarig* enligt GDPR. Den som därefter behandlar personuppgifter för en personuppgiftsansvarigs räkning, är att ses som *personuppgiftsbiträde*. Ett personuppgiftsbiträde är per definition alltid en part som står utanför den personuppgiftsansvariges organisation. Begreppen framgår av definitionerna i artikel 4 i GDPR.

Skriftligt personuppgiftsbiträdesavtal

När en part ska behandla personuppgifter för annans räkning krävs det enligt artikel 28 dataskyddsförordningen att parterna upprättar ett skriftligt avtal för att reglera formerna för personuppgiftshanteringen. Avtalet kan antingen vara ett fristående avtal eller vara tydligt avskilda bestämmelser som del av ett större avtal om leverans av tjänster eller liknande. Muntliga personuppgiftsbiträdesavtal är inte giltiga.

Det ställs enligt artikel 28 GDPR särskilda krav på personuppgiftsbiträdesavtalet. Till en början anges i artikel 28 punkt 1 GDPR att personuppgiftsansvarige endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen. I artikel 28 punkt 2 GDPR föreskrivs det vidare att ett personuppgiftsbiträdes eventuella anlitanande av underbiträden antingen kräver ett allmänt förhandstillstånd från den personuppgiftsansvarige eller i vart fall att den personuppgiftsansvarige informeras om anlitandet av underbiträden. Syftet med denna bestämmelse är att möjliggöra för den personuppgiftsansvarige att göra invändningar och ha kontroll. Enligt artikel 28 punkt 4 GDPR är personuppgiftsbiträdet fullt ansvarig för behandlingen som utförs av ett anlitat underbiträde.

Personuppgiftsbiträdesavtalets särskilda innehåll

I personuppgiftsbiträdesavtalet ska det enligt artikel 28 punkt 3 GDPR särskilt föreskrivas

1. att personuppgiftsbiträdesavtalet som reglerar hanteringen av personuppgifter är bindande för personuppgiftsbiträdet,
2. föremålet för behandlingen, dess varaktighet, art och ändamål, typer av personuppgifter och kategorier av

registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter,

3. att personuppgiftsbiträdet endast får behandla personuppgifterna i enlighet med dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller internationella organisationer,
4. att alla inom organisationen som är behöriga att behandla personuppgifterna, ska vara ålagda att iaktta sekretess eller lämplig lagstadgad tystnadsplikt,
5. att personuppgiftsbiträdet ska följa de principer som ställs upp i artikel 32 GDPR för upprätthållande av informationssäkerhet,
6. att personuppgiftsbiträdet ska tillse att av personuppgiftsbiträdet anlitat underbiträde ska ha samma skyldigheter som GDPR ställer på personuppgiftsbiträdet,
7. att personuppgiftsbiträdet ska genom lämpliga tekniska och organisatoriska åtgärder vara personuppgiftsansvarige behjälplig vid tillvaratagandet av de registrerades rättigheter enligt kapitel III i GDPR,
8. att personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige vid hantering av eventuella personuppgiftsincidenter och vid upprättande av konsekvensbedömningar i fall då det är tillämpligt,
9. att personuppgiftsansvarige ska vara tillförsäkrad tillgång till all information som krävs för att visa att GDPR:s krav efterlevs, vilket också kan ske genom att personuppgiftsansvarige anlitar revisor för bedömning, samt
10. att personuppgiftsbiträdet genast ska meddela personuppgiftsansvarig om biträdet anser att personuppgiftsansvariges anvisningar eller instruktioner står i strid med tillämplig dataskyddslagstiftning.

Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen, är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter. Genom tillsyn kan IMY kontrollera att GDPR och andra bestämmelser som kompletterar förordningen efterlevs.

Om en verksamhet riskerar bryta mot bestämmelserna i GDPR eller kompletterande regler kan IMY utfärda en *skriftlig varning*. IMY kan sålunda endast utfärda en varning innan en överträdelse har ägt rum. En varning talar om på vilket sätt behandlingen riskerar att strida mot reglerna.

Om en verksamhet bryter mot bestämmelserna i GDPR eller kompletterande regler kan IMY utfärda en *reprimand*. En reprimand är en slags tillrättavisning och är normalt bara aktuell vid mindre överträdelser.

IMY har i vissa situationer även möjlighet att utfärda *föreläggande* mot den som bryter mot GDPR att vidta olika åtgärder, exempelvis att tillgodose den registrerades begäran att få ett registerutdrag. IMY kan också införa en *begränsning* av eller ett *förbud* mot behandling av personuppgifter.

Nästan alla överträdelser av bestämmelserna i GDPR kan leda till *administrativa sanktionsavgifter*. Vilka överträdelser det rör sig om anges i GDPR och den kompletterande dataskyddslagstiftningen.

Ett exempel på när IMY kan besluta om att ta ut en sanktionsavgift är om behandlingen strider mot de grundläggande principerna i GDPR, såsom kravet på att personuppgifter bara får samlas in för berättigade ändamål. Ett annat exempel är om den registrerade inte får sina rättigheter tillgodosedda, såsom rätten till information och rättelse.

INTER:s affärsadvokater är specialister inom avtalsrelaterad juridik och har stor erfarenhet av att upprätta och tolka avtal. INTER:s affärsadvokater företräder regelbundet klienter

vid upprättande av personuppgiftsbiträdesavtal.