

Regionförvaltningsverkets meddelande till förmedlingsrörelser om EU:s allmänna dataskyddsförordning

EU:s allmänna dataskyddsförordning (General Data Protection Regulation, GDPR 2016/679) kommer att träda i kraft i alla EU-länder den 25 maj 2018. Utgångspunkten är att förordningen ska tillämpas på all hantering av personuppgifter. Den nationella dataskyddslagen som kommer att komplettera och precisera förordningen är avsedd att träda i kraft samma dag som förordningen (regeringens proposition RP 9/2018 rd). Den nya förordningen ska alltid tillämpas då personuppgifter hanteras i företagets datasystem. Förordningen tillämpas också på manuell hantering av personuppgifter t.ex. i ett kundkartotek eller en del av det.

Förordningen ålägger företag att dokumentera sina dataskyddsåtgärder och sin dataskyddspraxis genom att upprätta en skriftlig beskrivning av hur de hanterar personuppgifter.

Företaget måste också bedöma om det behöver utse en dataskyddsansvarig. Man behöver också på nytt bedöma om arkiv behövs. Enligt förordningen ska det finnas verkliga skäl till att ha arkiv.

För hanteringen av personuppgifter måste det alltid finnas något skäl som finns angivet i förordningen. Dessa skäl är lagstadgad skyldighet, samtycke, avtal och berättigat intresse. Hantering och förvaring av personuppgifter från t.ex. ett kundförhållande kan basera sig på avtal eller berättigat intresse.

Förvaring av handlingar som rör ett uppdrag

Lagen ålägger förmedlingsrörelser att förvara de handlingar som rör ett uppdrag i fem år från det att uppdragsavtalet upphörde (lagen om fastighetsförmedlingsrörelser och rörelser för förmedling av hyreslägenheter och hyreslokaler 15.12.2000/1075 10 §). Utgångspunkten är att alla handlingar som direkt eller indirekt rör uppdraget ska sparas. Allt som man kommer överens om ska dokumenteras så att det är möjligt att i efterhand visa vad som överenskommits. Det är också viktigt att spara e-postmeddelanden, t.ex. ska anbudsförfarandet finnas i skriftligt pappersformat eller i e-postformat. Dataskyddsförordningen poängterar dokumentering och att det är nödvändigt att spara uppgifter.

Efter förvaringstiden på fem år som lagen kräver bör man på nytt bedöma om det är nödvändigt att spara handlingarna. Materialet som sparas kan t.ex. anonymiseras.

Kundregister

Ett företag som har ett kundregister ska på begäran kunna visa att företaget beaktar dataskyddsbestämmelserna i planeringen och genomförandet av sin verksamhet. Detta förutsätter att det finns anvisningar om åtkomstkontroll, hantering och skydd avseende personuppgifter och anvisningar om personuppgifternas livscykel och att anvisningarna följs när uppgifterna hanteras.

Om en utomstående serviceproducent hanterar uppgifter som finns i företagets kundregister måste företaget upprätta ett skriftligt avtal om hanteringen av personuppgifter med serviceproducenten.

Om syftet med hanteringen av personuppgifterna är att sköta ett kundförhållande är det vanligtvis nödvändigt att spara personuppgifterna under hela kundförhållandet. När kundförhållandet tar slut bör den registeransvarige kontrollera om personuppgifterna fortfarande behövs eller om de kan raderas.

Efter att ett kundförhållande har upphört kan det vara nödvändigt att spara kunduppgifterna en begränsad tid för t.ex. fakturering, indrivning, rättsliga åtgärder eller reklamationer. Det är också möjligt att spara uppgifterna längre om uppgifterna sparas i sådan form att den registrerade inte längre kan identifieras. Om man t.ex. vill spara vissa uppgifter för statistikföring är detta möjligt om personuppgifterna raderas och det inte längre går att koppla uppgifterna till en viss person.

Hantering av personbeteckningar

Behandlingen av personbeteckningar regleras för närvarande utifrån 13 § i personuppgiftslagen (24.2.1999/53). I lagutkastet till den nya dataskyddslagen är grunderna för hanteringen av personbeteckningar i fortsättningen de samma som för närvarande. Om företaget redan tidigare har försäkrat sig om att det hanterar personbeteckningar på det sätt som anges i personuppgiftslagen behöver företaget inte ändra sina rutiner i och med dataskyddsförordningen.

Förvaring av arbetsavtal

En arbetsgivare är med stöd av 6 kap. 7 § i arbetsavtalslagen skyldig att ge arbetstagaren ett arbetsintyg, om intyget begärs inom tio år från det att anställningsförhållandet upphörde. Detta innebär alltså att en arbetsgivare ska spara uppgifter om längden på anställdas anställningsförhållanden och vilka arbetsuppgifter de hade i tio år. Efter tio år finns det inte längre några grunder för att spara gamla arbetsavtal.

Personuppgiftsansvarig och personuppgiftsbiträde

Företagets roll i hanteringen av personuppgifter avgör vilka skyldigheter och vilket ansvar hanteringen medför. Om företaget fattar beslut om vilka personuppgifter som ska samlas in och för vilket syfte de ska användas räknas företaget som personuppgiftsansvarig. Ett personuppgiftsbiträde å andra sidan hanterar personuppgifter för den personuppgiftsansvariges räkning. Ofta kan ett företag ha olika roller i olika avtalsförhållanden och olika situationer. Företagets roll måste därför bedömas från fall till fall.

T.ex. ett företag som erbjuder IT-tjänster kan vara personuppgiftsansvarig när företaget hanterar personuppgifter om sina egna kunder. Samtidigt kan samma företag ha rollen som personuppgiftsbiträde när det hanterar personuppgifterna om sina kunders slutkunder, alltså när företaget hanterar slutkundernas personuppgifter på det sätt som kunden har bestämt och för kundens räkning.

Dataskyddsverket som tillsynsmyndighet

Enligt utkastet till dataskyddslag ska det bildas **ett nytt dataskyddsverk som kommer att fungera som tillsynsmyndighet**. Verket ska ledas av dataombudsmannen. Regionförvaltningsverket övervakar inte att dataskyddsförordningen följs. Tillsynsmyndigheten har omfattande utredningsbefogenheter för att utföra sina uppgifter. Sanktionerna är olika varningar, anmärkningar och förelägganden.

Till de mest betydande påföljderna hör att påföra administrativa böter eller att tillfälligt eller permanent begränsa hanteringen av personuppgifter. Den administrativa påföljdsavgiften kan vara 20 miljoner euro eller fyra procent av omsättningen, beroende på vilken av dessa som är större.

Tilläggsinformation:

Dataombudsmannens anvisningar

<http://www.tietosuoja.fi/sv/index/euntietosuojaudistus.html>

Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning RP 9/2918 rd
<https://www.finlex.fi/sv/esitykset/he/2018/20180009.pdf>

Dataombudsmannens byrå
Växel: 029 56 66700
Byrås e-post: tietosuoja@om.fi