EUROPEISKA ERV OCH DEN NYA DATASKYDDSFÖRORDNINGEN, GDPR.

Information till våra företagskunder och samarbetspartners

Den 25 maj 2018 träder EU:s nya dataskyddsförordning, GDPR, i kraft. Vi har fått många frågor om vilka förberedelser vi har vidtagit med anledning av detta, framför allt eftersom vi som försäkringsbolag behandlar relativt stora mängder personuppgifter, som t.ex. namn, personnummer, bostadsadress och i vissa fall även uppgifter om hälsa.

Därför har vi tagit fram ett antal frågor och svar vi hoppas ska vara till hjälp. Om du inte hittar svar på din fråga här är du alltid välkommen att kontakta oss för mer information.

1. Hur förbereder sig Europeiska ERV för GDPR?

Vi tar dataskyddsfrågor på stort allvar och har sedan ett år tillbaka drivit ett särskilt GDPR-projekt som bland annat innefattat följande:

- identifiera och implementera nödvändiga åtgärder (”s.k. gapanalys”)
- arbeta fram nya interna processer och rutiner för regelefterlevnad
- gå igenom befintliga avtal
- utbilda hela organisationen
- instifta en ny kontrollfunktion, Dataskyddsombudet (*eng.* Data Protection Officer), som kontrollerar att verksamheten följer de lagar och förordningar som gäller inom dataskyddsområdet

Vi har granskat alla system och databaser där personuppgifter behandlas utifrån ett GDPR-perspektiv för att identifiera eventuella behov av förbättringsåtgärder. Vi har även gått igenom våra samarbeten med andra företag som behandlar personuppgifter för vår räkning, till exempel våra internationella assistansorganisationer, för att säkerställa att de lever upp till de nya dataskyddsreglerna.

2. Hur arbetar Europeiska ERV med GDPR:s informationssäkerhetskrav?

Med anledning av de nya dataskyddsreglerna har vi uppdaterat vår interna säkerhetspolicy. Dokumentet innehåller bland annat regler om fysisk säkerhet, säker överföring av data, säkerhetskopiering, behörighetsstyrning m.m. Detta arbete har gjorts i enlighet med internationella säkerhetsstandarder, såsom ISO 27002 och ISIS.

3. Hur länge sparar Europeiska ERV personuppgifter?

Vi sparar personuppgifter så länge det är nödvändigt, beroende på anledning till varför vi samlade in uppgifterna. Gäller det personuppgifter som vi är skyldiga att spara under viss tid så följer vi lagens föreskrifter. Till exempel måste försäkringsdokumentation sparas i ett tiotal år p.g.a. försäkringsavtalslagens regler om försäkringspreskription.

4. Är Europeiska ERV personuppgiftsansvarig eller personuppgiftsbiträde?

Europeiska ERV är personuppgiftsansvarig. Det gäller alla personuppgifter som behandlas inom ramen för vår verksamhet. Ett personuppgiftsbiträde får bara behandla uppgifter på instruktion av den personuppgiftsansvarige – och för dennes räkning – varför vi som försäkringsbolag inte kan vara personuppgiftsbiträde och samtidigt leva upp till de regler som gäller för vår verksamhet.

För att driva försäkringsverksamhet måste man ha tillstånd och regleringen kring detta är väldigt kontrollerad. Som försäkringsbolag är vi enligt lag skyldig att behandla personuppgifter på olika sätt. Bland annat är vi skyldiga att bevara en försäkringstagares personuppgifter under en viss tid även efter det att försäkringsavtalet upphört, eftersom en försäkringstagare har rätt att anmäla en skada i upp till 10 år från det datum då anspråket först kunde göras

gällande. Naturligtvis behandlar vi enbart personuppgifter i den utsträckning som krävs för att vi ska kunna uppfylla våra åtaganden gentemot såväl försäkringstagare som tillsynsmyndighet.

5. Var lagrar Europeiska ERV personuppgifter?

All data sparas i serverhallar i Sverige och EU/EES. Om personuppgifter lämnas ut till ett personuppgiftsbiträde, får personuppgifterna endast lagras på ett kontrollerat sätt och på våra instruktioner.

6. Vilka ytterligare åtgärder vidtar Europeiska ERV för att säkerställa efterlevnad av GDPR?

För oss på Europeiska ERV är dataskyddsfrågor inget nytt och ständigt aktuellt. I samband med att GDPR nu snart träder i kraft har vi därför vidtagit flera åtgärder, bland annat:

- nya processer för att säkerställa att de registrerades rättigheter upprätthålls, bland annat rätten till information, rätten till insyn, rätten till portabilitet, rätten till rättelse och rätten till radering
- genomgång av avtal med personuppgiftsbiträden för att säkerställa att de följer dataskyddsförordningens krav
- se till att all personuppgiftsbehandling har en laglig grund
- avsätta tillräckliga resurser för vårt arbete med korrekt personuppgiftshantering och för dataskyddsombudets interna tillsyn
- sätta rutiner för att anmäla, dokumentera och åtgärda eventuella personuppgiftsincidenter
- uppdatering av vår personuppgiftspolicy, våra försäkringsvillkor och andra försäkringshandlingar