

Politik for behandling og beskyttelse af personoplysninger. Maj 2018

ARGO
Håndværkervej 70
4000 Roskilde

+45 46 34 75 00
info@argo.dk

www.argo.dk
CVR nr. 13507406

Nye EU-regler beskytter dine personlige oplysninger endnu bedre – det samme gør ARGO I/S

Hos ARGO passer vi godt på de personlige oplysninger, som ARGO modtager om dig.

EU har besluttet at skærpe kravene til, hvordan virksomheder bruger og behandler personlige oplysninger. Derfor har ARGO gennemgået håndteringen af oplysninger om kunder (personer og enkeltmandsfirmaer), brugere og ansatte, således at ARGO lever op til de nye regler. Reglerne gælder for alle virksomheder – private som offentlige. ARGOs politik om personlige oplysninger er uddybet i det følgende:

Hvad er EU-persondataforordningen?

EU-persondataforordningen stiller krav til virksomheder om:

- at registrering og behandling af personoplysninger sker i overensstemmelse med udtrykkeligt angivne og legitime formål,
- at behandlingen skal være rimelig og gennemsigtig i forhold til personen, og
- at såvel virksomheden som dens databehandlere er underlagt dokumentationskrav i forhold til opfyldelse af forordningen.

Derudover giver EU-forordningen også større kontrol til personen i form af flere rettigheder, ligesom håndhævelse af reglerne er forbedret ved at stille krav om udpegelse af en databeskyttelsesrådgiver (DPO) i særlige tilfælde og underretning om brud på persondatasikkerheden til tilsynsmyndigheden og personen. Datatilsynet kan desuden udstede administrative bøder til både virksomheden og dens databehandlere.

Ifølge EU-forordningen er virksomheden ansvarlig for at implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger, baseret på en fortegnelse over behandlingsaktiviteter, en dokumenteret risikovurdering og databeskyttelsespolitikker. Dette sker bl.a. for at sikre og påvise over for tilsynsmyndigheden, at virksomhedens behandling af personoplysninger er i overensstemmelse med EU-forordningen. Virksomheden er desuden forpligtet til at designe systemer og opsætte systemers standardindstillinger, herunder indføre interne procedurer, således at de understøtter principperne for databeskyttelse.

Overlader virksomheden behandlingen af personoplysninger til en databehandler, stiller EU-forordningen krav om, at databehandleren stiller fornødne garantier for at have indført passende tekniske og organisatoriske foranstaltninger, der opfylder kravene i forordningen, og at vilkårene for databehandlingen fremgår af en skriftlig kontrakt mellem virksomheden og databehandleren.

Persondatapolitik

Politik for behandling og beskyttelse af personoplysninger er gældende for ARGO.

Politikken skal hjælpe til at sikre og dokumentere, at ARGO beskytter sine personoplysninger i overensstemmelse med reglerne for behandling af personoplysninger. Politikken bidrager desuden til, at ARGO oplyser om behandlingen og brugen af de registrerede personoplysninger.

Politikken gennemgås hvert år.

Fortegnelse over behandlingen af personoplysninger

ARGO behandler personoplysninger om:

- Medarbejdere
- Kunder
- Leverandører

ARGO har udarbejdet en fortegnelse over behandlingen af personoplysninger. Fortegnelsen giver overblik over de behandlinger, som ARGO er ansvarlig for.

Personoplysningerne er en forudsætning for, at ARGO kan indgå ansættelses-, kunde- og leverandørkontrakter.

Behandlingens formål og lovlighed

Formålet med denne politik er at sikre, at ARGO værner om personoplysningernes sikkerhed og følger den til enhver tid gældende lovgivning med henblik på at beskytte alle personoplysninger som ARGO er i besiddelse af.

Personoplysningerne behandles og arkiveres i forbindelse med:

- Personaleadministration, herunder rekruttering, ansættelse, fratrædelse og udbetaling af løn
- Stamdata for kunder samt ordrer og salg
- Stamdata for leverandører samt rekvisitioner og køb
- Kontrakter

ARGO vil sikre, at alle behandlinger af personoplysninger finder sted i overensstemmelse med principperne om lovlig behandling af personoplysninger og ARGO vil iagttage de vejledninger, som løbende offentliggøres af Datatilsynet samt sikre at medarbejdere modtager relevant træning i behandling af personoplysninger.

ARGO indsamler ikke flere personoplysninger end nødvendigt i forhold til opfyldelse af formålet.

Opbevaring og sletning

ARGO har indført følgende overordnede retningslinjer for opbevaring og sletning af personoplysninger:

- Personoplysninger opbevares i fysiske mapper i aflåst skab.
- Personoplysninger opbevares i it-systemer og på serverdrev.
- Personoplysninger opbevares ikke længere, end hvad der er nødvendigt for formålet med behandlingen.
- Personoplysninger for medarbejdere slettes fem år efter endt ansættelse, og personoplysninger om ansøgere slettes efter seks måneder.

Datasikkerhed

ARGO er ansvarlig for, at der udføres en overordnet risikovurdering på persondataområdet.

Den overordnede risikovurdering skal opdateres mindst en gang årligt og omfatte alle væsentlige områder for persondatabeskyttelse.

Det overordnede risikobillede skal resultere i angivelse af specifikke tiltag som kan implementeres i ARGO for at sikre et tilstrækkeligt sikkerhedsniveau for databeskyttelse. De specifikke tiltag kan både have til formål at undgå, at den pågældende risiko indtræder, og at reducere konsekvenserne af, at risikoen måtte indtræde.

ARGO skal ud fra risikovurderingen gennemføre følgende sikkerhedsforanstaltninger for beskyttelse af personoplysninger:

- Kun medarbejdere, som har et arbejdsbetinget behov for adgang til de registrerede personoplysninger, har adgang hertil enten fysisk eller gennem it-systemer med rettighedsstyring.
- Alle computere har adgangskode og medarbejderne må ikke overlade deres adgangskoder til andre.
- Computere skal have installeret firewall og antivirusprogram, som løbende opdateres.
- Personoplysninger slettes på forsvarlig vis ved udfasning og reparation af it-udstyr.
- USB-nøgler, eksterne harddiske mv. med personoplysninger skal opbevares i aflåst skuffe eller skab.
- Fysiske mapper er placeret på aflåst kontor eller i aflåste skabe.
- Personoplysninger i fysiske mapper slettes ved makulering.
- Alle medarbejdere skal modtage instruktion i, hvad de må gøre med personoplysninger samt, hvordan personoplysninger skal beskyttes.
- Politikker og forretningsgange skal være ajourførte.
- Databehandleraftaler, samtykkeerklæringer og aftalegrundlag skal være ajourførte.
- Instrukser til medarbejdere skal være ajourførte.
- Sletteforanstaltninger skal være ajourførte.

Videregivelse

Personoplysninger om medarbejdere kan blive videregivet til offentlige myndigheder, f.eks. SKAT og pensionsselskaber.

Databehandlere

ARGO benytter udelukkende databehandlere, der stiller de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske sikkerhedsforanstaltninger til opfyldelse af persondatarettens krav.

En forudgående undersøgelse af en ny databehandler indebærer, at der foretages en risikovurdering, som tager hensyn til de risici, som en behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Alle databehandlere underskriver en databehandleraftale forinden behandlingen iværksættes.

Rettigheder

ARGO varetager den registreredes rettigheder, herunder retten til indsigt, tilbagetrækning af samtykke, berigtigelse og sletning og orienterer de registrerede om ARGOs behandlinger af personoplysninger.

Der er desuden et vigtigt fokus for ARGO at sikre overholdelse af alle registrerede personer rettigheder. Alle medarbejdere, der beskæftiger sig med behandling af personoplysninger hos ARGO, skal derfor orienteres om omfanget af de registrerede personers rettigheder samt om hvordan de skal håndtere anmodninger fra de registrerede personer. Dette beskrives i konkrete retningslinjer. Alle registrerede personer har ret til at opnå indsigt i behandling af deres personoplysninger, hvis de anmoder herom.

Registrerede har ligeledes ret til at klage til Datatilsynet.

Brud på persondatasikkerheden

I tilfælde af brud på persondatasikkerheden, anmelder ARGO hurtigst muligt og inden 72 timer bruddet til Datatilsynet. IT-Chefen er ansvarlig for at dette sker. I anmeldelsen beskrives bruddet, hvilke grupper af personer bruddet vedrører og hvilke konsekvenser bruddet kan få for disse personer. Derudover redegøres for hvordan ARGO har eller vil afhjælpe bruddet. I tilfælde, hvor bruddet indebærer en høj risiko for de personer, om hvem ARGO behandler personoplysninger, vil ARGO endvidere underrette disse. ARGO dokumenterer alle brud på persondatasikkerheden.

Politikken ligger på sitet: www.argo.dk/persondatapolitik

Oplysning om persondataforordningen kan hentes på: www.datatilsynet.dk

Roskilde, maj 2018

Johnny Bregnhøj
Økonomi- og IT-chef