DATATILSYNET

Amgros I/S
Dampfærgevej 22
2100 København Ø

Sendt til: amgros@amgros.dk og
cch@amgros.dk

6. april 2016

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2016-42-2911
Sagsbehandler
Morten Tønning
Direkte 3319 3236

Vedrørende anmeldelse af behandlingen "Behandling af ESPD dokumentation"

Amgros I/S har efter persondatalovens[1] § 48 den 7. marts 2016 anmeldt behandlingen "Behandling af ESPD dokumentation" til Datatilsynet. Derved har Amgros I/S samtidig søgt om tilladelse efter lovens § 50, stk. 1, nr. 1.

Der er den 1. april 2016 betalt 2.000 kr. til dækning af gebyr i henhold til persondatalovens § 63, stk. 2, nr. 2.

I den anledning meddeler Datatilsynet hermed

TILLADELSE

til behandlingen
"Behandling af ESPD dokumentation"

Tilladelsen gives på følgende vilkår:

- Behandlingen af oplysningerne skal ske under iagttagelse af de sikkerhedskrav, der fremgår af bilag 1.

Tilladelsen gives endvidere under forudsætning af, at Amgros I/S i øvrigt iagttager persondatalovens regler. Der henvises i den forbindelse til Datatilsynets brev af 1. april 2016.

Ovenstående vilkår er gældende indtil videre. Datatilsynet forbeholder sig ret til senere at tage vilkåret op til revision, hvis der skulle vise sig behov for det.

Anmeldelsen vil snarest blive offentliggjort i fortegnelsen på Datatilsynets hjemmeside.[2]

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[2] www.datatilsynet.dk.

Bemærk, at eventuelle ændringer af de forhold, der er omfattet af anmeldelsen, skal meddeles Datatilsynet i overensstemmelse med persondatalovens § 51. Ændringer kan indberettes via Datatilsynets hjemmeside[3].

Med venlig hilsen

Morten Tønning

Bilag: Krav om datasikkerhed i forbindelse med anmeldelsespligtige behandlinger

[3] www.datatilsynet.dk/blanketter/anmeld-aendring/

Bilag 1

Krav om datasikkerhed i forbindelse med anmeldelsespligtige behandlinger

Persondataloven stiller krav om, at personoplysninger skal behandles sikkerhedsmæssigt forsvarligt.

Det betyder bl.a., at der skal være de nødvendige tekniske og fysiske foranstaltninger imod, at oplysningerne kommer til uvedkommendes kendskab eller misbruges.

I forbindelse med den anmeldte behandling af personoplysninger skal nedenstående specifikke minimumskrav om datasikkerhed iagttages:

1. Beskriv hvordan følsomme personoplysninger beskyttes, og hvordan nedenstående punkter i praksis er implementeret. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. Medarbejdere, der håndterer personoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

3. Personoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

   Når dokumenter (papirer, kartotekskort mv.) med personoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

4. Det skal registreres, hvis der er forgæves forsøg på at få adgang til itsystemer med følsomme personoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

5. Hvis følsomme personoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af følsomme personoplysninger på andre bærbare datamedier.

6. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

7. Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarliges lokaliteter, skal den dataansvarlige fastsætte særlige retningslinjer herfor, så det sikres, at de fastsatte vilkår iagttages.

8. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne. Udtagelige lagringsmedier, sikkerhedskopier af data m.v. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.

9. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

10. Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv.

11. Såfremt der er etableret eller etableres en løsning, hvor der fra et åbent net, f.eks. internettet, er adgang til følsomme personoplysninger via login (f.eks. adgang til at indsende, modtage, søge, læse, ændre, flytte eller slette oplysninger), skal adgangen baseres på et fler-faktor-login, f.eks. NemID's to-faktor-login.

12. Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger. Al transmission af følsomme personoplysninger over åbne net (f.eks. internettet) skal ske i krypteret form.

Inddatamateriale som indeholder personoplysninger

13. Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddatering. Materialet skal opbevares aflåst, når det ikke anvendes, og slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, hvortil det er indsamlet, dog senest efter en af den dataansvarlige fastsat frist. Ved tilintetgørelse skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Uddatamateriale som indeholder personoplysninger

14. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Materialet skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri. Når materialet ikke længere skal anvendes til de formål, som behandlingen varetager, dog senest efter en af den dataansvarlige fastsat frist, skal det slettes eller tilintetgøres.

Autorisation og adgangskontrol

15. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles ved hjælp af edb. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

16. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, samt personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

17. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i punkt 15 og 16. Kontrol heraf skal foretages mindst en gang hvert halve år.

18. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som behandles ved hjælp af edb, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Logning

19. I edb-registre skal der foretages maskinel registrering (logning) af alle anvendelser af følsomme personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes.