Målrettet arbejde med persondataforordningen for

DANSK PLANTAGEFORSIKRING

DANSK PLANTAGEFORSIKRING
Skolestræde 1, 1.
8800 Viborg
www.skovbrand.dk
Tlf.: 86 67 14 44
CVR: 27 09 56 15

Indholdsfortegnelse

Formål

Formålet med dette dokument er at dokumentere, at selskabet overholder kravene til behandling af personoplysninger.

Dansk Plantageforsikring behandler personoplysninger og benytter primært standard it-løsninger til behandlingen. I det følgende dokumenteres persondatabehandlingen samt de tekniske og organisatoriske sikkerhedsforanstaltninger, der er etableret i forbindelse med behandlingen.

Databeskyttelsesrådgiver (DPO)

Set i forhold til de risici der er forbundet med behandlingen samt mængden af personoplysninger, der behandles, vurderedes det, at Dansk Plantageforsikring ikke skal have en databeskyttelsesrådgiver tilknyttet.

Kontaktoplysninger på persondataansvarlig

Dansk Plantageforsikring har udpeget Direktør Gert Stampe som persondataansvarlig for selskabet.

Procedurer i forbindelse med henvendelser fra registrerede

I selskabet håndteres alle henvendelser af det administrative personale. I politikken for persondata, som alle selskabets kunder og ansatte gøres bekendt med på selskabets hjemmeside, er der anført kontaktoplysninger for disse henvendelser.

De registreredes vigtigste rettigheder efter databeskyttelsesforordningen er:

- Retten til at modtage oplysning om behandling af deres personoplysninger (oplysningspligt).
- Retten til at få indsigt i deres personoplysninger.
- Retten til at få urigtige personoplysninger rettet.
- Retten til at få deres personoplysninger slettet.
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring.
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering.
- Retten til at flytte deres personoplysninger (dataportabilitet).

Alle ovenstående rettigheder håndteres manuelt ved henvendelse som anført i selskabets politik for persondata.

Fortegnelser over behandlingsaktiviteter

Skadesforsikring – police og skade - og relaterede aktiviteter

Almindelige personoplysninger, med det formål at kunne gennemføre police- og skadesadministration og i øvrigt leve op til selskabets kontraktlige forpligtelser samt forpligtelser i henhold til forsikringsaftaleloven og bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse samt udførelse af opgaver i relation til police- og skadesadministration.

Kategorier af registrerede

Erhvervskunder inkl. ansatte og private plantageejere.

Kategorier af personoplysninger

- Navn, adresse, telefon, e-mail
- Bankkontooplysninger
- Forsikringssted, herunder matr. nr. og eventuelle kontaktpersoner på plantagen.

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- C5 (Policeadministration og bogføring)
- Microsoft Office pakken (skadesbehandling og korrespondance I Word/Excel/Outlook)

Tidsfrister for sletning / opbevaring

Der er en general tidsfrist for sletning og opbevaring på 20 år for såvel fysiske som elektroniske dokumenter, og dette vurderes forsvarligt, henset til at der kun opbevares almindelige personoplysninger, som for de flestes vedkommende er offentligt tilgængelige.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed vil have en minimal indflydelse på de registreredes rettigheder og frihedsrettigheder. Personoplysningerne, der behandles, vil ofte være offentligt tilgængelige.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring skadesbehandlingen, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskyttes mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring skadesbehandlingen, hvorfor både it-systemer, i særdeleshed backup, og administrative processer i forbindelse med databehandlingen skal beskyttes mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Se sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”.

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke, kendte sårbarheder eller planlagte forbedringer.

Leverandører

Almindelige selskabs- og personoplysninger, med det formål at kunne gennemføre almindelige indkøb m.v. og i øvrigt leve op til selskabets kontraktlige forpligtelser samt forpligtelser i henhold til købeloven og bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse samt udførelse af opgaver i relation til administration af indkøb m.v.

Kategorier af registrerede

Leverandører og i enkelte tilfælde enkelt personer

Kategorier af personoplysninger

- Fulde navn og kontaktoplysninger (herunder e-mail og telefonnummer)
- Adresse
- CVR-nummer
- Bankkontooplysninger

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- Navision (Bogføring)
- Microsoft Office pakken (dokumentation, mails m.v.)

Tidsfrister for sletning / opbevaring

Der er en general tidsfrist for sletning og opbevaring på minimum 5 år for såvel fysiske som elektroniske dokumenter af hensyn til bogføringsloven.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed vil have en minimal indflydelse på de registreredes rettigheder og frihedsrettigheder. Personoplysningerne, der behandles, vil ofte være offentligt tilgængelige.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring betaling af leverandørerne, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskyttes mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring bogføring og betalinger, hvorfor både it-systemer, i særdeleshed backup, og administrative processer i forbindelse med databehandlingen skal beskyttes mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Se sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”.

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke, kendte sårbarheder eller planlagte forbedringer.

Almindelige HR aktiviteter - jobansøgninger

Almindelige personoplysninger med det formål at kunne vurdere kandidater til stillingsopslag.

Grundlag for behandlingen

Samtykke.

Kategorier af registrerede

Ansøgere.

Kategorier af personoplysninger

- Navn, adresse, telefon, e-mail
- CV
- Kan indeholde andre personoplysninger, der fremsendes af den registrerede.

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- Microsoft Office pakken (dokumentation, mails m.v.)

Tidsfrister for sletning / opbevaring

Ingen specifikke tidsfrister. Oplysningerne opbevares dog ikke længere, end de er relevante. Slettes senest når stillingen er besat.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed vil have en minimal indflydelse på de registreredes rettigheder og frihedsrettigheder. Personoplysningerne, der behandles, er i mange tilfælde offentligt tilgængelige – eksempelvis på ansøgerens LinkedIn profil.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative systemer, der benyttes til andre formål, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskyttes mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative systemer, der benyttes til andre formål, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskyttes mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Se sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke kendte sårbarheder eller planlagte forbedringer.

Almindelige HR aktiviteter – ansatte m.v.

Almindelige og muligvis særlige (følsomme) personoplysninger behandles med det formål at kunne opfylde kontraktlige og lovpligtige ansættelsesretlige krav overfor ansatte og bestyrelsesmedlemmer. Herunder også forpligtelser i forhold til bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse.

Kategorier af registrerede

Nuværende og tidligere ansatte samt bestyrelsesmedlemmer.

Kategorier af personoplysninger

- Fulde navn og kontaktoplysninger (herunder privat e-mail og privat telefonnummer)
- Adresse
- CPR-nummer
- Bankkontooplysninger
- Lønsedler
- Historik på trækprocent og skattefradrag
- Pensionsoplysninger (*kan indeholde oplysning om fagforening og overenskomst*)
- Referater fra MUS-samtaler igennem årene
- Disciplinærsager (advarsler m.v.)
- Refusionsopgørelser vedr. barsel og sygdom
- Straffeattest
- Sygehistorik (herunder sygemeldinger)
- Ansøgning og CV.

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- Danløn (lønkørsel)
- Microsoft Office pakken (dokumentation, mails m.v.)

Tidsfrister for sletning / opbevaring

Der er en general tidsfrist for sletning og opbevaring på minimum 5 år for såvel fysiske som elektroniske dokumenter af hensyn til bogføringsloven.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed potentielt kan have negativ indflydelse på de registreredes rettigheder og frihedsrettigheder. Der indføres derfor begrænset adgang samt underskrives tavshedserklæring i ansættelseskontrakter, før der gives adgang.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring lønkørsel m.v., hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring lønkørsel m.v., hvorfor både it-systemer, i særdeleshed backup, og administrative processer i forbindelse med databehandlingen skal beskytte mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Kun administrative medarbejdere har adgang til disse oplysninger. Det er således kun medarbejdere, hvor det er direkte relevant, der har adgang til personoplysninger om deres kolleger. Afgrænsningen gælder som hovedregel alle.

Nogle af oplysningerne opbevares desuden fysisk i aflåst skab eller aflåst arkiv.

Selskabet har vurderet, at det ikke er muligt at implementere falske/opdigtede navne (pseudonymer) i forbindelse med behandlingen af HR-aktiviteterne, når der skal tages hensyn til det aktuelle tekniske niveau og omkostningerne ved implementering.

Se ydermere sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”.

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke kendte sårbarheder eller planlagte forbedringer.

Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger

Selskabet har implementeret følgende organisatoriske og tekniske foranstaltninger generelt:

- Antivirus på alle it-systemer, der behandler personoplysninger.
- Backup af alle it-systemer, der behandler personoplysninger.
- Anvendelse af standardsystemer til behandlingsaktiviteterne.
- Adgangsbegrænsning til personoplysninger, så der kun gives adgang, hvor det er nødvendigt.
- Adgangskontrol med brugernavne og password.
- Databehandleraftaler med leverandører, der behandler personoplysninger på selskabets vegne.
- Tavshedserklæringer med personale, der har behov for at behandle personoplysninger
- Vejledning i sikker behandling af personoplysninger og informationsaktiver for personale med adgang til informationssystemer.
- Gennemførelse af ovenstående risikovurdering og dokumentation af alle systemer, der behandler personoplysninger. Det for at sikre et oplyst grundlag for sikkerhedsniveauet for persondatabehandlingen i selskabet.

Øvrig dokumentation omkring persondata

Selskabet har implementeret følgende politikker m.v. der beskriver arbejdet med og beskyttelsen af persondata:

- Persondatapolitik
- Politik for IT-sikkerhed
- Beredskabsplan

Risikovurdering

#	Trussel	Sandsynlighed	Konsekvens	Samlet risikobillede	Forslag til yderligere sikkerhedstiltag for at imødegå de konstaterede trusler
1	Uautoriseret adgang til it-systemer.	HØJ	LAV	MIDDEL	Undgå at bruge faste passwords. Indfør personlige passwords samt krav til sværhedsgrad og ændring af passwords.
2	At en ansat får uretmæssig adgang til fortrolige data.	LAV	MIDDEL	ACCEPTABEL	Lav løbende kontrol af, at brugerrettigheder er korrekte.
3	Fyrede/fratrådte medarbejdere får ikke frataget adgangsrettigheder.	MIDDEL	MIDDEL	MIDDEL	Implementer procedurer for nedlukning af tidligere medarbejderes it-adgange.
4	Selskabet rammes af et ransomware eller virusangreb.	HØJ	LAV	MIDDEL	Der er Implementeret software, der blokerer trusler proaktivt (før der sker angreb).
5	Samme login og password bruges af flere.	MIDDEL	MIDDEL	MIDDEL	Hvis det ikke kan undgås, må logning gøres mere effektiv.
6	Datamedier, diske eller dokumenter med fortrolige data bliver stjålet/tabt/glemt, f.eks. under transport.	HØJ	LAV	MIDDEL	Indfør værktøjer til at slette data på computeren, hvis den mistes. Efterlad aldrig fortroligt materiale i bil, når den forlades.
7	Misbrug af anden brugers adgang da der ikke logges ud efter brug af systemet.	MIDDEL	MIDDEL	MIDDEL	Indfør automatisk logoff, når computeren har været inaktiv i 5 minutter (pauseskærm).
8	Brugere skifter ikke adgangskode løbende.	HØJ	MIDDEL	MIDDEL	Indfør passwordpolitik, med jævnlig ændring af passwords. Kontroller at den følges.
9	Der er fejl på backup, så data ikke kan genskabes ved datatab eller nedbrud.	LAV	HØJ	MIDDEL	Test jævnligt om backup virker ved at udføre tests af genoprettelse.
10	En medarbejder modtager og aktiverer virus eller trojansk hest via e-mail, browser eller usb-nøgle.	MIDDEL	HØJ	MIDDEL	Indfør sikkerhedsværktøjer, virusscanning af e-mail osv.
11	Brug af privat computer eller brug af firmacomputer til private formål åbner for misbrug eller hacker/virusangreb.	HØJ	MIDDEL	MIDDEL	Undlad at gøre brug af privat computer. Brug computer kun til firmaformål.
12	En ansat lokkes til at udlevere fortrolig/kritisk information til uvedkommende (social engineering).	LAV	MIDDEL	ACCEPTABEL	Informer medarbejdere, om hvad man skal passe på. Lad fortrolighedserklæringer indgå i ansættelsesaftaler/-kontrakter.