DKI Logistics A/S

DKI Logistics interne persondatapolitik

Indhold

1. Forord 3
2. Hvad er personoplysninger? – definitioner 3
   2.1. Personoplysninger 3
   2.2. Følsomme personoplysninger 3
   2.3. Behandling 3
   2.4. Den registrerede 3
   2.5. Den dataansvarlige 4
   2.6. Databehandleren 4
   2.7. Modtager 4
   2.8. Tredjemand 4
   2.9. Samtykke 4
   2.10. Brud på persondatasikkerheden 4
   2.11. Genetiske data 4
   2.12. Biometriske data 4
   2.13. Helbredsoplysninger 4
3. Overordnede retningslinjer 5
4. Virksomhedens oplysningspligt 5
5. Den registreredes rettigheder 6
   5.9. Indsigt 6
   5.10. Berigtigelse 6
   5.11. Sletning 6
6. Ret til begrænsning af behandling 6
7. Underretningspligt 7
8. Ret til indsigelse 7
9. Ret til dataportabilitet 7
10. Procedure ved henvendelse fra den registrerede 7
11. Tekniske foranstaltninger 7
12. Procedurer ved brud på persondatasikkerheden 8

13. Konsekvensanalyse 8
13.1. Relevans af konsekvensanalysen 8
14. Klager 9
15. Spørgsmål 9
16. Tekniske foranstaltninger og procedurer 9
17. Destruktion af data 9
18. Fysisk adgang 9
19. Opbevaring af personoplysninger 9
19.1. Digitale oplysninger 9
19.2. Ansøgninger 10
19.3. Gæster og medlemmer 10
19.4. Opbevaring på USB 10
20. Udveksling af informationer 10
21. E-mail 10
22. Markedsføring/CRM – har vi CRM?? 10
22.1. Direkte markedsføring via fysisk post 11
22.2. Direkte markedsføring via telefon til erhvervsdrivende 11
22.3. Direkte elektronisk markedsføring (e-mail, SMS, Messenger, mv.) 11
23. Arkivering 11
24. Uddannelse 11
25. Manglende overholdelse 11
26. Tvivlsspørgsmål 11

1. Forord

Denne politik henvender sig til alle medarbejdere hos DKI Logistics A/S, der som led i deres arbejde har behandlerpersonoplysninger om kunder, samarbejdspartnere, leverandører og medarbejdere. Politikken omfatter således medarbejdere, som har adgang til personoplysninger til brug for deres arbejde.

Politikken beskriver, hvordan persondata skal behandles i en række typisk forekommende situationer i DKI Logistics. Politikken er udarbejdet som led i DKI Logistics bestræbelser på at overholde gældende lovgivning, herunder EU-forordningen om persondata (herefter kaldet "GDPR") samt databeskyttelsesloven, der forventes vedtaget af Folketinget omkring 1. maj 2018.

Politikken omfatter indledningsvis en beskrivelse af de gældende regler og dernæst en nærmere beskrivelse af de væsentligste forhold, du skal være opmærksom på i din hverdag hos DKI Logistics.

Der er på følgende sider i denne politik et afsnit med definitioner af de væsentligste begreber i persondataforordningen og persondataloven.

2. Hvad er personoplysninger? – definitioner

GDPR indeholder en række vigtige definitioner, som her omtales.

2.1. Personoplysninger

Personoplysninger er oplysninger, som vedrører en identificeret eller identificerbar fysisk person (den registrerede). Det vil sige, at man enten umiddelbart ud fra oplysningerne eller via andre tilgængelige oplysninger kan knytte oplysningerne til en bestemt fysisk person.

2.2. Følsomme personoplysninger

Følsomme personoplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

2.3. Behandling

Behandling af persondata er omfattet af persondatalovgivningen, uanset om det sker elektronisk eller manuelt som led i en systematisk behandling. Ved behandling forstås både indsamling, registrering, systematisering, søgning, bearbejdning, opbevaring, videregivelse og sletning af personoplysninger.

Både elektronisk lagrede oplysninger, og oplysninger, der er udskrevet på papir, er omfattet af reglerne (undtaget er alene løsrevne papirbaserede oplysninger, f.eks. håndskrevne notater, der ikke indgår i en systematisk behandling). Når du har en pligt til at slette personoplysninger, er det vigtigt, at der både sker sletning af de elektronisk lagrede oplysninger og de der er udskrevet på papir – disse skal makuleres.

2.4. Den registrerede

Den registrerede er den fysiske person, oplysningerne vedrører.

2.5. Den dataansvarlige

Den dataansvarlige er den, der bestemmer formålene med behandlingen samt midlerne hertil, herunder hvilke oplysninger, der skal indsamles samt hvilke (it)-værktøjer der skal anvendes til at behandle disse.

2.6. Databehandleren

Der kan være antaget en databehandler af den dataansvarlige til at foretage en behandling af persondata på den dataansvarliges vegne og efter dennes instruks.

2.7. Modtager

Modtageren er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, uanset om det er en tredjemand eller ej.

2.8. Tredjemand

Tredjemand er en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges, der er beføjet til at behandle personoplysninger.

2.9. Samtykke

Samtykke fra den registrerede er enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.

2.10. Brud på persondatasikkerheden

Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

2.11. Genetiske data

Genetisk data er personoplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om den fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende fysiske person.

2.12. Biometriske data

Biometriske data er personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger.

2.13. Helbredsoplysninger

Helbredsoplysning er personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand.

3. Overordnede retningslinjer

Med henblik på at opfylde persondataloven samt persondataforordningen, er det væsentligt, at der alene indhentes nødvendige personoplysninger på såvel kunder/gæster, samarbejdspartnere som medarbejdere. De indhentede oplysninger bør ikke opbevares længere end nødvendigt.

Det betyder også, at det i hvert enkelt tilfælde skal vurderes, hvorvidt det er nødvendigt, at alle medarbejdere i virksomheden har adgang til de indhentede personoplysninger, herunder om det er hensigtsmæssigt at foretage en begrænsning af adgangen hertil.

Samtidig skal det i forbindelse med indhentelse af personoplysningerne vurderes, hvor længe det er nødvendigt at opbevare oplysningerne, således at oplysningerne ikke opbevares i længere tid, end det er nødvendigt for opfyldelse af det formål, de er indhentet for.

I forbindelse med ansættelse af medarbejdere samt i forbindelse med oprettelse af disse i relevante systemer, skal der ikke indhentes et samtykke fra de pågældende. Såfremt der skal indhentes yderligere personoplysninger, er det nødvendigt, at der indhentes samtykke inden oplysningerne, indhentes og behandles. I forbindelse med indhentelse af samtykket, er det nødvendigt, at det præcist angives, hvad formålet er med behandling af personoplysningerne – altså hvorfor ønsker vi at få f.eks. cpr.nr., pasoplysninger eller lignende.

4. Virksomhedens oplysningspligt

Virksomheden skal som dataansvarlig og databehandler altid give følgende oplysninger til den registrerede forinden personoplysningerne indhentes og behandles.

- Virksomhedens identitet og kontaktoplysninger.
- Kontaktoplysninger på en eventuel databeskyttelsesrådgiver.
- Hvad er formålet med behandlingen?
- De berørte kategorier af personoplysninger.
- De modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til.
- Hvor længe oplysningerne bliver opbevaret eller alternativet, hvilket kriterier der lægges til grund for opbevaringstiden.
- På hvilket grundlag behandlingen af personoplysninger foretages.
- Retten til at klage til Datatilsynet, jfr. nærmere nedenfor.
- Hvorfra personoplysningerne stammer, hvis de altså ikke er indsamlet fra den registrerede selv.
- Hvorvidt den registreredes persondata overføres til tredjelande eller en international organisation.
- Retten til indsigt.
- Retten til at bede om berigtigelse eller sletning af personoplysninger eller begrænsning af behandlingen heraf samt retten til at gøre indsigelse mod en sådan behandling.

- Retten til dataportabilitet.

For alle medarbejdere i virksomheden, gælder det, at de for at kunne udføre deres hverv er oprettet i forskellige systemer. Fælles for disse er at kun navn og firmamailadresse fremgår.

5. Den registreredes rettigheder

5.9. Indsigt

Den registrerede har ret til at få indsigt i, hvorvidt der behandles personoplysninger vedrørende den pågældende. Derudover har den registrerede ret til at få adgang til de registrerede oplysninger om sig selv.

5.10. Berigtigelse

Den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget. Dette skal ske uden unødig forsinkelse, dog senest 7 dage efter henvendelsen er modtaget., jfr. nedenfor om proceduren ved en sådan henvendelse.

5.11. Sletning af personoplysninger

Den registrerede har ret til at få personoplysninger om sig selv slettet;

- Hvis personoplysningerne ikke længere er nødvendige for at opfylde de formål, hvortil de er indsamlet eller på anden vis behandlet.
- Såfremt den registrerede trækker sit samtykke tilbage.
- Såfremt den registrerede gør indsigelse mod behandlingen af personoplysningerne.
- Såfremt den registreredes personoplysninger er blevet behandlet ulovligt, og/eller
- Såfremt personoplysningerne skal slettes for at overholde af en retlig forpligtelse, som vi måtte være underlagt.

6. Ret til begrænsning af behandling

Den registrerede har ret til at få begrænset behandlingen af de personoplysninger, som vi opbevarer og behandler vedrørende den registrerede

- Hvis rigtigheden af personoplysningerne bestrides – dette gælder i perioden indtil, at vi har undersøgt, hvorvidt personoplysningerne er korrekte.
- Hvis behandlingen er ulovlig og den registrerede modsætter sig sletning af personoplysninger og i stedet anmoder om at anvendelsen heraf sker i begrænset omfang.
- Hvis vi ikke længere har brug for personoplysningerne til behandling, men at de er nødvendige for at et retskrav kan fastlægges, gøres gældende eller forsvares, og
- Hvis den registrerede har gjort indsigelse mod behandlingen – i perioden mens det kontrolleres, om vi har legitime interesser til at behandle personoplysningerne, der går forud for den registrerede legitime interesser.

7. Underretningspligt

Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling.

Virksomheden er forpligtet til at underrette enhver modtager af den registreredes personoplysninger, herunder modparter, retten mv., om enhver berigtigelse eller sletning af eller begrænsning, medmindre dette viser sig umuligt eller uforholdsmæssigt vanskeligt.

Virksomheden skal oplyse den registrerede om disse modtagere, hvis den registrerede måtte bede herom.

8. Ret til indsigelse

Den registrerede har ret til at gøre indsigelser mod vores behandling af den registreredes personoplysninger.

Såfremt der måtte komme indsigelser fra den registrerede, skal vi undersøge, hvorvidt vi fortsat har legitime grunde til behandlingen, der går forud for den registreredes rettigheder. Indtil dette er afklaret, må vi ikke behandle eller bruge personoplysningerne.

9. Ret til dataportabilitet

Den registrerede har ret til at modtage personoplysninger om sig selv i et almindeligt anvendt og maskinlæsbart format eller få disse oplysninger videregivet til en anden dataansvarlig, hvis behandlingen er baseret på et samtykke eller på en kontrakt eller behandlingen foretages automatisk.

10. Procedure ved henvendelse fra den registrerede

Enhver henvendelse fra en registreret vedrørende

- Indsigt
- Berigtigelse
- Sletning
- Begrænsning
- Enhver anden indsigelse vedrørende vore behandling af persondata eller
- Dataportabilitet

skal videregives til den dataansvarlige, som står for håndteringen af alle henvendelser.

Der henvises til **"Anmeldelsesformular til myndigheder ved kompromittering af persondata", "Anmodning om ændringer af persondata", "Informationsproces når persondata er blevet kompromitteret"**

11. Tekniske foranstaltninger

Med henblik på at opnå en passende beskyttelse af personoplysningerne, implementeres passende

tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne kun opbevares, behandles og videregives i nødvendigt omfang. Derudover sikres det, at det ikke er muligt for uvedkommende at få adgang til personoplysningerne. Der henvises til **" IT-sikkerhedspolitik".**

12. Procedurer ved brud på persondatasikkerheden

Der refereres til Procedure **"Informationsproces når persondata er blevet kompromitteret".**

13. Konsekvensanalyse

Såfremt virksomheden får nye it-systemer eller anden ny teknologi (dette gælder ikke nuværende systemer) til behandling af personoplysninger og der i den forbindelse vurderes at være en høj risiko for, at disse oplysninger videregår til tredjemand, eller der på anden vis måtte være en risiko for, at andre kan få uberettiget adgang til personoplysningerne, skal virksomheden udarbejde en konsekvensanalyse. Dette skal ske forud for behandlingen af personoplysningerne.

13.1. Relevans af konsekvensanalysen

Konsekvensanalysen er navnlig relevant i det tilfælde,

- Hvor der foretages en systematisk og omfattende vurdering af personlige forhold, der er baseret på automatisk behandling.
- Hvor behandlingen i stort omfang omfatter særlige personoplysninger, herunder race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Analysen skal mindst omfatte:

- En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene ved behandlingen.
- En vurdering af om behandlingsaktiviteterne er nødvendige og står rimeligt i forhold til formålene.
- En vurdering af risiciene for de registreredes rettigheder.
- En beskrivelse af de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som sikrer beskyttelse af personoplysninger.

Forinden der sker behandling af personoplysninger med en ny teknologi, skal virksomheden kontakte Datatilsynet, såfremt konsekvensanalysen viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af os for at begrænse denne risiko.

I forbindelse med henvendelse til Datatilsynet, skal der indgives følgende oplysninger.

- Ansvarsområderne for den dataansvarlige og databehandleren, der involveret i behandlingen.

- Den planlagte behandlings formål og hjælpemidler.
- Foranstaltninger og garantier til beskyttelse af de registreredes rettigheder og frihedsrettigheder.
- En evt. databeskyttelsesrådgiverens kontaktoplysninger.
- Konsekvensanalyse vedrørende databeskyttelse samt
- Andre relevante oplysninger, som Datatilsynet måtte ønske.

14. Klager

Der er mulighed for at klage over behandlingen af personoplysninger. Klage indgives til Datatilsynet, Borgergade 28, 5, 1300 København K, dt@datatilsynet.dk.

15. Spørgsmål

Eventuelle spørgsmål vedrørende ovenstående kan rettes til den dataansvarlige i virksomheden.

16. Tekniske foranstaltninger og procedurer

Der henvises til **"IT-sikkerhedspolitik"** og de tilhørende respektive procedurer for detaljeret beskrivelse af tekniske foranstaltninger og procedurer.

17. Destruktion af data

Når der ikke længere er behov for at opbevare persondata, skal de slettes. Det er den enkelte leder/medarbejder, der har ansvaret for, at persondata ikke opbevares længere end det er nødvendigt.

Fysiske dokumenter indeholdende persondata er beskrevet i **"Slettepolitikken for DKI Logistics A/S"**

Såfremt et medie (f.eks. computere, telefoner, USB-nøgler mv), som har indeholdt data, skal fjernes eller destrueres, skal virksomheden sørge for, at dataene er slettet forsvarligt på det pågældende medie, således at det ikke er muligt på anden vis at opnå adgang til den slettede data.

18. Fysisk adgang

Det kræver en nøglebrik, at få adgang til virksomhedens kontorer. Denne nøglebrik må ikke videregives til tredjemand. Nøglebrikken afleveres, når en medarbejder fratræder.

19. Opbevaring af personoplysninger

Fysisk opbevaring af materiale, der indeholder persondata opbevares aflåst, når det ikke bruges og er kun tilgængeligt for betroede medarbejdere. Det fysiske materiale destrueres forsvarligt, når formålet med opbevaringen ophører.

19.1. Digitale oplysninger

Digitale oplysninger om medarbejdere opbevares således, at det alene er de(n) relevante medarbejder, som har adgang til oplysningerne.

19.2. Ansøgninger
Ansøgninger, herunder CV og karakterer mv., fra medarbejdere, som ikke opnår ansættelse, skal slettes efter ansættelsesprocessen er gennemført. Dette gælder dog ikke, hvis ansøgeren giver tilsagn til, at ansøgning mv. opbevares i en længere periode.

19.3. Gæster
Oplysninger om gæster skal opbevares fortroligt og forsvarligt, således de ikke kan tilgås af uvedkommende. Det er som udgangspunkt kun de relevante respektive medarbejdere, der har adgang til oplysningerne.

19.4. Opbevaring på USB
Opbevares personoplysninger på en USB-nøgle eller et lignende medie skal personoplysninger beskyttes ved brug af kryptering.

20. Udveksling af informationer
Personoplysninger skal kun i nødvendigt omfang videregives til tredjemand eller kolleger.

Såfremt oplysningerne videregives til en databehandler uden for virksomheden, skal der indgås en separat aftale med denne databehandler, således at det sikres, at kravene i denne politik / persondataforordning overholdes.

Virksomheden arbejder hen imod en **Clean Desk-politik**. Det betyder, at alle skriveborde og borde hver dag, når arbejdsdagen slutter, skal ryddes for papirer og andre personoplysninger.

21. E-mail
Personoplysninger skal kun i begrænset omfang fremgå af e-mails – det er f.eks. i de færreste tilfælde nødvendigt at nævne cpr.nr. Indeholder en e-mail følsomme personoplysninger skal e-mailen sendes krypteret. Emnefeltet må aldrig indeholde personoplysninger, da dette felt ikke kan krypteres.

Der henvises til ”**E-mail politikken for DKI Logistics”.**

22. Markedsføring
Behandling af personoplysninger som led i markedsføring skal ske i henhold til følgende retningslinjer:

Selve registreringen af en fysisk person med tilhørende kontaktoplysninger med henblik på markedsføring er i orden ud fra en interesseafvejningsregel, men husk oplysningspligten - der skal orienteres om registreringen senest en måned efter registreringen eller ved første kontakt – afhængig af, hvad der kommer først.

Hvad du så kan bruge registreringen til i form af markedsføring, afhænger af, hvilken form for markedsføring du påtænker, jf. nedenfor.

Husk i denne sammenhæng, at såkaldt imagemarkedsføring - herunder udsendelse af nyhedsbreve eller indbydelse til gratis arrangementer – sidestilles med markedsføring, hvor der reklameres for en konkret ydelse.

22.1. Direkte markedsføring via fysisk post

- Vi må gerne sende direkte markedsføring til navngivne personer med fysisk post, forudsat at vi forinden har tjekket, at de pågældende modtagere ikke har tilmeldt sig Robinsonlisten (forbrugere).
- Vi skal respektere, hvis modtagerne frabeder sig at modtage yderligere henvendelser fra os (gælder både forbrugere og erhverv).

22.2. Direkte markedsføring via telefon til erhvervsdrivende

- Vi må gerne ringe og tilbyde en konkret ydelse eller markedsføre os mere generelt overfor erhvervsdrivende.
- Den vi ringer op, kan dog frabede sig yderligere henvendelser, og vi skal i så fald registrere dette, så de ikke bliver ringet op igen.
- Vi må ikke benytte telefonopkald til markedsføring overfor forbrugere.

22.3. Direkte elektronisk markedsføring (e-mail, SMS, Messenger, mv.)

Elektronisk markedsføring må som udgangspunkt kun ske overfor personer efter forudgående samtykke fra modtageren. Er der tidligere indhentet samtykke til udsendelse af nyhedsbreve, er det tilladt at markedsføre tilsvarende produkter og services, hvis den pågældende er gjort opmærksom på, at denne kan modsætte sig markedsføring.

23. Arkivering

Arkivering af persondata er beskrevet i de respektive procedurer og dokumenter for de respektive systemer.

24. Uddannelse

Alle medarbejdere vil løbende og i nødvendigt omfang blive oplyst om it- sikkerhed, beskyttelse af persondata samt kravene i persondataforordningen.

25. Manglende overholdelse

Manglende overholdelse af denne politik kan medføre ansættelsesretlige konsekvenser i form af advarsel, opsigelse eller bortvisning.

26. Tvivlsspørgsmål

Er du i tvivl om forståelse af denne instruks, så spørg den persondataansvarlig, som hos DKI Logistics er Frank Frøkiær.