Persondataforordningen for Leif Koch A/S

Indholdsfortegnelse

Formål

Formålet med dette dokument er at dokumentere, at Leif Koch A/S overholder kravene til behandling af personoplysninger.

Leif Koch A/S behandler i minimalt omfang personoplysninger og benytter primært branche it-løsninger til behandlingen. I det følgende dokumenteres persondatabehandlingen samt de tekniske og organisatoriske sikkerhedsforanstaltninger, der er etableret i forbindelse med behandlingen.

Databeskyttelsesrådgiver (DPO)

Behandling af persondata hos Leif Koch A/S udføres som støttefunktion til kerneaktiviteterne og udgør et minimalt omfang. Set i forhold til de risici der er forbundet med behandlingen, følsomheden, samt mængden af personoplysninger, der behandles, vurderer vi, at Leif Koch A/S ikke skal have en databeskyttelsesrådgiver tilknyttet.

Kontaktoplysninger på persondataansvarlig

Kroeze Andersen, 2041 1253, ka@leifkoch.dk

Procedurer i forbindelse med henvendelser fra registrerede

Hos Leif Koch A/S håndteres alle henvendelser af det administrative personale. I persondatapolitikken, som alle ansatte er bekendt med, har vi anført vores 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 persondatapolitikken.

Fortegnelser over behandlingsaktiviteter

Kundeafregninger og relaterede aktiviteter

Almindelige personoplysninger med det formål at kunne gennemføre forbrugsafregninger og i øvrigt leve op til vandværkets kontraktlige forpligtelser samt forpligtelser i henhold til vandforsyningsloven og bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse samt udførelse af en opgave.

Kategorier af registrerede

Kunder og leverandører.

Kategorier af personoplysninger

- Navn, adresse, telefon, e-mail
- Kundenummer, kursusbevis,

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over data behandlere.

Databehandlere

- PKF Munkebo Vendelev (Revisor / bogholder)

Tidsfrister for sletning / opbevaring

Ingen tidsfrister, dog minimum 5 år 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 forbrugerafregning, 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, 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

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 data behandlere.

Databehandlere

- Ingen

Tidsfrister for sletning / opbevaring

Ingen specifikke tidsfrister. Oplysningerne opbevares dog ikke længere, end de er relevante. Slettes senest 1 måned efter at 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 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 systemer, der benyttes til andre formål, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte 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 mv.

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

- Billede (portræt og fra firmafester)
- 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*)
- Flextidsoplysninger
- Korrespondance udvekslet mellem medarbejderen/organisationschefen/cheferne vedrørende specifikke forhold omkring den pågældende medarbejder
- 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 data behandlere.

Databehandlere

- Dataløn (lønkørsel)

Tidsfrister for sletning / opbevaring

Ingen tidsfrister, dog minimum 5 år 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, 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 mv., 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 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. De grupper der i visse tilfælde har udvidet adgang er: HR-afdelingen, it, bogføring og ledelsen.

Nogle af oplysningerne opbevares desuden fysisk i aflåst skab.

Leif Koch A/S 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

Leif Koch A/S har et ønske om, senest med udgangen af 2019, at supplere de nuværende tekniske og organisatoriske sikkerhedsforanstaltninger med detaljeret logning af adgangen til følsomme personoplysninger.

Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger

Leif Koch A/S 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 branchetypiske it-systemer til behandlingsaktiviteterne.
- Adgangsbegrænsning til personoplysninger, så der kun gives adgang, hvor det er nødvendigt.
- Databehandleraftaler med leverandører, der behandler personoplysninger på Leif Koch A/S´ 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 vandværket

Revisionshistorik

Version	Note	Dato	Redigeret af
V0.9	Første udkast til skabelon	20-11- 2017	Kroeze Andersen
V1.00	Skabelon tilrettet Leif Koch A/S	20-04-2018	Kroeze Andersen

Referencer

Dokumentet indeholder elementer og inspiration fra følgende:

1. Datatilsynets "12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til".
2. EU forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger ("Persondataforordningen").
3. Focus Advokaters "Sådan bliver din virksomhed klar til at håndtere persondata efter de nye regler".
4. Bird & Bird "Guide til den nye Persondataforordning".
5. DI's skabelon for Privacy Impact Assessment.
6. ISO/IEC 27002:2013 Information Technology — Security Techniques — Code of practice for Information Security Management http://www.iso.org
7. Information Security Forum (ISF) – Standard of Good Practice for Information Security (SOGP) 2011 https://www.securityforum.org/