GDPR

Databeskyttelsespolitik

For IGAARD, 37309567, Krogsgårdsvej 54, 5672 Broby, vers. 1.00 af 01.06.2018.

Denne politik er udarbejdet af Jan Igaard med input fra diverse jurister samt EU.

Indledning

IGAARD indsamler og behandler personoplysninger i forbindelse med virksomhedens ledelse og drift.

Disse personoplysninger omfatter kunder, leverandør, kontraktsparter, medarbejdere, samarbejdspartnere. og andre, som virksomheden er eller skal i kontakt med.

Denne databeskyttelsespolitik beskriver, hvordan disse personoplysninger indsamles, behandles, opbevares og slettes for at leve op til virksomhedens standarder og for at sikre, at virksomheden altid overholder den relevante lovgivning.

Formål

Denne databeskyttelsespolitik har til formål at sikre, at IGAARD:

- Overholder databehandling- og beskyttelseslovgivning, herunder Lov om behandling af persondata, nr. 429 af 31/05/2000 (herefter persondataloven) og EUROPAPARLAMENTETS OG - RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 (herefter persondataforordningen).
- Persondataloven
- At beskytte medarbejdere, kunder og samarbejdspartneres rettigheder og frihedsrettigheder.
- At føre en gennemsigtig og åben behandling af persondata, herunder bl.a. hvordan vi indsamler og behandler personoplysninger.
- Begrænse risikoen ved vores indsamling og behandling af persondata samt beskytte organisationen fra risikoen ved en databrud.

Databeskyttelseslovgivning

Persondataloven samt persondataforordningen beskriver hvordan organisationer – herunder IGAARD – må indsamle, behandle og opbevare personoplysninger.

Disse regler gælder for behandlingen af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et fysisk register.

Det fremgår af lovgivningen, at persondata skal behandles på en rimelig og gennemsigtig måde og skal opbevares sikkert og ikke videregives eller offentliggøres uretmæssigt.

Persondataforordningen og de regler og krav, den stiller til en organisation ved behandling af personoplysninger, er understøttet af følgende principper:

- At personoplysninger skal behandles lovligt (have et grundlag), rimeligt (på en måde, at man kan forvente) og gennemsigtigt (man skal være åben og klar omkring, hvordan man håndterer dem).

- Der skal være et konkret og sagligt formål med behandlingen.
- Organisationen skal minimere de data, de indsamler og behandler til de mest relevante og nødvendige.
- Data skal være korrekte og ajourført – eller slettet.
- Persondata må kun opbevares så længe, det er nødvendigt i forhold til formålet
- Persondata skal behandles med integritet og fortrolighed
- Der skal iværksættes tilstrækkelige sikkerhedsforanstaltninger for at beskytte og imødegå brud på og krænkelser af personrettigheder og frihedsrettigheder.
- Data skal ikke videregives eller overdrages til organisationer eller lande uden for E.U., med mindre organisationen eller landet stiller relevante og tilstrækkelige garantier for beskyttelse af persondata.

Personer, risiko og ansvar

Denne databeskyttelsespolitik omfatter

Hovedkontoret IGAARD og fotograf Jan Igaard.

Konsulenter og andre personer eller virksomheder er udfører arbejde for, eller på vegne af IGAARD.

Denne databeskyttelsespolitik omfatter alle data, som virksomheden indsamler og behandler, der vedrører identificerbare personer, selv om disse personoplysninger falder udenfor persondatalovens eller forordningens rækkevidde. Disse oplysninger inkluderer:

Navn på enkelte personer

E-mail adresser

Telefonnummer

Databeskyttelse og risiko

Denne databeskyttelsespolitik har til formål at øge datasikkerheden og forhindre og begrænse risici, f.eks.:

- Brud på fortrolighed. F.eks. at oplysninger videregives eller offentliggøres fejlagtigt eller på en måde, som er uhensigtsmæssig eller ulovlig.
- Manglende gennemsigtighed og valgmuligheder. F.eks. alle fysiske personer skal have kendskab til og frit kunne vælge hvilken personoplysninger, vi behandler om dem.
- Skade på omdømme. F.eks. hvis vores it-systemer bliver hacket og uvedkommende får adgang til vores data og evt. også misbruger disse, hvad enten der var tale om alm. eller personfølsomme oplysninger, erhvervshemmeligheder m.v.

Ansvar

Alle, der arbejder for eller sammen med IGAARD, er ansvarlige for at sikre, at persondata, som de behandler, indsamler og opbevarer behandles lovligt, rimeligt og åbent med integritet og fortrolighed.

Alle, der behandler personoplysninger i egenskab af leder, medarbejder, konsulent, eller databehandler i virksomheden, er ansvarlig for at sikre, at disse data behandles i overensstemmelse med denne politik.

Følgende kategorier af personer har det overordnede ansvar på følgende nøgleområder:

- Generalforsamlingen og Bestyrelsen (eller direktion eller ejer) har det overordnede ansvar for at sikre, at lovgivning omkring behandling af persondata overholdes, og at de nødvendige ressourcer til etablering og vedligeholdelse af relevante sikkerhedsforanstaltninger samt kontrolforanstaltninger, er til rådighed.

Vores dataansvarlige, Jan Igaard er ansvarlig for følgende:

- at holde bestyrelsen og generalforsamlingen opdateret om virksomhedens ansvar i forhold til databehandling og beskyttelse samt risici herved og forhold, der påvirker dette ansvar.
- Gennemgå alle databeskyttelsesprocedurer og relaterede politikker i henhold til en på forhånd aftalt tidsplan.
- Arrangere efteruddannelse samt rådgivning omkring persondatabehandling og beskyttelse for alle ledere, medarbejdere og konsulenter i virksomheden i rimelige intervaller, samt når det er nødvendigt som følge af lovændringer, principale afgørelser m.v.
- Håndtering af spørgsmål om databehandling og beskyttelse fra ledere, medarbejdere og konsulenter
- Håndtering samt svar på anmodninger fra registrerede personer, herunder anmodninger om indsigt, berigtigelse, dataportabilitet, begrænsning, og indsigelse i, af og over de oplysninger, som virksomheden behandler og den måde, de gør det på.
- Forhandling og godkendelse af alle databehandleraftaler, der indgås med personer og virksomheder, der behandler persondata på [indsat virksomhedens navn] vegne.

Vores IT-ansvarlig, Jan Igaard, +45 30443484 er ansvarlig for:

- At sikre, at alle it-systemer, tjenester og udstyr, som anvendes til opbevaring af persondata, opfylder de sikkerhedsstandarder, som kræves for at opretholde en tilstrækkelig sikkerhed i forhold til de risici, der er ved virksomhedens behandlinger af personoplysninger.
- At udføre løbende sikkerhedskontrol af hardware og software for at sikre, at disse fungerer.
- Evaluere og vurdere tredjeparts tjenesteudbydere som virksomheden overvejer at gøre brug af til opbevaring og behandling af persondata, f.eks. cloudløsninger, ekstern server m.v.

Vores marketingansvarlig, Jan Igaard, +45 30443484 er ansvarlig for:

- At godkende privat politikker og anden kommunikation omkring persondatabehandling og beskyttelse i e-mails og breve, på hjemmesiden, de sociale medier m.v.
- At håndtere henvendelser og spørgsmål fra journalister, media outlets eller aviser m.v.
- At sikre, at vores marketingsafdeling og medarbejderne og de marketingsinitiativer, der iværksættes i øvrigt, overholder gældende persondatalovgivning og principper, herunder bl.a. sikring af indhentning af lovpligtige samtykkeerklæringer m.v.

Generelle retningslinjer for medarbejderne

Adgang til personoplysninger begrænses mest muligt til de medarbejdere, der har behov for at kunne behandle en specifik personoplysning for at kunne udføre deres arbejde og løse bestemte opgaver.

Personoplysninger, som en medarbejder bliver fortrolig med i forbindelse med sit arbejde, må ikke deles med andre medarbejdere eller uforstående på uformel vis eller uden samtykke. Såfremt en medarbejder har brug for adgang til nogle specifikke personoplysninger, som man normalt ikke har adgang til for at kunne løse en bestemt arbejdsopgave, kan disse oplysninger rekvireres ved at tage kontakt til sin nærmeste chef.

IGAARD tilbyder efteruddannelse og rådgivning til alle medarbejdere omkring deres ansvar, når de behandler personoplysninger.

Alle medarbejdere skal sikre de personoplysninger som de behandler, ved at tage fornuftige og nødvendige forholdsregler og følge nedenstående retningslinjer.

En medarbejder skal benytte adgangskoder når muligt og må kun anvende dem, der vurderes af systemet til at være stærke. En medarbejders brugernavne og adgangskoder er fortrolige og må ikke deles med andre medarbejdere eller andre uvedkommende. Virksomhedens IT-ansvarlig kan kontaktes, såfremt man har glemt sine adgangskoder, eller man oplever problemer med at logge på it-systemerne.

Personoplysninger må ikke deles med uvedkommende, hverken indenfor organisationen eller udenfor.

Der skal løbende foretages en revision af de personoplysninger, som en medarbejder behandler, herunder indsamler og opbevarer for at sikre, at de er opdateret og ikke forældet, og at de slettes, når de ikke længere er påkrævet; ikke længere tjener et formål eller der er et retsgrundlag herfor.

Hvis en medarbejder er i tvivl om, hvordan de skal agere i forhold til behandling af personoplysninger i forbindelse med deres arbejde, er de forpligtet til at tage kontakt til deres nærmeste chef eller virksomhedens dataansvarlig.

Opbevaring af data

Følgende afsnit beskriver hvordan og hvor vores persondata er opbevaret. Spørgsmål vedrørende opbevaring af persondata kan rettes til vores dataansvarlige.

Når persondata er opbevaret fysisk i papirform, skal disse papirer opbevares et sikkert sted, hvor uautoriserede personer ikke har adgang til dem.

Disse retningslinjer gælder i øvrigt for persondata, som oprindeligt har været opbevaret digitalt, men er printet ud:

Når papir, der indeholder persondata, ikke er i brug, skal de opbevares i en låst skuffe eller skab.

Medarbejdere skal sikre sig, at de ikke efterlader papirer, der indeholder persondata, hvor andre uautoriserede personer har adgang til dem, f.eks. ved en printer, på sit skrivebord,når man er væk m.v.

Papirer, der indeholder persondata, skal makuleres når de ikke længere skal bruges.

Når persondata er opbevaret elektronisk eller på et andet digitalt media, skal de beskyttes mod uautoriserede adgang, utilsigtet sletning og forsøg på hacking.

It-systemer, hvor der opbevares persondata, skal være beskyttet med stærke adgangskoder, der ændres løbende, og som ikke deles med andre medarbejdere.

Hvis persondata er opbevaret på flytbare medier (f.eks. en cd, dvd, usb-pind), skal disse være låst inde i et skab el.lign., når de ikke er i brug.

Persondata må kun opbevares på bestemte drev og servere, der er udpeget af ledelsen i IGAARD og må kun uploades til en af virksomheden godkendt cloud-løsning.

En server, hvor der opbevares persondata, skal være placeret et sikkert sted, væk fra kontorarealet m.v.

Der skal tages en backup af persondata regelmæssigt efter aftalte intervaller, og der skal testes i henhold til virksomhedens standard backup procedurer.

Persondata skal aldrig gemmes direkte på laptops eller andre mobile enheder såsom iPads, smartphones m.v.

Alle servere samt computere, hvor der behandles persondata, skal være beskyttet af godkendte sikkerhedssoftware samt firewall.

Anvendelse af data

Persondata er værdifulde for virksomheden alene, når de kan anvendes til de nævnte formål, men når vi indsamler og behandler persondata, vil der altid være en risiko for, at de behandlede oplysninger tabes, beskadiges eller stjæles.

Når en medarbejder behandler persondata, skal vedkommende altid sørge for at dennes computerskærm er låst, når den er uden opsyn.

Persondata skal ikke deles indbyrdes uden et konkret formål, f.eks. for at kunne løse fælles opgave, og skal ikke sendes via e-mail, m.m. dette sendes krypteret.

Alle persondata skal sendes krypteret, når de sendes elektronisk. Vores IT-afdeling (eller ansvarlige) vil altid kunne bistå medarbejderne i, hvordan man sender persondata til autoriserede eksterne kontakter, herunder samarbejdspartner, kunder og leverandører.

Persondata skal ikke sendes til organisationer eller virksomheder udenfor E.U. m.m. dette er udtrykkeligt aftalt med ledelsen og efter instruks.

Medarbejdere bør ikke gemme persondata på deres arbejdscomputer men skal bruge adgangen til og opdatere i de centralt liggende persondata.

Rigtigheden af data

IGAARD er forpligtet til at sikre, at persondata til enhver tid er korrekte og opdaterede, og at vi tager de nødvendige skridt for at berigtige forkert eller misvisende persondata.

Jo mere betydningsfuld rigtigheden af persondata er for personen, f.eks. når der træffes afgørelse på baggrund heraf, jo større krav stilles der til, at vi som virksomhed overholder denne forpligtelse.

Som medarbejder hos IGAARD, er man, når man behandler persondata i forbindelse med udførelsen af sit arbejde, ansvarlig for at sikre, at de behandlede persondata er korrekte og opdaterede så vidt muligt.

Persondata skal opbevares på så få steder som muligt. Medarbejdere skal undgå at oprette indtil flere datasæt, hvis muligt.

Medarbejdere skal gøre alt, hvad de kan for at sikre, at persondata er opdateret, herunder f.eks. altid få bekræftet rigtigheden, når man tager kontakt til vedkommende.

IGAARD vil altid gøre det nemt for et datasubjekt (den registrerede) til at berigtige og ændre sine personoplysninger hos os, f.eks. via hjemmesiden.

Så snart det konstateres, at bestemte persondata er urigtig eller vildledende skal disse opdateres uden ugrundet ophold og ellers straks. Dette kan f.eks. ske, hvis en person ikke længere kan træffes på det registrerede telefonnummer. I dette tilfælde, skal det registrerede telefonnummer slettes fra databasen.

Anmodninger fra datasubjekts (de registrerede)

Alle fysiske personer, hvorom der i virksomheden er behandlet persondata, har ret til følgende:

Indsigt i de personoplysninger, som vi behandler om vedkommende og formålet hermed.

Indsigt i, hvordan de selv kan få adgang til disse oplysninger

Indsigt i, hvordan de selv kan opdatere og berigtige disse oplysninger

Information om, hvordan virksomheden lever op til sine forpligtelser i henhold til persondataloven og persondataforordningen og at vi kan stille garanti for en tilstrækkelig sikring af data, og at vi har de nødvendige ressourcer og kompetencer hertil.

I øvrigt har en registrerede ret til at anmode om følgende:

- At virksomheden berigtiger forkerte eller misvisende personoplysninger
- At virksomheden videresender vedkommendes personoplysninger til personen selv til eget brug eller til en anden databehandler.
- At gøre indsigelse mod virksomhedens behandling af vedkommendes personoplysninger
- At begrænse virksomhedens behandling af vedkommendes personoplysninger, f.eks. til kun at omfatte evt. reklamation eller tvister
- At klage over vores behandling af deres personoplysninger

Hvis en person kontakter virksomheden med en anmodning om indsigt i disse oplysninger, er der tale om en anmodning fra en registreret.

En anmodning fra en registreret bør fremsendes via e-mail, til vores dataansvarlig Jan Igaard, +45 30443484, jan@igaard.dk

Den dataansvarlig kan fremsende en standard form til den registrerede, men vedkommende er ikke forpligtet til at anvende denne. Den registrerede skal dog gøres opmærksom på, at dette vil kunne fremskynde processen.

Den dataansvarlig skal svare på alle anmodninger fra en registreret så vidt muligt inden for 14 dage fra modtagelse af en anmodning, dog senest indenfor en måned.

Den dataansvarligt skal alle tilfælde, hvor der kan opstå tvivl om en registrerets identitet, bekræfte vedkommendes identitet inden der videregives information til vedkommende.

Offentliggørelse af data

Under visse omstændigheder, skal IGAARD videregive personoplysninger til offentlige myndigheder eller private virksomheder eller organisationer i henhold til lov eller dom. Dette sker oftest uden den registreredes forudgående samtykke eller viden.

Inden den dataansvarlig videregiver disse personoplysninger, som beskrevet, skal vedkommende sikre at anmodningen er lovlig og legitim, herunder efter at have forespurgte ledelsen og / eller søgte juridisk bistand.

Oplysningspligt ved indsamling af persondata

IGAARD vil altid sikre, at fysiske personer, herunder enkeltmandsvirksomheder o. lign. bliver gjort opmærksom på, at man indsamler og behandler oplysninger om dem, samt hvorfor man gøre det. Det er vigtigt at de forstår:

Hvordan og hvorfor vi behandler deres personoplysninger og hvordan de udøver deres individuelle rettigheder.

-|-|-|-|-