Politik

Håndtering af personfølsomme data

Sådan arbejder

Comadan a/s med

Persondataforordningen

Politik

Håndtering af personfølsomme data

Indholdsfortegnelse

Generelt – beslutning og ansvar.

Ledelsen er ansvarlig for, at virksomheden pr. 25 maj 2018 overholder og efterlever Databeskyttelsesforordningen jf. EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ("GDPR") samt gældende national lovgivning og retningslinjer.

Ledelsen har besluttet, at virksomheden skal udarbejde den påkrævede dokumentation herunder en databeskyttelsespolitik inklusiv alle relevante procesbeskrivelser for virksomhedens behandling af personoplysninger for at sikre, at virksomheden lever op til Databeskyttelsesforordningen herunder forordningens dokumentationskrav.

Virksomheden er dataansvarlig og bestræber sig på, at opretholde og fortsætte med at opbygge en databeskyttelses- og privatlivskultur for at beskytte alle de personoplysninger, der indsamles og behandles i virksomheden.

Behandlingen af personoplysninger er som udgangspunkt relateret til virksomhedens egne medarbejdere, men omhandler også behandling af personoplysninger relateret til virksomhedens forretningsaktiviteter. Denne politik beskriver således de regler og retningslinjer, som virksomheden har bestemt, skal benyttes ved behandling af personoplysninger for egne medarbejdere samt øvrige relevante registrerede.

Dette dokument har to formål: Dels at tjene som et praktisk instrument i virksomhedens arbejde med beskyttelsen af persondata, dels som en skriftlig dokumentation af indsatsen for at overholde Persondataforordningen. Kunder, leverandører, medarbejdere, samarbejdspartnere og andre interessenter kan via dette dokument opnå sikkerhed om, at vi som virksomhed gør alt hvad vi kan for at beskytte deres data og behandle disse data i overensstemmelse med både lovgivning og god databehandlingsskik.

Det vurderes ikke at være aktuel at have en databeskyttelsesansvarlig (DPO) som defineret i GDPR tilknyttet.

Ansvarlig for persondata i virksomheden samt løbende opdatering af dette dokument er:

Jens Nygaard Jensen
T: +45 41 26 73 81
E: jens@comadan.com

hvortil forbedringsforslag, samt enhver overtrædelse af denne politik samt databrud skal indberettes til.

Comadan a/s
Randers d. 20. April 2018

Jens Nygaard Jensen
CEO

Generelt om personoplysninger

Definition - Hvad er personoplysninger?

- **Alt hvad der kan identificere en fysisk person:**
  - Udover navn, adresse, CPR-nr. er det også digitale "spor", så som billeder, adgangskort, adgangslog, cookies pa hjemmesider m.v.

- **Oplysninger om virksomheder er kun omfattet, hvis det er om enkeltmandsvirksomheder**
  - (kan relateres til en person). Selskabsoplysninger er således ikke omfattet.

Personoplysninger kategoriseres således:

Almindelige personoplysninger	• Navn, adresse, telefonnummer, email, fødselsdato, uddannelse, beskæftigelse, boligforhold, bil, løn, skat, sygefravær.
Semifølsomme personoplysninger	• Cpr. nr., strafbare forhold, personlighedstest, privatøkonomi
Følsomme personoplysninger (kun behandles ved dokumenteret samtykke)	• Helbredsoplysninger, politisk- seksuel- orientering, race, religion, fagforeningsforhold, genetiske data.

Generelle betingelser for indsamling:

- **Lovlighed, rimelighed og gennemsigtighed**
  - Der må kun behandles persondata, hvis der er en lovlig grund til det (fra persondatareglerne), og alle forhold omkring databehandlingen (hvilke oplysninger, hvordan de indsamles, hvorfor de indsamles osv.) skal altid være gennemskuelige for den registrerede person.

- **Formålsbegrænsning**
  - Der må kun indsamle persondata, hvis der er et præcist formål med indsamlingen. Årsagen til indsamlingen skal give mening i forhold til den opgave, som oplysningerne bruges til. Persondata indsamlet til én opgave må ikke bruges til at udføre en anden. Der må ikke samles data bare fordi de er "rare" at have.

- **Dataminimering**
  - Der skal indsamle så få persondata, som overhovedet muligt i forhold til det formål, som oplysningerne ønskes anvendt til.

- **Rigtighed**

  - Det skal kontrolleres, at der ikke behandles persondata, som er forkerte eller misvisende. Hvis en kontrol viser, at der behandles forkerte eller misvisende persondata, skal disse slettes eller rettes.

- **Opbevaringsbegrænsning**
  - Persondata skal slettes, hvis de ikke længere er nødvendige for den opgave, som var grunden til indsamlingen.

- **Integritet og fortrolighed**
  - Behandling af persondata skal være sikker (behandlingssikkerhed).
  - Der skal derfor indføre tilstrækkelig IT-sikkerhed og sikkerhed i forhold til medarbejdere og interne procedurer, som sørger for, at persondata ikke bliver tilgængelig for uvedkommende personer, og som sørger for, at persondata ikke ændres eller slettes utilsigtet.

- **Ansvarlighed**
  - Når virksomheden behandler persondata, er virksomheden ansvarlig for at respektere den registrerede persons rettigheder, og virksomheden skal derfor kunne påvise og dokumentere, at behandlingen af persondata overholder persondatareglerne.

Den registreredes rettigheder:

- **Oplysningspligten.**
  - Krav om at den registrerede person skal have besked om, hvis der behandles oplysninger om den pågældende.

- **Indsigtsret**
  - Personen kan bede om at få at vide, hvilke oplysninger om den pågældende selv, som en myndighed eller virksomhed mv. behandler. Hvis den registrerede beder om det, skal der også gives en udskrift eller kopi af oplysningerne.

- **Berigtigelse**
  - Dataansvarlig har pligt til at rette forkerte personoplysninger.

- **"Retten til at blive glemt"**
  - Ret til at få personoplysninger slettet -hvis oplysningerne ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet, hvis et samtykke, som er nødvendigt for behandlingen, trækkes tilbage eller hvis behandlingen er ulovlig.

Virksomhedens generelle indstilling til personoplysninger

Beskyttelsen af personoplysninger er af stor betydning for virksomheden. Det gælder både i relation til egne medarbejdere, for kunder og leverandører samt andre registrerede, hvor virksomheden behandler personoplysninger.

Virksomheden ønsker grundlæggende at beskytte fysiske personers privatliv og fortrolighed. Virksomheden anerkender, at ikke kun egne medarbejdere, men også kunder, leverandører og andre registrerede, som virksomheden kommer i kontakt med i løbet af en arbejdsdag, med rette har krav på at vide, at deres respektive personoplysninger ikke vil blive brugt til andet formål end det oprindelige.

For at overholde gældende lovgivning og praksis vil personoplysninger blive indsamlet og behandlet i henhold til formålet, samt opbevaret sikkert og ikke videregivet til andre personer / tredjeparter uden samtykke fra den registrerede.

Behandling af sensitive personoplysninger

Såfremt virksomheden behandler en eller flere sensitive personoplysninger slettes disse oplysninger efter brug / eller senest 3 år efter at virksomhedens relationer til personen er ophørt.

Sensitive personoplysninger overføres ikke til lande udenfor EU / EØS-området, medmindre der foreligger et klart lovgrundlag, og et tilstrækkeligt beskyttelsesniveau af den registreredes sensitive personoplysninger i det pågældende land.

Vedhæftet som bilag 1 til denne politik er en liste over de sensitive personoplysninger, som virksomheden indsamler og behandler inkl. formål og behandlingsgrundlag. Listen opdateres regelmæssigt.

Områder hvor Virksomhedsnavn Behandler personoplysninger:

- Organisatoriske IT & fysiske rammer
- Behandlingsaktivitet HR funktion
- Behandlingsaktivitet samarbejdspartner.

Organisatoriske, IT & fysiske rammer

Lokaler

Virksomhedens lokaler beliggende på messingvej 60, 8940 Rander SV. Er udenfor arbejdstiden aflåst og sikret med et alarmsystem der via vagtcentral reagerer på alarmer.
Virksomhedens medarbejdere er forsynet med nøgle og alarmbrik der giver adgang til virksomheden.

Gæster

Det er virksomhedens politik, at gæster ikke må færdes alene. Hvis der mødes ukendte personer uden eskorte af en kollega, bør vedkommendes ærinde undersøges. Virksomhedens medarbejdere må ikke at lade uvedkommende følge efter sig ind af aflåste døre og skal i stedet henvise dem til hovedindgangen. Ved mistænkelig adfærd kontaktes ledelsen.

Arbejdspladser

Alle medarbejdere skal låse deres PC, når arbejdsstationen forlades, også kortvarigt. Medarbejdere er underlagt en clean desk politik, som indebærer, at medarbejderne skal fjerne alle dokumenter der indeholder personfølsomme oplysninger fra deres skrivebord, når de forlader arbejdspladsen. Derudover er skal de følge en front down politik, som indebærer at dokumenter med personoplysninger vendes med den blanke side op eller på anden måde afdækkes, når medarbejderen efterlader dokumenter på arbejdsstationen.

IT – generelt

Der henvises til bilag " IT-sikkerhed for mindre virksomheder" Bilag 3
Virksomheden vil gerne være sikker på, at der kun behandles personoplysninger, der er nødvendige for de bestemte formål. Virksomhedens IT-systemer forsøges tilpasset således, at der kun indsamles den nødvendige datamængde og opbevaring af personoplysningerne sker ikke i længere tid end nødvendigt.

Password-sikkerhed

Virksomheden ønsker at opretholde et høj sikkerhedesniveau vedrørende brug af passwords. Virksomhedens politik på for området er derfor, at medarbejdernes bruger ID og/eller password ikke må udleveres til andre.
Bruger ID og/eller password skal holdes hemmeligt således at uvedkommende ikke kan gøre brug af dem.
Passwords skal ændres password, hvis der er mistanke om, at det er blevet set af andre.
Medarbejderne skal undgå at anvende samme password til private og arbejdsmæssige formål.

E-mails

Det er ikke tilladt for virksomhedens medarbejdere at anvende deres personlige e-mail til virksomhedsrelateret kommunikation. Private e-mails sendt fra firma e-mail skal tydeligt mærkes som private.

E-mails (både udgående og indgående) bør løbende slettes, når der ikke længere er behov for, at disse opbevares. Behovet for at opbevare e-mails er en personlig vurdering, men med udgangspunkt bør alle e-mails der er over et år gamle slettes.

E-mails indeholdende følsomme eller særlige oplysninger, som CPR nr. eller helbredsoplysninger, skal som udgangspunkt slettes fra mail-systemet så snart de er behandlet eller, efter behov, gemmes på sikret drev, således at e-mails med særlige eller følsomme oplysninger ikke opbevares i e-mail systemet i mere end 30 dage.

Behandlingsaktivitet HR funktion.

Comadan behandler personoplysninger om sine medarbejdere, især i relation til ansættelsesforholdet.
HR funktionen varetages af Jens Nygaard Jensen

Områder med adgang til personoplysninger sikres således, at uvedkommende ikke kan få adgang til disse. Det sker ved at opbevare personoplysninger i aflåst skab, når lokalet ikke er under opsyn. Løbende, afhængig af mængden af bilag, kan personoplysninger fra aflåst skab arkiveres i et aflåst arkiveringsrum.

Der anvendes lønbureau som er beskyttet med kodeord – hvormed der er indgået en databehandleraftale.

For at dokumentere virksomhedens forskellige dataflows, har virksomheden beskrevet og dokumenteret alle relevante processer, hvor der indsamles og behandles personoplysninger. Disse procesbeskrivelser udgør et tillæg til denne politik og er vedhæftet som bilag 2.

Der henvises til Samtykkeerklæring og oplysningspligt vedr. medarbejdere Bilag 4

Databehandleraftaler indenfor "Behandlingsaktivitet HR funktion".

Comadan har indgået databehandleraftaler med alle sine databehandlere, og har disse aftaler registeret i sine systemer og som bilag til denne aftale – specifikt er der:

- Proløn (lønsystem)
- Bogholder
- Revisor

Udover dette sker der ifølge loven videregivelse af personoplysninger til f.eks. E-Boks, Arbejdsskadestyrelsen, SKAT, Pensions & forsikringsudbydere m.v.

Behandlingsaktivitet samarbejdspartner.

Comadan behandler personoplysninger vedrørende virksomhedens kunder, leverandører, partnere og andre tredjeparter (øvrige registrerede) af hensyn til at kunne betjene disse.

For at dokumentere virksomhedens forskellige dataflows, har virksomheden beskrevet og dokumenteret alle relevante processer, hvor der indsamles og behandles personoplysninger. Disse procesbeskrivelser udgør et tillæg til denne politik og er vedhæftet som bilag 2.

Databehandleraftaler indenfor " Behandlingsaktivitet samarbejdspartner".

Comadan har indgået databehandleraftaler med alle sine databehandlere, og har disse aftaler registeret i sine systemer og som bilag til denne aftale – specifikt er der:

- IT-relation (server og infrastruktur)
- Buch (Hjemmeside)
- Systemcenter Randers (ERP – NAV2017)
- Bogholder
- Revisor

LISTE OVER BILAG:

Bilag 1: Kortlægning af persondata
Bilag 2: Data flow for persondata
Bilag 3: " IT-sikkerhed for mindre virksomheder"