LANinform
v/Martin Kaufmann
Hjortensgade 30, 8000 Århus C

Persondataforordningen

Generel beskrivelse af behandling af persondata i virksomheden.

24.04.2018

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 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.

Da der ikke er ansatte holder ledelsen (indehaver) sig orienteret om persondataforordningen.

Behandlingen af personoplysninger er som udgangspunkt relateret til virksomhedens indehaver, 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 indehaver 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 aktuelt at have en databeskyttelsesansvarlig (DPO) som defineret i GDPR tilknyttet.

Virksomheden har ingen ansatte men er enkeltmandsfirma og kun indehaver har fuld eller delvis adgang til personoplysninger pr. 1. maj 2018.

Ansvarlig for persondata i virksomheden samt løbende opdatering af dette dokument er:
Martin Kaufmann
til hvem forbedringsforslag, samt enhver overtrædelse af denne politik samt databrud skal indberettes til.

Firma LANinform
Århus C, den 24. april 2018

Martin Kaufmann

Generelt om personoplysninger

Personoplysninger kategoriseres således:

- **Almindelige personoplysninger:**
  - Navn, adresse, telefonnummer, e-mail, fødselsdato, uddannelse, beskæftigelse, boligforhold, bil, løn, pensions- og skatteforhold , sygefravær og lign.

- **Semifølsomme personoplysninger:**
  - CPR-nummer, straffeattest, personlighedstest, privatøkonomi og lign.

- **Følsomme personoplysninger:**
  - Helbredsoplysninger, politisk/seksuel orientering, race, religion, fagforeningsforhold, genetiske data og lign.

Generelle betingelser for indsamling:

- **Lovlighed, rimelighed og gennemsigtighed**
  - Der må kun behandles persondata, hvis der er en lovlig grund til det (fra persondatareglerne).
  - 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 indsamles 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 eller måske skal bruges senere.

- **Dataminimering**
  - Der skal indsamles 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 omgående.

- **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.

- **Risikovurdering**
  - Der skal altid foretages en risikovurdering af de risici eller den negative påvirkning den registrerede udsættes for, når vedkommendes personoplysninger behandles.
  - Risikoen kan bestå i faktisk eller potentiel risiko i forhold til at blive udsat for diskrimination, for identitetstyveri, økonomisk tab, tab af omdømme eller datafortrolighed.

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, eller 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 indehaver, 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 indehaver, 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 følsomme personoplysninger

Såfremt virksomheden behandler en eller flere følsomme personoplysninger slettes disse oplysninger efter brug eller senest ved udløbet af 3 år fra datoen, hvor virksomheden modtog de pågældende følsomme personoplysninger. Undtagelse herfra er oplysninger om sygefravær/dagpengerefusion, da de anses for værende en del af regnskabsmaterialet som skal gemmes i 5 år.

Følsomme personoplysninger overføres ikke til lande udenfor EU / EØS-området.

Organisatoriske, IT & fysiske rammer

Lokaler

Virksomhedens kontor ligger i privat hjem uden adgang for fremmede.

Virksomhedens kontor er ved enhver situation, hvor indehaver har forladt lokaliteterne, aflåst.

Gæster

Gæster må ikke færdes alene i virksomhedens kontorlokale. Ved mødeafholdelse med gæster, afholdes disse i lokaler, hvor der ikke opbevares personfølsomme data.

Arbejdspladser

Indehaver skal, når der arbejdes med persondata, slukke skærmen, når arbejdsstationen forlades, også kortvarigt. Indehaver skal fjerne eller afdække dokumenter med persondata fra skrivebord, når arbejdspladsen forlades. Affald med personfølsomme data indsamles og opbevares forsvarligt indtil destruktion.

IT – generelt

Der henvises til bilag 1 ” IT-sikkerhed for mindre virksomheder”.

Virksomhedens IT er organiseret med brug af bærbar PC/Mac, med programmer og data kørende på server under egen kontrol, som er placeret i Schweiz. Der tages kontinuerlig krypteret cloud-baseret back-up til Front Safe i DK.

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 højt sikkerhedsniveau vedrørende brug af passwords. Virksomhedens politik på for området er derfor, at indehavers bruger-id og/eller password ikke må udleveres til andre.
Bruger-id og/eller password må ikke nedskrives på papir, i software-filer, på telefon eller andre steder.
Password skal ændres, hvis der er mistanke om, at det er blevet set af andre.
Indehaver skal undgå at anvende samme password til private og arbejdsmæssige formål.

E-mails

E-mails (både udgående og indgående) slettes som udgangspunkt ikke jf. virksomhedens kutyme, da det bruges som hændelseslog/-arkivering.

Derfor skal e-mails med semifølsomme eller følsomme oplysninger sendes krypteret såvel internt som eksternt.

E-mails indeholdende semifølsomme (fx CPR.nr) eller følsomme (fx helbred) oplysninger, skal som udgangspunkt slettes fra Outlook 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/personaleadministration.

Da virksomheden ikke har ansatte behandles der ikke personoplysninger iht. personaleadministration.

Behandlingsaktivitet Kundeadministration.

Virksomheden behandler personoplysninger vedrørende virksomhedens kunder af hensyn til at kunne betjene disse.
Virksomhedens kunder er udelukkende virksomheder, hvorfor der ikke registreres personoplysninger udover kontaktpersoners e-mail, direkte telefonnummer o. lign.

For at dokumentere virksomhedens forskellige dataflows, har virksomheden beskrevet og dokumenteret alle relevante processer, hvor der indsamles og behandles personoplysninger vedr. kunder.
Disse procesbeskrivelser udgør et tillæg til denne politik og er vedhæftet som bilag 5.

Behandlingsaktivitet Leverandøradministration.

Virksomheden behandler personoplysninger vedrørende virksomhedens leverandører og andre tredjeparter (øvrige registrerede) af hensyn til at kunne betjene disse.
Virksomhedens leverandører er udelukkende virksomheder, hvorfor der ikke registreres personoplysninger udover kontaktpersoners e-mail, direkte telefonnummer o. lign.

For at dokumentere virksomhedens forskellige dataflows, har virksomheden beskrevet og dokumenteret alle relevante processer, hvor der indsamles og behandles personoplysninger vedr. leverandører og andre tredjeparter.
Disse procesbeskrivelser udgør et tillæg til denne politik og er vedhæftet som bilag 6.

Procedure ved henvendelse fra registreret person.

Virksomheden er forpligtet til at håndtere anmodninger om indsigt i samt berigtigelse og begrænsning af registreringer uden unødigt ophold.
Registrerede personer har ret til at få oplyst alle de personoplysninger, virksomheden har indsamlet samt formål med behandlingen, kategori for registrerede personoplysninger, hvorfra oplysningerne stammer (hvis ikke indsamlet hos den registrerede selv), hvortil oplysningerne evt. videregives samt tidsrum for opbevaring eller kriterier herfor.
Indehaveren træffer beslutning om, hvorvidt en anmodning skal imødekommes eller ej samt iværksætter behandlingen hos respektive ansvarlige, så besvarelsen kan ske indenfor højst 1 måned.
Ligeledes har registrerede personer ret til berigtigelse eller sletning/anonymisering eller begrænsning af personoplysningerne, hvis dette kan foretages under hensyntagen til lovkrav mv.

Ved registreredes anmodning om berigtigelse:

- Oplysningerne opdateres straks, så de er korrekte, og den registrerede oplyses herom. Hvis ønske ikke kan efterkommes oplyses den registrerede om dette inkl. begrundelse samt om muligheden for klage til Datatilsynet

Ved registreredes anmodning om begrænsning af behandling:

- Virksomheden skal begrænse behandling dvs. kun behandle oplysninger med registreredes samtykke i tilfælde af at
  - Personoplysningerne bestrides af den registrerede og skal efterprøves/undersøges
  - Behandlingen er ulovlig og den registrerede modsætter sig sletning og anmoder om begrænsning
  - Personoplysningerne ikke længere er nødvendige for behandling men for at et retskrav kan fastlægges, gøres gældende eller forsvares
  - Den registrerede har gjort indsigelse mod behandling og indtil det fastslås at der er legitim baggrund for at fastholde registrering

Ved registreredes anmodning om sletning:

- Hvis personoplysningerne kan slettes uden konsekvens iht. andre lovkrav, gøres dette uden ophold. Dette gælder både for elektronisk og fysisk opbevarede oplysninger.

Ved registreredes anmodning om dataportabilitet

- Virksomheden skal medvirke til direkte overførsel af personoplysninger til andre dataansvarlige ved anmodning fra den registrerede.

Ved registreredes indsigelse mod behandlingen

- Med mindre virksomheden har tungtvejende grunde i at behandle personoplysningerne (fx retssag) skal virksomheden imødekomme den registreredes indsigelse mod behandlingen. I så fald skal den registrerede have et begrundet afslag og oplysning om klagemulighed hos Datatilsynet.

Ved henvendelse fra en registreret gennemgås procesbeskrivelse for områdets behandlingsaktiviteter for afklaring af, hvor data forefindes, og berigtigelse, begrænsning eller sletning foretages iht. ovenstående. Herefter rapporteres der til den registrerede. Dette gøres straks muligt og senest 1 måned efter modtagelse af anmodningen.
Hvis der er formodning om chikanehensigt fra den registrerede, oplyses denne om nægtelse af at efterkomme anmodningen samt muligheden for at klage til Datatilsynet.

Håndtering ved databrud.

Et databrud karakteriseres som *en hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.* Det dækker således situationer, hvor uvedkommende får adgang til personoplysninger (hacking, tyveri, bortkomst af computer/smartphone/tablet el.lign.), og situationer, hvor personoplysninger mistes enten ved uheld eller indehavers utilsigtede sletning. Databrud dækker også tilfælde, hvor der sker ulovlig håndtering af personoplysninger (videregivelse uden hjemmel) eller hvor uvedkommende (såvel intern som ekstern person) får mulighed for at tilgå personoplysningerne.

Der skal ved databrud ske anmeldelse, med mindre det er helt usandsynligt at databruddet indebærer en risiko for fysiske personers rettigheder. Vurdering af, om det er tilfældet, skal ske umiddelbart efter bruddet.
Ved formodning om databrud skal der således omgående ske vurdering af typen af sikkerhedsbrud, art/grad af følsomhed og omfang, risiko for identifikation, mulige konsekvenser for den/de registrerede mv.

Anmeldelse af databrud med risiko skal ske til Datatilsynet straks efter vurderingen og uden unødigt ophold og senest inden for 72 timer. Anmeldelsen skal indeholde minimum:

- beskrivelse af karakteren af bruddet på persondatasikkerheden,
- kategorier og antallet af registreringer,
- beskrivelse af sandsynlige konsekvenser,
- beskrivelse af foranstaltninger som er igangsat for at håndtere bruddet samt begrænse dets mulige skadevirkninger,
- samt kontaktoplysninger på person i virksomheden, som kan kontaktes for yderligere oplysninger

I tilfælde af at databruddet indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal der også ske underretning til hver enkelt af de registrerede, hvis personoplysninger er berørte af bruddet uden unødigt ophold.

Vurderingen af "høj risiko" skal tage hensyn til sandsynligheden for, at oplysninger offentliggøres (fx helbredsoplysninger) eller udnyttes (fx mulighed for identitetstyveri) og eventuelle konsekvenser, hvis det sker. Orienteringen skal indeholde minimum de samme oplysninger som til Datatilsynet dvs. beskrivelse af karakteren af bruddet, sandsynlige konsekvenser, foranstaltninger samt kontaktoplysninger.

Alle databrud skal dokumenteres internt og evt. væsentlige beslutninger som følge heraf, skal dokumenteres. Kopier af dokumentation gemmes sammen med anmeldelse (-r) til Datatilsynet sammen med øvrigt materiale vedr. Persondataforordningen, for et samlet billede af virksomhedens håndtering heraf.

LISTE OVER BILAG:

Bilag 1: IT-sikkerhed for mindre virksomheder
Bilag 2: Oplysninger vedrørende den dataansvarlige virksomhed
Bilag 3: Principper og vejledning
Bilag 4: Overvejelser i forbindelse med behandling af persondata
Bilag 5: Procesbeskrivelse behandlingsaktivitet Kundeadministration
Bilag 6: Procesbeskrivelse behandlingsaktivitet Leverandøradministration
Bilag 7: Databehandler beskrivelse fra Front Safe (vedr. back up – krypteres)