Politik og retningslinjer for persondata

1. POLITIK FOR ATRIO Arkitekter ApS

Vores politik omkring persondata skal overordnet set medvirke til at sikre etablering og opretholdelse af retningslinjer for overholdelse af den til enhver tid gældende lovgivning om persondata.

2. AFGRÆNSNING OG OMFANG

Retningslinjerne gælder for alle virksomhedens medarbejdere.

Retningslinjerne gælder for alle persondata på såvel medarbejdere, kunder, leverandører mv. Altså på behandling af oplysninger om fysiske personer, herunder enkeltmandsvirksomheder.

Dermed gælder voesr politik og retningslinjer for alle data, der er ”personhenførbare”.

3. RETNINGSLINJER

3.1 Sondring mellem forskellig persondata

Sondringen mellem almindelige og følsomme personoplysninger har betydning ved den risikovurdering, som skal foretages i forhold til behandlingssikkerhed. Her vil beskyttelse af følsomme oplysninger vægte højere end beskyttelse af almindelige oplysninger.

Visse data f.eks. i bogholderisystemet omkring kunders køb af varer og løn til den enkelte medarbejder kan ikke slettes i systemet, idet vi dermed efter vores opfattelse vil være i strid med bogføringsloven. Vi vil ved en senere anskaffelse af et nyt system tilstræbe, at vi får et system, hvor vi i videst mulig omfang kan anonymisere dataene efter 5 år.

Såfremt det er nødvendigt af hensyn til andre regler f.eks. dokumentation af byggesager, vil disse andre regler blive overholdt.

Persondata som firmaet håndterer:

Løn- og pensionsdata.
Ansøgninger og ansættelseskontrakter.
Kundekartotek med kontakter.
Sagsbibliotek.
Mailkorrespondance.

3.2 Registrerede personers rettigheder efter persondataforordningen

Fysiske personer har følgende rettigheder efter persondataforordningen:

- Retten til at modtage oplysning om en behandling af personoplysninger(oplysningspligt)
- Retten til at få indsigt i personoplysninger
- Retten til at få urigtige personoplysninger berigtiget
- Retten til at få 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 personoplysninger (dataportabilitet)

Disse rettigheder respekterer vi ud fra følgende overordnede retningslinjer:

- Alle medarbejdere har kendskab til regler om persondata og har læst denne politik
- Alle kunder er oplyst om deres rettigheder

- Henvendelser fra personer omkring vores håndtering af persondata vil ske inden for 30 dage
- Vi anvender ikke data fra/om vores kunder til andet end det aftalte formål
- Vi sørger for altid at have de korrekte personoplysninger noteret
- Vi har procedure for sletning af persondata, se afsnit 3.3.1 nedenfor.
- Vi anvender ikke data i markedsføringsmæssig henseende medmindre vi har samtykke hertil.
- Vi vil opfylde krav til dataportabilitet på en kundes anmodning.
- Vi indhenter og opbevarer ikke mere data end nødvendigt.

3.3 Behandling af persondata
Behandling af almindelige oplysninger om personer må kun finde sted, hvis én af betingelserne er opfyldt, hvilket vi respekterer:

a) Kunden har givet samtykke til behandling af sine personoplysninger til et specifikt formål.
b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i
c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
d) Behandling er nødvendig for at beskytte den registreredes/en anden persons vitale interesser.
e) Behandling er nødvendig ift. udførelse af en opgave i samfundets interesse eller en opgave, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
f) Behandling er nødvendig, for at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Alle ansatte skal underskrive en erklæring, hvor de har bekræftet, at vi ligger inde med de i forhold til løn og andet relevante oplysninger. Generelt tilstræbes, at vi kun har for daglig drift relevante oplysninger liggende på medarbejderne.

3.3.1 Procedurer fra sletning af data
Herunder er beskrevet de procedurer, som vi har i forhold til sletning af persondata på vores kunder.

Sletning af persondata i:

- Mail-systemer: Data i mailsystemer slettes løbende ud fra vurdering af sagens aktualitet og vigtighed.
- Telefoner: Uaktuelle kunder slettes løbende.
- Forskellige computer-drev inkl. kopimaskiner og andre steder, hvor konkrete data lagres: Data på komputerdrev fjernsupporteres af Jysk IT Support. Data er krypteret.
- Fysiske mapper: Data opbevares i filarkiv. Data slettes ikke umiddelbart.

Alt materiale på udgåede kunder slettes efter 5 år. Dette er hovedreglen. Hertil gælder følgende undtagelser:

- Hvis saglig grund til at gemme i længere tid
- Hvis sandsynligt, at en kunde efter denne tidshorisont vil henvende sig for at få data udleveret
- Forhold som jfr. pkt. 3.1 skal opbevares af hensyn til anden lovgivning, eller hvor en sletning vil medføre, at fuldstændigheden i f.eks. bogholderiet dermed går tabt.

Der skal være en konkret grund, som skal være en anden end, at det er belejligt for os at gemme alt.

3.4 IT sikkerhed
Der er koder på alle vores computere og telefoner. Fysiske koder gemmes i aflåst skab.

Vi har i forhold til risikoen ved vor behandling af persondata indført en passende IT sikkerhed med såvel fornødne tekniske som organisatoriske sikkerhedsforanstaltninger mod, at data i opbevaringsperioden hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid lovgivningen.

Vi anvender i overensstemmelse med god praksis firewalls, backup- samt antivirus-procedurer til at forhindre tab af data eller dele deraf i forbindelse med strømsvigt, brand, virusangreb eller andre produktionsforstyrrelser.

3.4.1 Hjemmeside
På vores hjemmeside bruger vi ikke cookies.

3.5 Fysisk sikkerhed
Alt fysisk persondata vedrørende vores kunder foreligger i kundemapper og ikke som løse dokumenter i skuffer mv.

Eksterne personer efterlades aldrig alene, hvor der står ikke-relevant persondata tilgængelig.

Virksomhedens lokaler er altid aflåst, når vi ikke selv er tilstede.

Der er alarmsystem på virksomhedens lokaler, der altid er slået til, når der ikke er nogen.

Kun medarbejdere, herunder rengøringspersonale har nøgle til virksomhedens lokaler. I forhold til rengøringspersonale har de ikke adgangsmulighed til computere eller aflåset skabe.

3.6 Information til de personer vi har persondata på (de registrerede)
Ved indsamling af personoplysninger, skal vi give de registrerede en række oplysninger i forbindelse med indsamlingen, herunder oplysninger om vores identitet samt formålet med behandlingen af de indsamlede data, og vores retlige grundlag for behandling af personoplysninger.

Hvis behandlinger udelukkende bygger på samtykke, så skal dette samtykke kunne dokumenteres.

3.6.1 Beskrivelse af de samtykker vi indhenter
Vi indhenter ikke samtykke hos alle vores fysiske kunder på, at vi må opbevare deres kontaktoplysninger og data. Vi oplyser dem om at vi har deres data via vores hjemmeside og via mail. Ad den vej får de mulighed for at afvise os retten til dette.

3.7 Databehandleraftaler
Når vi deler persondata med andre, så har vi brug for en databehandleraftale. Disse vil vi få indhentet hos følgende:

- Proløn
- Revisor
- Advokat
- IT-supporter
- Webudbyder
- Telefon- og internetudbyder

3.8 Oplysningspligt ved brud på sikkerhed/læk af data
Hvis der er alvorlige sikkerhedsbrud eller hvis der er sket læk af personfølsomme data, så skal de relevante personer straks oplyses herom. Dette er vigtigt for at kunne overholde kravet om, at dette skal rapporteres til Datatilsynet inden for 72 timer.

5. Datasikkerhed i forbindelse med personaleadministration
Datatilsynet har udarbejdet en 12-punkts liste, som indeholder minimumskrav ved behandling af personaleoplysninger. Det er herunder dokumenteret skriftligt, hvilke tiltag vi gjort for at opfylde de enkelte punkter.

Krav	Tiltag for opfyldelse af krav
1. Beskriv, hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.	ATRIO Arkitekter har kun en begrænset organisation og alle personfølsomme oplysninger kan kun tilgås af Finn og Palle samt betroede medarbejdere. Se i øvrigt svar til nedenstående punkter
2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.	Alle papirer vedr. ansættelsesforhold er i aflåst skab. Elektroniske oplysninger arkiveres på computere, som kun kan tilgås med personlige passwords.
3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.	Dette sker kun ved en medarbejder eller ejerne. Organisationen er så begrænset, at ejerne vil være i direkte kontakt med alle situationer og personligt overvåger, at ingen personfølsomme oplysninger udleveres uretmæssigt.
4. Personaleoplysninger på papir – fx i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug. Når dokumenter (papirer, kartotekskort m.v.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.	Se punkt 2. Alle ansøgninger markuleres efter 1 måned med mindre andet aftales med ansøgeren. Alle oplysninger vedr. en ansat makuleres senest 5 år efter ansættelsens ophør. Såfremt oplysninger skal opbevares efter anden lov, kan dette betyde, at oplysninger opbevares længere.
5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.	Alle computere har personligt password. Bogholderiet beskyttes af kode, således kun ejere og bogholder har adgang.
6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.	Såfremt log eller andet firewall giver anledning hertil, vil der blive fulgt op, sammen med ekstern IT-ansvarlig
7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan fx bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.	Der lagres ikke permanent oplysninger af personfølsom karakter på USB eller tilsvarende.
8. Pc'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.	Dette er installeret og fornys
9. Hvis der benyttes hjemmesideformularer, hvor	Der er ingen personfølsomme oplysninger på

følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.	vores hjemmeside og den giver ikke mulighed for at lagre sådanne.
10. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.	Vi sender ikke personfølsomme oplysninger på mail eller tilsvarende. Hvis vi efter 1/1 2019 får brug for dette vil vi konkret vurdere, hvordan dette kan se under hensyn til reglerne om sikker kommunikation
11. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.	Vi bruger en fast leverandør og vil hver gang vurdere, hvorledes vi kan sikre, at der ikke sker unødig risiko for, at personfølsomme oplysninger kan udnyttes af andre.
12. Ved brug af en ekstern databehandler til håndtering af oplysninger skal persondatalovens § 42 om skriftlig databehandleraftale m.v. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.	Vi indhenter databehandleraftaler fra eventuelle eksterne databehandlere.

Der kan være billede af medarbejderne på hjemmesiden og disse kan også fremgå af markedsføringsmateriale m.v. Dette er omfattet af medarbejdernes samtykkeerklæring.

Medarbejdere som fratræder vil straks – så vidt muligt - blive slettet på hjemmesiden, men historisk materiale og eventuelle billeder i markedsføringsmateriale vil kun kunne slettes, hvis det er praktisk muligt.

Generelt tilstræber vi, at sådanne billeder alene bruges i den omfang, som det er relevant for virksomheden og disse vil skulle ligge inden for rammerne af virksomhedens samtykke.

Øvrigt billedmateriale f.eks. i forbindelse med firmaarrangementer vil alene blive opbevaret i virksomheden og alene være til virksomhedens ansatte interne brug. Sådanne billeder kan i særlige tilfælde opbevares i mere en 5 år som et led i dokumentationen af virksomhedens historie.

5.1. Sletning af personaledata

Personaledata slettes løbende, når data ikke længere er nødvendige for virksomheden.

Ved uopfordrede ansøgninger anslås dette til at være 1 måned. Hvis en uopfordret ansøgning ønskes gemt længere tid, beder vi den pågældende ansøger om lov til at gemme udover den tid, der ellers er anslået som nødvendig. Ansøgningen skal dog senest slettes efter 1 år.

Når en medarbejder fratræder slettes fysisk data desuden senest efter 1 år fra fratrædelsesdatoen. Det er Palle Nielsen eller Finn West Møller, der konkret foretager denne fysiske sletning. Undtagelsen hertil er, hvis det af hensyn til bogføringsloven, arbejdsmiljøreglerne eller på anden vis er et krav, at tingene gemmes længere.