

## Politik for behandling og beskyttelse af personoplysninger

Databeskyttelsespolitikken gælder for Brix & Kamp A/S.

Politikken skal hjælpe til at sikre og dokumentere, at virksomheden beskytter sine personoplysninger i overensstemmelse med reglerne for behandling af personoplysninger. Politikken bidrager desuden til, at virksomheden oplyser om behandlingen og brugen af de registrerede personoplysninger.

Politikken gennemgås hvert år.

### Fortegnelse over behandlingen af personoplysninger

Virksomheden behandler personoplysninger om:

- Medarbejdere
- Kunder
- Leverandører

Virksomheden har udarbejdet en fortegnelse over behandlingen af personoplysninger. Fortegnelsen giver overblik over de behandlinger, som virksomheden er ansvarlig for.

Personoplysningerne er en forudsætning for, at Virksomheden kan indgå ansættelses-, kunde- og leverandørkontrakter.

### Behandlingens formål og lovlighed

Personoplysningerne behandles og arkiveres i forbindelse med:

- Personaleadministration, herunder rekruttering, ansættelse, fratrædelse og udbetaling af løn
- Stamdata for kunder samt ordrer og salg
- Stamdata for leverandører samt rekvisitioner og køb
- Kontrakter
- Prækvalifikationer/konkurrencer

Behandlingen er lovlig i medfør af hjemmel som angivet i vedhæftede fortegnelse.

Virksomheden benytter ikke personoplysningerne til andre formål end de listede. Virksomheden indsamler ikke flere personoplysninger end nødvendigt i forhold til opfyldelse af formålet.

### **Opbevaring og sletning**

Virksomheden har indført følgende overordnede retningslinjer for opbevaring og sletning af personoplysninger:

- Personoplysninger opbevares i fysiske mapper.
- Personoplysninger opbevares i it-systemer og på separat serverdrev.
- Personoplysninger opbevares ikke længere, end hvad der er nødvendigt for formålet med behandlingen.
- Personoplysninger for medarbejdere slettes fem år efter endt ansættelse, og personoplysninger om ansøgere slettes efter seks måneder.

### **Datasikkerhed**

Virksomheden har ud fra vedhæftede risikovurdering gennemført følgende sikkerhedsforanstaltninger for beskyttelse af personoplysninger:

- Kun medarbejdere, der har et arbejdsbetinget behov for adgang til de registrerede personoplysninger, har adgang hertil enten fysisk eller gennem it-systemer med rettighedsstyring.
- Alle computere har adgangskode, og medarbejderne må ikke overlade deres adgangskoder til andre.
- Computere skal have installeret firewall og antivirusprogram, der løbende opdateres.
- Computere indstilles til automatisk lukning/timeout på 15 min.
- Personoplysninger slettes på forsvarlig vis ved udfasning og reparation af it-udstyr.
- USB-nøgler, eksterne harddiske mv. med personoplysninger skal opbevares i aflåst skuffe eller skab.
- Fysiske mapper er placeret på aflåst kontor eller i aflåste skabe.
- Personoplysninger i fysiske mapper slettes ved makulering.
- Mailkorrespondance i forbindelse med rekruttering, personaleadministration og lønbehandling sker via specifik mailadresse.
- Generel medarbejder information, sker via link eller genveje på de personlige computere til Pdf filer, der beskyttes mod udskrivning.
- Alle medarbejdere skal modtage instruktion i, hvad de må gøre med personoplysninger samt, hvordan personoplysninger skal beskyttes.

### **Videregivelse**

Personoplysninger om medarbejdere kan blive videregivet til offentlige myndigheder fx SKAT, pensionsselskaber, forsikringsselskaber og kunder. Sidstnævnte kun ved krav om fremsendelse af cv'er i forbindelse med ved deltagelse i tilbudsgivning, prækvalifikationer eller konkurrencer.

### **Databehandlere**

Virksomheden benytter udelukkende databehandlere, såfremt databehandlerne stiller de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske sikkerhedsforanstaltninger til opfyldelse af persondatarettens krav. Alle databehandlere underskriver en databehandleraftale forinden behandlingen iværksættes.

### **Rettigheder**

Virksomheden varetager den registreredes rettigheder, herunder retten til indsigt, tilbagetrækning af samtykke, berigtigelse og sletning og orienterer de registrerede om virksomhedens behandlinger af personoplysninger. Registrerede har ligeledes ret til at klage til Datatilsynet.

### **Brud på persondatasikkerheden**

I tilfælde af brud på persondatasikkerheden, anmelder virksomheden hurtigst muligt og inden 72 timer bruddet til Datatilsynet. Økonomichef Helle Jørgensen er ansvarlig for, at dette sker. I anmeldelsen beskrives bruddet, hvilke grupper af personer, det vedrører og, hvilke konsekvenser bruddet kan få for disse personer samt, hvordan Virksomheden har eller vil afhjælpe bruddet. I tilfælde, hvor bruddet indebærer en høj risiko for de personer, om hvem Virksomheden behandler personoplysninger, vil Virksomheden endvidere underrette disse. Virksomhedens dokumenterer alle brud på persondatasikkerheden på "W:\B & K\Persondataforordningen\Dokumentation\Sikkerhedsbrud".