VEJLEDNING

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

# Tekniske og organisatoriske sikkerhedsforanstaltninger:

Databeskyttelsesforordningen stiller krav om, at man, når man behandler personoplysninger, skal sikre sig et passende niveau af organisatoriske og tekniske sikkerhedsforanstaltninger. Dette går kort sagt ud på, at virksomheden skal sikre sig, at de systemer og lokationer de bruger til behandling af personoplysninger, skal have et passende sikkerhedsniveau.

Med begrebet et ”passende sikkerhedsniveau” menes, at sikkerhedsniveauet skal tilpasses størrelsen af den enkelte virksomhed, men også de behov, den enkelte virksomhed har i forhold til de personoplysninger, der behandles. Ved vurderingen af et passende sikkerhedsniveau, skal der tages hensyn til de risici behandlingen af personoplysninger udgør i forhold til forhindring af:

* hændelig eller ulovlig ødelæggelse af data
* tab af data
* at data ikke bliver ændret uretmæssigt
* at data ikke bliver videregivet ulovligt
* at der ikke på anden måde sker uautoriseret adgang til data

Databeskyttelsesforordningen oplister selv en række forslag til sikkerhedsforanstaltninger:

* Pseudonymisering og kryptering af persondata,
* Sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester,
* Procedurer for regelmæssig afprøvning, vurdering og evaluering af sikkerhedsforanstaltningernes effektivitet,
* Den dataansvarlige og databehandlerens sikring af, at enhver fysisk person, der udfører arbejde for dem og får adgang til persondata, kun må behandle disse efter instruks fra den dataansvarlige,

# Enkel-GDPR anbefaler følgende organisatoriske sikkerhedsforanstaltninger for at opretholde et passende sikkerhedsniveau:

Organisering:

Det er en god idé at udpege en person i virksomheden/organisationen, som skal have det overordnede overblik og ansvar for at interne procedurer og regler overholdes, kontrolleres, tilpasses og gennemgås.

Uddannelse og introduktion:

Alle medarbejdere som behandler personoplysninger bør undervises i persondatalovgivningen, samt virksomhedens/organisationens interne procedurer, politikker og regler.

Derudover bør alle nye medarbejdere ved ansættelse introduceres for de interne regler, politikker og procedurer vedrørende behandlingen af personoplysningerne.

Digital behandling/behandling i papirform:

Det bør efterstræbes, at al behandling af personoplysninger forgår digitalt. Det vil sige, at udskrift eller anden form for håndtering af personoplysninger i papirform bør begrænses i størst muligt omfang.

Hvis opbevaring af personoplysninger i papirform er nødvendigt, bør papirerne opbevares i aflåste skabe, hvor kun relevante personer har adgang.

Som minimum bør der én gang hver 14. dag ryddes op i skabe mm. for at rydde op i papirer indeholdende personoplysninger. Hvis der ikke længere eksisterer et formål med at opbevare de pågældende oplysninger i papirform (hvis eksempelvis dokumenterne nu foreligger i digital form), bør disse papirer makuleres i en krydsmakulator.

Kontrol:

For at kontrollere, at virksomhedens/organisationens politikker, procedurer, regler mv. overholdes, bør der foretages stikprøvekontroller. På denne måde kan det effektivt kontrolleres om alle de organisatoriske sikkerhedsforanstaltninger overholdes i hele organisationen.

# Enkel-GDPR anbefaler følgende tekniske sikkerhedsforanstaltninger for at opretholde et passende sikkerhedsniveau:

Teknisk beskyttelse mod uautoriseret adgang:

Alle IT-systemer og -enheder bør beskyttes mod uautoriseret adgang ved opsætning af følgende tekniske sikkerhedsforanstaltninger:

* Firewall
* Antivirus-foranstaltninger
* Spamfiltre
* Løbende opdatering af software

Derudover bør alle netværk i virksomheden/organisationen opsættes med de nødvendige sikkerhedsforanstaltninger med henblik på beskyttelse mod uautoriseret brug og adgang.

Sikkerhedskopiering:

Alle IT-systemer i virksomheden/organisationen, hvor der opbevares personoplysninger, bør sikkerhedskopieres jævnligt, så al data kan gendannes i tilfælde af fejl.

Fysiske personers adgang til IT-systemer:

Det bør sikres, at kun de medarbejdere det er relevant for, har adgang til de IT-systemer, hvor der opbevares eller på anden måde behandles personoplysninger.

Derudover kan det være en god idé at etablere et autorisationssystem, hvor hver enkelt medarbejder får et individuelt og unikt brugernavn til en individuel brugerprofil. Sådanne brugernavne bør aldrig genanvendes, selvom en medarbejder er fratrådt og en anden tiltræder. Når en medarbejder fratræder, bør sådanne brugerprofiler slettes straks.

Alle medarbejderes adgang til og brug af IT-systemer bør endvidere logges, således at der til enhver tid kan føres kontrol med brug og adfærd af den enkelte brugerprofil.

Herudover bør det sikres, at det kun er den enkelte medarbejder, der kan få adgang til denne medarbejders brugerprofil på det pågældende IT-system. Hver medarbejder bør ydermere have en individuel adgangskode, som bør ændres hver tredje måned. I den forbindelse skal denne adgangskode være ny i forhold til tidligere anvendte koder for den enkelte medarbejder.

Det er dertil også en anbefaling, at alle arbejdsstationer låser efter 5 minutters inaktivitet og kun kan låses op igen med en individuel skærmlås. Medarbejderne bør ikke have mulighed for at give tilladelse til at brugernavn og adgangskode huskes – både i forhold til hardware og software.

E-mails:

Der skal altid bruges sikker/krypteret mail ved fremsendelse af e-mails indeholdende personoplysninger om CPR-numre, strafbare forhold og følsomme personoplysninger.

Alle mails, der indeholder personoplysninger og som er relevante at gemme, bør arkiveres uden for indbakken og herefter slettes fra selve indbakken. Herudover bør der jævnligt ryddes op i indbakken, sendt post og slettet post, så der ikke gemmer sig mails, som indeholder personoplysninger i disse nævnte mapper.

Data på digitale enheder:

Der bør alene opbevares personoplysninger på mobile enheder (telefoner, iPads, laptops, USB-stik mv.), såfremt disse enheder er beskyttet med et sikkerhedsgodkendt krypteringsprogram.

Der bør føres fuld kontrol med alle digitale enheder tilhørende virksomheden, så alt indhold på en enhed kan destrueres ved tyveri eller mistet enhed.

Det bør ikke være muligt at opbevare eller flytte personoplysninger på/til medarbejderes eller andres private enheder.

Destruering / bortskaffelse af hardware:

Al hardware bør destrueres og bortskaffes på sikker vis.

Kontrol af tekniske sikkerhedsforanstaltninger:

Der bør minimum én gang i kvartalet foretages en afprøvning, vurdering og evaluering af de tekniske sikkerhedsforanstaltninger.