# Persondatasikkerhed – Tjekliste

## Om datasikkerhed

Databeskyttelsesforordningen og de gældende danske regler lægger vægt på, at sikkerheden omkring behandlingen – og herunder opbevaring – af personoplysninger er i orden. Alle aftenskoler er derfor forpligtede til at opretholde den nødvendige *høje* niveau af databeskyttelsen. Men da sikkerhedsbilledet i IT-verdenen ændrer sig fra dag til dag med kontinuerlig vækst i produktionen af nye hardware- og softwareelementer, er der ikke en udtømmende facitliste over alle tænkelige sikkerhedsforanstaltninger, som en virksomhed eller fysisk person skal implementere.

Det generelle krav er er, at virksomheder skal beskytte alle personoplysningerne med tilstrækkelige sikkerhedsforanstaltninger. Det er dog op til den enkelte skole at vurdere, hvilke sikkerhedsforanstaltninger der er nødvendige i en given situation.

I tilfælde af sikkerhedsbrud (se vores infomateriale) kan tilsynsmyndigheden kræve at få indsigt i de sikkerhedsforanstaltninger som skolen har truffet for at minimere risikoen for et evt. brud.

## Baggrund og formål

Med udgangspunkt i Datatilsynets anbefalinger har vi udarbejdet nedenstående Datasikkerhed - Tjekliste, som skolerne kan bruge i deres vurdering af, om de nødvendige sikkerhedsforanstaltninger er til stede. Listen er i sagens natur ikke endelig, og skolerne kan frit tilføje flere elementer eller fjerne elementer, som ikke er relevante for skolen.

Tjeklisten er opdelt i Opgavebeskrivelse samt en Statusbeskrivelse. Opgavebeskrivelsen indeholder informationer om de enkelte sikkerhedsforanstaltninger som skolen bør tage højde for. Statusbeskrivelsen er skolens egen beskrivelse af status på implementeringen af de angivne foranstaltninger. Denne beskrivelse kan både indeholde kort ja/nej svar eller en lidt mere uddybende forklaring.

De fleste elementer kan suppleres og relateres til skolens øvrige dokumentation. F.eks. relateres ”Adgang til oplysningerne begrænset kun til personer med saglige formål” til både Fortegnelsen og Intern adgang til data tjeklisten. Hosting af servere, serverparks og cloud-løsninger er ikke behandlet her.

Denne Persondatasikkerhed tjekliste er kun til internt brug og er tænkt som en praktisk hjælp til skolerne, når de skal til at danne overblik over skolens aktuelle datasikkerheds status.

Vi har allerede forudfyldt nogle Statusbeskrivelser for skoler, der bruger DOFPro/VuptiWeb. Alle andre felter skal skolen selv udfylde.

# Tjekliste for Persondatasikkerhed

|  |  |
| --- | --- |
| **Opgave** | **Status/beskrivelse** |
| Adgang til oplysningerne begrænset kun til personer med saglige formål. | - |
| Medarbejdere har fået instrukser om, hvordan de behandler og beskytter oplysningerne. | - |
| Personaleoplysninger på papir er aflåst, når de ikke er i brug. | - |
| Personaleoplysninger på papir makuleres eller destrueres på anden vis, når de skal smides ud. | - |
| Der anvendes adgangskode for at få adgang til IT-udstyr med personoplysninger. | - |
| Adgangskoder overlades ikke til andre og er ikke tilgængelige, så andre kan se den. | - |
| Der udføres kontrol over tildelte koder mindst hver halve år. | - |
| Det registreres og reageres på, hvis der er ulovligt forsøg på at få adgang til IT-systemer med følsomme personaleoplysninger. | - |
| Persondata opbevaret på flytbare medier (USB, CD’er, Blue-Ray osv.) er beskyttet med adgangskode og kryptering og/eller opbevares i aflåst skab eller skuffe. | - |
| Computere koblet til Internet har opdateret firewall og antivirus beskyttelse. | - |
| Overførslen af CPR eller følsomme data via vores hjemmeside er beskyttet med kryptering. \* | Ja. Hjemmesiden er beskyttet med godkendt Comodo sikkerhedscertifikat. |
| Ved overførslen af CPR via en e-mail, er data krypteret. \*\* | Nej. |
| Ved destruering eller reparation af IT-udstyr, sørges der for, at oplysninger ikke kan komme til uvedkommendes kendskab. | - |
| Der er indgået en skriftlig databehandleraftale med eksterne databehandlere. | - |
| På hjemme-PC’er, som bruges til databehandling, er data krypteret.\*\* | Nej, men alle PC’er og applikationer, hvor personoplysninger behandles, er beskyttet med stærk adgangskode. |
| Der er givet instruktion vedrørende opbevaring og tilintetgørelse af udskrifter på hjemmearbejdspladser. | - |
| Der er fastsat interne retningslinjer for anvendelsen af hjemme PC-en, som også bruges privat. | - |
| Forbindelse mellem hjemmearbejdspladsen (PC) og kontoret (server) er beskyttet mod uvedkommendes indtagen. Dette sker via beskyttede/krypterede kanaler (VPN), passwordbeskyttelse osv. | - |
| Ved offentliggørelse af ansattes private oplysninger (f.eks. billede) indhentes et udtrykkeligt samtykke. | - |
| Der er defineret en klar politik vedr. fratrådt medarbejders e-mail konti jf. Datatilsynets retningslinjer. | - |
| Der er taget højde for straffelovens regler om brevhemmelighed vedr. arbejdsgiverens eventuelle læsning af den ansattes private e-mails. | - |
| Oplysningerne overføres kun til sikre tredjelande, områder/sektorer. | - |

*\*\*At e-mails med CPR krypteres, samt at dataene på hjemme-PC’er er krypteret, anbefales, men er er pt. ikke et lovkrav.*