Databeskyttelsespolitik for Tølløse Privat- og Efterskole

Overordnet organisering af behandlingen af personoplysninger

Tølløse Privat- og Efterskole (herefter TPOE) ønsker som hovedregel at anvende digitale systemer til behandling og opbevaring af data, herunder personoplysninger. De digitale systemer, der benyttes, leveres af eksterne professionelle leverandører, der sikkert hoster og stiller systemerne til rådighed, så TPOE ikke selv har behov for at råde over kompetence til at stå for den daglige drift af sådanne systemer.

TPOE ønsker i videst muligt omfang at organisere behandling og opbevaring af personoplysninger i dedikerede digitale systemer, så personoplysninger ikke findes fordelt på flere systemer, og så de ikke findes i både elektronisk og manuel form.

1. Formål

Databeskyttelsespolitikken beskriver det ***ledelsesgodkendte niveau*** for datasikkerheden på TPOE. Den indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af TPOE's ***Databeskyttelseshåndbog*** (GDPR-doc I-4) med de underliggende retningslinjer og forretningsgange.

De retningslinjer, der udformes for at understøtte databeskyttelsespolitikkens hovedmålsætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til datasikkerhed ved behandling af personoplysninger i det daglige arbejde.

Databeskyttelsespolitikken er især formuleret med henblik på beskyttelse af personoplysninger, men den finder også anvendelse på TPOE's øvrige data, f.eks. økonomiske oplysninger.

Datasikkerhed udgør en **nøgleværdi** og er en naturlig del af TPOE's digitale og manuelle databehandling, herunder især behandlingen af personoplysninger.

2. Omfang

Databeskyttelsespolitikken er gældende for alle, der er tilknyttet TPOE som medarbejdere, ledelse, bestyrelse, leverandører og samarbejdspartnere.

Alle ***leverandører og samarbejdspartnere***, som har fysisk eller online adgang til TPOE's digitale systemer, data og personoplysninger, skal gøres bekendt med denne databeskyttelsespolitik og forpligte sig til at følge den.

Databeskyttelsespolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af TPOE's digitale databehandlingssystemer samt manuelle arkiver og registre.

3. Hovedmålsætninger og sikkerhedsniveau

TPOE har følgende sikkerhedsmålsætning:

"Tølløse Privat- og Efterskole har et passende og tilstrækkeligt teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data, ved hel eller delvis anvendelse af digital databehandling, on-lineadgang samt for behandling af papirbaserede personoplysninger."

Et passende og tilstrækkeligt databeskyttelsesniveau[1] søges opnået ved tekniske og organisatoriske foranstaltninger, der sikrer:

- ***vedvarende fortrolighed, integritet, tilgængelighed og robusthed*** af TPOE's digitale databehandlingssystemer og databehandlingstjenester i forhold til den risikovurdering der gennemføres for de enkelte systemer og personoplysninger.
- anvendelse af ***pseudonymisering og kryptering,*** hvor det er relevant, herunder ved dataudveksling med databehandlere og eksterne parter og offentlige myndigheder
- evnen til rettidigt at ***genoprette tilgængelighed*** af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse
- procedurer for regelmæssig **afprøvning*, vurdering og evaluering*** af databeskyttelsessikkerheden
- beskyttelse af TPOE's IT-aktiver, personoplysninger og øvrige data i TPOE's varetægt.

Et tilstrækkeligt sikkerhedsniveau ***fastholdes*** ved:

- at der ***vedvarende*** forefindes ***retningslinjer og forretningsgange***, som sikrer, at databehandlings-behandlingssikkerheden er en integreret del af TPOE's drift og daglige arbejde. Målet er at sikre en kontinuerlig forbedringsproces, der løbende vedligeholder og optimerer databeskyttelses-politikken, retningslinjer og forretningsgange.
- at det igennem ***kontrakt- og leverandørstyring*** sikres, at brugen af eksterne leverandører, konsulenter og samarbejdspartnere lever op til den gældende databeskyttelseslovgivning og TPOE's databeskyttelsesniveau.
- at der i forbindelse med indførelse af ***nye digitale systemer*** gennemføres:
    - passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er ***nødvendige,*** behandles
    - hvis det skønnes nødvendigt, gennemføres en analyse af konsekvenserne for beskyttelse af oplysninger ved den påtænkte behandling af personoplysninger (***konsekvensanalyse***)
- at TPOE følger op på datasikkerheden igennem løbende vedligeholdelse og optimering af databeskyttelsespolitikken og de dertil hørende retningslinjer og forretningsgange.

4. Organisation og ansvar

Sikkerhedsmålsætning:

"***Alle medarbejdere har ansvar for datasikkerheden. De er bekendte med og efterlever skolens databeskyttelsespolitik, retningslinjer og forretningsgange, som er beskrevet i TPOE's Databeskyttelseshåndbog (GDPR-doc I-4).***"

Planlægning, implementering og kontrol af datasikkerheden varetages af skolens daglige ledelse, der også er ansvarlig for implementering og vedligeholdelse af sikkerhedssystemerne og er ansvarlig for opfølgning på sikkerhedshændelser og eventuelle brud på datasikkerheden.

Den daglige ledelse fastsætter i sin ***Databeskyttelseshåndbog*** (GDPR-doc I-4), ***hvem der har ansvaret*** for hvert af TPOE's, ***digitale og manuelle databehandlingssystemer***, styring af ***systemadgang og netværks-adgang***, tildeling af rettigheder, indgåelse af ***IT-kontrakter og andre kontrakter***, ***indkøb af hardware og installation af software,*** behandling af ***henvendelser fra de***

[1] Som beskrevet i Databeskyttelsesforordningen artikel 32

registrerede, opsamling og styring af ***anmeldelse af brud på persondatasikkerheden*** til både Datatilsynet og til de registrerede, der er berørt af bruddet

Databeskyttelsespolitikken revurderes og godkendes én gang årligt, eller eventuelt i forbindelse med situationer, der nødvendiggør det.

Ledelse og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Medarbejdere, der konstaterer eller oplever brud på datasikkerheden, skal anmelde det hurtigst muligt til nærmeste ledere eller den udpegede kontaktperson for personoplysninger.

Den nødvendige viden og kompetence om databeskyttelse og sikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring databeskyttelse og sikkerhed.

Den daglige ledelse er ansvarlig for, at databeskyttelsespolitikken overholdes, og bestyrelsen påser, at det sker.

5. Databeskyttelseshåndbogen

Databeskyttelsespolitikken uddybes af den daglige ledelse i skriftlige retningslinjer og forretningsgange.

Databeskyttelseshåndbogen (GDPR-doc I-4) indeholder bl.a. retningslinjer for:

1. *medarbejdernes håndtering af IT-sikkerhed*
2. *adgangsstyring*
3. *behandling af data på mobile enheder*
4. *anvendelse af sikker mail*
5. *netværksstyring*
6. *styring af sikkerhedshændelser (brud)*
7. *behandling af personoplysninger*
8. *styring af IT-leverandører og databehandlere*

Tilsammen udgør denne databeskyttelsespolitik, ***Databeskyttelseshåndbogen*** (GDPR-doc I-4), øvrige retningslinjer, beredskabspolitik og forretningsgange, TPOE´s samlede dokumenterede grundlag for overholdelse af gældende regler om behandling af personoplysninger.

6. Principper og forretningsgange for behandling af personoplysninger

Den daglige ledelse fastsætter principper og forretningsgange for behandling af personoplysninger, der sikrer overholdelse af Databeskyttelsesforordningen og Persondataloven.

Forretningsgangene, der ***dokumenteres***, omfatter:

- ***Principper for behandling af personoplysninger***
- Anvendelse af ***samtykke*** som grundlag for behandling af personoplysninger
- Procedurer for udøvelse af den ***registreredes rettigheder,*** herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabilitet

- ***Fortegnelser udarbejdet over behandlingsaktiviteter*** med personoplysninger

7. Risikovurdering og klassifikation af data

Risikovurdering
Skolen ønsker at være bevidst om enhver risiko og ud fra en risikovurdering opnå, at et passende og tilstrækkeligt sikkerhedsniveau etableres både elektronisk og fysisk.

Den daglige ledelse deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici ved automatisk og manuel databehandling.

En gang årligt, evaluerer den daglige ledelse den aktuelle risikovurdering og vurderer om revurdering og opdatering er påkrævet. Det samme skal ske ved betydelige ændringer i opgaver, leverandører og digitale systemer.

Klassifikation
For at sikre, at digitale systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, integritet (pålidelighed) og fortrolighed.

Tilgængelighed
I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

For TPOE er det især vigtigt med høj tilgængelighed til data og digitale systemer, der indeholder oplysninger, som anvendes i forbindelse med behandling af personoplysninger, personaleadministration, herunder lønudbetaling – og indberetninger til myndigheder.

Tilgængeligheden sikres først og fremmest gennem bestemmelser i de IT-kontrakter og/eller databehandleraftaler, der indgås med leverandørerne.

Integritet og pålidelighed
Med integritet og pålidelighed menes, at data om og i de digitale systemer er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.

Det er for skolen især vigtigt med høj integritet og pålidelighed i data og IT-systemer, der indeholder oplysninger, som anvendes i forbindelse med behandling af personoplysninger og personaleadministration.

Integritet og pålidelighed sikres først og fremmest gennem den kvalitetskontrol, der finder sted under de fastlagte forretningsgange for behandling af personoplysninger og -sager.

Fortrolighed
Med ***fortrolighed*** menes der, at kun autoriserede personer har ret til at tilgå personoplysningerne, og personoplysningerne kun skal være tilgængelige for autoriserede personer.

Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse har anden hjemmel i lovgivningen.

I ***Databeskyttelseshåndbogen*** (GDPR-doc I-4) angives hvilke personer, der har adgang til personoplysninger om elever, pårørende og medarbejdere.

8. Overholdelse af databeskyttelsespolitikken

Alle medarbejdere på TPOE er forpligtet til at efterleve den til enhver tid gældende data-beskyttelsespolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle medarbejdere modtager ved deres ansættelse et eksemplar af den aktuelle og gældende ***Databeskyttelseshåndbog*** (GDPR-doc I-4) og instrueres om digital adgang til skolens øvrige dokumentationsmateriale om datasikkerhed.

9. Afvigelser

Hvis der opstår situationer, hvor kravene i Databeskyttelsespolitikken helt undtagelsesvist ikke kan efterleves, skal det undtagelsesfrit godkendes af den daglige ledelse og dokumenteres, og der indføres alternative sikringsforanstaltninger.

10. Udarbejdelse og ikrafttrædelse

Ændringer i sikkerhedsdokumentationen forelægges og godkendes af den daglige ledelse.

Databeskyttelsespolitikken er godkendt af bestyrelsen for Tølløse Privat- og Efterskole på sit møde den __. _____ 2023 og træder i kraft samme dato.

Tølløse den / 2023

_____

Peter Krogh Jacobsen, Bestyrelsesformand