

Retningslinje om brud på persondatasikkerheden

Anvendelsesområde

Retningslinje om brud på persondatasikkerheden er udarbejdet i overensstemmelse med kravene i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (betegnet "forordningen" i det følgende) og gælder for alle ansatte på Tornbjerg Gymnasium, der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af Tornbjerg Gymnasium.

Formål

Formålet med denne retningslinje er at sikre, at Tornbjerg Gymnasium håndterer eventuelle brud på persondatasikkerheden korrekt og i overensstemmelse med forordningens krav. Dette indebærer bl.a., at der sker anmeldelse til Datatilsynet, og at den registrerede underrettes i de tilfælde, hvor det er påkrævet.

Definitioner

Personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Den registrerede er den fysiske person, som personoplysningerne vedrører, eksempelvis medarbejdere, elever, leverandører, samarbejdspartnere og andre.

Behandling af personoplysninger skal fortolkes bredt. Begrebet "behandling" dækker over enhver aktivitet eller en række af aktiviteter, som personoplysninger gøres til genstand for. Det kan eksempelvis være indsamling, registrering, organisering, systematisering, opbevaring, ændring, søgning, formidling og sletning.

Dataansvarlig er den person eller myndighed/organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler er den, der behandler personoplysninger på den dataansvarliges vegne – dvs. arbejder under instruks af den dataansvarlige. Databehandler er i henhold til forordningen forpligtet til at føre fortegnelse over behandlingskategorier, der føres på vegne af den dataansvarlige.

Brud på persondatasikkerheden dækker over alle tilfælde, der fører til hændelig eller ulovlig tilintetgørelse, tab, eller ændring af personoplysninger såvel som uautoriseret videregivelse af eller adgang til personoplysninger.

Databeskyttelsesrådgiveren (DPO) er en uafhængig person med ekspertise i databeskyttelsesret og – praksis, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler hos Tornbjerg Gymnasium. Databeskyttelsesrådgiverens funktion er at understøtte, at Tornbjerg Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er en integreret del af Tornbjerg Gymnasium, og kan efter omstændighederne have andre arbejdsopgaver.

Tekniske og organisatoriske sikkerhedsforanstaltninger skal vurderes ved en risikovurdering af behandlingen af personoplysninger. Tekniske sikkerhedsforanstaltninger er blandt andet antivirusprogrammer og firewalls, som sikrer, at uvedkommende ikke kan få adgang til it-systemer med personoplysninger.

Organisatoriske sikkerhedsforanstaltninger består blandt andet i, at vores medarbejdere er instrueret i og uddannet til at håndtere behandlingen af personoplysningerne korrekt og sikkert.

Hvordan håndterer Tornbjerg Gymnasium et brud på persondatasikkerheden?

Det kan have omfattende konsekvenser for den registrerede, hvis et brud på persondatasikkerheden ikke håndteres på en passende og rettidig måde. Konsekvenserne kan eksempelvis være tab af kontrol over den registreredes personoplysninger, forskelsbehandling, identitetstyveri, finansielle tab, tab af omdømme eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Det skal derfor sikres, at Tornbjerg Gymnasium har en klar procedure for håndtering af brud på persondatasikkerheden, når Tornbjerg Gymnasium er henholdsvis dataansvarlig og databehandler

Når Tornbjerg Gymnasium er dataansvarlig

Hvis der sker et brud på persondatasikkerheden, skal Tornbjerg Gymnasium, som hovedregel, og senest inden for 72 timer fra Tornbjerg Gymnasium er blevet bekendt med bruddet, anmelde det til Datatilsynet.

Såfremt Tornbjerg Gymnasium kan dokumentere, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske anmeldelse til Datatilsynet.

Tornbjerg Gymnasium skal således foretage en risikovurdering af hvad bruddet har haft af betydning for den registrerede.

I vurderingen af risikoen skal der tages udgangspunkt i de konsekvenser sikkerhedsbruddet kan have for den registrerede, samt hvad sandsynligheden for disse konsekvenser er.

Afhængigt af hvilken grad af risici vores risikovurdering kommer frem til, skal følgende procedurer følges:

Risici:	Procedure:
Bruddet indebærer ingen risiko for den registrerede	Ej anmeldelsespligt til datatilsynet
Bruddet indebærer en risiko for den registrerede	Anmeldelsespligt til Datatilsynet
Bruddet indebærer en høj risiko for den registrerede	Anmeldelsespligt til Datatilsynet, samt underretning til den registrerede

Risici og procedure uddybes nedenfor:

Bruddet indebærer ingen risiko for den registrerede

I de tilfælde hvor den udførte risikovurdering viser, at det er usandsynligt, at bruddet på persondatasikkerheden har indebåret en risiko for den registreredes rettigheder, er bruddet ikke anmeldelsespligtigt til Datatilsynet.

Bruddet indebærer en risiko for den registrerede

Hvis risikovurderingen viser, at sikkerhedsbruddet indebærer en risiko for den registrerede, er Tornbjerg Gymnasium forpligtet til at anmelde bruddet til Datatilsynet. Anmeldelsen skal ske hurtigst muligt, og senest 72 timer fra Tornbjerg Gymnasium er blevet bekendt med bruddet.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
2. Kategorier af registrerede
3. Antal af berørte registrerede
4. Kategorier af personoplysninger
5. Antal af berørte registreringer af personoplysninger
6. Navn og kontaktoplysninger på Tornbjerg Gymnasiums databeskyttelsesrådgiver
7. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
8. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Tornbjerg Gymnasium har truffet eller foreslår truffet for at mindske skaden.

Se endvidere bilag 1, som indeholder en skabelon til brug for anmeldelse.

Bruddet indebærer en høj risiko for den registrerede

I de tilfælde hvor den udførte risikovurdering viser, at bruddet på persondatasikkerheden har indebåret en høj risiko for den registreredes rettigheder, skal bruddet anmeldes til Datatilsynet og de registrerede skal desuden, som hovedregel, underrettes – se dog undtagelser for underretning nedenfor. Hvis det skulle ske, at Tornbjerg Gymnasium i vores risikovurdering er nået frem til, at bruddet ikke indebærer en høj risiko for den registrerede, kan Tornbjerg Gymnasium i visse tilfælde alligevel blive pålagt at underrette den registrerede, såfremt Datatilsynet i deres undersøgelse af bruddet vurderer, at der har været tale om en høj risiko.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
2. Kategorier af registrerede
3. Antal af berørte registrerede
4. Kategorier af personoplysninger
5. Antal af berørte registreringer af personoplysninger
6. Navn og kontaktoplysninger på Tornbjerg Gymnasiums databeskyttelsesrådgiver
7. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
8. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Tornbjerg Gymnasium har truffet eller foreslår truffet for at mindske skaden.

Anmeldelsen kan sendes til dt@datatilsynet.dk eller via Datatilsynets hjemmeside. Se endvidere bilag 1, som indeholder en skabelon til brug for anmeldelse

Underretningen til den registrerede skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet
2. Navn og kontaktoplysninger på Tornbjerg Gymnasiums databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet

4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Tornbjerg Gymnasium har truffet eller foreslår truffet for at mindske skaden.

Se endvidere bilag 2, som indeholder en skabelon til brug for underretning af den registrerede.

Situationer hvor Tornbjerg Gymnasium, på trods af høj risiko, ikke er forpligtet til at underrette den registrerede.

Én af følgende betingelser skal være opfyldt:

1. Tornbjerg Gymnasium har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
2. Tornbjerg Gymnasium har efter bruddet truffet foranstaltninger, der sikrer, at den høje risiko for den registreredes rettigheder sandsynligvis ikke længere er reel
3. Det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved den registrerede underrettes på en tilsvarende effektiv måde.

Databeskyttelsesrådgiveren

Tornbjerg Gymnasiums databeskyttelsesrådgiver inddrages altid, når der sker et brud på persondatasikkerheden.

Når Tornbjerg Gymnasium er databehandler

Tornbjerg Gymnasium er forpligtet til at dokumentere alle brud på persondatasikkerheden. Efter anmodning fra Datatilsynet, skal vi udlevere denne dokumentation.

Dokumentationen skal som minimum indeholde følgende:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
2. Kategorier af registrerede
3. Antal af berørte registrerede
4. Kategorier af personoplysninger
5. Antal af berørte registreringer af personoplysninger
6. Navn og kontaktoplysninger på Tornbjerg s databeskyttelsesrådgiver
7. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
8. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Tornbjerg Gymnasium har truffet eller foreslår truffet for at mindske skaden.
9. Dokumentation for anmeldelse til Datatilsynet og evt. underretning til den registrerede.

Kontrol og dokumentation

Tornbjerg Gymnasium skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af Tornbjerg Gymnasiums bestyrelse.

Tornbjerg Gymnasium skal kunne dokumentere (påvise), at:

1. Vi foretager den nødvendige risikovurdering i forhold til den registreredes rettigheder
2. Vi anmelder brud på persondatasikkerheden i de tilfælde, hvor det er påkrævet
3. Anmeldelsen indeholder de minimumskrav, som forordningen stiller
4. Vi underretter den registrerede om brud persondatasikkerheden i de tilfælde, hvor bruddet har indebåret en høj risiko for den registrerede
5. Vi har instrueret vores databehandlere i at underrette os, hvis der sker et brud
6. Vi overholder den løbende kontrol

Kontrol og dokumentation

Bestyrelsen på Tornbjerg Gymnasium sikrer, at overholdelsen af *retningslinjer om brud på persondatasikkerheden* er dokumenteret, og at dokumentationen løbende opdateres.

Dokumentejer, godkender og versionering

Ejer: Susanne Wulff Jørgensen swj@tornbjerg-gym.dk

Godkender: Jens Uffe Hansen uh@tornbjerg-gym.dk

Dato:	Version:	Forfatter:	Ændringsbeskrivelse:
23.05.18	1.0	SWJ	Tilrettet og opdateret version
25.08.22	2.0	SWJ	Tilrettet og opdateret version

Bilag 1: Anmeldelse til Datatilsynet

1. Gå ind på www.datatilsynet.dk
2. Vælg "anmeld brud på persondatasikkerheden" og lav selve anmeldelsen
3. For at kunne udfylde anmeldelsen skal du bruge NemID

Navn på dataansvarlig og dennes databeskyttelsesrådgiver:

Organisationsnavn:	Tornbjerg Gymnasium:
CVR/EAN-nummer:	29553939 / 5798000558304
Adresse:	Skærmhatten 15 5220 Odense SØ
Kontaktperson: DPO/Andreas Esbech	<i>Klik på link</i> https://itcfyn.dk/om-it-center-fyn/persondata/

Bilag 2: Skabelon til underretning af registrerede

Dato (xx.xx.xxxx)

Kære (xxxx)

Vi må desværre meddele dig, at Tornbjerg Gymnasium (d. xx.xx.xxxx) har fået kompromitteret vores persondatasikkerhed. Dette sikkerhedsbrud er allerede anmeldt til Datatilsynet under sagsnr.: (DT-00193).

Beskrivelse af sikkerhedsbrud

Indsæt beskrivelse – eksempelvis: ("en af vores medarbejdere har ved en fejl delt et udtræk af personoplysninger fra et af vores kernesystemer med en ekstern. Dette udtræk inkluderede oplysninger om dig på følgende område...").

(Indsæt kategorier – eksempelvis:)

- *Navn*
- *Adresse*
- *Telefonnummer*
- *Fødselsdato*
- *CPR-nummer*
- *Etnisk oprindelse*
- *Land for pasudstedelse*
- *Pasnummer*

Vi behandler dine personoplysninger, som led i at kunne *(indsæt formål)*.

Konsekvenser for din person ved sikkerhedsbruddet

Da datasikkerhedsbruddet indeholder *(følsomme oplysninger)* om dig, gør vi dig opmærksom på, at det vil kunne indebære at offentligheden kan have fået adgang til dine personoplysninger.

Foranstaltninger for at afhjælpe bruddet på persondatasikkerheden

Indsæt beskrivelse – eksempelvis: ("Vi har allerede nu sørget for at destruere alle versioner af de pågældende udtræksfiler, der ligger inden for grænserne af organisation. Den eksterne person, som data har været delt med, er også blevet kontaktet og har slettet sin version af oplysningerne.

Oplysningerne har imidlertid i kort tid været delt på et online fildrev, og vi er pt. i dialog med udbyderen, for at sikre at data også fjernes i eventuelle backupper, samt at høre om de har været udsat for nogen former for kriminalitet i det tidsrum, hvor data har eksisteret på deres servere").

Yderligere informationer og kontakt til os

Såfremt du har yderligere spørgsmål til kompromitteringen af dine personoplysninger, beder vi dig venligst tage kontakt til vores databeskyttelsesrådgiver, se nedenfor.

Andreas Esbech/DPO – Klik på nedstående link:

<https://itcfyn.dk/om-it-center-fyn/persondata/>

Endnu engang må vi beklage den risiko, vi har udsat dig for.

På vegne af Tornbjerg Gymnasium

(xxxx)