Retningslinjer om 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.

Når Vordingborg Gymnasium & HF er dataansvarlig

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

Såfremt Vordingborg Gymnasium & HF 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.

Vi 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 underretningspligt over for den registrerede.

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 Vordingborg Gymnasium & HF forpligtet til at anmelde bruddet til Datatilsynet. Anmeldelsen skal ske hurtigst muligt, og senest 72 timer fra Vordingborg Gymnasium & HF er blevet bekendt med bruddet.

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 vi i vores risikovurdering er nået frem til, at bruddet ikke indebærer en høj risiko for den registrerede, kan vi 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.

Anmeldelser til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt;
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på Vordingborg Gymnasium & HF's databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Vordingborg Gymnasium & HF har truffet eller foreslår truffet for at mindske skaden.

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 Vordingborg Gymnasium & HF's databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Vordingborg Gymnasium & HF 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 Vordingborg Gymnasium & HF, på trods af høj risiko, ikke er forpligtet til at underrette den registrerede.

Én af følgende betingelser skal være opfyldt:

1. Vordingborg Gymnasium & HF 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. Vordingborg Gymnasium & HF 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
Vordingborg Gymnasium & HF's databeskyttelsesrådgiver inddrages altid, når der sker et brud på persondatasikkerheden.

Når Vordingborg Gymnasium & HF er databehandler

I de tilfælde, hvor Vordingborg Gymnasium & HF er databehandler for en anden dataansvarlig, underretter vi, uden unødig forsinkelse, den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Fortegnelse over sikkerhedsbrud

Vordingborg Gymnasium & HF 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;
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på Vordingborg Gymnasium & HF's databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Vordingborg Gymnasium & HF har truffet eller foreslår truffet for at mindske skaden.
5. Dokumentation for anmeldelse til Datatilsynet og evt. underretning til den registrerede.

Kontrol og dokumentation

Vordingborg Gymnasium & HF skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes.

Vordingborg Gymnasium & HF skal kunne dokumentere (påvise), at:
- Vi foretager den nødvendige risikovurdering i forhold til den registreredes rettigheder
- Vi anmelder brud på persondatasikkerheden i de tilfælde, hvor det er påkrævet
- Anmeldelsen indeholder de minimumskrav, som forordningen stiller
- Vi underretter den registrerede om brud persondatasikkerheden i de tilfælde, hvor bruddet har indebåret en høj risiko for den registrerede
- Vi har instrueret vores databehandlere i at underrette os, hvis der sker et brud
- Vi overholder den løbende kontrol

Revisionshistorik			
Version	Note	Dato	Redigeret af
v.1.00		25-05-2018	LU

Bilag 1: skabelon til anmeldelse til Datatilsynet

Dataansvarliges sagsnr.: _____

Navn på dataansvarlig og dennes databeskyttelsesrådgiver

Organisationsnavn	Vordingborg Gymnasium & HF
CVR / EAN	
Adresse	
Kontaktperson	
Telefon	
E-mail	

Involverede databehandlere

Databehandler

Organisationsnavn	
CVR / EAN	
Adresse	

Underdatabehandler 1

Organisationsnavn	
CVR / EAN	
Adresse	

Underdatabehandler 2

Organisationsnavn	
CVR / EAN	
Adresse	

Beskrivelse af sikkerhedsbruddet

Beskrivelse af karakteren af bruddet, herunder kategorier af personoplysninger, behandlinger og antal af berørte registrerede

Har bruddet eksponeret følsomme personoplysninger for den registrerede? | |

Konsekvensanalyse af sikkerhedsbrud

Beskrivelse af sandsynlige konsekvenser for den registrerede ved bruddet på persondatasikkerheden

Mitigerende foranstaltninger

Beskrivelse af de foranstaltninger, som Vordingborg Gymnasium & HF foreslår eller har iværksat for at afhjælpe bruddet på persondatasikkerheden

Bilag 2: skabelon til underretning af registrerede

[xx.xx.xxxx]

Kære [xxx]

Vi må desværre meddele dig, at [indsæt skole] [den xx.xx.xxxx] har fået kompromitteret vores persondatasikkerhed. Dette sikkerhedsbrud er allerede anmeldt til Datatilsynet, undersagsnr.: [DT-00193].

Beskrivelse af sikkerhedsbrud
[Indsæt beskrivelse, eksempelvis: "en af vore 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 områder]:

[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 sikkerhedsbruddet 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
Vi har allerede nu sørget for at [indsæt konkrete foranstaltninger – eksempelvis "destruere alle versioner af de pågældende udtræksfiler der ligger inden for grænserne af vores 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 er fjernet 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:

Kontaktperson	Flemming Rasmussen
Telefon	20601942
E-mail	Fr@efif.dk

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

På vegne af Vordingborg Gymnasium & HF