DANSK OPLYSNINGS FORBUND

Ny Østergade 7, 1. sal
4000 Roskilde
Tlf. 70 20 60 20
www.danskoplysning.dk
post@danskoplysning.dk

Brud på persondatasikkerheden

Marts 2018

Baggrund og formål

Et af de mest omtalte emner i Databeskyttelsesforordningen relateres til brud på persondatasikkerheden, idet forordningen introducerer nogle meget konkrete forpligtelser:

- Krav om intern dokumentation om brud på persondatasikkerheden,
- Anmeldelsespligt til Datatilsynet og
- Underretningspligt mht. de registrerede.

Formål med dette afsnit er at forklare nogle af hovedelementer vedr. disse forpligtelser.

Yderligere informationer kan indhentes i Datatilsynets Vejledning om håndtering af brud på persondatasikkerheden (februar 2018), samt lovteksten i databeskyttelsesforordningens kapitel IV, afdeling 2 og afsnittene 5.11. og 5.12. i betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

Hvad er et brud på persondatasikkerheden?

Et brud på persondatasikkerheden defineres som: *"et brud i sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller anden de behandlet."*

Selvom brud på persondatasikkerheden tit forbindes med sikkerhedsbrud i de anvendte IT-systemer, relateres det også til skolens egen behandling af personoplysninger.

Således betragtes det også som et brud på persondatasikkerheden, når uautoriserede personer inden eller uden for skolen, får adgang til personoplysningerne. Det kan ske ved direkte uautoriseret adgang, eller hvis skolens personale, bevist eller ubevist, videregiver oplysningerne til en uautoriseret tredje part.

Når skolens medarbejdere ved et uheld sletter eller ændrer personoplysningerne, er der også tale om et brud.

Af andre eksempler kan det nævnes: tab af USB-stik med personoplysningerne; tyveri af skolens pc'er; hacking af serveren, hvor personoplysninger opbevares; uautoriseret login på skolens administrationsprogram mm.

Hvilke brud skal anmeldes Datatilsynet?

Som udgangspunkt skal Datatilsynet informeres om de fleste brud på persondatasikkerheden. Det er dog undtagelser, hvis det vurderes, at bruddet ikke indebærer en risiko for fysiske personers rettigheder.

Risikoen for fysiske personers rettigheder og frihedsrettigheder defineres som noget der bl.a. omfatter: *diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.*

Risikovurdering er skolens egen ansvar, og det er skolen selv, der skal lave en konkret vurdering af konsekvenserne af bruddet på persondatasikkerheden. Datatilsynet anbefaler, at følgende forhold altid indgår den konkrete risikovurdering:

1. **Typen af sikkerhedsbrud**
   Typer kan være: sletning, ændring, videregivelse, tyveri osv. Det er nemlig stor forskel for konsekvensvurdering, om personoplysningerne 'blot' er blevet slettet, eller om de er endt i de forkerte hænder med risiko for misbrug eller offentliggørelse.
2. **Oplysningernes art**
   Hvilke persondata (art) der er tale om, har en konkret betydning for risikovurdering. F.eks. vil oplysninger om ens helbred veje tungere end navn og adresse. Her skal man dog foretage en konkret vurdering, idet nogle personer kan bo på et bosted eller have adressebeskyttelse, hvor offentliggørelse kan få alvorlige konsekvenser for den pågældende.
3. **Oplysningernes omfang**
   Omfanget spiller en rolle kombineret med oplysningernes art. F.eks. har navn og adresse et lille omfang med evt. lille risiko. Men kompromittering af nogle få personfølsomme informationer kan på anden side have en stor betydning. På samme måde kan kompromittering af en større mængde mindre følsomme oplysninger (navn, adresse, telefon, e-mail, FB, Twitter mm.) tilsammen have skadelige konsekvenser.
4. **Den tidsmæssige udstrækning af bruddet.**
   Det må forudsættes, at bruddets varighed har en vis betydning for risikovurdering. F.eks. hvis en skoles PC ubeskyttet har stået 'til rådighed' til et ukendt antal uautoriserede personer i en længere periode.
5. **Risikoen for, at de registrerede kan identificeres**
   Et af hovedelementerne i forordningen er muligheden for at identificere fysiske personer ud fra de givne persondata. Hvis personoplysningerne f.eks. er krypteret, er der en meget lille risiko for, at de registrerede kan identificeres og hermed også en lille risiko at kompromittering kan have alvorlige konsekvenser.
6. **Konsekvenser bruddet kan have for de registrerede**
   Konsekvenser relateres direkte til ovenstående definition af risikoen for fysiske personers rettigheder og frihedsrettigheder. Derudover vil kompromittering af oplysninger om sårbare, udsatte personer eller børn altid kunne vurderes at have større skadevirkning.

7. **Hvorvidt bruddet omfatter særlige registrerede**
   Udover sårbare, udsatte personer eller børn kan det være andre persongrupper, hvis personoplysninger relateres til særlige omstændigheder. Det kan være personer under vidnebeskyttelse, offentlig kendte personer eller personer med særlige stillinger (domstole, militæret, politiet mm.)
8. **Antallet af berørte fysiske personer**
   Normalt vil antallet af berørte fysiske personer have en betydning for risikovurderingen: Jo flere berørte personer, desto større skade og desto sværere bliver det at rydde op efterfølgende. Det formindsker dog ikke alvorligheden ved kompromittering af oplysninger om én eller nogle få personer.

Hvilke brud skal ikke anmeldes Datatilsynet?

Hvis skolen vurderer, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder, skal det ikke anmeldes Datatilsynet.

Risikofri brud på persondatasikkerheden kan f.eks. skyldes de sikkerhedsforanstaltninger, som skolen har truffet, hurtig reaktion, eller de konkrete omstændigheder ved bruddet.

I takt med, at forordningen implementeres i Danmark, forventes der også lidt mere præcis definition af anmeldelsespligten. Vi kan dog ikke forvente en eksplicit facitliste, og anmeldelsespligten vurderes fra sag til sag og i forhold til det samlede aktuelle risikobillede.

På nuværende tidspunkt kan vi nævne nogle få eksempler, hvor bruddet på datasikkerheden ikke skal anmeldes Datatilsynet:

En skoleleder har tabt et USB-stik med deltagernes data i. Hukommelsen er beskyttet med stærk kryptering. Her vurderes det, at der er usandsynligt, at nogen vil kunne dekryptere informationerne.
En deltagerliste er ved en fejl sendt til DOF sekretariat. Skolen vurderer, at man har tillid til, at DOF ikke vil misbruge oplysningerne, og at mailen vil blive slettet.
En underviser på skolen har ved en fejl modtaget deltagerinformationer fra et andet hold. Skolen vurderer, at det er tale om en intern sag, og at skolen har stor tillid til, at underviseren ikke vil misbruge informationerne.
En medarbejder har ved en fejl offentliggjort deltagernes data på hjemmesiden. Det er sket om natten, og medarbejderen har hurtigt fjernet informationerne. Ved at kigge i logfiler kan man se, at der ikke var nogle besøgende på hjemmesiden på det tidspunkt, og at siden heller ikke er besøgt af Google eller andre søgemaskiner. Det vurderes, at det ikke er sandsynligt, at nogen har opdaget oplysningerne på hjemmesiden.

Skolens IT-systemer er nede i en periode pga. stormsvigt. Nedetiden har ingen konsekvenser for aftenskoles deltagere.
Skolen sender ved en fejl en tilmeldingskvittering til en forkert deltager. Skolen bliver gjort opmærksom på fejlen og aftaler med modtageren, at mail slettes. Skolen har tillid til, at modtager vil slette mailen. Skolen skal *sandsynligvis* ikke anmelde hændelsen idet det vurderes, at bruddet ikke indebærer en risiko for den registrerede.
Skolens bogfører sender ved en fejl en lønseddel til en forkert medarbejder. Skolen aftaler, at medarbejderen straks sletter lønsedlen. Da det er tale om internt brud på sikkerheden, og da skolen har tillid til medarbejderen, skal sagen ikke anmeldes Datatilsynet.
Ved et uheld sletter en af skolens medarbejdere data om en eller flere deltagere. Der er ingen økonomisk udestående med disse deltagere, og det kan ikke have nogle negative økonomiske konsekvenser.
Dataet på skolens server er blevet slettet pga. en systemfejl. Skolen har en backup som hurtigt indlæses. Skolen skal derfor ikke anmelde sagen.

Hvornår skal bruddet anmeldes Datatilsynet?

Som hovedregel skal et brud på persondatasikkerheden, som indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, anmeldes Datatilsynet uden *unødig* forsinkelse og senest **72 timer** efter, skolen er blevet bekendt med bruddet.

72 timers frist skal helst overholdes, og her tages der ikke hensyn til weekender, ferier eller helligdage. Forordningen tillader dog, at bruddet også anmeldes efter udløbet af fristen, hvor anmeldelsen i så fald suppleres med en begrundelse for forsinkelsen.

Hvor og hvordan anmeldes bruddet på persondatasikkerheden?

I løbet af foråret 2018 vil der på virk.dk blive oprettet en digital løsning for anmeldelser af sikkerhedshændelser. Der vil blive tale om en elektronisk blanket, som udfyldes og godkendes.

Hvilke informationer skal indgå i anmeldelsen?

Vi kan forvente, at den kommende indberetningsform på virk.dk vil være struktureret således, at det står klart, hvilke informationer anmeldelsen skal indeholde.
Pt. oplyser Datatilsynet, at anmeldelsen som minimum skal indeholde:

- Bruddets karakter, herunder kategorierne og antal berørte registrerede og registreringer.
- Navn og kontaktoplysninger, hvor yderligere oplysninger kan indhentes.
- Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden (se ovenfor).

- Beskrivelse af de trufne foranstaltninger for håndtering af bruddet og evt. foranstaltninger for at minimere mulige skadevirkninger.

Derudover er det også en god ide at udlevere yderligere informationer om bruddet for at skabe større forståelse og sikre, at forpligtelsen til at anmelde brud på persondatasikkerhed er overholdt.

Hvem anmelder bruddet til Datatilsynet?

Anmeldelse er skolens ansvar, og skolen bør udpege en eller flere personer, som bemyndiges til at anmelde eventuelle brud. Skolen kan også bemyndige skolens Databehandler og sørge for, at dette er nedskrevet i Databehandlingsaftalen. Det juridiske ansvar for rettidig anmeldelse forbliver dog hos skolen selv.

Skal de registrerede informeres om bruddet?

Når et brud indebærer en ***høj*** risiko for fysiske personers rettigheder og frihedsrettigheder, skal skolen også underrette de registrerede om bruddet uden unødig forsinkelse.

Desværre har databeskyttelsesforordningen ikke en definition for "*høj risiko*", og derfor må formuleringen alene hvile på skolens egen risikovurdering. Det siger sig selv, at jo mere alvorlige konsekvenser et brud kan medføre, desto større risiko vil være for de registrerede. Skolen må derfor selv vurdere, hvornår risikoen kan betragtes som høj.

Et eksempel på høj risiko kunne være kompromittering af brugernes navne, mails og adgangskoder. Da mange mennesker genbruger adgangskoder til forskellige konti, er risikoen for alvorlige konsekvenser relativ høj. Derudover skal skolen nulstille adgangskoderne og forklare brugerne, hvorfor det sker. På den måde har brugerne også mulighed for selv at ændre deres adgangskoder andre steder.

Et andet eksempel på "høj" risiko kunne være, hvis en skole i en periode har offentliggjort (f.eks. på hjemmesiden) deltagernes data inklusiv CPR-nr. Hvis der er en stor sandsynlighed for, at Google eller andre søgemaskiner har nået at indeksere hjemmesiden og herunder deltagernes personoplysninger, bør deltagerne informeres om hændelsen.

Datatilsynet kan også selv pålægge skolen underretningspligt, hvis de vurderer, at et anmeldt brud indebærer en høj risiko.

Selve underretning skal formuleres i klart og letforståeligt sprog og skal som minimum indeholde:

- Navn og kontaktoplysninger, hvor yderligere oplysninger kan indhentes.
- Beskrivelse af sandsynlige konsekvenser er bruddet på persondatasikkerheden.

- Beskrivelse af de trufne foranstaltninger for håndtering af bruddet og evt. foranstaltninger for at minimere mulige skadevirkninger.

Jf. lovforslaget til en ny databeskyttelseslov (L 68) kan kravet om underretning af brud på persondatasikkerheden til den registrerede suspenderes med hensyn til efterforskning af strafbare forhold, herunder forstyrrelser i driften af IT-systemer.

Intern dokumentation

Alle brud på persondatasikkerheden skal dokumenteres, uanset om skolen er forpligtet til at anmelde bruddet til Datatilsynet eller ej. Denne dokumentationspligt hænger sammen med persondataforordningens krav om ansvarlighed, og skolen har pligt til at udlevere dokumentation til Datatilsynet efter en evt. anmodning.

Der stilles ikke specifikke formkrav til dokumentationen, men Datatilsynet anbefaler, at følgende punkter behandles:

Brud på persondatasikkerheden hos [Skolenavn]	Beskrivelse af bruddet
Dato og tidspunkt for bruddet	
Hvad er der sket?	
Årsagen til bruddet?	
Hvilke (typer) personoplysninger er omfattet af bruddet?	
Hvilke konsekvenser har bruddet for de berørte personer?	
Hvilke afhjælpende foranstaltninger er truffet?	
Hvorvidt der er sket anmeldelse til Datatilsynet eller ej (hvis ja, hvornår)?	
Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet?	
Er der sket underretning af de berørte personer (hvis ja, hvornår)?	
Hvis nej, begrundelse for ikke at underrette de berørte personer?	

Datatilsynets flowchart