LAVUK STJERNEN
Center for Selvejende Dagtilbud

Formålet med forretningsgangen er at Sikre overholdelse af databeskyttelseslovgivningen i forbindelse med persondatabrud. Det er bestyrelsen og den daglige leder der har ansvaret for at al persondatahåndtering foregår lovmæssigt korrekt.

Det der sætter processen i gang er, når en medarbejder i et dagtilbud får kendskab til et potentielt persondatabrud eller kan konstatere at der er sket et konkret brud. Det kan også være en henvendelse fra borgere eller pårørende der henvender sig.

Reglen er:

- **At alle medarbejdere i Center for selvejende Dagtilbud (CSD) har pligt til at anmelde persondatabrud.**

Herunder er oplistet de roller der ud over medarbejderen er omfattet proces og forretningsgang.

I Center for Selvejende Dagtilbud er det udviklingskonsulent Mille Nordstrand der er nøgleperson.

Rolle/funktion	**Beskrivelse**	**Ansvar/opgaver**
CSD nøgleperson	En udpeget person hos CSD, der varetager de organisatoriske og kommunikationsmæssige opgaver i forbindelse med persondatabrud hos CSD. Personen bør have tilstrækkeligt kendskab til CSD, samt adgang til nødvendige oplysninger og systemer, for at kunne undersøge bruddet og samarbejde med relevante parter.	Håndtere og koordinere it-, juridiske- og kommunikationsmæssige opgaver i forbindelse med persondatabruddet Herunder: • Oprette og beskrive/dokumentere sagen • Standse bruddet i det omfang, det er muligt • Orientere DPO og CSD-ledelsen • Udarbejde anmeldelsen af persondatabrud til Datatilsynet • Evt. underretning af den registrerede. • Dokumentere / opdatere persondatabrudenes forløb i fra start til slut.
DPO	Databeskyttelsesrådgiveren (DPO) er CSD's kontaktpunkt vedrørende rådgivning og tilsyn med efterlevelse af Databeskyttelsesforordningen.	DPO har ansvaret for: • Vejlede CSD nøgleperson i alle forhold vedr.

	Der henvises til stillingsbeskrivelse for DPO.	persondatabruddet i takt med at denne anmoder herom. • At underrette Datatilsynet.
KIT	KIT (Koncern IT) er vidensorganisation og sparringspartner for DPO og CSD i forbindelse med potentielle persondatabrud der har relation til KK-systemer.	KIT har ansvaret for følgende opgaver: • Opsamle og opbevare information om persondatabrud, ved brud der påvirker KK systemer • Bistå CSD med efterforskning og analyse ved behov • Afrapportere til DPO-funktionen

NR.	AKTIVITET	UDFØRER	HANDLINGER I AKTIVITETEN	VEJLEDNING / RÅDGIVNING
Start	CSD-medarbejder får kendskab til et potentielt persondatabrud og anmelder det til Nøgleperson	CSD-medarbejder	CSD-medarbejder orienterer Nøgleperson om det potentielle sikkerhedsbrud via telefon, mail til en speciel postkasse eller mundtligt.	CSD interne retningslinjer
1	Modtag og vurdér information om potentielt brud	CSD Nøgleperson	Nøgleperson modtager indberetningen fra medarbejderen og vurderer, hvorvidt det kan betragtes som et sikkerhedsbrud, evt. med rådgivning fra DPO.	Afsnit 1 - Vejledning til håndtering af brud på persondatasikkerheden Søg rådgivning hos DPO
2	Stands bruddet	CSD Nøgleperson	CSD Nøgleperson iværksætter straks alle relevante tiltag for at stoppe Sikkerhedsbruddet og minimere skaden.	Søg rådgivning hos DPO
3	Orienter ledelsen	CSD Nøgleperson	Når en indberetning om potentielt Sikkerhedsbrud modtages, underrettes ledelsen og DPO, og aktiviteter herunder sættes i gang. Ledelsen og DPO underrettes løbende om Situationen og orienteres om udviklingen.	

4	Indsaml fakta og dan overblik	CSD Nøgleperson	Nøglepersonen danner Sig et overblik over bruddet og navnlig omstændighederne omkring dette	Afsnit 1 – Vurdering af Sikkerhedsbrud
5	Kontakt evt. leverandører	CSD Nøgleperson	Underretning af involverede leverandører. Leverandørerne anmodes om at udarbejde en detaljeret redegørelse over hændelsesforløbet, baggrunden for fejlen, konsekvenserne heraf, hvordan fejlen er rettet og hvordan det Sikres, at det ikke kan ske igen. Leverandørens redegørelse af Sikkerhedsbruddet bedes udarbejdes for at oplyse de informationspunkter, som ikke allerede er indsamlet under aktivitet nr. 4 *"Indsaml fakta og dan overblik"*.	
6	Iværksæt evt. tekniske og organisatoriske foranstaltninger	CSD Nøgleperson	Alle relevante tiltag for at stoppe bruddet og minimere skaden sættes omgående i gang. Hvis it-system er omfattet, træffes nødvendig beslutning om det pågældende system skal stoppes.	
7	Anmeldelse til Datatilsynet?	CSD Nøgleperson & DPO	Der foretages en indledende vurdering af fejlens omfang og konsekvenser – evt. i samarbejde med leverandøren eller andre implicerede aktører, og med rådgivning fra DPO. Vurderingen skal medføre en beslutning om, hvorvidt bruddet skal anmeldes til Datatilsynet. Hvis der ikke skal anmeldes gå til Aktivitet nr. 10: *"Dokumenter*	Afsnit 2 – Vurdering af anmeldelse til Datatilsynet Rådgivning fra DPO Afsnit 4 - Indhold af anmeldelse til Datatilsynet

			beslutninger og hændelsesforløb" Den juridiske vurdering udføres på baggrund af overblikket fra aktivitet nr. 4 og 5 samt vejledning afsnit 2. CSD-nøgleperson fremsender oplæg til anmeldelse til Datatilsynet til DPO. Oplæg til anmeldelse til Datatilsynet kvalitetssikres af DPO, som sender til Datatilsynet.	
8	Underretning til den registrerede?	CSD Nøgleperson	Vigtigt: Hvis der ikke sker anmeldelse til Datatilsynet, skal der ikke foretages underretning af registrerede. Der foretages en vurdering af fejlens omfang og konsekvenser i forhold til registreredes rettigheder og frihedsrettigheder. Med "registrerede" forstås de personer (oftest borgere), hvis oplysninger er omfattet af Sikkerhedsbruddet, og som dermed er berørte Ved den evt. udarbejdelse af underretninger til de berørte registrerede, bør CSD nøgleperson søge rådgivning hos juridiske kompetencer og fra kommunikationskompetencerne med henblik på at udforme underretningerne således, at antallet af efterfølgende henvendelser fra borgere i form af f.eks.	Afsnit 3 – Vurdering af underretning til registrerede Rådgivning fra DPO Afsnit 5 – Indhold af underretning af den registrerede Afsnit 6 - Vejledninger til Borgeren om afhjælpning af konsekvenserne for Sikkerhedsbruddet

			(akt)indsigtsanmodninger minimeres. Det er fx relevant ved større brud samt ved brud, som grundet deres (type)indhold og omfang må forventes at medføre en vis bevågenhed. Oplæg til underretning til de berørte registrerede, kvalitetssikres af DPO og returneres til CSD nøgleperson, der Sikrer at de registrerede underrettes. Det er kun de borgere, som er direkte berørt af Sikkerhedsbruddet, som skal underrettes. Ikke-berørte borgere vil evt. blive orienteret via pressen som følge af aktivitet nr. *9: "Forestå evt. intern/ekstern kommunikation"*.	
9	Forestå evt. intern/ekstern kommunikation	CSD Nøgleperson	**Evt. øvrig intern og ekstern kommunikation** På baggrund af aktivitet nr. 8: *"Anmeld til Datatilsynet og evt. registrerede"* ovenfor, udarbejdes en plan for den øvrige interne og eksterne kommunikation. Sørg for, at al intern og ekstern kommunikation udsendes samtidigt, hvis dette er påkrævet, og at budskaberne er ens. **Evt. kommunikation til øvrige medarbejdere** Udarbejdelse af eventuelle meddelelser til relevante medarbejdere.	

10	Dokumenter beslutninger og hændelsesforløb	CSD Nøgleperson	Der udarbejdes endelig dokumentation for Sikkerhedsbruddet med henblik på opfyldelse af dokumentationskravet, samt at iagttage foranstaltninger for at minimere riSiko for gentagelser. Dokumentationen skal udarbejdes uagtet evt. beslutninger om undladelse af underretning til Datatilsynet samt evt. berørte registrerede. Dokumentationen journaliseres i [journaliseringssystem].	Rådgivning fra DPO
11	Opdater og luk sag	CSD Nøgleperson	Beslutninger og håndtering af brud dokumenteres i CSD's system	
Slut	Persondatabrud håndteret	CSD Nøgleperson	Processen afsluttes og informationer om håndteringen af persondatabruddet lagres.	

Vejledning til håndtering af brud på persondatasikkerheden

1. VURDER BRUD & INDSAMLING AF FAKTA

Et brud på persondatasikkerheden er i databeskyttelsesforordningens artikel 4, stk. 1, nr. 12, defineret som:

"Et brud på Sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet."

VURDERING AF BRUD PÅ PERSONDATASIKKERHEDEN - omfatter dermed alle tænkelige tilfælde, hvor personoplysninger behandles på en utilsigtet måde. Det er alt lige fra en mail der

sendes til forkert modtager, til en hacker der får adgang til et system, og krypterer alle institutionens data.

Der indsamles fakta:

- Type af hændelse (de tekniske omstændigheder bag hændelsen)
- Omfanget af skaden, herunder:
    - Hvilke kategorier af personoplysninger er berørt
    - Hvilke foranstaltninger er allerede truffet for at håndtere og/eller begrænse skaden (kryptering eller lignende)
    - Cirka antal berørte registrerede (borgere mv.)
- Er eksterne leverandører involveret.
- Berørte systemer
    - Hvis KK system: Orienteres KIT, med henblik på at modtage information og dokumentation.
    - Hvis andet system: Identificeres leverandøren af systemet, og de inddrages i nødvendigt omfang fx teknisk assistance.

2. VURDER OM DER SKAL SKE ANMELDE TIL DATATILSYNET

Anmeldelse til Datatilsynet skal ske hvis bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Som udgangspunkt bør alle brud anmeldelse til Datatilsynet.

Gennem en besvarelse af følgende spørgsmål kan det dog bedømmes, om en anmeldelse til Datatilsynet kan undtages.

Hvis en undtagelse skal komme på tale, må bruddet ikke indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Som minimum skal følgende forhold alle kunne dokumenteres:

- Starttidspunktet for Sikkerhedsbruddet.

- Sluttidspunktet for Sikkerhedsbruddet.

- Omfanget af Sikkerhedsbruddet.

- Årsagen til Sikkerhedsbruddet.

- Personoplysninger er ikke kommet til uvedkommendes kendskab – og selvom personoplysninger er kommet til uvedkommendes kendskab, kan det påvises:

    - Hvem de uvedkommende modtagere af oplysninger er,

    - at de uvedkommende modtagere af personoplysningerne mangler enten viljen eller muligheden for at udnytte oplysningerne, og

    - at de uvedkommende modtagere af oplysninger ikke længere er i besiddelse af oplysningerne.

UDDYBENDE BESKRIVELSE AF KRITRIER FOR / UNDLADELSE AF ANMELDELSER TIL DATATILSYNET

Hvornår skal der foretages anmeldelse til Datatilsynet

Som nævnt ovenfor, skal der foretages anmeldelse til Datatilsynet, hvis det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Det vil i praksis betyde, at udgangspunktet er, at alle Sikkerhedsbrud medfører en pligt til anmeldelse til Datatilsynet.

En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. 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 Borgeren. Det kan fx være i følgende Situationer:

- Offentliggørelse af beskyttet adresse: Institutionen offentliggør et brev på institutionens hjemmeside, hvor en borgers beskyttede adresse fremgår. Sådan en offentliggørelse medfører en pligt til anmeldelse til Datatilsynet og til at foretage underretning til Borgeren.

- Offentliggørelse af login og password: Institutionen offentliggør en række Borgeres login og password til institutionens hjemmeside. Hjemmesiden indeholder kun få og ikke følsomme oplysninger. Da mange Borgere bruger de samme login- og passwordoplysninger til forskellige hjemmesider og tjenester, kan oplysningerne derfor give uvedkommende – indirekte – adgang til andre hjemmesider, som indeholder de berørte Borgeres følsomme oplysninger. Sådan en offentliggørelse vil derfor medføre pligt til anmeldelse til Datatilsynet og til at foretage underretning til Borgerne.

Hvornår anmeldelse til Datatilsynet ikke er nødvendig.

Selvom udgangspunktet er, at alle Sikkerhedsbrud medfører en pligt til anmeldelse til Datatilsynet, er der Situationer, hvor det er usandsynligt, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Det kan fx være i følgende Situationer:

- Tabt lagringsmedie: Hvis det konstateres, at et lagringsmedie (fx USB-nøgle eller harddisk) indeholdende personoplysninger er mistet, men at mediet er krypteret så stærkt, at det er usandsynligt, at uvedkommende kan bryde krypteringen.

- Utilsigtet offentliggørelse på hjemmeside: Hvis det konstateres, at der ved en fejl er uploadet personoplysninger på institutionens hjemmeside, men at det ved gennemgang af loggen kan konkluderes, at den pågældende hjemmeside ikke har haft besøgende (fx hvis der er tale om en specialiseret underside), og at det samtidig kan konkluderes, at hjemmesiden ikke er blevet "crawlet" af fx Googles søgemaskine.

- Strømnedbrud: Institutionen rammes af et strømnedbrud, der varer i ca. 10 minutter, hvor det ikke er muligt at tilgå forvaltningens it-systemer, herunder elektroniske journaler. Ingen oplysninger er mistet, og arbejdet kan herefter fortsætte.

- Vildfaren krypteret e-mail: En sagsbehandler sender via digital post en besvarelse af en ansøgning til en forkert borger. Dog er besvarelsen af ansøgningen pakket i en krypteret fil, hvortil sagsbehandleren havde planlagt at eftersende kodeord, hvorfor modtageren ikke kan åbne den krypterede fil.

- Nabofesten: En institution vil sende et brev vedrørende nabovarsel om en stor fest i nabolaget. Ved en fejl sender institutionen via digital post brevet til en forkert borger. Brevet indeholder den oprindelige borgers navn og adresse og intet andet. Borgeren, der modtager brevet, gør

straks institutionen opmærksom på fejlen. Institutionen aftaler skriftligt med borgeren, der har modtaget brevet, at vedkommende sletter det.

3. VURDER OM DER SKAL SKE UNDERRETNING TIL REGISTREREDE

Underretning til registrerede (Borgeren) skal ske, hvis bruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Det praktiske udgangspunkt er, at hvis der foretages anmeldelse til Datatilsynet, skal der ligeledes foretages underretning til Borgeren.

Undtaget kunne være tilfælde, hvor at bruddet godt nok indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, men hvor man samtidig har en begrundet forventning om, at risikoen ikke realiseres (altså at der sker noget i praksis).

Hvor skal der / kan det undlades at foretage underretning til Borgeren
Forskellen mellem hvornår registrerede skal underrettes og hvornår det kan undlades er ikke stor, og vil oftest baseres på en detaljeret vurdering af den enkelte hændelse.

Som minimum skal ét af følgende forhold kan dokumenteres følgende kunne dokumenteres, hvis der skal ske en undtagelse:

- Risikoen for Sikkerhedsbruddet er ikke høj. Risikoen vurderes ud fra en samlet vurdering af:

- Hvilken type Sikkerhedsbrud er der tale om? Er personoplysningerne offentliggjort på internettet (høj risiko), eller har man bare glemt, hvor præcist i et opbevaringsarkiv, man har gemt oplysningerne (lav risiko)?

- Hvad er sammenhængen, følsomheden og mængden af oplysningerne?

- Hvor nemt er det for uvedkommende at identificere de personer, som oplysningerne vedrører?

- Hvor stor er risikoen for, at Borgeren oplever et tab af rettigheder og frihedsrettigheder som følge af Sikkerhedsbruddet?

- Er der tale om en særlig udsat type af Borger – fx børn eller socialt udsatte?

- Hvor mange Borgere vedrører oplysningerne?

- Hvilken forvaltning/enhed er ansvarlig for Sikkerhedsbruddet?

- Der er gennemført passende tekniske og organisatoriske foranstaltninger, således at det kan påvises, at:

    - Eventuelle uvedkommende modtagere af oplysningerne er forhindret i at tilgå og benytte oplysningerne – fx hvis oplysningerne er krypterede.

- Den høje risiko for Borgernes tab af rettigheder og frihedsrettigheder er ikke længere reel, og det kan påvises, at:

    - Oplysningerne ikke har været tilgået og benyttet af uvedkommende, mens risikoen stadig var reel.

- Hvis underretning kræver en uforholdsmæssig indsats – fx i tilfælde af, at indsatserne for at foretage individuelle underretninger ikke står i mål med de – negligerbare – konsekvenser, som de registrerede potentielt kan opleve.

Herunder gives derfor en række eksempler, der kan indikere hvornår anmeldelse kunne undlades:

- Hvis en e-mail er blevet fremsendt til få og identificerede borgere, som ikke kan tænkes at kunne – og ville – udnytte oplysningerne.

- Hvis et tabte lagringsmedie er udstyret med en høj kryptering

- Hvis der konstateres et "hul" i Sikkerheden på en hjemmeside, men at hullet hurtigt lukkes, og det samtidig kan dokumenteres, at hullet ikke har været udnyttet.

- Hvis ét af kommunens sagsarkiver oversvømmes, og dokumenter på disse sager, som har været afsluttet i over 25 år, mistes. I så fald vil en meddelelse på kommunens hjemmeside være tilstrækkelig.

4. INDHOLD AF ANMELDELSER TIL DATATILSYNET

I henhold til Databeskyttelsesforordningens artikel 33 anmeldelses nedenstående til Datatilsynet:

- En beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

- Navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

- En beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden

- En beskrivelse af de foranstaltninger, som Institutionen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Anmeldelse sker gennem virk.dk på:

https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_Sikkerhed

5. INDHOLD AF UNDERRETNING AF DEN REGISTRERede

I henhold til Databeskyttelsesforordningens artikel 34 anmeldelses nedenstående til dig som registreret:

En beskrivelse af karakteren af bruddet på persondatasikkerheden i et klart og forståeligt sprog

[Indsæt en beskrivelse af karakteren af bruddet på persondatasikkerheden i et klart og forståeligt sprog:]

Navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

[Indsæt navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes:]

En beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden

[Indsæt en beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden:]

En beskrivelse af de foranstaltninger, som institutionen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

[Indsæt en beskrivelse af de foranstaltninger, som institutionen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger:]

6. VEJLEDNING TIL BORGEREN OM AFHÆLPNING AF KONSEKVENSER VED SIKKERHEDSBRUD

Standardvejledninger til Borgeren om afhjælpning af konsekvenserne for Sikkerhedsbruddet

I forbindelse med underretning til Borgerne, skal kommunen samtidig orientere om, hvordan Sikkerhedsbruddets potentielle risici kan minimeres.

En sådan underretning skal altid være tilpasset, men det kan alligevel forventes, at der vil opstå typetilfælde, hvortil der kan forberedes standardtekster. Sådanne tekster kan fx være:

NemID:

"Oplysninger om dit NemID er kommet til uvedkommendes kendskab, og du bør straks spærre dit nøglekort. Du spærrer dit nøglekort ved at logge på med dit NemID og adgangskode. Der sendes ikke automatisk et nyt nøglekort. For at bestille et nyt nøglekort online skal du legitimere dig med dit danske pas eller kørekort."

CPR.nr:

"Oplysninger om dit CPR.nr. er kommet til uvedkommendes kendskab, og du bør straks kontakte den sælger, virksomhed eller offentlige myndighed, som du har mistanke til, kan misbruge dit CPR.nr. Her skal du oplyse, at din identitet er blevet misbrugt, og at du derfor ikke anser dig for bundet af aftalen eller forholdet. Du kan i særlige tilfælde få et nyt personnummer, såfremt det er blevet misbrugt".