Internt dokumentationsregister ved brud på datasikkerheden:

Brud på persondatasikkerheden hos XX arbejdsplads:	**Beskrivelse af bruddet**:
1. Dato og tidspunkt for bruddet:	
2. Beskrivelse af, hvad der er sket:	
3. Årsagen til bruddet:	
4. Hvilken type personoplysning er berørt?	
5. Hvilke konsekvenser har bruddet for de berørte personer?	
6. Hvilke afhjælpende foranstaltninger er truffet?	
7. Er der sket anmeldelse af bruddet til Datatilsynet? Hvis ja, hvornår:	
7.1. Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet:	
8. Er der sket underretning af de berørte personer? Hvis ja, hvornår og hvordan:	
8.1. Hvis nej, angiv begrundelse for ikke at underrette de berørte personer:	
9. Andre relevante oplysninger	

Anmeldelse af brud på persondatasikkerheden skal ske til Datatilsynet (dt@datatilsynet.dk eller telefonnr.: 33 19 32 00) uden unødig forsinkelse og om muligt **senest 72 timer** efter at vi er blevet bekendt med bruddet. Der vil komme en it-løsning for indberetning af brud som vil ligge på **virk.dk** Se link på virk.dk: https://indberet.virk.dk/myndigheder/stat/ERST/Underretning_om_brud_paa_persondatasikkerheden

Se også på Datatilsynets hjemmeside: https://www.datatilsynet.dk/anmeld-brud-paa-persondatasikkerheden/

Det er muligt, at anmelde brud på datasikkerheden **efter** 72 timer. I så fald skal forsinkelsen begrundes.

Kan vi ikke give Datatilsynet alle de ovenstående relevante oplysninger, kan anmeldelsen ske trinvis.

Procedure for hvad skal du gøre, når du konstaterer et brud

1. Vurder, om bruddet skal anmeldes. Hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske anmeldelse. Rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller –svindel, økonomisk tab, skade på omdømme, tab af fortrolige data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.
Vurderingen skal tage sit udgangspunkt i den risiko for de berørte personer, som er opstået som følge af bruddet på persondatasikkerheden.

2. Hvad kan du lægge vægt på ved risikovurderingen?

a. typen af sikkerhedsbrud, er der sket tab af oplysninger, brud på fortrolighed eller en integritetskrænkelse
b. oplysningernes art og omfang
c. risikoen for, at registrerede kan identificeres
d. konsekvenser bruddet kan have for de registrerede
e. antallet af berørte fysiske personer.

3. Kontakt leder/formand/kontaktperson XXX. I tilfælde af dennes fravær eller hvis du ikke kan komme i kontakt med vedkommende, så kontakt XXX. Det er enten XXX eller YYY som foretager anmeldelsen til Datatilsynet.

4. Uden unødig forsinkelse skal der ske underretning af den/de registrerede efter bruddet er påvist.

5. Udfyld ovenstående skema.

6. Anmeld bruddet til Datatilsynet.

7. Efter aftale med leder/formand/kontaktperson XXX kontaktes evt. Kirkeministeriets it-afdeling (70 20 25 35).

Hvad er brud på persondatasikkerheden?
Kun hvis der sker hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, som er omfattet af databeskyttelsesforordningens definition af et brud på persondatasikkerheden.

Eksempler på brud på persondatasikkerheden:
1. Du er kommet til at ændre eller slette personoplysninger ved et uheld.

2. Brud på serveren, hvor uvedkommende har fået indsigt i personoplysninger, f.eks. cpr.-nr., e-mail adresser.

3. Du har videregivet personoplysninger bevidst eller ubevidst om en borger til en anden borger eller måske ligefrem til flere uvedkommende personer, fx sendt en mail med personoplysninger til en forkert modtager.

Underretning af den registrerede
Underretningen skal ske direkte via e-mail, opringning eller lign. Pressemeddelelse eller opslag på arbejdspladsens hjemmeside vil ikke være tilstrækkeligt.

Karakteren af bruddet skal beskrives for den registrerede og skal som minimum indeholde:
* navn og kontaktoplysninger for databeskyttelsesrådgiveren (Rasmus Paaske Larsen i Kirkeministeriet) eller anden relevant kontaktperson (det kan være XXX eller YYY med angivelse af direkte telefonnummer og e-mail).
*beskrive de sandsynlig konsekvenser af bruddet på persondatasikkerheden
*beskrive de foranstaltninger vi har truffet eller vil træffe for at håndtere bruddet, herunder foranstaltninger for at begrænse de mulige skadevirkninger
*give råd om, hvordan negative konsekvenser af bruddet kan undgås (skift af adgangskode eller lignende).

Hvad er personoplysninger?
Det er enhver information om en identificeret eller identificerbar fysisk person. Det kan være indirekte eller direkte identifikation.

Eks.: Helbredsoplysninger, telefonnummer, fagforeningsmæssigt tilhørsforhold, cpr-nr., navn, e-mail, IP-adresse, billeder, CV

Læs mere i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf