Forretningsgang Håndtering af brud på persondatasikkerheden - TR		Dokument nr. i 360: 19/249328/2
Gældende fra:	**01.02.23**	**Dato:** **01.02.2023**
Gældende for:	**FOA Randers**	**Version: 1**
Behandling af:	Oplysninger om brud på persondatasikkerheden ved TR	**Sider 4**
Formål/funktion:	At sikre, at brud på persondatasikkerheden håndteres	**Sagsansvarlig:** Lene Hartmann og Nana Højlund

Opgave	Beskrivelse	Evt. henvisning
Rapportering af brud fra tillidsvalgte	TR skal straks efter, at bruddet er opdaget tage kontakt til en repræsentant fra afdelingen enten: Lene Hartmann: 2044 4407 Nana Højlund: 2044 4401 Sektorformand Lotte Helbo Kristiansen: 2044 4408 Sektorformand Karin Mathiesen: 2044 4411 Sektorformand Andre Vangsgaard: 2044 4402 I tilfælde af et brud på persondatasikkerheden eller mistanke herom skal det rapporteres til IT-sikkerhedslederen. Det gælder både elektroniske og fysiske data. Rapportering skal ske omgående, da vi har en frist på **72 kalendertimer** til at beskrive, vurdere og evt. indrapportere til Datatilsynet. Nedenstående forretningsgang skal herefter følges. Den berørte TR skal være med til at oplyse sagen.	
Intern rapportering af brud	Rapporter via punktet Persondata-forordningen i Topdesk/ persondataforordningen. Orienter afdelingsformand Lene Hartmann og Anna-Kathrine L. Hansen, der herefter kontakter forbundets DPO/ GDPR-projektgruppe alternativt kontaktes Ring samtidig DPO op på tlf: 4697 2393 eller 4697 2628.	Datatilsynets vejledning om håndtering af brud på persondatasikkerheden: https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf Topdesk: https://topdesk.foa.dk/tas/public/ssp/

Stop bruddet og dokumenter det	Første prioritet er at stoppe databruddet. AK eller Lene kontakter den, der har indrapporteret mistanken om brud/ brud. Derudover kontaktes DPO og øvrige relevante personer for at indsamle informationer om bruddet med henblik på at sikre en passende reaktion, herunder at stoppe bruddet. Det forudsættes at IT-sikkerhedslederen altid har adgang til relevante ressourcer i organisationen givet den korte tidsfrist (også uden for normal arbejdstid). IT sikkerhedsleder opretter sag i 360 til håndtering og dokumentation af bruddet og kobler de relevante teamdeltagere på sagen. Skabelon til indsamling af dokumentation anvendes.	Skabelon til intern dokumentation af brud på persondatasikkerheden *(vedlagt nederst i dette dokument)*
Risikovurdering – skal bruddet anmeldes til datatilsynet og skal de registrerede orienteres?	I fællesskab med den dataansvarlige og relevante personer foretager IT-sikkerhedslederen en risikovurdering af bruddet, herunder konsekvenser for den registrerede, jf. Datatilsynets vejledning omkring brud (afsnit 3). Bemærk, at vurderingen kan ændre sig, hvis der kommer nye oplysninger. Endelig beslutning omkring indrapportering til Datatilsynet træffes af den dataansvarlige. Endelig beslutning omkring orientering af de(n) registrerede træffes af den dataansvarlige.	https://www.datatilsynet.dk/anmeld-brud-paa-persondatasikkerheden/
Anmeldelse til datatilsynet	Afdelingen skal i tilfælde af et brud på persondatasikkerheden uden unødig forsinkelse og om muligt inden 72 timer – med hjælp af IT-sikkerhedslederen - foretage anmeldelse af bruddet til Datatilsynet via Virk.dk, medmindre det er usandsynligt, at bruddet medfører en risiko for personers rettigheder eller frihedsrettigheder. I Datatilsynets vejledning omkring brud (bilag B) findes en liste over eksempler, hvor det gennemgås hvorvidt der skal ske anmeldelse til Datatilsynet.	https://www.datatilsynet.dk/anmeld-brud-paa-persondatasikkerheden/
Underretning til den registrerede	Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, skal FOA udover anmeldelse til Datatilsynet også foretage underretning af den registrerede.	

	IT-sikkerhedslederen aftaler i den konkrete situation med den dataansvarlige, hvem der gør hvad. Der kan være situationer, hvor der ikke er krav om underretning, eller hvor det ikke er muligt at foretage en direkte underretning. Underretningen skal ske uden unødig forsinkelse. Den skal som minimum indeholde: • Kontaktoplysninger hvor yderligere informationer kan indhentes • Beskrivelse af de sandsynlige konsekvenser af bruddet • Beskrivelse af de foranstaltninger som er truffet eller foreslår truffet for at håndtere bruddet herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger • Eventuelle specifikke råd om hvordan den registrerede kan beskytte sig mod mulige negative konsekvenser	
Kommunikation	It-sikkerhedsleder og GRPD-projektleder aftaler med den dataansvarlige, hvad der skal kommunikeres ud i organisationen, og hvorvidt der skal etableres et særligt beredskab til at håndtere henvendelser fra de registrerede eller andre, herunder information til reception og telefonvagter.	
Evaluering og forbedring	It-sikkerhedslederen fortager sammen med GDPR- projektleder efterfølgende en evaluering og opsamling på sikkerhedsforanstaltninger, der kan hindre en tilsvarende situation. Relevante parter inddrages og der rapporteres til den øverste ledelse (dataansvarlig).	
Registrer hændelse i log	Både den dataansvarlige (hvis afdeling) og IT-sikkerhedsleder registrerer hændelsen i en log.	
Slettefrister	Se slettepolitik for konkrete slettefrister: Slettepolitik - gældende version. http://360.foa.dk/GetFile.aspx?fileId=28749529&redirect=true (DPO oplyser, at slettepolitikken er under revision og forventes opdateret 2. halvår 22)	

Skabelon til intern dokumentation

Brud på persondatasikkerheden	Beskrivelse af bruddet
1. Dato og tidspunkt for bruddet	
2. Hvad er der sket	
3. Årsagen til bruddet	
4. Hvilke typer persondata er berørt	
5. Hvilke konsekvenser har bruddet for de berørte personer	
6. Hvilke afhjælpende foranstaltninger er truffet	
7. Er der sket anmeldelse til Datatilsynet	
7.1 Hvis ja, hvornår	
7.2 Hvis nej, begrundelsen for ikke at foretage anmeldelse	
8. Er der sket underretning af de berørte personer	
8.1 Hvis ja – hvornår	
8.2 Hvis nej – begrundelse for ikke at underrette de berørte personer	