Retningslinjer for håndtering af sikkerhedsbrud

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
2.2	26-10-2022	Mindre redaktionelle rettelser	Sikkerhedsrådgiver	Sikkerhedsteam
2.3	26-04-2024	Uddybning af kommunens opfølgning/evaluering af brud	Sikkerhedsrådgiver	Sikkerhedsteam
2.4	13-05-2025	Rettelse i definition samt flere generelle og mindre redaktionelle ændringer	Sikkerhedsrådgiver	Sikkerhedsteam

Formål

Disse retningslinjer har til formål at sikre en ensartet håndtering af sikkerhedshændelser i Jammerbugt Kommune. Retningslinjerne indeholder blandt andet en overordnet procedurebeskrivelse for håndteringen af brud samt en ansvars- og rollefordeling.

Definition af sikkerhedsbrud

Et sikkerhedsbrud defineres 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.

Brud på persondatasikkerheden er ofte hændelser, hvor der enten hændeligt (noget sker utilsigtet eller ved en tilfældighed) eller tilsigtet (typisk ved hacking eller misbrug) sker noget med personoplysninger, som kan påvirke oplysningernes fortrolighed, f.eks. ved at data bliver tilgængelige for uvedkommende. Det kan også være hændelser, som kan medføre, at oplysningerne bliver utilgængelige for den dataansvarlige (tab af tilgængelighed), eller at oplysningerne ændres, så de er forkerte (tab af integritet).

Eksempler på brud på persondatasikkerhed kan være:

- Længerevarende systemnedbrud, som medfører, at en borger ikke kan modtage sin ydelse
- Auto-complete medfører, at e-mails bliver sendt til forkerte modtagere
- Beskyttet adresse eksponeres fejlagtigt efter ændring i it-system
- Fejludlevering af personoplysninger ved sagsbehandling
- Tab/tyveri af transportable enheder med ukrypteret data
- For bred adgang til data i systemer mv.
- Ondsindet software (ransomware) medfører tab og misbrug af data

Sikkerhedsbrud kan medføre en række potentielle konsekvenser for den/de registrerede. Nedenstående liste er eksempler, da listen ikke er udtømmende:

- Forskelsbehandling

- Identitetstyveri
- Økonomiske konsekvenser, herunder finansielle tab
- Skade på omdømme
- Sociale konsekvenser
- Indflydelse på privatliv
- Skade på legitime interesser
- Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
- Manglende udøvelse af kontrol med egne personoplysninger

Procedure for håndtering af sikkerhedsbrud
Ved opdagelse af sikkerhedsbrud iværksættes følgende procedure:

- Medarbejder opdager hændelse og forsøger straks at stoppe hændelsen. Skader forsøges begrænses så vidt muligt. Dette kan fx være at forsøge at tilbagekalde en mail, der er sendt til en forkert modtager. Eller det kan være at lukke specifikke brugeradgange, som mistænkes for at være illegitime.
- Medarbejderen, som opdager hændelsen, underretter sin nærmeste leder og kontakter evt. kommunens sikkerhedsrådgiver for hjælp og vejledning.
- Medarbejderen skal dernæst få overblik over personoplysningernes art og omfanget, herunder antallet af berørte personer og hvilke personoplysninger der er omfattet af bruddet. Medarbejderen udfylder blanketten 'Rapportering af sikkerhedsbrud', som findes på Tryk, og sender blanketten til sikkerhedsrådgiveren via sikkerhedsbrud@jammerbugt.dk.
- Sikkerhedsrådgiveren vurderer risiko og potentielle konsekvens af bruddet samt inddrager (alt efter bruddets karakter og alvor) kommunens øverste it-sikkerhedsansvarlige, chefen for Digitalisering, IT og Borgerservice og databeskyttelsesrådgiveren. I tilfælde af sikkerhedsbrud i it-systemer orienterer sikkerhedsrådgiveren systemejer og evt. systemforvalter.
- Sikkerhedsrådgiveren journaliserer relevant dokumentation for bruddet i SBSYS samt fører bruddet til intern log.
- Efterfølgende evaluerer kommunen årsagen til bruddet for at undersøge, om der kan igangsættes tekniske eller organisatoriske sikkerhedsforanstaltninger, som kan mindske risikoen for fremtidige lignende brud, afhængig af sikkerhedsbruddets karakter:
    - Lederen af den afdeling, hvor sikkerhedsbruddet indtraf, har ansvaret for at vurdere, om der er arbejdsprocesser i afdelingen, som kan tilrettes og forbedres, så der ikke sker gentagelser af bruddet. Der opfordres generelt til, at de pågældende afdelinger orienterer om brud på personalemøder eller lignende. Dokumentation for opfølgning på anmeldte sikkerhedsbrud skal sendes til sikkerhedsrådgiveren, som journaliserer dette. I de tilfælde, hvor brud er sket i it-systemer, er systemejeren ansvarlig for at sikre opfølgningen på bruddet.
    - Sikkerhedsrådgiveren vurderer, om hvert enkelt brud i sig selv samt det generelle trusselsbillede i kommunens log over sikkerhedsbrud giver anledning til implementering/ændring af generelle tekniske eller organisatoriske sikkerhedsforanstaltninger, fx hvis en risiko er af tværgående karakter. Større, generelle ændringer vil så vidt muligt blive besluttet af sikkerhedsteamet.

Sikkerhedsrådgiver vurderer løbende i processen i samråd med chefen for Digitalisering, IT og Borgerservice og evt. databeskyttelsesrådgiveren, hvorvidt bruddet bør indberettes til Datatilsynet og har også ansvaret for eventuelt at indberette bruddet **uden unødig forsinkelse og senest 72 timer efter, at kommunen er blevet bekendt med bruddet.**

Ansatte i Jammerbugt Kommune, der opdager et sikkerhedsbrud, skal hurtigst muligt orientere sikkerhedsrådgiveren herom. Dette gælder, uanset om de ansatte kun har få, mangelfulde oplysninger om bruddet på daværende tidspunkt. Sikkerhedsrådgiveren kan vælge at foretage en første indberetning til Datatilsynet, inden der er klarhed over fx omfang eller årsag til sikkerhedsbrud. Når sikkerhedsbruddet senere bliver bedre belyst, kan sikkerhedsrådgiveren vælge at uddybe den første indberetning.

På grund af den stramme tidsramme for indberetning af sikkerhedsbrud er det afgørende, at ansatte i Jammerbugt Kommune prioriterer håndteringen af sikkerhedsbrud, indtil sagen kan betragtes som værende færdigbehandlet og afsluttet.

Særligt i forhold til mistanke om phishing-mails gælder det, at medarbejdere orienterer Servicedesk herom. Servicedesk vil herefter vejlede den pågældende medarbejder i sikker håndtering af den mistænkelige mail og vil have mulighed for at udsende kommunikation til alle brugere om stigende eller generelle trusler inden for phishing-mails, hvis dette er nødvendigt.

Registrering af sikkerhedsbrud
Alle sikkerhedsbrud føres til intern log, så kommunen altid har et fuldstændigt overblik over samtlige sikkerhedsbrud begået i kommunen.

Den interne log gennemgås efter behov på møder i sikkerhedsteamet for at drøfte potentielle forbedringer af tekniske og organisatoriske sikkerhedsforanstaltninger. Derudover udarbejder sikkerhedsrådgiveren awareness-kampagner og lignende tiltag ud fra aktuelle sikkerhedshændelser. Loggen bidrager derfor til en løbende vurdering og håndtering af aktuelle risici for de registrerede.

Anmeldelse til Datatilsynet
Sikkerhedsbrud anmeldes til Datatilsynet, hvis bruddet udgør en risiko for personers rettigheder eller frihedsrettigheder 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 den registrerede.

Datatilsynet skal i så fald underrettes uden unødig forsinkelse og om muligt senest 72 timer, efter den dataansvarlige er blevet bekendt med bruddet. Det vil sige, at kommunen indberetter brud til Datatilsynet, hvis det ikke kan udelukkes, at der er en sandsynlighed for, at bruddet på persondatasikkerheden indebærer en risiko for den registreredes rettigheder eller frihedsrettigheder.

Ethvert brud vil blive vurderet særskilt ud fra, hvorvidt det udgør en risiko for personers rettigheder eller frihedsrettigheder. Det er kun, hvis det er usandsynligt, at bruddet på persondatasikkerhed indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, at der ikke sker anmeldelse til Datatilsynet.

Vurderingen heraf foretages af sikkerhedsrådgiveren i samråd med databeskyttelsesrådgiveren. Chefen for Digitalisering, IT og Borgerservice godkender alle anmeldelser, og i tilfælde af uenighed mellem sikkerhedsrådgiver, databeskyttelsesrådgiver og chefen for Digitalisering, IT og Borgerservice træffer chefen den endelige beslutning i forhold til, hvorvidt et brud skal anmeldes til Datatilsynet.

Vejledning til vurdering
Som et udgangspunkt vil brud på fortrolighed via videregivelse til eksterne aktører (dvs. aktører, som ikke er ansat i Jammerbugt Kommune, og derfor ikke er underlagt tavshedspligt) ikke blive anmeldt til Datatilsynet, hvis bruddet kun omhandler videregivelse af få almindelige personoplysninger på en registreret (fx kontaktoplysninger), eller hvis modtageren af oplysningerne er underlagt tavshedspligt eller er myndighedsperson.

Som et udgangspunkt vil brud på fortrolighed via videregivelse til interne aktører (dvs. aktører, som er ansat i Jammerbugt Kommune, og derfor er underlagt tavshedspligt) ikke blive anmeldt til Datatilsynet. Dette vil altid skulle begrundes ud fra en konkret vurdering. Undtagelser hertil kan være, hvis bruddet omfatter videregivelse af særligt fortrolige og følsomme personoplysninger som fx en underretning på et barn.

Ligeledes vil brud på fortrolighed grundet forsendelse til korrekt modtager via usikre mailforbindelser som et udgangspunkt ikke blive anmeldt til Datatilsynet. Det vurderes generelt usandsynligt, at sådanne brud vil medføre en risiko for den registrerede, idet kommunen benytter TLS-kryptering på alle mailforsendelser. Der kan dog være undtagelser hertil, fx hvis bruddet omfatter en større mængde følsomme personoplysninger.

Underretning af den registrerede
Hvis der er høj risiko for, at sikkerhedsbruddet kan skade den registrerede, har personen ret til en orientering.

Sikkerhedsrådgiveren træffer i samråd med databeskyttelsesrådgiveren og chefen for Digitalisering, IT og Borgerservice beslutning om, hvorvidt den registrerede bør orienteres. I tilfælde af uenighed mellem sikkerhedsrådgiver, databeskyttelsesrådgiver og chefen for Digitalisering, IT og Borgerservice, træffer chefen den endelige beslutning i forhold til, hvorvidt de registrerede skal underrettes.

Når en registreret underrettes om et sikkerhedsbrud, vil personen som minimum modtage en skriftlig orientering, som følger en fast brevskabelon, kommunen har udarbejdet til formålet. I skabelonen vil kommunen blandt andet:

- Beklage bruddet
- Orientere om bruddets mulige konsekvenser for den registrerede
- Beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger, som kommunen har truffet eller planlægger at træffe
- Orientering om klagemuligheder herunder videregive kontaktoplysninger på en person i kommunen, som kan uddybe kommunens håndtering af bruddet, fx DPO'en

Sammen med ovennævnte orientering vedhæfter kommunen desuden et oplysningsbrev, idet den registreredes oplysninger vil blive behandlet i forbindelse med registreringen af underretningen herunder tilkobling af sagspartoplysninger.

Sikkerhedsrådgiveren udarbejder evt. i samråd med databeskyttelsesrådgiveren den konkrete tekst i oplysningsbrevet, og afdelingen, hvor bruddet er sket, er forpligtet på at bistå sikkerhedsrådgiveren alt efter behov. En kopi af den skriftlige underretning gemmes som dokumentation i SBSYS, og den registrerede tilkobles som sagspart.

Udsendelse af underretning
Det aftales ud fra det konkrete tilfælde, hvem der udsender den skriftlige underretning af den registrerede, alt efter hvad der bedst giver mening i forhold til det enkelte brud. Hvis en medarbejder fx har opdaget bruddet og allerede har haft kontakt til borgeren eller på anden vis har en arbejdsmæssig relation til borgeren, vil det i de fleste tilfælde være mest hensigtsmæssigt, at den pågældende medarbejder underretter borgeren.

De registrerede kan også underrettes ud fra hensyn til forvaltningsretlige principper, fx for at fremme det gode samarbejde. Hvis årsagen til underretningen skyldes forvaltningsretlige principper fremfor databeskyttelsesretlige hensyn, noteres dette i skemaet for indberetning af sikkerhedsbruddet. I dette tilfælde vil den pågældende afdeling stå for at underrette de registrerede.

I nogle tilfælde vil det være mest hensigtsmæssigt, at sikkerhedsrådgiveren foretager underretningen. Det kan være, hvis bruddet kræver en generel orientering fx på kommunens hjemmeside.

Journalisering af den registreredes oplysninger
Som udgangspunkt behandler kommunen ikke yderligere oplysninger om de registrerede i forbindelse med håndtering af sikkerhedsbrud, ligesom det heller ikke er nødvendigt at oprette den registrerede som sagspart i SBSYS. Det skyldes hensynet til den registrerede og for ikke at foretage unødvendige databehandlinger.

I få tilfælde kan det være nødvendigt at gemme oplysninger på den registrerede, hvis der er noget på spil for den registrerede, eller hvis det kan være til dennes fordel. Det gælder fx, når sikkerhedsbrud har haft en særlig alvorlig karakter, eller hvor kommunen har mistanke om, at borgeren kan finde på at klage til databeskyttelsesrådgiveren eller Datatilsynet. En undtagelse hertil er, hvis opgaven er forbundet med et uforholdsmæssigt stort arbejde, fx over 1000 personer.

Kommunen vil altid registrere den registrerede som sagspart og dermed behandle den registreredes oplysninger på ny, hvis kommunen har valgt at underrette den pågældende registrerede.

Kommunen vil i førnævnte tilfælde efterspørge et CPR-nummer hos den registrerede, hvis ikke det allerede er en kendt oplysning for kommunen. Herefter oprettes den registrerede som sagspart på SBSYS-sagen.