20. september 2022

Version:	ID-nummer:	Reference til ISO27001:	Reference til NSIS:
2.0		5.26	4.1.6
Ansvarlig vedligeholdelse:	**Godkendt af:**	**Godkendt den:**	**Næste revision:**
Informationssikkerheds-udvalget	Informations-sikkerhedsudvalget	20. september 2022	2023

Procedure for håndtering af brud på persondatasikkerheden

Denne procedure beskriver, hvordan Ishøj Kommune håndterer brud på persondatasikkerheden i henhold til databeskyttelsesforordningens bestemmelser.

Procedurens opbygning

Proceduren er delt op i 2 forskellige procedurer, som vedrører forskellige grupper:

1) En procedure for de ansatte i kommunen, hvis de oplever/forårsager et sikkerhedsbrud
2) En procedure for de lokale informationssikkerhedskoordinatorer, som skal håndtere sikkerhedsbruddet.

Idéen med opdelingen er, at de ansatte blot skal forholde sig til den konkrete procedure, der er relevant for dem.

Ansvar og tilgængelighed

Ansvaret for håndtering af sikkerhedsbrud ligger hos centerchefen. Kommunens centerchefer, skal derfor sikre, at alle ansatte har kendskab til kravet om indberetning af sikkerhedsbrud og kender til den konkrete del af proceduren, som er relevant for dem.

Informationssikkerhedsudvalget har ansvaret for, at proceduren er opdateret og tilgængelig på kommunens intranet og i SBSYS i sin fulde form, at Byrådet og Koncernledelsen er bekendt med denne, at proceduren bliver evalueret og revideret samt, at de involverede parter er indforstået med roller og ansvar i forbindelse med et sikkerhedsbrud.

Den enkelte centerchef har ansvaret for, at den del af proceduren, som er relevant for kommunens ansatte, er tilgængelig for dem samt, at den gennemgås årligt på leder- og personalemøder. Alle ansatte skal vide, hvor de kan finde proceduren, hvis de får behov for den. Proceduren kan være tilgængelig i både digital og fysisk form.

Den centrale informationssikkerhedsgruppe har ansvaret for at gennemgå proceduren med de lokale sikkerhedskoordinatorer, så de ved, hvordan de indberetter et sikkerhedsbrud.
Godkendelse og revision

Proceduren skal revideres mindst én gang årligt og godkendes af Informationssikkerhedsudvalget. Ved væsentlige ændringer skal proceduren godkendes af Koncernledelsen.

20. september 2022

Anmeldelse af sikkerhedsbrud – for kommunens ansatte og politikere

Ishøj Kommune har pligt til at tage hånd om sikkerhedsbrud, der vedrører personoplysninger, som kommunen er dataansvarlig for. Hvis du får kendskab til et sikkerhedsbrud, skal du hurtigst muligt anmelde dette til din lokale sikkerhedskoordinator ved at følge nedenstående procedure.

Hvad er et sikkerhedsbrud?

Fortrolighed

Der er tale om et brud på persondatasikkerheden, hvis en person får adgang til, modtager eller ser personoplysninger, de ikke burde have adgang til. Det kan være om andre borgere, ansatte i kommunen eller om deres pårørende. Det kan eksempelvis være i tilfælde, hvor:

- En ansat har mistet et arbejdsredskab såsom mobil, pc, tablet, som indeholder personoplysninger.
- En ansat sender eller formidler personoplysninger til en forkert borger.
- Offentliggørelse af personoplysninger på en hjemmeside, i politiske dagsordener, i medier, samtaler eller andet uden samtykke.
- Et system med personoplysninger bliver hacket, eller et kodeord bliver misbrugt til at få adgang til personoplysninger.

Brud på integritet

Der er ligeledes tale om et brud på persondatasikkerheden, hvis du oplever, at de oplysninger du har om en borger er forkerte pga. en fejl i systemet eksempelvis.

Brud på tilgængelighed

Der er også tale om et brud på persondatasikkerheden, hvis du ikke kan tilgå oplysninger om en borger, fordi dit fagsystem er utilgængeligt.

Vær opmærksom på, at kommunen i nogle tilfælde har pligt til at anmelde et sikkerhedsbrud til Datatilsynet indenfor 72 timer. Det er derfor vigtigt, at du anmelder et sikkerhedsbrud hurtigst muligt. Det kan ligeledes være nødvendigt at informere de(n) registrerede/borgere(n) om bruddet.

Hvis du opdager et sikkerhedsbrud

Hvis du oplever et brud på persondatasikkerheden, skal du gøre følgende hurtigst muligt:

Du skal kontakte nærmeste leder samt din lokale informationssikkerhedskoordinator, der tager stilling til håndtering af hændelsen. En liste over lokale informationssikkerhedskoordinatorer findes på Uglen. Hvis det ikke lykkes at anmelde bruddet telefonisk, kan du udfylde nedenstående skema og sende dette til nærmeste leder og din lokale informationssikkerhedskoordinator.

Navn	
Kontaktoplysninger	(Telefon og mail)
Stilling	(Titel, afdeling, center)
Beskriv sikkerhedsbruddet	(hvad er der sket?)

Hvilke oplysninger drejer bruddet sig om?	(Er det navne, cpr.numre, helbredsoplysninger, adresser, økonomiske oplysninger mv.?)
Hvor mange personer er ca. berørt af bruddet?	
Hvordan er bruddet på persondatasikkerheden opstået?	
Dato for brud	(Hvornår har du opdaget bruddet)
Hvornår har du anmeldt bruddet?	(Dato for anmeldelse til leder/den lokale informationssikkerhedskoordinator)
Hvem har du anmeldt bruddet til?	(navn på person eller mailadresse)

Vær opmærksom på, at du kan blive kontaktet af din lokale informationssikkerhedskoordinator eller sikkerhedsgruppen, hvis der er behov for yderligere oplysninger om sikkerhedsbruddet. Det er desuden vigtigt, at du gemmer alle oplysninger om sikkerhedsbruddet som dokumentation.

Respons til anmelder og begrænsning af kommunikation

Din lokale informationssikkerhedskoordinator giver dig og din leder besked, når sikkerhedsbruddet er håndteret.

Vi gør opmærksom på, at du har tavshedspligt om sikkerhedshændelsen, medmindre du får andet at vide af din leder.

Læs mere

Ønsker du at læse mere om databeskyttelsesforordningens bestemmelser om sikkerhedsbrud, kan du se i bilag 1.

20. september 2022

Behandling og anmeldelse af sikkerhedsbrud - De lokale informationssikkerhedskoordinatorer

1. Stop ulykken

Få stoppet sikkerhedsbruddet hurtigst muligt! Få evt. fat i relevante samarbejdspartnere, hvis det er nødvendigt. Det kan være:

- Sikkerhedsbrud på en af kommunens hjemmesider – Kontakt lederen af Kommunikationsafdelingen (Katharina Ahrensberg, 43576222, kah@ishoj.dk
- Sikkerhedsbrud i et system – Kontakt systemets leverandør eller IT-afdelingen
- Skole-IT, hvis det vedrører skole- eller dagtilbudsområdet (Mads Larsen, 24 69 63 03, 5mal@ishoj.dk)

2. Lav en indledende vurdering af bruddet

Indhent den nødvendige dokumentation og information om sikkerhedsbruddet.
Hvis det vurderes, at der ikke er en risiko for den registrerede i forbindelse med bruddet, så gøres følgende:

- Løs problemet, så der ikke sker et brud igen
- Beskriv hændelsen, og hvordan den er håndteret samt, hvorfor der ikke er en særlig risiko forbundet med den
- Journaliser forløb på sagen sikkerhedsbrud i SBSYS
- Orienter DPO'en.

Hvis det vurderes, at bruddet er forbundet med en risiko for den registrerede, så skal der laves en risikovurdering i samarbejde med den centrale informationssikkerhedsgruppe.

Risikovurderingen foretages ud fra en vurdering af:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller brud på integritet.
- Oplysningernes art og omfang
- Risikoen for registrerede
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte)
- Antallet af berørte personer.

I forbindelse med vurdering af risici kan DPO'en inddrages. Hvis der er behov, indhentes der yderligere oplysninger fra personen, der har anmeldt bruddet.

Hvis der er en risiko for, at de(n) berørte person(er)s rettigheder eller frihedsrettigheder kan blive krænket, skal der foretages en anmeldelse til Datatilsynet. Hvis risikoen vurderes at være høj, skal der ligeledes ske en underretning af de(n) berørte person(er). Hvis de(n) registrerede skal underrettes, beslutter sikkerhedsgruppen, hvem der foretager underretningen. Som udgangspunkt vil det være en medarbejder, leder eller centerchefen fra det berørte område.

Vurdering af risici for kommunen og kommunens omdømme

Hvis sikkerhedsbruddet indebærer en risiko for kommunens omdømme, *skal* informationssikkerheds-udvalget involveres. Informationssikkerhedsudvalget sørger for at indkalde en krisecelle[1], hvis dette er nødvendigt. Det kan eksempelvis være i situationer, hvor der er en

- Risiko for at hændelsen fører til mediebevågenhed
- Risiko for økonomiske konsekvenser i form af bøde
- Risiko for kommunens omdømme
- Risiko for de ansatte
- Risiko for, at det kan have økonomiske konsekvenser for kommunen generelt – eks. via tab af aktiver, kontrakt, udbud mv.

Krisecellen kan bestå af følgende personer alt efter situationens omfang og alvor:

- Lederen for det berørte område/driftsted
- Centerchefen for det berørte område
- Direktøren for det berørte område
- Kommunaldirektøren (har ansvaret for at orientere Borgmesteren, som herefter kan orientere Byrådet)
- Lederen af IT-afdelingen (mødebooker og mødestyrer)
- Medlem af sikkerhedsgruppen (Referent)
- Leder af Kommunikationsafdelingen
- Centerchef for sikkerhedsområdet
- Anmelder af bruddet
- Jurist fra Center for Ledelse og Strategi

Anmeldelse til Datatilsynet

Hvis bruddet skal anmeldes til Datatilsynet gøres dette af den lokale informationssikkerhedskoordinator. Anmeldelsen foretages via virk.dk: Indberetning af brud på sikkerhed | Virk.
Kvittering for anmeldelse skal journaliseres på den pågældende sag i SBSYS.

Underretning af de(n) registrerede

Hvis der forelægger en høj risiko for de(n) registrerede, skal der foretages en underretning af de(n) registrerede uden unødig forsinkelse. Underretningen til den registrerede skal beskrive karakteren af bruddet på persondatasikkerheden og som minimum:

3) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
4) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
5) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Underretningen foretages af det fagcenter, hvor bruddet er sket. Underretningen skal journaliseres i SBSYS.

[1] Dvs. en gruppe af centrale personer, som sammen håndterer sikkerhedsbruddet.

Dokumentation

Relevante dokumenter og fund journaliseres i sagen vedr. sikkerhedsbrud i SBSYS, herunder beskrivelse af sikkerhedsbruddet (anmeldelsen), vurdering af risici, kvittering for anmeldelse til Datatilsynet, håndtering af hændelsen, underretning af registrerede mv. I SBSYS-sagen ligger der et ark i kladdeform som skal udfyldes. Herudover skal relevant dokumentation fra bruddet gemmes i sagen. Hvis dokumentationen indeholder personoplysninger, slettes disse eller alternativt skal de gemmes i en særskilt lukket sag, som der herefter henvises til i arket.

Læring i forbindelse med bruddet

Erfaringerne fra bruddet skal bruges til at nedsætte sandsynligheden for, at et lignende brud kan forekomme igen. Det kan evt. være ved at implementere eller opdatere procedurer, forbedre IT-sikkerheden eller indgå i dialog med leverandøren. Hvis der opleves gentagne sikkerhedsbrud i samme system, bør det overvejes om kontrakten skal ophæves.

Respons til anmelder

Anmelderen af sikkerhedsbruddet skal altid have en tilbagemelding, hvori der står:

- tak for anmeldelsen
- hvad har vi gjort for at håndtere hændelsen
- er bruddet meldt til Datatilsynet
- er kommunens DPO underrettet
- er de(n) registrerede underrettet
- hvad gør kommunen for at sikre, at det ikke sker igen

Tilbagemeldingen foretages som udgangspunkt af den lokale informationssikkerhedskoordinator.
Læs mere

Ønsker du at læse mere om databeskyttelsesforordningens bestemmelser om sikkerhedsbrud, kan du se i bilag 1.

Bilag 1: Yderligere information

Databeskyttelsesforordningen definerer følgende som informationssikkerhedshændelser:
"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".

Et brud på persondatasikkerheden er samtidig en informationssikkerhedshændelse. Dette begreb er i ISO 27000-standarden defineret som:
"En identificeret forekomst af en system-, tjeneste- eller netværkstilstand, der indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af kontroller, eller en tidligere ukendt situation, der kan være relevant for sikkerheden".

Lovmæssige krav:

Efter forordningen skal alle brud på persondatasikkerheden dokumenteres, hvis det indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Endvidere skal visse brud anmeldes til Datatilsynet inden for 72 timer.

I Ishøj Kommune har vi valgt, at alle brud skal registreres i kommunen, uagtet om de skal meldes til datatilsynet. Hvis bruddet på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, herunder for eksempel en risiko for diskrimination, identitetstyveri eller bedrageri, skal den dataansvarlige tillige, uden unødig forsinkelse, underrette den eller de registrerede om bruddet.

Typer af brud på persondatasikkerhed

Som eksempler på brud på persondatasikkerheden kan nævnes:

- Andre personer end den eller de personer hos den dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.
- Den dataansvarliges ansatte ændrer eller sletter personoplysninger ved et uheld.
- Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.
- Den dataansvarliges ansatte videregiver ubevidst eller bevidst personoplysninger om en borger/kunde til en anden borger/kunde – eller måske ligefrem til flere andre uvedkommende personer.
- En ansat mister eller glemmer sin mobil/tablet eller bærbar computer eller andet medie som indeholder personlige data.
- Når manglede kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

Læs mere i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden: https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf

Læs mere om databeskyttelsesforordningen: https://www.datatilsynet.dk/generelt-om-databeskyttelse/

Ændringslog

Årsag til revision Beskriv kort, hvad der er tilpasset og hvorfor	**Dato**	**Initialer**
Opdateret ift. NSIS krav	8. september	36637