VEJLEDNING TIL RETNINGSLINJER FOR HÅNDTERING AF SIKKERHEDS-BRUD VEDRØRENDE PERSONOPLYSNINGER

Baggrund
Databeskyttelseslovgivningen indeholder en række forpligtelser i tilfælde af et sikkerhedsbrud, der indeholder personoplysninger.

Nedenfor findes udkast til retningslinjer, der har til formål, at den enkelte boligorganisation er i stand til at håndtere et sikkerhedsbrud, ved dels at have implementeret nogle værktøjer til vurdering af risikoen (risikoanalyse), og dels at have defineret de interne roller, således at forpligtelserne i databeskyttelseslovgivningen kan overholdes.

Skabelonen
***Skabelonen** skal vejlede relevante medarbejdere i, hvordan de skal håndtere sikkerhedsbrud, herunder hvordan de kan vurdere risikoen ud fra benyttelsen af en risikomatrix. Ligeledes vil skabelonen kunne vejlede i, hvilke sikkerhedsbrud der henholdsvis skal anmeldes til Datatilsynet eller underrettes til den registrerede – igen ud fra en risikoanalyse.*

I skabelonen er der indsat en række kantede parenteser, hvor den enkelte boligorganisation selv skal udfylde boligorganisationens navn samt tage stilling til, hvilke formuleringer der anvendes, herunder om der behandles oplysninger af den nævnte karakter og i den nævnte situation.

*Visse af afsnittene indeholder en **foreslået formulering**, som dog efter omstændighederne må tilrettes, således at dokumentet afspejler boligorganisationens faktiske forhold. Det kan således heller ikke udelukkes, at der skal tilføjes yderligere.*

Årsagen til dette er, at indholdet i skabelonen skal give et retvisende billede af de faktiske forhold i boligorganisationen, således at den bliver praktisk anvendelig for medarbejderne.

Rådgivning
Det bemærkes, at indholdet i ovenstående eller skabelonen er ikke og kan ikke erstatte juridisk rådgivning. Materialet kan ikke træde i stedet for boligorganisationens egen vurdering af, hvorledes der skal disponeres i en given situation.

Boligorganisationen opfordres i alle tilfælde til at undersøge, om professionel rådgivning er nødvendig. BL kan til enhver tid kontaktes, hvis der er spørgsmål til ovenstående tekst eller skabelonen, ligesom der er indgået en særlig aftale med advokatfirmaet Accura, der kan hjælpe (kontakt BL for nærmere information).

RETNINGSLINJER FOR HÅNDTERING AF SIKKERHEDSBRUD VEDRØRENDE PERSONOPLYSNINGER

1 INDLEDNING

1.1 Disse retningslinjer vedrører boli.nu, Danmarksgade 81, 7000 Fredericia (herefter "Boligorganisationen", "vi", "vores", "os") håndtering af sikkerhedsbrud. Under punkt 2-3 defineres, hvad et sikkerhedsbrud er. Derefter følger vores konkrete retningslinjer for håndtering af sikkerhedsbrud under punkt 4-8.

1.2 Hos Boligorganisationen er Administrationschef Kristian Post ansvarlig for vores håndtering af sikkerhedsbrud. Når et sikkerhedsbrud eller risikoen for dette opdages, skal Administrationschef Kristian Post derfor straks orienteres herom via e-mail på kp@boli.nu,

1.3 Spørgsmål til disse retningslinjer skal rettes til Direktør Jens Christian Lybecker på 23 62 69 81 eller jcl@boli.nu.

2 GENERELT OM SIKKERHEDSBRUD

2.1 Boligorganisationen har en general pligt til at behandle personoplysninger på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (i lovgivningen benævnt som "integritet og fortrolighed"). Vi er endvidere forpligtede til at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, vi har identificeret, og for bl.a. at undgå brud på persondatasikkerheden.

2.2 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*" (herefter "Sikkerhedsbrud" eller "Sikkerhedsbruddet").

2.3 I Boligorganisationen kan et Sikkerhedsbrud indebære, at der sker uautoriseret eller ulovlig behandling samt tab, tilintetgørelse eller beskadigelse mv. af personoplysninger som vi behandler for fysiske personer, der direkte eller indirekte kan identificeres.

2.4 Hos Boligorganisationen behandles der personoplysninger i en række forskellige situationer. Dette drejer sig bl.a.om beboere, medarbejdere, besøgende (som fx optages via tv-overvågning) og kontaktpersoner. De personer vi behandler personoplysninger om, benævnes i det følgende som de "Registrerede".

3 KONSEKVENSER AF ET SIKKERHEDSBURD

3.1 Hos Boligorganisationen skelner vi mellem tre forskellige risikoscenarier i forhold til et Sikkerhedsbrud:

i) Ingen eller en ubetydelig risiko (dette er tilfældet, hvis det er usandsynligt, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder)

ii) Risiko (dette er tilfældet, hvis det er sandsynligt, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder)

iii) Høj risiko (dette er tilfældet, hvis Sikkerhedsbruddet vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder)

3.2 Ved *ingen eller ubetydelig risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder for alle Sikkerhedsbrud i overensstemmelse med punkt 4.

3.3 Ved *risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder efter punkt 4 samt anmelde Sikkerhedsbruddet til Datatilsynet i overensstemmelse med punkt 5.

3.4 Ved *høj risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder efter punkt 4, anmelde Sikkerhedsbruddet til Datatilsynet efter punkt 5 samt underrette den Registrerede om Sikkerhedsbruddet i overensstemmelse med punkt 6.

3.5 Ved risikovurderingen i forbindelse med et Sikkerhedsbrud skal det derfor fastlægges, hvilket risikoscenarie der konkret foreligger i forhold til den Registrerede. Dette afgøres hos Boligorganisationen på den ene side af de konsekvenser for den Registrerede, som et Sikkerhedsbrud kan indebære, samt på den anden side sandsynligheden for, at konsekvenserne indtræder.

3.6 Konsekvensen ved et Sikkerhedsbrud kan være:

1) Ubetydelig
2) Betydelig
3) Alvorlig

3.7 Sandsynligheden for at konsekvensen indtræder kan være:

1) Usandsynlig
2) Sandsynlig
3) Meget sandsynlig

De i punkt 3.6 og 3.7 angivne værdier benytter vi hos Boligorganisationen til at vurdere det konkrete risikoscenarie baseret på følgende formel: Konsekvens x sandsynlighed = risikoværdi

3.8 Dette indebærer, at følgende risikoværdier udløser følgende risikoscenarie (jf. i øvrigt den som **bilag 1** vedhæftede risikomatrix):

Risikoværdi	Risikoscenarie	Action
1	Ingen eller ubetydelig risiko	Se punkt 4
2-4	Risiko	Se punkt 4 og 5
6-9	Høj risiko	Se punkt 4, 5 og 6

3.9 Gennemførelsen af risikovurderingen vil basere sig på en konkret vurdering i det enkelte tilfælde. Følgende forhold bør dog altid indgå i den konkrete vurdering:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse;
- Oplysningernes art og omfang;
- Risikoen for at registrerede kan identificeres;
- Konsekvenser bruddet kan have for de registrerede;
- Hvorvidt bruddet omfatter særlige registrerede (fx hvis der er tale om børn eller særligt udsatte);
- Antallet af berørte fysiske personer

3.10 Nedenfor har vi opstillet en række eksempler på Sikkerhedsbrud. Det skal understreges, at nedenstående blot er eksempler, og ikke en facitliste, hvorfor der altid skal foretages en konkret risikovurdering af det enkelte Sikkerhedsbrud.

Eksempel	Konsekvens	Sandsynlighed	Risikoværdi
Boligorganisationens it-system bliver hacket og alle medarbejderoplysninger lægges ud på internettet.	Konsekvensen kan være alvorlig (tab af integritet mv.), idet der potentielt kan være tale om, at uvedkommende kan tilgå fortrolige og følsomme personoplysningerne (dvs. konsekvensværdien er 3).	Idet oplysningerne er offentligt tilgængelige, er det sandsynligt, at de tilgås af uvedkommende (dvs. sandsynlighedsværdien er 2)	Risikoværdien er 6 (3 x 2). Der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4, foretages anmeldelse til Datatilsynet, jf. punkt 5 og foretages underretning af de Registrerede, jf. punkt 6.
Ventelisten indeholdende navn og opnoteringsnummer sendes på en mail til en forkert modtager. Mailen tilbagekaldes med det samme (og tilbagekaldelsen lykkes).	Konsekvensen kan være tab af integritet mv. Dog er der alene tale om almindelige oplysninger (navne og numre) (dvs. konsekvensværdien kan efter omstændighederne sættes til 1).	Idet oplysningerne sendes til en forkert modtager, men tilbagekaldes med det samme, er det usandsynligt, at uvedkommende tilgår oplysningerne (dvs. sandsynlighedsværdien er 1)	Risikoværdien er 1 (1 x 1), hvorefter der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4.
Oplysninger om alle beboere, der modtager kommunal støtte, sendes til en forkert kommune.	Konsekvensen kan være betydelig (tab af integritet mv.), idet der potentielt kan være tale om videregivelse af fortrolige oplysninger (dvs. konsekvensværdien kan sættes til 2).	Det er næppe meget sandsynligt, at uvedkommende tilgår oplysningerne, og såfremt dette skulle ske, vil der formentlig være tale om medarbejdere underlagt tavshedspligt (dvs. sandsynlighedsværdien er højest 2)	Risikoværdien er 4 (2 x 2), hvorefter der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4, og foretages anmeldelse til Datatilsynet, jf. punkt 5.

4 DOKUMENTATION AF SIKKERHEDSBRUD

4.1 Enhver medarbejder der opdager et Sikkerhedsbrud skal **straks** orientere administrationschef Kristian Post på kp@bolinu og 23 49 36 54, som vil behandle Sikkerhedsbruddet. Dette gælder også, hvis der er tvivl om, hvorvidt der rent faktisk er tale om et Sikkerhedsbrud.

4.2 Administrationschef Kristian Post kontakter herefter KTP Data eller anden relevant afdeling med henblik på at afdække omfanget af Sikkerhedsbruddet og eventuelt iværksætte yderligere undersøgelser, således, at vi kan begrænse skaden og påse, at personoplysningerne bliver slettet (fx fra internettet, herunder fra søgemaskiner) eller eventuelt afhentet eller returneret fra uberettigede modtagere.

4.3 For alle Sikkerhedsbrud dokumenterer administrationschef Kristian Post de faktiske omstændigheder i en elektronisk log, således at denne afspejler resultatet af undersøgelserne om Sikkerhedsbruddet. Loggen skal som minimum indeholde de oplysninger, som fremgår af **bilag 2**.

4.4 Når den samlede information om Sikkerhedsbruddet er indsamlet, foretager administrationschef Kristian Post en risikovurdering i overensstemmelse med punkt 3 og bilag 1 med henblik på at afdække, om der skal ske henholdsvis anmeldelse til Datatilsynet og underretning af den Registrerede i overensstemmelse med punkt 5 eller 6 nedenfor. Til brug for denne vurdering anvendes bilag 1, og kopi af hvordan bilag 1 er benyttet vedlægges loggen (fx indscannet med afkrydsning af det relevante risikoscenarie).

4.5 Den tekniske fremgangsmåde for identifikation, kontrol med Sikkerhedsbruddet, forhindring af yderligere spredning, sikring imod lignende fremtidige Sikkerhedsbrud, yderligere undersøgelser, etc. er nærmere beskrevet i vores it-sikkerhedspolitik.

5 ANMELDELSE TIL DATATILSYNET

5.1 Ved et Sikkerhedsbrud skal der ske anmeldelse til Datatilsynet, medmindre det er usandsynligt, at Sikkerhedsbruddet indebærer en risiko for de Registrerede personers rettigheder. Anmeldelsen til Datatilsynet foretages af administrationschef Kristian Post.

5.2 Anmeldelse til Datatilsynet skal ske **inden for 72 timer** efter, at vi er blevet bekendt med Sikkerhedsbruddet. I særlige tilfælde, hvor vi ikke har mulighed for at overholde fristen på 72 timer, kræver dette en god begrundelse, som vi skal kunne forklare overfor Datatilsynet.

5.3 En anmeldelse af et Sikkerhedsbrud til Datatilsynet skal indeholde følgende informationer:

- Karakteren af bruddet på persondatasikkerheden mv.
- Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
- 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.

5.4 Hvis ikke vi har alle oplysninger til brug for ovenstående, skal vi i første omgang give de oplysninger, som vi har, og samtidig orientere Datatilsynet om, at vi løbende vil indlevere de manglende oplysninger relateret til anmeldelse af Sikkerhedsbruddet.

5.5 Anmeldelsen sker via den elektroniske indberetningsløsning, der består af en elektronisk blanket, som skal udfyldes af administrationschef Kristian Post efter forudgående godkendelse af administrationschef Kristian Post. Anmeldelsen kan indgives via følgende link: https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed

6 UNDERRETNING AF DEN REGISTRERERE

6.1 Hvis et Sikkerhedsbrud medfører høj risiko for den Registrerede, skal denne underrettes om Sikkerhedsbruddet uden unødig forsinkelse. Underretningen af den Registrerede foretages af administrationschef Kristian Post.

6.2 Underretningen skal skrives i et let forståeligt sprog, og skal som minimum indeholde følgende informationer:

i) Angivelse af at Boligorganisationen er dataansvarlig, og at eventuelle spørgsmål eller andre henvendelser skal ske til administrationschef Kristian Post, kp@boli.nu og 23 49 36 54,
ii) de sandsynlige konsekvenser af Sikkerhedsbruddet,
iii) og de foranstaltninger som vi har truffet eller foreslår truffet for at håndtere Sikkerhedsbruddet.

6.3 Administrationschef Kristian Post vil dog vurdere om en af nedenstående undtagelser til underretningspligten er opfyldt:

(i) Vores implementerede sikkerhedsforanstaltninger har gjort, at de berørte personoplysninger er uforståelige for en tredjemand (fx fordi de er krypterede).
(ii) Vi har efterfølgende foretaget skridt, som gør, at der ikke længere er en reel risiko for den Registrerede (fx ved at en fil med personoplysning har været tilgængelig på internettet er slettet inden, at den er blevet åbnet af en tredjemand).
(iii) Det vil kræve en uforholdsmæssig stor indsats at underrette alle implicerede Registrerede, hvorfor vi i stedet kan underrette dem via en offentlig meddelelse (dette vil alene i meget sjældne tilfælde være relevante, da vi som udgangspunkt har alle kontaktoplysninger på de Registrerede).
(iv) Hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende private interesser, herunder forretningshemmeligheder, immaterielle rettigheder, kontraktforhold eller afgørende hensyn til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

6.4 Selv om administrationschef Kristian Post vurderer, at der ikke skal ske underretning af de Registrerede, kan Datatilsynet beslutte, at dette skal ske.

7 HVEM ER FORPLIGTET?

7.1 Boligorganisationen er dataansvarlig i relation til behandlingen af personoplysninger, hvis denne afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af de omhandlede personoplysninger.

7.2 Boligorganisationen er derfor dataansvarlig for behandling af personoplysninger om Registrerede personer, hvilket indebærer, at vi skal overholde forpligtelserne ved et Sikkerhedsbrud vedrørende personoplysninger for denne personkreds.

7.3 Hvis vi benytter databehandlere til behandling af personoplysninger, har vi i de indgåede databehandleraftaler forpligtet den relevante databehandler til omgående at informere os om ethvert Sikkerhedsbrud. Databehandleren vil i sådanne tilfælde give os de oplysninger, som vi måtte have brug for til at foretage (i) risikovurderingen af Sikkerhedsbruddet, jf. punkt 3 og (ii) dokumentation, anmeldelse og/eller underretning af Sikkerhedsbruddet, jf. punkt 4-6.

8 RAPPORTERING

8.1 Ledelsen i Boligorganisationen skal orienteres om alle sikkerhedsbrud. Ledelsen skal endvidere orienteres, såfremt nærværende retningslinjer ikke overholdes, samt hvis der opstår forhold vedrørende disse retningslinjer, som har betydning for vurdering af Boligorganisationens risikoprofil på persondataområdet.

9 TILSIDESÆTTSLE AF RETNINGSLINJER

9.1 Tilsidesættelse af de nævnte retningslinjer kan give anledning til ansættelsesretlige konsekvenser, herunder advarsel og i yderste fald opsigelse eller bortvisning.

10 AJOURFØRING

10.1 Ledelsen i Boligorganisationen er bemyndiget til at tage disse retningslinjer op til revision, når det vurderes relevant.

02/04-2024

BILAG 1: RISIKOMATRIX

Konsekvens → **----------** **Sandsynlighed ↓**	**1. Ubetydelig**	**2. Betydelig**	**3. Alvorlig**
3. Meget sandsynligt	**3**	**6**	**9**
2. Sandsynligt	**2**	**4**	**6**
1. Usandsynligt	**1**	**2**	**3**

BILAG 2: DOKUMENTATIONSLOG (baseret på Datatilsynets vejledning om sikkerhedsbrud)

Sikkerhedsbrud hos Boligorganisationen	**Beskrivelse af bruddet:**
1. Dato og tidspunkt for bruddet?:	
2. Hvad er der sket?:	
3. Årsagen til bruddet?:	
4. Hvilken type personoplysninger 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)?:	
8.1. Hvis nej, begrundelse for ikke at underrette de berørte personer?:	