21. Retningslinjer for håndtering af sikkerhedsbrud vedrørende personoplysninger

1. Indledning

1.1 Disse retningslinjer vedrører Nykøbing F. Boligselskabs håndtering af sikkerhedsbrud. Under punkt 2.2 defineres, hvad et sikkerhedsbrud er. Derefter følger vores konkrete retningslinjer for håndtering af sikkerhedsbrud under punkt 4.8.

1.2 Hos Nykøbing F. Boligselskab er sekretariatet/direktøren ansvarlig for vores håndtering af sikkerhedsbrud. Når et sikkerhedsbrud eller risikoen for dette opdages, skal sekretariatschef Lotte Pedersen derfor straks orienteres herom på lap@nfbo.dk , tlf. 54 84 19 74 – cc. Dorte Jørgensen på doj@nfbo.dk.

1.3 Spørgsmål til disse retningslinjer skal rettes til Lotte Pedersen på lap@nfbo.dk.

2. Generelt om sikkerhedsbrud

2.1 Nykøbing F. Boligselskab har en generel 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 Nykøbing F. Boligselskab 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 Nykøbing F. Boligselskab behandles der personoplysninger i en række forskellige situationer. Dette drejer sig bl.a. om beboere, medarbejdere, besøgende (som f.eks. optages via tv-overvågning) og kontaktpersoner. De personer, vi behandler personoplysninger om, benævnes i det følgende som de ”registrerede”.

3. Konsekvenser af et sikkerhedsbrud

3.1 Hos Nykøbing F. Boligselskab skelner vi mellem tre forskellige risikoscenarier ved 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 Nykøbing F. Boligselskab 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.

Konsekvensen ved et sikkerhedsbrud kan være:

1) Ubetydelig
2) Betydelig
3) Alvorlig

3.6 Sandsynligheden for at konsekvensen indtræder kan være:

1) Usandsynlig
2) Sandsynlig
3) Meget sandsynlig

3.7 De i punkt 3.5 og 3.6 angivne værdier benytter vi hos Nykøbing F. Boligselskab 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 risikomatrix, der er vedhæftet som bilag 1):

Risikoværdi	**Risikoscenarie**	**Action**
1	Ingen eller ubetydelig risiko	Se punkt 4
2	Risiko	Se punkt 4 og 5
~~3~~	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
- Om bruddet omfatter særlige registrerede (f.eks. 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. Der skal altid foretages en konkret risikovurdering af det enkelte sikkerhedsbrud.

Eksempel	Konsekvens	Sandsynlighed	Risikoværdi
Nykøbing F. Boligselskabs 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), hvorefter 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 det lykkes).	Konsekvensen kan være tab af integritet mv. Dog er der 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 mindre sandsynligt, 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, at uvedkommende kan tilgå fortrolige oplysninger (dvs. konsekvensværdien kan efter omstændighederne sættes til 2).	Det er næppe meget sandsynligt, at uvedkommende tilgår oplysningerne, og hvis det skulle ske, vil der formentlig være tale om medarbejdere underlagt tavshedspligt (dvs. sandsynlighedsværdien er højst 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 Lotte Pedersen på lap@nfbo.dk, tlf. 54 84 19 74 – cc. Dorte Jørgensen på doj@nfbo.dk

- som vil behandle sikkerhedsbruddet. Dette gælder også, hvis der er tvivl om, hvorvidt der rent faktisk er tale om et sikkerhedsbrud.

4.2 Lotte Pedersen kontakter herefter de relevante personer eller samarbejdspartnere med henblik på at afdække omfanget af sikkerhedsbruddet og eventuelt iværksætte yderligere undersøgelser, så vi kan begrænse skaden og påse, at personoplysningerne bliver slettet (f.eks. fra internettet, herunder fra søgemaskiner) eller eventuelt afhentet eller returneret fra uberettigede modtagere.

4.3 For alle sikkerhedsbrud dokumenterer Lotte Pedersen de faktiske omstændigheder i en elektronisk log, så loggen afspejler resultatet af undersøgelserne om sikkerhedsbruddet. Loggen skal som minimum indeholde de oplysninger, som fremgår af bilag 2 - dokumentationsloggen.

4.4 Når den samlede information om sikkerhedsbruddet er indsamlet, foretager Lotte Pedersen sammen med Dorte Jørgensen 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 (f.eks. 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/andet – det må vi lige se på)

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 Lotte Pedersen – eller i dennes fravær af Kate Petersen, økonomi.

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 vi kunne forklare overfor Datatilsynet.

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

i) Karakteren af bruddet på persondatasikkerheden mv.
ii) Navn på og oplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

iii) De sandsynlige konsekvenser af bruddet på persondatasikkerheden
iv) De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet op 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 Anmeldelse sker via den elektroniske indberetningsløsning, der består af en elektronisk blanket, som skal udfyldes af sekretariatschefen , efterforudgående godkendelse af direktøren. Anmeldelse kan indgives via følgende link: https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed

6. Underretning af den registrerede

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 Lotte Pedersen

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

i) Angivelse af at Nykøbing F. Boligselskab er dataansvarlig, og at eventuelle spørgsmål eller andre henvendelser skal ske til Lotte Pedersen på lap@nfbo.dk eller tlf. 54 84 19 74 og Dorte Jørgensen, doj@nfbo.dk.
ii) de sandsynlige konsekvenser af sikkerhedsbruddet
iii) og de foranstaltninger som vi har truffet eller foreslår truffet for at håndtere sikkerhedsbruddet

6.3 Lotte Pedersen 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 (f.eks. fordi de er krypterede)
(ii) Vi har efterfølgende foretaget skridt, som gør, at der ikke længere er en reel risiko for den registrerede (f.eks. 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 Lotte Pedersen vurderer, at der ikke skal ske underretning af de registrerede, kan Datatilsynet beslutte at dette skal ske.

7. Hvem er forpligtet?

7.1 Nykøbing F. Boligselskab er dataansvarlige i relation til behandlingen af personoplysninger, hvis disse afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af de omhandlede personoplysninger.

7.2 Nykøbing F. Boligselskab 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 Direktøren i Nykøbing F. Boligselskab skal orienteres om alle sikkerhedsbrud. Direktøren skal derudover orienteres, hvis retningslinjerne ikke er overholdt, og hvis der opstår forhold vedrørende disse retningslinjer, som har betydning for vurdering af Nykøbing F. Boligselskabs risikoprofil på persondataområdet.

9. Tilsidesættelse 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 Nykøbing F. Boligselskab er bemyndiget til at tage disse retningslinjer op til revision, når det vurderes relevant og minimum 1 gang årligt.

29. februar 2024/version 2/Tidl. Pkt. 1.8. – nu 21.

21. Retningslinjer for håndtering af sikkerhedsbrud vedrørende personoplysninger

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**

21. Retningslinjer for håndtering af sikkerhedsbrud vedrørende personoplysninger

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?:	