17. Politik for datasikkerhed ved boligadministration - generelt

1. Indledning

1.1 I forbindelse med boligadministration skal sikkerhedsbestemmelserne i databeskyttelsesforordningen[1] iagttages. Det indebærer bl.a., at Nykøbing F. Boligselskab som den dataansvarlige virksomhed, skal leve op til kravene om datasikkerhed.

1.2 I medfør databeskyttelsesforordningen artikel 5, stk. 1, litra f, skal der træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelsesforordningen.

1.3 Efter databeskyttelsesforordningens artikel 24 gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med databeskyttelses-forordningen. Disse foranstaltninger skal om nødvendigt revideres og ajourføres, og hvis det står i rimeligt forhold til behandlingsaktiviteterne, skal de nævnte foranstaltninger omfatte implementering af passende databeskyttelsespolitikker.

1.4 Derudover følger det af databeskyttelsesforordningens artikel 32, at vi under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. (alt efter hvad der relevant):

- pseudonymisering og kryptering af personoplysninger,
- evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester,
- evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse,
- en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

1.5 Ved vurderingen af hvilket sikkerhedsniveau der er passende, skal vi efter artikel 32 navnlig tage hensyn til de risici, som behandling udgør. Sådanne risici kan være hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

1.6 Denne politik er udtryk for de sikkerhedsforanstaltninger i forbindelse med personaleadministration, som Nykøbing F. Boligselskab har truffet baseret på vores risikovurdering i forbindelse med boligadministration. Politikken gælder uanset om behandlingen af personoplysninger sker på arbejdspladsen, i hjemmet eller andre steder. Se i øvrigt Nykøbing F. Boligselskabs IT-sikkerhedspolitik, som du finder på Intranettet under punktet GDPR.

2. Definitioner

2.1 Ved "Personoplysninger" forstås i denne politik enhver form for information om en identificeret eller identificerbar fysisk person, herunder information om medarbejdere, beboere og personer på venteliste.

2.2 Ved "it-systemer" eller "it-systemet" forstås i disse retningslinjer Nykøbing F. Boligselskabs eller det af Nykøbing F. Boligselskab benyttede software, netværk (interne såvel som eksterne) og hardware, herunder bærbare og stationære computere, tablets, smartphones og andre mobile samt stationære enheder mv., der benyttes i forbindelse med elektronisk databehandling af personoplysninger.

2.3 Ved "Behandling" forstås enhver aktivitet som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overgivelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

2.4 Ved "Sletning" af personoplysninger forstås, at de omhandlede personoplysninger uigenkaldeligt fjernes fra alle de lagringsmedier, hvor de har været lagret, og at personoplysningerne på ingen måde kan genskabes. Dette gælder for samtlige lagringsmedier, der har været i anvendelse i forbindelse med den pågældende behandling af personoplysninger.

2.5 Ved "Sikkerhedsbrud" forstås 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.

3. Ansvar

3.1 Nykøbing F. Boligselskab er som udgangspunkt dataansvarlig for de personoplysninger, som behandles om bl.a. medarbejdere, beboere og personer på venteliste i Nykøbing F. Boligselskabs it-systemer.

3.2 Sekretariatet har det interne ansvar for Nykøbing F. Boligselskabs it-sikkerhed. Sekretariatet sikrer, at der kommunikeres it-sikkerhedsmæssige retningslinjer ud

til medarbejdere, samarbejdspartnere samt øvrige personer, der er involveret i anvendelsen af personoplysninger hos Nykøbing F. Boligselskab.

3.3 Nykøbing F. Boligselskabs medarbejdere må alene handle indenfor den stillingsfuldmagt, de besidder i form af deres ansættelsesforhold hos Nykøbing F. Boligselskab.

3.4 Den enkelte medarbejder/bruger er ansvarlig for at sikre, at disse retningslinjer og øvrige it-sikkerhedspolitikker mv. efterleves.

4. Generelle principper

4.1 Al behandling af personoplysninger skal ske i overensstemmelse med de grundlæggende principper, der følger af databeskyttelseslovgivningen. Dette indebærer, at personoplysninger skal

- behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til de registrerede (f.eks. beboere, opnoterede på ventelister, pårørende, ansatte mv.)
- indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål
- være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles
- være korrekte og om nødvendigt ajourførte
- opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles
- behandles 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.

4.2 Ovennævnte grundlæggende principper gælder for al behandling af personoplysninger, som foretages af Nykøbing F. Boligselskab.

5. Fysisk sikring

5.1 Generelt

5.1.1 Alle lokaler mv., hvor der behandles personoplysninger, skal være sikret på en sådan måde, at uvedkommende ikke har adgang til lokalerne mv. Dette indebærer, at der i fornødent omfang skal ske aflåsning og tilsluttes alarm mv., når lokalerne forlades, ligesom der ikke må være adgang for ikke-autoriseret personale mv.

5.1.2 For ejendomskontorerne gælder, at kun ejendomsfunktionærerne har nøgle til ejendomskontoret. Alle papirer eller andet, der indeholder personoplysninger, låses ned/gemmes væk, når kontoret forlades. Papirer med personoplysninger makuleres efter endt brug.

5.1.3 For administrationen gælder, at kun personalet har nøgler til kontoret. Papirer med personoplysninger sikres i aflåste skabe og makuleres efter endt brug.

5.1.4 Se bilag 18.2 – Oversigt over behandling af personoplysninger via mail mv. – punkt 4: Arkivering og makulering af fysisk materiale.

5.2 Serverrum

5.2.1 Serverrummet på administrationens adresse indeholder udstyr til brug for databehandling, men der er ikke personoplysninger på boligselskabets egen server.

5.2.2 Serverrum med personoplysninger befinder sig hos DataInform A/S, med hvem der er indgået en Databehandleraftale.

5.3 Udstyr

5.3.1 It-udstyr, som indeholder personoplysninger, skal opbevares i sikrede lokaler, jf. pkt. 5.1 og 5.2 ovenfor.

5.3.2 Bærbare pc'er, mobiltelefoner, tablets og andre datamedier/mobilt it-udstyr må ikke efterlades uden overvågning på steder, hvor ikke-autoriseret personale har adgang.

5.3.3 Der henvises i øvrigt til pkt. 11 nedenfor.

6. Autorisationsordning

6.1 Der gives alene adgang til it-systemer med personoplysninger for medarbejdere, som direkte er autoriserede hertil, jf. denne autorisationsordning.

6.2 Autorisationsordningen indebærer, at der kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Sådanne personer betragtes som uvedkommende, og disse har derfor ikke adgang til oplysningerne.

6.3 Ved vurderingen af, hvilke medarbejdere der autoriseres, lægges der vægt på, hvad den enkelte bruger har behov for at være autoriseret til. Konkret har vi vurderet, at brugerne er autoriseret til de programmer, der er behov for til at udføre jobbet, jf. bilag 18.1 – Autorisationslisten.

6.4 For brugere, som ikke længere har behov for de autorisationer, de har fået udstedt, inddrages autorisationerne. Det gælder f.eks. medarbejdere, som flytter til et arbejdsområde, der ikke relaterer sig til administration af lejeforhold, eller hvis ansættelsesforholdet ophører.

6.5 Udover medarbejdere, der er beskæftiget med administration af lejeforhold, kan der endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver. Dette er personer, som udfører revision, og personer som udfører teknisk vedligeholdelse, driftsovervågning, fejlretning mv. Der er fastlagt særlige retningslinjer for udstedelse og inddragelse af sådanne autorisationer, herunder også retningslinjer for udstedelse af autorisationer, der kun behøver at være midlertidige.

6.6 Ved nyansættelser og interne rokereringer vurderer økonomifunktionen sammen med direktøren – baseret på ovenstående retningslinjer – om de organisatoriske ændringer tillige giver anledning til ændrede adgangsrettigheder.

6.7 En gang årligt foretager økonomifunktionen sammen med direktøren en gennemgang og vurdering af relevansen af de tildelte rettigheder/autorisationer. Dette indebærer bl.a., at der konkret tages stilling til, hvorvidt en bruger kun skal kunne foretage forespørgsler, eller om brugeren også skal kunne inddatere oplysninger, samt om brugeren skal kunne slette oplysninger. Hvis der er brugere, som alene autoriseres til enkelte af de nævnte funktioner, er systemerne teknisk indrettet således, at brugerne kun gives mulighed for adgang til oplysningerne i overensstemmelse med de givne autorisationer.

7. Virusbeskyttelse mv.

7.1 Nykøbing F. Boligselskab har indgået databehandleraftale med DataInform A/S, der sikrer systemet mod virus, orme, trojanske heste mv. Derudover er vores egen server, der kun indeholder internetadgang, startfiler og firewall, sikret med antivirus software, der administreres af Skymaster A/S.

8. Firewall

8.1 I forhold til firewallen skal det ligeledes beskrives/være procedurer herfor, herunder med henblik på at kunne opdage og undgå web-baserede angreb. Det skal i den forbindelse sikres, at firewallen f.eks. kun må tillade protokoller og trafik, som er forretningsmæssigt begrundet, og at firewallen blokerer al ind- og udgående trafik, som ikke er specifikt tilladt. Se bilag 36 for en beskrivelse af opsætningen af Firewallen.

9. Passwordpolitik

9.1 Denne passwordpolitik gælder samtlige it-systemer og alle personer, som har fået udleveret et brugernavn. Alle brugere er udstyret med passwords, og det er brugerens ansvar, at disse er udformet og omgås hensigtsmæssigt.

9.2 Vi anbefaler, at du behandler dine passwords efter følgende regler:

- Passwordet skal have en længde på mindst 8 tegn – og helst 12 tegn
- Du skal skifte password med jævne mellemrum – mindst hver 3. måned. Hos EG bolig skiftes passwordet, når systemet beder om det.
- Du skal udforme dit password, så det er komplekst og svært at bryde, og det skal bestå af en kombination af små bogstaver, store bogstaver og tal. Dette er mindre vigtigt, hvis passwordet består af minimum 12 tegn

9.3 Vi anbefaler, at du ikke gør følgende, når du opretter et password:
- Bruge brugernavnet eller dele heraf
- Bruge dit eget navn eller dele heraf
- Bruge din familie, dine venners eller dit kæledyrs navne
- Anvende ord stavet bagfra som password
- Anvende ord med tal foran eller bagved som password
- Anvende numre der kan identificeres med dig (f.eks. din fødselsdag)
- Anvende logiske tastekombinationer (f.eks. ”qwerty” eller ”asdfgh”)

9.4 Hvis du har indtastet forkert password 3 gange, låses din konto, og du skal kontakte administrationen for at få den åbnet igen.

9.5 Hvis du frygter, at et af dine password er blevet afluret skal du straks ændre passwordet og kontakte administrationen.

9.6 Dine passwords er personligt og må ikke overdrages til andre - heller ikke i forbindelse med ferie. Du må ikke bruge "husk password"-faciliteter, ligesom du ikke må nedskrive dit password og gemme det i nærheden af tastaturet. Du må ikke bruge det password, som du bruger til Nykøbing F. Boligselskabs systemer, til private tjenester.

10. E-mails

10.1 Hvis de under pkt. 10.2 nævnte oplysningstyper sendes med e-mail via internettet, skal der ske kryptering. I praksis sker dette ved anvendelse af sikker mail via Outlook, via e-boks eller via et af de programmer vi anvender til behandling af data.

10.2 Sikker mail anvendes som minimum, hvis følgende oplysninger sendes via e-mail (uanset om det er nævnt direkte i mailen eller i vedhæftede filer mv.):

- Personnummer, samt
- Helbredsoplysninger (herunder oplysninger om handikap),
- Oplysninger om strafbare forhold, eller
- Andre følsomme oplysninger omfattet af databeskyttelsesforordningens artikel 9.

10.3 Der henvises i øvrigt til bilag 16 Politik for brug af IT systemer mv., hvor der findes en nærmere beskrivelse af generel benyttelse af e-mails mv. og bilag 18.2 Oversigt over behandling af personoplysninger v/mail mv.

11. Printning mv.

11.1 Udprintet materiale, der indeholder personoplysninger, skal opbevares på forsvarlig vis og på en sådan måde, at uvedkommende ikke får adgang hertil.

11.2 Udprintet materiale skal makuleres, når det ikke længere benyttes.

11.3 Printere skal placeres på en sådan måde, at printerne er utilgængelige for uvedkommende.

12. Sletning

12.1 Personoplysninger, der behandles for varetagelsen af Nykøbing F. Boligselskabs opgaver, slettes når behandlingen af personoplysningerne ikke længere er nødvendig af hensyn til de formål, hvortil oplysningerne er indsamlet eller behandlet.

Der henvises i øvrigt til Nykøbing F. Boligselskabs slettepolitik, hvori de nærmere fastsatte sletteprocedurer er oplistet. Sletningspolitikken findes i 22 Retningslinjer for sletning af personoplysninger og i bilag 37 Beskrivelse af sletning i EG Bolig.

13. Reparation og service

13.1 Generelt

13.1.1 I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

13.1.2 I det følgende beskrives det konkret, hvilke foranstaltninger der er truffet mod, at uvedkommende får adgang til oplysningerne i ovennævnte tilfælde.

13.2 Reparation og service

Reparation og service af udstyr udføres på arbejdspladsen. Reparation udføres primært af Skymaster A/S, mens service af programmer primært udføres af DataInform A/S.

13.3 Kassering

13.3.1 Ved kassering af udstyr, som indeholder personoplysninger, destrueres udstyret, ved kørsel direkte til forbrænding.

13.4 Salg

13.4.1 I det omfang vi vælger at sælge udstyr, der har været benyttet til lagring af personoplysninger, vil der forinden ske effektiv sletning. Sletningen udføres af Skymaster A/S, hvis vi ønsker at sælge udstyr.

14. Hjemmearbejdspladser mv.

14.1 Generelt

14.1.1 Ved hjemmearbejdsplads forstås en arbejdsplads, som etableres ved adgang til Nykøbing F. Boligselskabs it-systemer fra andre steder end arbejdspladsen (f.eks. fra hjemmet), så medarbejderen kan udføre visse arbejdsopgaver uden at skulle møde fysisk på arbejdspladsen.

14.1.2 Ved arbejde fra en hjemmearbejdsplads finder anvendelsen af personoplysninger sted i et andet miljø, og der er derfor en række særlige forhold, som der skal tages hånd om. Generelt skal det derfor sikres, at personoplysninger heller ikke i denne sammenhæng kommer uvedkommende til kendskab.

14.1.3 Krav til hjemmearbejdspladser gælder også for andre fjernarbejdspladser, herunder ved adgang fra smartphones, tablets og lignende.

14.2 Lokal lagring af oplysninger

14.2.1 Alle personoplysninger, der behandles elektronisk, og som er nødvendig for varetagelse af Nykøbing F. Boligselskabs opgaver, skal lagres i Nykøbing F. Boligselskabs centrale it-systemer.

14.2.2 Personoplysninger kan undtagelsesvist lagres på "skrivebordet" og lokale drev mv., så længe der er tale om dokumenter eller lignende under udarbejdelse, og hvor der er behov for løbende at tilføje nye oplysninger i forbindelse med behandlingen. En sådan behandling må alene ske kortvarigt – og maksimalt 30 dage – og personoplysningerne skal straks det er muligt overføres til Nykøbing F. Boligselskabs centrale it-systemer og slettes fra "skrivebordet" og lokale drev mv.

14.3 Lokal udskrivning af oplysninger

14.3.1 Der må som udgangspunkt ikke udskrives dokumenter mv. indeholdende personoplysninger fra hjemme-printer mv.

14.3.2 Hvis der undtagelsesvist udskrives dokumenter hjemme, skal det sikres, at personoplysningerne ikke kommer uvedkommende til kendskab, herunder ved at udskrifterne opbevares aflåst. Når udskrifterne ikke længere skal benyttes, skal de medbringes til arbejdspladsen med henblik på makulering.

14.4 Øvrige forhold

14.4.1 De øvrige punkter i disse retningslinjer gælder også ved behandling af personoplysninger og brug af It-systemer i forbindelse med hjemmearbejdspladser mv

15. Databehandlere

15.1 Der må udelukkende bruges databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i databeskyttelsesforordningen

15.2 Ved brug af en ekstern databehandler til håndtering af oplysninger, skal databeskyttelsesforordningens artikel 28 om skriftlig databehandleraftale mv. følges.

15.3 Der henvises til vores den samlede og opdaterede oversigt over Nykøbing F. Boligselskabs databehandlere – Bilag 38.

16. Sikkerhedsbrud

16.1 Ethvert sikkerhedsbrud skal håndteres i overensstemmelse med Nykøbing F. Boligselskabs retningslinjer for håndtering af sikkerhedsbrud. Se 21 Retningslinjer for håndtering af sikkerhedsbrud, som er tilgængelig på intranettet.

17. Tilsidesættelse af retningslinjerne

17.1 Manglende overholdelse af ovenstående retningslinjer kan medføre ansættelsesretlige konsekvenser, herunder advarsler, opsigelse samt i yderste fald bortvisning.

18. Diverse

18.1 Denne politik tages op til revision én gang årligt og opdateres, hvis dette er nødvendigt.

18.2 Er der spørgsmål til indholdet, kan der rettes henvendelse til Lotte Pedersen på lap@nfbo.dk eller 54 84 19 74.

25. april 2024/version 5