18. Politik for datasikkerhed ved personaleadministration

1. Indledning

1.1 I forbindelse med personaleadministration skal sikkerhedsbestemmelserne i databeskyttelsesforordning[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 navnligt tage hensyn til de risici, som behandling udgør. Sådanne risici kan

[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)

være hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af 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 personaleadministration. Derudover er politikken inspireret af de specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration, som Datatilsynet tidligere har stillet (før databeskyttelsesforordningens ikrafttræden), baseret på den tidligere databeskyttelseslovgivning. Den tidligere databeskyttelses-lovgivning indeholdt bl.a. en bestemmelse om, at dataansvarlige skulle træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt blev tilintetgjort, fortabt eller forringet, samt mod, at de kom til uvedkommendes kendskab, blev misbrugt eller i øvrigt blev behandlet i strid med loven.

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. Adgangsbegrænsning

4.1 Adgang til personaleoplysninger skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

4.2 Der gives alene adgang til personoplysninger for HR-medarbejdere eller andre (herunder aktuelle samt kommende ledere), som direkte er autoriserede hertil, jf. bilag 18.1 Autorisationslisten. Autorisationsordningen beskrives i det følgende.

4.3 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. Dette indebærer, at alle andre personer, også øvrige medarbejdere hos Nykøbing F. Boligselskab, i forbindelse med behandling af personoplysninger i HR-sammenhæng betragtes som uvedkommende, og disse har derfor ikke adgang til oplysningerne.

4.4 Ved vurderingen af hvilke medarbejdere der autoriseres, lægges der vægt på, hvad den enkelte bruger har behov for at være autoriseret til. Konkret vil den pågældende henvises til autorisationslisten, hvori det nærmere beskrives, hvilke oplysninger brugeren herved autoriseres (godkendes) til at anvende.

4.5 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 HR, eller hvis ansættelsesforholdet ophører.

4.6 Udover medarbejdere, der er beskæftiget med HR-opgaver, kan der tillige 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 af sådanne autorisationer og for inddragelse heraf, herunder også retningslinjer for udstedelse af autorisationer, der kun behøver at være midlertidige.

4.7 Ved nyansættelser og interne rokereringer vurderer ledelsen – baseret på ovenstående retningslinjer – om de organisatoriske ændringer tillige giver anledning til ændrede adgangsrettigheder.

4.8 En gang årligt foretager ledelsen 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.

4.9 Der henvises til bilag 18.1 Autorisationslisten, hvor der findes en nærmere beskrivelse af autorisationsordningen.

5. Instruktion og oplæring

5.1 Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

5.2 Der er således ikke en bestemt måde, der er mere rigtig end en anden, så længe det blot sikres, at det kan dokumenteres, at der er foretaget instruktion og oplæring i, hvad der må gøres med oplysningerne, og hvordan de skal beskyttes.

6. Papirbaserede personaleoplysninger

6.1 Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

6.2 Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

6.3 Mappe med personaleoplysninger opbevares til alle tider i pengeskabet, der står i mødelokalet på 1. sal. Mappen tages kun ud, når den skal anvendes – typisk i forbindelse med lønudarbejdelse - og sættes på plads efter endt brug. Papirer, der i

løbet af dagen bruges til f.eks. oprettelse af medarbejdere i lønsystem eller andet, makuleres efter indtastning.

Enkelt papirer med personaleoplysninger makuleres i makuleringsmaskinen, der er anbragt ved siden af kopimaskinen på 1. sal, Slotsgade 20. Drejer det sig om større mængder af papir skal disse køres direkte til forbrænding. Afhentning aftales med administrationen, der sørger for at bestille afhentning og direkte kørsel til forbrændingen.

7. Adgangskoder

7.1 Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode.

7.2 Personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den.

7.3 Om benyttelse af adgangskoder bemærkes følgende:

7.3.1 Vi anbefaler at adgangskoden skal have en længde på mindst 8 tegn og helst 12 tegn og opbygges af en blanding af tal og store og små bogstaver. Dette er mindre vigtigt, hvis passwordet er på minimum 12 tegn. Der henvises til Nykøbing F. Boligselskabs Politik for brug af IT-systemer mv., hvor der findes en nærmere beskrivelse af adgangskoder/passwords.

8. Adgangsforsøg

8.1 Det skal registreres af DataInform A/S, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg, hvilket gøres af DataInform A/S.

9. Firewall og viruskontrol

9.1 It-udstyr koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

9.2 Der henvises til Nykøbing F. Boligselskabs Politik for datasikkerhed ved boligadministration og IT sikkerhedspolitik, hvor der findes nærmere beskrivelse af bl.a. firewall og viruskontrol.

10. E-mailkorrespondance

10.1 Følsomme personaleoplysninger og personnumre må alene sendes med e-mail via internettet, hvis dette sker krypteret.

I praksis sker dette ved anvendelse af sikker mail via Outlook, e-boks eller via Dataløn/Visma. Der henvises til bilag 18.2 Behandling af personoplysninger via mail mv.

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

- Personnummer,
- Helbredsoplysninger,
- Oplysninger om medlemskab af en fagforening,
- Oplysninger om strafbare forhold
- Andre følsomme oplysninger omfattet af databeskyttelsesforordningens artikel 9 og 10

Se i øvrigt afsnit 18.2: Oversigt over behandling af personoplysninger v/mail mv.

11. Reparation og service

11.1 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.

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

11.2.1 Reparation og service

11.2.1.1 Der henvises til Nykøbing F. Boligselskabs Politik for datasikkerhed ved boligadministration, hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med reparation og service af udstyr.

11.2.2 Kassation

11.2.2.1 Der henvises til Nykøbing F. Boligselskabs Politik for datasikkerhed ved boligadministration, hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med kassation af udstyr.

11.2.3 Salg

11.2.3.1 Der henvises til Nykøbing F. Boligselskabs Politik for datasikkerhed ved boligadministration, hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med salg af brugt udstyr.

12. Sikkerhedsbrud

12.1 Ved et sikkerhedsbrud forstås 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

12.2 Ethvert sikkerhedsbrud skal håndteres i overensstemmelse med Nykøbing F. Boligselskabs retningslinjer for håndtering af sikkerhedsbrud, der er tilgængelig på www.nfbo.dk/Intranettet.

13. Databehandlere

13.1 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.

13.2 Ved brug af en databehandlere skal der indgås en databehandleraftale, der lever op til kravene efter databeskyttelsesforordningens artikel 28, ligesom der skal føres fornødent tilsyn med databehandlere.

13.3 Hos Nykøbing F. Boligselskab benyttes følgende databehandlere, der behandler personaleoplysninger på vegne af os:

13.3.1 Lønbureau: Visma - Dataløn

13.3.2 Ekstern it-leverandør: Datainform A/S

13.3.3 Virksomhed, der hoster hjemmeside: E-team

13.3.4 Virksomhed, der hoster servere: Datainform A/S

13.4 Der er med ovenstående databehandlere indgået skriftlige databehandleraftaler, der regulerer vores overlevering af personoplysninger, og som har til formål at sikre, at databeskyttelseslovgivningens sikkerhedsregler overholdes.

14. Tilsidesættelse af denne politik

14.1 Manglende overholdelse af denne politik kan medføre ansættelsesretlige konsekvenser, herunder advarsler, opsigelse samt i yderste fald bortvisning.

15. Diverse

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

15.2 Ændringer i politikken i relation til den enkelte medarbejder vil – medmindre andet følger af vores arbejdsretlige forpligtelser mv. – træde i kraft, når medarbejderen er blevet gjort bekendt hermed via de sædvanlige kanaler.

15.3 Har du spørgsmål eller kommentarer til denne politik, kan du kontakte sekretariatschef Lotte Pedersen, lap@nfbo.dk eller tlf. 54 84 19 74.

15.4 Der henvises til politik for datasikkerhed ved boligadministration, der er tilgængelig her www.nfbo.dk/intranettet.

25. april 2024/version 4