SUNDBY-HVORUP Boligselskab

Politik for data-sikkerhed ved boligadministration

INDHOLD

1. INDLEDNING

1.1 I forbindelse med boligadministration skal sikkerhedsbestemmelserne i forordning nr. 2016/679 om beskyttelse af personoplysninger (herefter "databeskyttelsesforordningen") iagttages. Det indebærer bl.a., at Sundby-Hvorup Boligselskab (herefter "Boligorganisationen"), 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 databeskyttelsesforordningen. 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 eller adgang til Personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

1.6 Denne politik er udtryk for de overordnede sikkerhedsforanstaltninger, som Boligorganisationen har truffet baseret på databeskyttelsesforordningen i forbindelse med boligadministration. Retningslinjerne gælder uanset om behandlingen af Personoplysninger sker på arbejdspladsen, i hjemmet eller andetsteds. Der henvises i øvrigt til Sundby-Hvorup Boligselskabs IT leverandør EG samt ISAE 3000-erklæring.

2. DEFINITIONER

2.1 Ved ”Personoplysninger” forstås i disse retningslinjer 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 Boligorganisationens eller det af Boligorganisationen 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, fx indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

2.4 Ved "Sletning" af Personoplysninger forstås, at de omhandlede Personoplysninger uigenkaldeligt fjernes fra alle de lagringsmedier, hvorpå 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 Boligorganisationen er som udgangspunkt dataansvarlig for de Personoplysninger, som behandles om bl.a. medarbejdere, beboere og personer på venteliste i Boligorganisationens It-systemer.

3.2 Sundby-Hvorup Boligselskabs direktør har det interne ansvar for Boligorganisationens it-sikkerhed. Direktøren sikrer, at der kommunikeres it-sikkerhedsmæssige retningslinjer ud til medarbejdere, samarbejdspartnere samt øvrige personer, der er involveret i anvendelsen af Personoplysninger hos Boligorganisationen.

3.3 Boligorganisationens medarbejdere må alene handle indenfor den stillingsfuldmagt de besidder i form af deres ansættelsesforhold hos Boligorganisationen.

3.4 Den enkelte medarbejder/bruger er ansvarlig for at sikre, at nærværende 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 (fx 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 Boligorganisationen.

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 Administrationen er aflåst uden for alm. arbejdstid. Dokumenter indeholdende personoplysninger opbevares primært elektronisk, men i de tilfælde de forligger fysisk opbevares disse utilgængeligt i skabe/skuffer eller separate rum, således lejere, kunder eller andre uvedkommende ikke kan tilgå disse.

5.1.3 Varmemesterkontorerne er aflåst uden for kontortiden. Det er kun medarbejdere i det enkelte team, som har nøgle til kontoret. Der foreligger kun alm. personoplysninger på varmemester kontorerne, og disse opbevares utilgængelig i skabe/skuffer eller separate rum, således lejere, kunder eller andre uvedkommende ikke kan tilgå disse.

Alle medarbejderoplysninger, som ikke forefindes elektronisk, opbevares aflåst.

5.2 Serverrum

5.2.1 Der henvises til EG, da Sundby-Hvorup Boligselskabs IT-løsning hostes af denne IT leverandør.

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. autorisationsordningen.

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. Denne vurdering foretages af nærmeste leder. Konkret vil den pågældende bruger modtage et skema, hvoraf det fremgår hvilke programmer, drev, mapper og systemer denne har adgang til, herunder også behandlingsformål.

6.4 For brugere, som ikke længere har behov for de autorisationer, de har fået udstedt, inddrages autorisationerne. Det gælder fx 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 af sådanne autorisationer og for inddragelse heraf, herunder også retningslinjer for udstedelse af autorisationer, der kun behøver at være midlertidige.

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

6.7 En gang halvårligt foretager HR 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 Der henvises til EG, Sundby-Hvorup Boligselskabs IT leverandør, herunder EG's ISAE 3000-erklæring. Sundby-Hvorup Boligselskab opererer via en fjernskrivebordsløsning.

8. FIREWALL

8.1 Der henvises til EG, Sundby-Hvorup Boligselskabs IT leverandør, herunder EG's ISAE 3000-erklæring. Sundby-Hvorup Boligselskab opererer via en fjernskrivebordsløsning.

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 Du skal behandle dit password efter følgende regler:

- Passwordet skal have en længde på mindst 8 tegn
- Du skal skifte password med jævne mellemrum – mindst hver 3. måned
- 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

9.3 Du må ikke gøre følgende, når du opretter et password:

- Bruge brugernavnet eller dele heraf
- Bruge dit eget navn eller dele heraf
- Anvende ord stavet bagfra som password
- Anvende numre der kan identificeres med dig (fx din fødselsdag)
- Anvende logiske tastekombinationer (fx ”qwerty” eller ”asdfgh”)

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

9.5 Hvis du frygter, at dit password er blevet afluret skal du straks kontakte din nærmeste leder, samt kontakte EG med henblik på, at få et nyt password.

9.6 Dit password 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 Boligorganisationens systemer, til private tjenester.

10. E-MAILS

10.1 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.

11. BÆRBARE DATAMEDIER

11.1 USB-nøgle eller lignende bærbare medie, skal beskyttes. Der kan fx bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.

12. PRINTNING MV.

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

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

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

12.4 Sundby-Hvorup Boligselskab har sat SafeQ på deres hovedprintere, så maskinen ikke printer før den gældende medarbejder lægger en brik på maskinen og står ved maskinen. Store opgaver til omdeling kan dog printes uden at bruge en brik.

13. SLETNING

13.1 Personoplysninger, der behandles for varetagelsen af Boligorganisationens 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 Boligorganisationens slettepolitik, hvori de nærmere fastsatte sletteprocedurer er oplistet. Sletningspolitikken, kan findes på vores hjemmeside.

14. REPARATION OG SERVICE

14.1 Generelt

14.1.1 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.

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

14.2 Reparation og service

14.2.1 Ved reparation og service af udstyr fjernes eventuelle Personoplysninger i videst muligt omfang fra udstyret. Herudover er reparations- og servicepersonalet pålagt, at oplysninger, som de måtte blive bekendt med under deres arbejde, skal behandles som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes.

Hvis der benyttes eksternt personale til reparations- og serviceopgaver, har disse underskrevet en erklæring om tavshedspligt.

14.3 Kassation

14.3.1 Ved kassation af udstyr, som indeholder Personoplysninger, destrueres udstyret, så der ikke er mulighed for at læse indholdet. Dette sker konkret ved destruering af harddisk.

15. HJEMMEARBEJDSPLADSER MV.

15.1 Generelt

15.1.1 Ved hjemmearbejdsplads forstås en arbejdsplads, som etableres ved adgang til Boligorganisationens It-systemer fra andre steder end arbejdspladsen (fx fra hjemmet), således at medarbejderen kan udføre visse arbejdsopgaver uden at skulle give fysisk møde på arbejdspladsen.

15.1.2 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.

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

15.2 Lokal lagring af oplysninger

15.2.1 Alle Personoplysninger, der behandles elektronisk, og som er nødvendig for varetagelse af Boligorganisationens opgaver, skal lagres i Boligorganisationens centrale It-systemer.

15.2.2 Personoplysninger kan undtagelsesvist lagres på ”skrivebordet” og lokale drev mv., så længe der er tale om dokumenter eller lignende under udarbejdelse, og hvori 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 Boligorganisationens centrale It-systemer og slettes fra ”skrivebordet” og lokale drev mv.

15.3 Lokal udskrivning af oplysninger

15.3.1 Der må som udgangspunkt ikke udskrives dokumenter mv. indeholdende Personoplysninger fra hjemme-printer mv.

15.3.2 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.

15.4 Øvrige forhold

15.4.1 De øvrige punkter i nærværende retningslinjer gælder også ved behandling af Personoplysninger og brug af It-systemer i forbindelse med hjemmearbejdspladser mv.

16. DATABEHANDLERE

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

17. SIKKERHEDSBRUD

17.1 Ethvert Sikkerhedsbrud skal håndteres i overensstemmelse med Boligorganisationens retningslinjer for håndtering af sikkerhedsbrud, der er tilgængelige på Sundby-Hvorup Boligselskabs hjemmeside, samt ved henvendelse til Sundby-Hvorup Boligselskabs direktør.

18. TILSIDESÆTTELSE AF RETNINGSLINJERNE

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

19. DIVERSE

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

19.2 Er der spørgsmål til indholdet, kan der rettes henvendelse til Sundby-Hvorup Boligselskab på telefon-nummer: 98173066

19.3 Der er politik for datasikkerhed ved personaleadministration, der er tilgængelig på vores hjemmeside.