POLITIK FOR DATASIKKERHED VED BOLIGSELSKABET SCT. JØRGEN

INDLEDNING

I forbindelse med boligadministration skal sikkerhedsbestemmelserne i forordning nr. 2016/679 om beskyttelse af personoplysninger (herefter "databeskyttelsesforordningen") iagttages. Det indebærer bl.a., at Boligselskabet Sct. Jørgen som den dataansvarlige virksomhed, skal leve op til kravene om datasikkerhed.

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.

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.

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.

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.

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. [

DEFINITIONER

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.

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.

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.

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.

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.

ANSVAR

Boligorganisationen er som udgangspunkt dataansvarlig for de Personoplysninger, som behandles om bl.a. medarbejdere, beboere og personer på venteliste i Boligorganisationens It-systemer.

IT-afdelingen ved BDK (Boligkontoret Danmark har det interne ansvar for Boligorganisationens it-sikkerhed. It-afdelingen sikrer, at der kommunikeres it-sikkerhedsmæssige retningslinjer ud til medarbejdere, samarbejdspartnere samt øvrige personer, der er involveret i anvendelsen af Personoplysninger hos Boligorganisationen.

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

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

GENERELLE PRINCIPPER

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.

Ovennævnte grundlæggende principper gælder for al behandling af Personoplysninger, som foretages af Boligorganisationen.

FYSISK SIKRING

Generelt

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.

Der er alarm ved Boligselskabets yderdør, som kun medarbejdere har adgang til. Derudover er der sat en ekstra alarm ved døren til udlejningen, og til første salen som rummer økonomi, drift, kommunikation og byg.

Der er ikke separat serverrum ved Boligselskabet Sct. Jørgen, i det serverkapaciteten er placeret ved BDK.

Udstyr

It-udstyr, som indeholder Personoplysninger, skal opbevares i sikrede lokaler (med lås og alarm)
Bærbare pc'er, mobiltelefoner, tablets og andre datamedier/mobilt it-udstyr må ikke efterlades uden overvågning på steder, hvor ikke-autoriseret personale har adgang.

Det er vigtigt at medarbejdere låser sin PC når man midlertidigt forlader denne for at gå til møder, frokost eller lignende.

AUTORISATIONSORDNING

Der gives alene adgang til It-systemer med Personoplysninger for medarbejdere, som direkte er autoriserede hertil, jf. autorisationsordningen.

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.

- Ved vurderingen af, hvilke medarbejdere der autoriseres, lægges der vægt på, hvad den enkelte bruger har behov for at være autoriseret til.
-
- 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.

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.

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

En gang halvårligt foretager den nærmeste leder 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.

VIRUSBESKYTTELSE MV.

Boligselskabet Sct. Jørgen anvende de antivirusprogrammer, som databehandeler BDK tildeler os og er ansvarlige for

FIREWALL

Boligselskabet Sct. Jørgen har indgået serviceaftale med Netdesign som står for vedligeholdelse og opdatering af firewall.

PASSWORDPOLITIK

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.

Hos Boligselskabet Sct. Jørgen er passwords genereret og tildelt af Boligkontoret Danmarks IT-afdeling. Medarbejdernes password er på 8 tegn, og medarbejderne kan ikke selv ændre passwords

I forbindelse med BO Viborg er passwordpolitikken følgende:

- 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

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

- Bruge brugernavnet eller dele heraf
- Bruge dit eget navn eller dele heraf

- Bruge din familie, dine venners eller din kæledyrs navne
- Anvende ord stavet bagfra som password
- Anvende ord med tal foran eller bagved som password
- Anvende numre der kan identificeres med dig (fx din fødselsdag)
- Anvende logiske tastekombinationer (fx ”qwerty” eller ”asdfgh”)

Hvis du frygter, at dit password er blevet afluret skal du straks ændre denne.

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.

E-MAILS

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 i form af anvendelse af hovedpostkassen. Det er vigtigt at man ikke besvarer mails uden at slette persondata fra en ikke sikker mail.

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.

BÆRBARE DATAMEDIER

Personoplysninger, må ikke lagres på en USB-nøgle eller lignende bærbart medie.

PRINTNING MV.

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

Udprintet materiale skal makuleres, når det ikke længere benyttes.

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

SLETNING

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 www.bsjviborg.dk

REPERATION OG SERVICE

Generelt

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.

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

Reparation og Service
Reparation og service foretages internt af IT-afdelingen hos Boligkontoret Danmark.

Kassation
Boligselskabet Sct. Jørgen sørger selv for at destruere IT udstyr der indeholder persondata.

Salg
Boligselskabet Sct. Jørgen sælger ikke udstyr der indeholder persondata

HJEMMEARBEJDSPLADSER MV.

Generelt

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.

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.

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

Lokal lagring af oplysninger

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

Personoplysninger må kun lagres på citrixdrev." Lokal udskrivning af oplysninger

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

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.

Øvrige forhold

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

DATABEHANDLERE

Ved brug af en ekstern databehandler til håndtering af oplysninger, skal databeskyttelsesforordningens artikel 28 om skriftlig databehandleraftale mv. følges. Vi indgår databehandleraftaler på de relevante områder, hvor data videregives.

SIKKERHEDSBRUD

Ethvert Sikkerhedsbrud skal håndteres i overensstemmelse med Boligorganisationens retningslinjer for håndtering af sikkerhedsbrud, der er tilgængelige på www.bsjviborg.dk

TILSIDESÆTTELSE AF RETNINGSLINJERNE

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

DIVERSE

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

Er der spørgsmål til indholdet, kan der rettes henvendelse til Tilde Gotfredsen på tigo@bsjviborg.dk

Der politik for datasikkerhed ved personaleadministration, der er tilgængelig her: bsjviborg.dk

Version 1, maj måned 2018