OVERORDNEDE RETNINGSLINJER FOR SIKKERHED VED BEHANDLING AF PERSONOPLYSNINGER MV.

INDHOLD

1. Indledning

1.1 Denne politik indeholder Boligforeningen Ungdomsbos overordnede sikkerhedsmæssige retningslinjer for brug af Boligforeningen Ungdomsbos behandling af personoplysninger, herunder ved brug af it-systemer. Retningslinjerne gælder på arbejdspladsen, i hjemmet eller andetsteds. Retningslinjerne suppleres i Boligforeningen Ungdomsbos it-sikkerhedspolitik.

1.2 Ved "personoplysninger" forstås i disse retningslinjer enhver form for information om en identificeret eller identificerbar fysisk person, jf. persondatalovens § 3, nr. 1, herunder information om medarbejdere, lejere og personer på venteliste.

1.3 Ved "it-systemer" eller "it-systemet" forstås i disse retningslinjer Boligforeningen Ungdomsbos eller det af Boligforeningen Ungdomsbos 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. Ansvar

2.1 Boligforeningen Ungdomsbo er som udgangspunkt dataansvarlig for de personoplysninger, som behandles om bl.a. medarbejdere, lejere og personer på venteliste i Ungdomsbos it-systemer.

2.2 IT-administrator er ansvarlig for Boligforeningen Ungdomsbos it-sikkerhed. IT-administrator sikrer, at der kommunikeres it-sikkerhedsmæssige retningslinjer ud til medarbejdere, samarbejdspartnere samt øvrige personer, der er involveret i anvendelsen af personoplysninger hos Boligforeningen Ungdomsbo.

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

3. Fysisk sikring

3.1 Generelt

3.1.1 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.

3.1.2 Hvilke tiltag der er gjort i de forskellige lokaler mv., hvor der behandles personoplysninger]

3.2 Serverrum
Boligforening Ungdomsbo har ingen serverrum.

3.2.1 Serverrum og lignende områder, hvor der opbevares udstyr indeholdende personoplysninger, skal holdes aflåst og beskyttes med passende adgangskontrolsystem. Kun medarbejdere med rutinemæssige arbejdsopgaver må autoriseres med permanent adgang til serverrum og lignende sikrede områder. Se punkt 3.2

3.2.2 Der opbevares ikke data på egne servere. Boligforeningen Ungdomsbo har en hostingaftale hos Mentor IT CVR 25576861.

3.3 Udstyr

3.3.1 It-udstyr, som indeholder personoplysninger, skal opbevares i sikrede lokaler, jf. pkt. 3.1 og 3.2 ovenfor.

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

3.3.3 Der henvises i øvrigt til pkt. 9 nedenfor.

4. Autorisationsordning

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

4.2 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.

4.3 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 bruger modtage en mail, hvori det nærmere beskrives, hvilke oplysninger brugeren herved autoriseres (godkendes) til at anvende.

4.4 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.

4.4.1 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.

4.5 Ved nyansættelser og interne rokereringer vurderer IT-administrator – baseret på ovenstående retningslinjer – om de organisatoriske ændringer tillige giver anledning til ændrede adgangsrettigheder.

4.6 En gang halvårligt foretager IT-administrator 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.

5. Virusbeskyttelse mv.

5.1 Se punkt 3.2.2. Det er vores leverandør Mentor-IT CVR 25576861, der som databehandler varetager vedligehold af vores terminalløsning på vores vegne, hvor persondata opbevares.

6. Firewall

6.1 Se punkt 3.2.2. Det er vores leverandør Mentor-IT CVR 25576861, der som databehandler varetager vedligehold af vores netværk/firewall på vores vegne, hvor persondata opbevares bagved. De overvåger/monitere vores firewall / netværk. Der er taget stilling til, at nødvendig trafik har adgang gennem vores firewalls.

7. Passwordpolitik

7.1 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.

7.2 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

7.3 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”)

7.4 Hvis du har indtastet forkert password [3] gange, låses din konto, og du skal kontakte IT-administrator for at få den åbnet igen.

7.5 Hvis du frygter, at dit password er blevet afluret skal du straks kontakte IT-ansvarlig.

7.6 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 Boligforeningen Ungdomsbos systemer, til private tjenester.

8. E-mails

8.1 Datatilsynet anbefaler, at hvis følsomme personaleoplysninger og personnumre sendes med e-mail via internettet, skal der ske kryptering. Boligforeningen Ungdomsbo følger Datatilsynets anbefaling. Dette indebærer, at vi alene sender fortrolige og/eller følsomme oplysninger pr. e-mail, hvis korrespondancen er krypteret. I praksis sker dette ved anvendelse af sikker mail i form af [kort beskrivelse af teknisk løsning, fx e-boks].

8.2 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.):

- Personnummer, samt
- Helbredsoplysninger (herunder oplysninger om handicap),
- Oplysninger om strafbare forhold, eller
- Andre følsomme oplysninger omfattet af persondatalovens §§ 7 og 8.

8.3 [Der henvises i øvrigt til it-sikkerhedspolitikken [andet], hvor der findes en nærmere beskrivelse af benyttelsen af e-mails mv.]

9. Bærbare datamedier

9.1 Personoplysninger, der lagres på en USB-nøgle eller lignende bærbart 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.

9.2 [Hos Boligforeningen Ungdomsbo er alle USB-nøgler og andre bærbare datamedier forsynet med adgangskode og beskyttet af kryptering, således at udstyret ikke kan bruges af andre end den autoriserede bruger.]

[Hertil kommer, at alle USB-nøgler og andre bærbare datamedier indeholdende personoplysninger uden for arbejdstid opbevares i et aflåst skab. Det relevante personale har fået udlevet nøgler hertil. Det samme gælder inden for arbejdstiden, hvis det nævnte udstyr ikke er under opsyn.]

9.3 Der henvises til [it-politikkens punkt [**]] [andet], hvor der findes en nærmere beskrivelse af anvendelse af bærbare datamedier mv.

10. Printning mv.

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

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

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

11. Sletning

11.1 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.

11.2 Personoplysninger, der behandles for varetagelsen af Boligforeningen Ungdomsbos opgaver, slettes når behandlingen af personoplysningerne ikke længere er nødvendig af hensyn til de formål, hvortil oplysningerne er indsamlet eller behandlet. Følgende generelle sletteprocedurer gælder for Boligforeningen Ungdomsbo:

11.2.1 Lejere og øvrige beboere

[Her fastsættes den generelle slettefrist for oplysninger om lejere mv. – det kan fx være 5 år efter lejemålets ophør]

11.2.2 Personer på venteliste

Personer på venteliste slettes 15 mdr efter deres status er ændres fra aktiv/bero til sletmarkeret.

11.2.3 Medarbejdere og pårørende

Boligforeningen Ungdomsbo følger regnskabslovens opbevaringskrav og sletter personaledata herefter. Kontaktinfo på pårørende slettes ved fratrædelse.

Medarbejdere der er gået på efterløn/pension efter ansættelse i Boligforeningen Ungdomsbo, opbevares kontaktinfo til brug for invitation til sociale arrangementer. Fravælger den tidligere medarbejder deltagelse i sociale arrangementer slettes kontaktinfo.

11.2.4 Ansøgere til stillinger

Ansøgninger fra jobsøgende slettes 3 mdr. efter ansættelsesdatoen.

11.3 Uanset ovenstående generelle sletteprocedurer kan personoplysninger konkret slettes efter kortere eller længere tidsrum, hvis dette er nødvendigt. Vurderingen af, om der skal ske sletning efter kortere eller længere tid end de generelle sletteprocedurer, afhænger af de konkrete omstændigheder i den enkelte situation. Fx kan en indsigelse give anledning til, at der slettes efter kortere tid, hvorimod behandling af en tvist mv. kan begrunde, at oplysningerne i det konkrete tilfælde opbevares i et længere tidsrum, end de generelle slettefrister tilsiger.

12. Reparation og service

12.1 Generelt

12.1.1 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.

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

12.2 Reparation og service

12.2.1 [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.]

12.2.2 Der henvises til [it-sikkerhedspolitikkens punkt [**]] [andet], hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med reparation og service af udstyr.

12.3 Kassation

12.3.1 [Ved kassation af udstyr, som indeholder personoplysninger, destrueres udstyret, så der ikke er mulighed for at læse indholdet. Dette sker konkret ved overskrivning af de

relevante datamedier under anvendelse af et specialprogram, som overskriver data flere gange i overensstemmelse med en anerkendt specifikation (fx DOD 5220.22-M).]

12.3.2 Der henvises til [it-sikkerhedspolitikkens punkt [**]] [andet], hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med kassation af udstyr.

12.4 Salg

12.4.1 [I det omfang vi vælger at sælge udstyr, der har været benyttet til lagring af personoplysninger, vil der forinden ske effektiv sletning. Dette sker konkret ved overskrivning af de relevante datamedier under anvendelse af et specialprogram, som overskriver data flere gange i overensstemmelse med en anerkendt specifikation (fx DOD 5220.22-M).]

12.4.2 Der henvises til [it-sikkerhedspolitikkens punkt [**]] [andet], hvor der findes en nærmere beskrivelse af vores forholdsregler i forbindelse med salg af brugt udstyr.

13. Hjemmearbejdspladser

13.1 Generelt

13.1.1 Ved hjemmearbejdsplads forstås en arbejdsplads, som etableres ved adgang til Boligforeningen Ungdomsbos 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. Krav til hjemmearbejdspladser gælder også for andre fjernarbejdspladser, herunder ved adgang fra smartphones, tablets og lignende.

13.1.2 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

13.2 **Lokal lagring af oplysninger**

13.2.1 Alle personoplysninger, der behandles elektronisk, og som er nødvendig for varetagelse af Boligforeningen Ungdomsbos opgaver, skal lagres i Boligforeningen Ungdomsbos centrale it-systemer.

13.2.2 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 Boligforeningen Ungdombos centrale it-systemer og slettes fra "skrivebordet" og lokale drev mv.

13.3 **Lokal udskrivning af oplysninger**

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

13.3.2 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.

13.4 Øvrige forhold

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

14. Databehandlere

14.1 Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges.

14.2 Hos Mentor IT CVR 25576861 og EG CVR 84667811 benyttes følgende databehandlere, der har adgang til eller behandler personaleoplysninger på vegne af os:

14.2.1 Ekstern : It-leverandør : EG CVR 84667811 – software ”EG Bolig” og Mentor IT CVR 25576861 Hardware

14.2.2 Hosting : Mentor IT CVR 25576861

14.2.3 Andre: Brunata CVR 22166514, Dansk Kabel TV CVR 17981684 og Nordby Fjernvarme CVR 16934690

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

15. Tilsidesættelse af retningslinjerne

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