Procedurebeskrivelse (Fortegnelse)

1. Navn og kontaktoplysninger.

Rent Herning (”**Virksomheden**”) er dataansvarlig, og dette dokument indeholder en fortegnelse over alle kategorier af behandlingsaktiviteter, som udøves under Virksomhedens ansvar.

2. Formål med behandling.

Virksomheden behandler personoplysninger med henblik på: At kunne udleje beboelses- og/eller erhvervslejemål og indkøbe for Virksomheden nødvendige materialer og serviceydelser fra leverandører.

3. Kategorier af registrerede personer.

Der behandles oplysninger om følgende kategorier af registrerede personer:

1. Jobansøgere
2. Ansatte
3. Tidligere ansatte
4. Pårørende til ansatte
5. Leverandører
6. Lejere
7. Potentielle lejere (ventelister)
8. Partsrepræsentanter

4. Kategorier af personoplysninger.

Følgende kategorier af almindelige personoplysninger indgår i den specifikke behandling af de registrerede personer:

1. Identifikationsoplysninger – Lejere (Herunder: navn, alder, mailadresse, telefonnummer, antal familiemedlemmer, i visse tilfælde helbredsoplysninger (eksempelvis handicaps)

2. Identifikationsoplysninger – Leverandører og leverandøremner (Eksempelvis navn, mailadresse, arbejdstelefonnummer, stillingsbetegnelse, arbejdsadresse og IP-adresse)
3. Oplysninger til brug for administration af løbende lejeforhold (Herunder: kontonummer, personnummer, oplysninger om antal familiemedlemmer og pårørende – til underretning i tilfælde af ulykke/sygdom)
4. Oplysninger til brug for vurdering af potentielle lejere (Herunder: kontaktoplysninger og oplysninger om antal familiemedlemmer samt eventuelt relevante helbredsoplysninger (eksempelvis om handicaps)
5. Oplysninger vedrørende ansættelsesforhold til brug for administration – medarbejdere (Herunder: identifikationsoplysninger, alder, personnummer, ægteskabelig status, arbejdsområde, tjenestested, lønforhold, pensionsoplysninger, forsikringsoplysninger vedrørende sundhedsforsikring, A-kasse, oplysninger af relevans for indeholdelse i løn – herunder skatteoplysninger, personalepapirer, uddannelse, eksamensbevis, pårørende – til underretning i tilfælde af ulykke/sygdom, CV, udtalelser fra tidligere arbejdsgivere)
6. Oplysninger til brug for vurdering af jobansøgere (Herunder: identifikationsoplysninger, nuværende og tidligere stillinger, uddannelse, eksamensbevis, CV, personlighedstest)

Følgende kategorier af følsomme personoplysninger indgår i den specifikke behandling af de registrerede personer:

1. Oplysninger vedrørende ansættelsesforhold til brug for administration – medarbejdere (Eksempelvis sygefravær, fagforeningsmæssigt tilhørsforhold, straffeattest, personlighedstest)
2. Oplysninger til brug for administration af løbende lejeforhold – helbredsoplysninger nødvendige og relevante for indretning af lejemålet
3. Oplysninger til brug for vurdering af potentielle lejere – helbredsoplysninger nødvendige og relevante for indretning af lejemålet

Virksomheden indsamler og behandler *ikke* følgende kategorier af følsomme personoplysninger: Race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, oplysninger om genetisk data (såsom DNA), oplysninger om biometrisk data (såsom fingeraftryk), seksuelle forhold og seksuel orientering.

Virksomheden indsamler eller behandler ikke oplysninger om strafbare forhold.

5. Modtagere af personoplysninger i tredjelande eller internationale organisationer.

Virksomheden overfører ikke personoplysninger til databehandlere i tredjelande uden for EU eller til internationale organisationer.

6. Sletning af oplysninger.

Virksomheden sletter/returnerer personoplysninger efter følgende regler:[1]

1. Oplysning om lejere slettes som udgangspunkt 10 år efter ophør af lejeforholdet, jf. sikring af mulighed for at kunne forsvare retsstilling i forhold til regulering af leje.
2. Ansøgning fra potentielle lejere slettes samtidig med afslag til ansøgeren.
3. Potentielle lejere kan efter ønske fra lejeren blive omfattet af en venteliste. Medmindre andet aftales slettes information om den registrerede på ventelisten efter 2 år.
4. Identifikationsoplysninger og oplysninger om lønforhold mv. (som indgår i virksomhedens regnskabsmateriale) om tidligere ansatte slettes senest 5 år fra udgangen af det regnskabsår, hvor ansættelsesforholdet ophørte, jf. bogføringsloven.
5. Oplysninger om tidligere ansatte, som ikke indgår i virksomhedens regnskabsmateriale, slettes senest 5 år efter ansættelsesforholdets ophør. Fristen for sletning er begrundet

i, at risikoen for erstatningskrav fra den ansatte mod virksomheden ophører efter 5 år, jf. forældelsesloven.

6. Oplysninger om jobansøgere til opslåede stillinger slettes 3 måneder efter, at den opslåede stilling er blevet besat. Fristen for sletning er begrundet i, at nyansatte har en prøveperiode på 3 måneder, hvor ansættelsesforholdet gensidigt kan opsiges med 14 dages varsel.
7. Oplysninger indeholdt i uopfordrede jobansøgninger slettes samtidig med afslag til ansøgeren.
8. Såfremt Virksomheden ønsker at gemme en ansøgning fra en potentiel medarbejder indhentes samtykke til opbevaring for ansøgeren. Ansøgning mv. slettes senest 6 måneder efter samtykket er givet.
9. Dokumentation for udgifter afholdt i forbindelse med modernisering mv., som er relevant for fastsættelse af lejestørrelse, slettes først på det tidspunkt, hvor de ikke længere er relevante i forhold til at forsvare eller opretholde udlejeres retsstilling desangående.

Samtlige ovennævnte frister for sletning kan konkret fraviges, såfremt der er en saglig begrundelse herfor, herunder eksempelvis verserende retssag mod den registrerede.

7. **Tekniske og organisatoriske sikkerhedsforanstaltninger.**

Ved blandt andet design og databeskyttelse gennem standardindstillinger træffer Virksomheden de fornødne tekniske og organisatoriske foranstaltninger, som måtte være nødvendige for at sikre, at personoplysningerne ikke hændeligt eller ulovligt tilintetgøres, offentliggøres, bliver brugt til andet end formålet, fortabes, ændres eller bliver misbrugt af uvedkommende mv. Til sikring af foranstående fortager Virksomheden følgende tekniske og organisatoriske foranstaltninger:[2]

1. Etablerer og vedligeholder log-in og adgangskodeprocedure til it-systemer, herunder servere, samt opsætter en firewall og antivirussoftware mv. til sikring af vedvarende fortrolighed, integritet og robusthed af it-systemerne.

2. Der anvendes personlige koder for at få adgang til pc'ere og smartphones. Koder ændres mindst én gang hvert halve år.
3. Tilrettelægger pseudonymisering og/eller kryptering af personoplysningerne.
4. Sikrer at eventuelle papirformater mv. indeholdende personoplysninger behandles og opbevares efter samme regler som gældende for elektroniske formater samt sikkerhedsmakuleres og –destrueres.
5. Etablerer sikring af bygninger hvori hardware er placeret samt anvender opdateret hardware af høj kvalitet
6. Tilrettelægger tekniske og organisatoriske foranstaltninger til sikring af, at alene medarbejdere/ejere med saglige arbejdsrelaterede formål har adgang til personoplysningerne, og at medarbejdere/ejere er bekendte og ajourførte med de etablerede sikkerhedsforanstaltninger og relevante regler for behandling af personoplysningerne.
7. Sikrer at de medarbejdere/ejere, der er autoriseret til at behandler personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt lovbestemt tavshedspligt.
8. Sikrer procedurer til genoprettelse af tilgængeligheden af og adgang til personoplysningerne i tilfælde af en fysisk eller teknisk utilsigtet hændelse.
9. Etablerer en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de i pkt.

8. **Brud på persondatasikkerheden.**

Ved brud på persondatasikkerheden forstås et brud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er behandlet. Ved alle brud vil der manuelt blive forsøgt begrænsning af skaden og genoprettelse hurtigst muligt.

Såfremt et brud medfører en risiko for fysiske personers rettigheder og frihedsrettigheder – hvilket blandt andet omfatter risiko for diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den

registrerede – sker der anmeldelse til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer efter, at man er blevet bekendt med bruddet.

Ved risikovurderingen vil følgende momenter blive inddraget:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse
- Oplysningernes art og omfang
- Risikoen for at registrerede kan identificeres
- Konsekvenser bruddet kan have for de registrerede
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte)
- Antallet af berørte fysiske personer

Anmeldelse vil blive foretaget af kontaktpersonen, jf. pkt. Casper Søndergaard - l casper@rentherning.dk

Hvis et brud indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, vil de berørte registrerede uden unødig forsinkelse blive direkte underrettet om bruddet. Underretning vil ske via e-mail, brev, sms eller lignende.

Hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, foretages der ikke anmeldelse til Datatilsynet eller den registrerede.

Ved brud, der skal anmeldes, sker indberetning til myndighederne via Datatilsynets digitale indberetningsløsning på virk.dk.

Uanset om et brud anmeldes eller ej, vil virksomheden i tilfælde af brud udarbejde en skriftlig redegørelse for bruddet, som minimum vil indeholde følgende punkter:

- Dato og tidspunkt for bruddet
- Hvad skete der i forbindelse med bruddet?
- Hvad er årsagen til bruddet?
- Hvilke (typer) personoplysninger er omfattet af bruddet?
- Hvilke konsekvenser har bruddet for de berørte personer?
- Hvilke afhjælpende foranstaltninger er truffet?
- Hvorvidt der er sket anmeldelse til Datatilsynet eller ej?

9. **Konsekvensanalyse.**

En dataansvarlig skal foretage en konsekvensanalyse, hvis en type behandling – navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål – sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

En konsekvensanalyse er navnlig påkrævet, hvis 1) der sker en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, 2) der behandles følsomme oplysninger i stort omfang, eller 3) der sker systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Virksomheden har vurderet, at virksomhedens behandling af personoplysninger ikke medfører behov for at foretage en konsekvensanalyse.

10. **Øvrige oplysninger.**

Denne fortegnelse foreligger såvel skriftligt som elektronisk.