RETNINGSLINJER FOR HÅNDTERING AF SIKKERHEDSBRUD VEDRØRENDE PERSONOPLYSNINGER

1 INDLEDNING

1.1 Disse retningslinjer vedrører UBSBOLIG A/S' (herefter "Virksomheden") håndtering af sikkerhedsbrud. Under punkt 2-3 defineres, hvad et sikkerhedsbrud er. Derefter følger vores konkrete retningslinjer for håndtering af sikkerhedsbrud under punkt 4-8.

1.2 Hos Virksomheden er den Persondataansvarlige (herefter PDA'en) ansvarlig for vores håndtering af sikkerhedsbrud. Når et sikkerhedsbrud eller risikoen for dette opdages, skal PDA'en derfor straks orienteres herom.

1.3 Spørgsmål til disse retningslinjer skal rettes til PDA'en.

1.4 PDA'ens kontaktoplysninger kan på ethvert tidspunkt findes på hjemmesiden.

2 GENERELT OM SIKKERHEDSBRUD

2.1 Virksomheden har en generel pligt til at behandle personoplysninger 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, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (i lovgivningen benævnt som "integritet og fortrolighed"). Vi er endvidere forpligtede til at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, vi har identificeret, og for bl.a. at undgå brud på persondatasikkerheden.

2.2 Et sikkerhedsbrud defineres som "*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*" (herefter "Sikkerhedsbrud" eller "Sikkerhedsbruddet").

2.3 I Virksomheden kan et Sikkerhedsbrud indebære, at der sker uautoriseret eller ulovlig behandling samt tab, tilintetgørelse eller beskadigelse mv. af personoplysninger som vi behandler for fysiske personer, der direkte eller indirekte kan identificeres.

2.4 Hos Virksomheden behandles der personoplysninger i en række forskellige situationer. Dette drejer sig bl.a.:

i) jobansøgere,

ii) medarbejdere,

iii) tidligere medarbejdere,

iv) personer opnoteret på venteliste,

v) nuværende beboere,

vi) tidligere beboere,

vii) besøgende og andre ud over ovenstående, der optages via tv-overvågning,

viii) samt andre fysiske personer, der direkte eller indirekte kan identificeres.

ix) Leverandører for såvidt at de er registrerede som enkeltmandsfirmaer eller I/S'er

(samlet set benævnt "Registrerede").

3 KONSEKVENSER AF ET SIKKERHEDSBURD

3.1 Hos Virksomheden skelner vi mellem tre forskellige risikoscenarier i forhold til konsekvenser og sandsynlighed for den Registrerede ved et Sikkerhedsbrud. Den konkrete vurdering foretages af PDA'en. De forskellige risikoscenarier er:

i) Ingen eller en ubetydelig risiko

ii) Nogen risiko

iii) Høj risiko

3.2 Ved *ingen eller ubetydelig risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder for alle Sikkerhedsbrud i overensstemmelse med punkt 4.

3.3 Ved *risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder efter punkt 4 samt anmelde Sikkerhedsbruddet til Datatilsynet i overensstemmelse med punkt 5.

3.4 Ved *høj risiko* for den Registrerede skal vi dokumentere de faktiske omstændigheder efter punkt 4, anmelde Sikkerhedsbruddet til Datatilsynet efter punkt 5 samt underrette den Registrerede om Sikkerhedsbruddet i overensstemmelse med punkt 6.

3.5 Ved risikovurderingen i forbindelse med et Sikkerhedsbrud skal det derfor fastlægges, hvilket risikoscenarie, der konkret foreligger i forhold til den Registrerede. Dette afgøres hos Virksomheden på den ene side af de konsekvenser for den Registrerede, som et Sikkerhedsbrud kan indebære, samt på den anden side sandsynligheden for, at konsekvenserne indtræder.

3.6 Konsekvensen ved et Sikkerhedsbrud kan være:

1) Mindre betydningsfuld
2) Mindre alvorlig
3) Betydningsfuld (fx økonomisk tab eller tab af integritet, som kan genoprettes)
4) Alvorlig (fx økonomisk tab eller tab af integritet, der ikke kan genoprettes)
5) Meget alvorlig (tab, som ikke kan genoprettes, helbredsmæssige eller livstruende konsekvenser)

3.7 Sandsynligheden for at konsekvensen indtræder kan være:

1) Ikke sandsynlig
2) Mindre sandsynlig
3) Mere sandsynlig og ofte forekommende
4) Mere sandsynlig, ofte forekommende og har en lang varighed
5) Meget sandsynlig

3.8 De i punkt 3.6 og 3.7 angivne værdier benytter vi hos Virksomheden til at vurdere det konkrete risikoscenarie baseret på følgende formel:

Konsekvens x sandsynlighed = risikoværdi

3.9 Dette indebærer, at følgende risikoværdier udløser følgende risikoscenarie (jf. i øvrigt den som **bilag 1** vedhæftede risikomatrix):

Risikoværdi	**Risikoscenarie**	**Action**
1, 2, 3, 4, 6	Ingen eller ubetydelig risiko	Se punkt 4
5, 8, 9	Risiko	Se punkt 4 og 5
10, 12, 15, 16, 20, 25	Høj risiko	Se punkt 4, 5 og 6

3.10 Gennemførelsen af risikovurderingen vil basere sig på en konkret vurdering i det enkelte tilfælde. Nedenfor har vi opstillet en række eksempler på Sikkerhedsbrud. Det skal understreges, at nedenstående blot er eksempler, og ikke en facitliste, hvorfor der altid skal foretages en konkret risikovurdering af det enkelte Sikkerhedsbrud.

Eksempel	Konsekvens	Sandsynlighed	Risikoværdi
Virksomhedens it-system bliver hacket og alle medarbejderoplysninger lægges ud på internettet.	Konsekvensen kan være tab af integritet mv., idet der potentielt kan være tale om, at uvedkommende kan tilgå fortrolige og følsomme personoplysningerne (dvs. konsekvensværdien er 4).	Idet oplysningerne er offentligt tilgængelige, er det sandsynligt, at de tilgås af uvedkommende (dvs. sandsynlighedsværdien er 4)	Risikoværdien er 16 (4 x 4), hvorefter der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4, foretages anmeldelse til Datatilsynet, jf. punkt 5 og foretages underretning af de Registrerede, jf. punkt 6.
Ventelisten sendes på en mail til en forkert modtager. Mailen tilbagekaldes med det samme.	Konsekvensen kan være tab af integritet mv. Dog er der tale om almindelige oplysninger (fx navne) (dvs. konsekvensværdien er maksimalt 2).	Idet oplysningerne sendes til en forkert modtager, men tilbagekaldes med det samme, er det mindre sandsynligt, at uvedkommende tilgår oplysningerne (dvs. sandsynlighedsværdien er 2)	Risikoværdien er 4 (2 x 2), hvorefter der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4.
Oplysninger om alle beboere der modtager kommunal støtte sendes til en forkert kommune.	Konsekvensen kan være tab af integritet mv., idet der potentielt kan være tale om, at uvedkommende kan tilgå fortrolige oplysninger (dvs. konsekvensværdien er 3).	Idet oplysningerne alene sendes til en forkert kommune, er det mindre sandsynligt, at uvedkommende tilgår oplysningerne (dvs. sandsynlighedsværdien er 2)	Risikoværdien er 6 (3 x 2), hvorefter der skal føres dokumentation af Sikkerhedsbruddet, jf. punkt 4.

4 DOKUMENTATION AF SIKKERHEDSBRUD

4.1 Enhver medarbejder der opdager et Sikkerhedsbrud skal **straks** orientere PDA'en, som vil behandle Sikkerhedsbruddet. Dette gælder også, hvis der er tvivl om, hvorvidt der rent faktisk er tale om et Sikkerhedsbrud.

4.2 PDA'en kontakter herefter, hvis PDA'en skønner det nødvendigt, D&D-gruppen med henblik på at afdække omfanget af Sikkerhedsbruddet og eventuelt iværksætte yderligere undersøgelser, således, at vi kan begrænse skaden og påse, at personoplysningerne bliver slettet (fx fra internettet, herunder fra søgemaskiner) eller eventuelt afhentet eller returneret fra uberettigede modtagere.

4.3 For alle Sikkerhedsbrud dokumenterer PDA'en de faktiske omstændigheder i en elektronisk log, således at denne afspejler resultatet af undersøgelserne om Sikkerhedsbruddet. Loggen skal indeholde oplysninger om:

i) Hvem i Virksomheden, der har opdaget Sikkerhedsbruddet.

ii) Hvornår Sikkerhedsbruddet blev opdaget og hvornår hændelsen, der resulterede i Sikkerhedsbruddet faktisk skete.

iii) Hvilke Registrerede der er berørt af Sikkerhedsbruddet.

iv) Mulige konsekvenser forbundet med Sikkerhedsbruddet

v) Sandsynligheden af at de identificerede mulige konsekvenser af Sikkerhedsbruddet indtræder.

vi) Hvilke skridt der er foretaget for at forhindre Sikkerhedsbruddets gentagelse eller yderligere spredning.

vii) Om der er foretaget anmeldelse til Datatilsynet og underretning til den Registrerede, og hvornår dette er sket.

4.4 Når den samlede information om Sikkerhedsbruddet er indsamlet, foretager PDA'en en risikovurdering i overensstemmelse med punkt 3 og bilag 1 med henblik på at afdække, om der skal ske henholdsvis anmeldelse til Datatilsynet og underretning af den Registrerede i overensstemmelse med punkt 5 eller 6 nedenfor. Til brug for denne vurdering anvendes bilag 1, og kopi af hvordan bilag 1 er benyttet vedlægges loggen (fx indscannet med afkrydsning af det relevante risikoscenarie).

4.5 Ved sikkerhedsbrud konsulterer PDA'en eventuelle databehandleraftaler såfremt Virksomheden ikke selv er dataansvarlige med henblik på at orientere eventuelle dataansvarlige såfremt dette er påkrævet af en sådan aftale.

4.6 Den tekniske fremgangsmåde for identifikation, kontrol med Sikkerhedsbruddet, forhindring af yderligere spredning, sikring imod lignende fremtidige Sikkerhedsbrud, yderligere undersøgelser, etc. er nærmere beskrevet i vores Politik for brug af IT-systemer.

5 ANMELDELSE TIL DATATILSYNET

5.1 Ved et Sikkerhedsbrud skal der ske anmeldelse til Datatilsynet, medmindre det er usandsynligt, at Sikkerhedsbruddet indebærer en risiko for de Registrerede personers rettigheder. Anmeldelsen til Datatilsynet foretages af PDA'en.

5.2 Anmeldelse til Datatilsynet skal ske **inden for 72 timer** efter, at vi er blevet bekendt med Sikkerhedsbruddet. I særlige tilfælde, hvor vi ikke har mulighed for at overholde fristen på 72 timer, kræver dette en god begrundelse, som vi skal vi kunne forklare overfor Datatilsynet.

5.3 En anmeldelse af et Sikkerhedsbrud til Datatilsynet skal indeholde følgende informationer:

i) Beskrivelse af karakteren og kategorierne af personoplysningerne omfattet af sikkerhedsbruddet,

ii) det omtrentlige antal berørte Registrerede personer,

iii) det omtrentlige antal berørte personoplysninger,

i) angivelse af at Virksomheden er dataansvarlig, og at eventuelle spørgsmål eller andre henvendelser skal ske til PDA'en,

iv) de sandsynlige konsekvenser af Sikkerhedsbruddet,

v) og de foranstaltninger som vi har truffet eller foreslår truffet for at håndtere Sikkerhedsbruddet.

5.4 Hvis ikke vi har alle oplysninger til brug for ovenstående, skal vi i første omgang give de oplysninger, som vi har, og samtidig orientere Datatilsynet om, at vi løbende vil indlevere de manglende oplysninger relateret til anmeldelse af Sikkerhedsbruddet.

6 UNDERRETNING AF DEN REGISTRERede

6.1 Hvis et Sikkerhedsbrud medfører høj risiko for den Registrerede, skal denne underrettes om Sikkerhedsbruddet uden unødig forsinkelse. Underretningen af den Registrerede foretages af PDA'en.

6.2 Underretningen skal skrives i et let forståeligt sprog, og skal som minimum indeholde følgende informationer:

i) Angivelse af at Virksomheden er dataansvarlig, og at eventuelle spørgsmål eller andre henvendelser skal ske til PDA'en og kontaktoplysninger på denne,

ii) de sandsynlige konsekvenser af Sikkerhedsbruddet,

iii) og de foranstaltninger som vi har truffet eller foreslår truffet for at håndtere Sikkerhedsbruddet.

6.3 PDA'en vil dog vurdere om en af nedenstående undtagelser til underretningspligten er opfyldt:

(i) Vores implementerede sikkerhedsforanstaltninger har gjort, at de berørte personoplysninger er uforståelige for en tredjemand (fx fordi de er krypterede).

(ii) Vi har efterfølgende foretaget skridt, som gør, at der ikke længere er en reel risiko for den Registrerede (fx ved at en fil med personoplysning har været tilgængelig på internettet er slettet inden, at den er blevet åbnet af en tredjemand).

(iii) Det vil kræve en uforholdsmæssig stor indsats at underrette alle implicerede Registrerede, hvorfor vi i stedet kan underrette dem via en offentlig meddelelse (dette vil alene i meget sjældne tilfælde være relevante, da vi som udgangspunkt har alle kontaktoplysninger på de Registrerede).

(iv) Hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende private interesser, herunder forretningshemmeligheder, immaterielle rettigheder, kontraktforhold eller afgørende hensyn til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

6.4 Selv om PDA'en vurderer, at der ikke skal ske underretning af de Registrerede, kan Datatilsynet beslutte at dette skal ske.

7 HVEM ER FORPLIGTET?

7.1 Virksomheden er dataansvarlige i relation til behandlingen af personoplysninger, hvis disse afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af de omhandlede personoplysninger.

7.2 Virksomheden er derfor dataansvarlig for behandling af personoplysninger om Registrerede personer, hvilket indebærer, at vi skal overholde forpligtelserne ved et Sikkerhedsbrud vedrørende personoplysninger for denne personkreds.

7.3 Hvis vi benytter databehandlere til behandling af personoplysninger, har vi i de indgåede databehandleraftaler forpligtet den relevante databehandler til omgående at informere os om ethvert Sikkerhedsbrud. Databehandleren vil i sådanne tilfælde give os de oplysninger, som vi måtte have brug for til at foretage (i) risikovurderingen af Sikkerhedsbruddet, jf. punkt 3 og (ii) dokumentation, anmeldelse og/eller underretning af Sikkerhedsbruddet, jf. punkt 4-6.

8 RAPPORTERING

8.1 Ledelsen i Virksomheden skal orienteres, såfremt nærværende retningslinjerne ikke er overholdt, samt hvis der opstår forhold vedrørende disse retningslinjer, som har betydning for vurdering af Virksomhedens risikoprofil på persondataområdet.

9 TILSIDESÆTTSLE AF RETNINGSLINJER

9.1 Tilsidesættelse af de nævnte retningslinjer kan give anledning til ansættelsesretlige konsekvenser, herunder advarsel og i yderste fald opsigelse eller bortvisning.

10 AJOURFØRING

10.1 Ledelsen i Virksomheden er bemyndiget til at tage disse retningslinjer op til revision, når det vurderes relevant og minimum 1 gang årligt.

Revideret den 15.10.19

UBSBOLIG

BILAG 1: RISIKOMATRIX

Konsekvens → **Sandsynlighed ↓**	**1. Mindre betydningsfuld**	**2. Mindre alvorlig**	**3. Betydningsfuld**	**4. Alvorlig**	**5. Meget alvorlig**
5. Meget sandsyn-ligt	5	10	15	20	25
4. Sandsynligt, sker ofte og har længere varighed	4	8	12	16	20
3. Mere sandsyn-ligt/ sker ofte	3	6	9	12	15
2. Mindre sandsyn-ligt	2	4	6	8	10
1. Ikke sandsynligt	1	2	3	4	5