BILAG 2

DEAS' sikkerhedsniveau og foranstaltninger

DEAS' SIKKERHEDSNIVEAU

Behandlingen af personoplysninger i forbindelse med administration af foreninger indebærer behandling af mange Registrerede, men under kategorien almindelige personoplysninger, der ikke er omfattet af persondataforordningens art. 9 eller 10.

Det indebærer, at der alene gælder et almindeligt sikkerhedsniveau.

På denne baggrund har DEAS fastsat rammerne for de tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige og aftalemæssige sikkerhedsniveau for behandling af Personoplysningerne.

DEAS' FORANSTALTNINGER

DEAS har iværksat foranstaltninger inspireret af følgende kriterier i kontrolstandarderne ISO27001 og ISO27002:

Fortrolighed - omhandler beskyttelse af følsomme data fra uautoriseret offentliggørelse
Integritet – vedrører såvel nøjagtighed og fuldstændighed af data som gyldighed i forbindelse med forretningsværdier og forventninger.
Tilgængelighed – vedrører tilgængelighed af data og systemer, når det er krævet af forretningsprocesser nu og i fremtiden.

DEAS vil i alle tilfælde og som minimum gennemføre følgende foranstaltninger, som er omfattet af aftalen med Kunden på baggrund af gensidig risikovurdering:

Systemsikring
Til sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester har DEAS udarbejdet en IT-sikkerhedspolitik for håndtering af data generelt, og herunder for håndtering af persondata. Den IT-politik revideres minimum én gang årligt og godkendes af DEAS' direktion.

Datarestore
I tilfælde af en fysisk eller teknisk hændelse, der medfører tab af data genoprettes tilgængeligheden.

For funktionskritiske områder foretager DEAS restoretests på månedlig basis. Funktionskritiske områder er f.eks. vores administrationsplatforme med lejerdata. Dette er en del af kontrolkataloget, som auditeres af IT-revisionen.

Kontroller
DEAS gennemfører regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed ud fra følgende værdisæt og nøgleelementer:

Organisering – beskrivelse af ansvar og opgaver.
Risikostyring – afstemning af konsekvens/forventning i forhold til sandsynlighed for brud
Politik og procedurer – beskrivelse af tiltag og udførelse
Kontroller – manuelle og automatiske kontroller.

DEAS vil årligt få foretaget et ekstern ISAE 3402 type 2 erklæring til sikring af at DEAS IT har relevante og effektive IT-kontroller samt at DEAS efterlever disse.

DEAS benytter Deloitte til at foretage denne kontrol og afgive erklæring, som på opfordring kan eftersendes til Kunden.

Beskyttelse af data, hvor de transmitteres

I det tilfælde, hvor DEAS gør brug af underdatabehandlere fx cloud eller SAAS løsninger eller hvor DEAS gør brug af eksterne udviklingsleverandører hvortil der sker persondata udveksling imellem en underleverandør og DEAS, så sker det ved brug af en af følgende typer af eksterne dataforbindelser:

For asynkrone dataudvekslinger – fil deling
(Denne gælder for FindBolig.nu – dvs. eksternt udviklingsleverandør)

1. For automatiske udveksling af personlysninger omfattet af denne aftale anvendes krypteret filudveksling med certifikat (Secure FTP). Der filtreres yderligere på IP-adresser, således at alene på forhånd godkendte/whitelistede IP-adresser kan tilgå SFTP serveren.
2. Oplysningerne lagres i overensstemmelse med DEAS' IT-sikkerhedspolitik og beredskabsplan, hvorefter der foretages løbende backup af data på servere, der er opstillet udenfor DEAS' lokaliteter.
3. Adgang til personoplysninger er begrænset til de medarbejdere i DEAS, der er beskæftiget med tildeling af lejeboliger.

For synkrone dataudvekslinger – webservices
(Gælder for Cloud eller SAAS løsning som fx 24syv app, Microbizz, I-syn, …)
For data udveksling af personlysninger baseret på webservices anvendes krypteret SSL/HTTPS trafik

Data tilgængelighed begrænses og rettighedsstyres til personer og funktioner, der arbejdsmæssigt har behov for adgang til data.

DEAS datacenter er fysisk sikret med brandalarm, fugtsikring, røgkanon, inergenanlæg, UPS strømbeskyttelse og adgangskontrol. Adgang til datacenter er stærkt begrænset – og omfatter kun de enkelte medarbejdere, der reelt har behov for denne type adgang. Dette auditeres ligeledes årligt af IT-revisionen.

Hjemme-/fjernarbejdspladser
DEAS' medarbejdere og evt. eksterne konsulenter der arbejder remote for DEAS har adgang til at foretage databehandling fra hjemmearbejdspladser via web adgang.

Fjernarbejdspladser – sikkerhed:

1. Adgang til DEAS' IT-systemer fra medarbejdernes hjemmearbejdspladser er sikret ved anvendelse af "two factor authentication", der fordrer, at brugeren anvender og opfylder to godkendelseskriterier for at opnå adgang til IT-systemerne.
2. Medarbejderen skal genkendes via brugernavn og adgangskode samt et engangskodeord (token kode), der efter systemgodkendelse sendes via sms (SMS Passcode) til medarbejderens mobiltelefon.
3. Engangskodeordet kan kun anvendes på den session, der har initieret SMS Passcode. Dette forhindrer misbrug fra uvedkommende, der uretmæssigt måtte tilegne sig brugernavn, adgangskode og engangskodeordet.
4. Medarbejder har efter DEAS opkobling system- og databehandlingsadgang i henhold til deres AD profil og systemrettigheder på samme måde og niveau, som hvis de fysisk arbejdede fra en DEAS lokation

Krav vedrørende logning
DEAS foretager logning på vores data og processer som integreret del af vores applikationer, hvor dette er vurderet nødvendigt.

På systemkritiske områder foretager DEAS løbende gennemgang og vurdering af disse logs. Dette er desuden en del af kontrol kataloget, som auditeres årligt af IT-revisionen.

---oooOooo---

Opdateret oversigt over sikkerhedsniveau og foranstaltninger, der erstatter tidligere versioner af dette Bilag 2 udleveres til Kunden på dennes anmodning.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jørgen Michael Ørbech
Bestyrelsesformand
På vegne af: 108-234 E/F Universitetshaven VEST
Serienummer: PID:9208-2002-2-158389834892
IP: 82.147.226.9
2018-05-25 10:04:55Z
NEM ID

Steen Pilemand
Bestyrelsesmedlem
På vegne af: 108-234 E/F Universitetshaven VEST
Serienummer: PID:9208-2002-2-828737980356
IP: 82.147.226.97
2018-05-28 09:08:55Z
NEM ID