Famly Sikkerhedsbilag

Tekniske og organisatoriske sikkerhedsforanstaltninger i overensstemmelse med artikel 32 i GDPR.

De tekniske og organisatoriske sikkerhedsforanstaltninger, som Famly har på plads med henblik på at forhindre ukorrekt destruktion, ændring, oplysning, adgang og andre ukorrekte former for behandling af oplysninger, der eksporteres af Kunden til Famly, herunder følgende:

1. Fortrolighed (GDPR Artikel 32, stk. 1 litra b)

Fysisk sikkerhed

Uautoriseret adgang (i fysisk forstand) skal forhindres.

Tekniske og organisatoriske foranstaltninger til at kontrollere adgangen til lokaler og faciliteter, især for at kontrollere tilladelse:

- Famlys kontorer er beskyttet med branddetektering samt elektroniske sikkerheds- og indbrudsalarmer. Der opbevares ingen kundedata på Famlys kontorer eller på lokale medarbejdercomputere. Alle data er tilgængelige fra Famlys kontorer via sikre krypterede forbindelser med datacenteret.

- De datacentre, der anvendes af Famly, er state of the art ved hjælp af innovative arkitektoniske og tekniske tilgange. Vores udbyder har mange års erfaring med design, konstruktion og drift af store datacentre. Denne erfaring er blevet anvendt på platformen og infrastrukturen. Datacentre er anbragt i ikke-identificerbare faciliteter. Fysisk adgang er strengt kontrolleret både ved ydre grænser og ved indgange af professionelt sikkerhedspersonale, der benytter videoovervågning, indbrudsalarmer og andre elektroniske midler. Autoriseret personale skal gennemgå to-faktor-godkendelse mindst to gange for at få adgang til datacenteret. Alle besøgende og entreprenører er forpligtet til at præsentere identifikation og er skrevet ind og hele tiden eskorteret af autoriseret personale. Alt fysisk adgang til datacentre er logget og kontrolleret rutinemæssigt.

- Fysiske medier: Fysiske medier (fx transskriptioner), der indeholder personlige data fra Famly IT-løsningen, skal opbevares i låste skabe, når de ikke er i brug og indtil destruktionstidspunktet, jf. afsnittet om fysiske medier nedenfor. Kun ansatte med et bestemt behov kan få adgang til sådanne fysiske medier.

Teknisk sikkerhed

Uautoriseret adgang til IT systemerne skal forhindres.

Tekniske (ID/password sikkerhed) og organisatoriske (brugerdata) foranstaltninger til brugeridentifikation og -godkendelse:

- Firewalls: Der anvendes opdaterede firewalls til beskyttelse af netværket på Famlys kontor mod uautoriseret adgang. Tilsvarende gælder for Driftscentret, hvor firewalls og andre tekniske metoder anvendes til beskyttelse af Driftscentrets netværk mod uautoriseret adgang.

- Anti-virus/anti-malware: IT-enheder, som af Famly anvendes til at tilgå Famlys it-løsning, herunder servere som anvendes til driften, er i det omfang det er muligt og relevant, beskyttet med opdateret antivirus- og anti-malware-software.

- Kryptering: I forbindelse med overførsel af data i Famlys it-løsning via offentlige kommunikationsforbindelser, herunder når it-løsningen tilgås af brugere, anvendes sikker kryptering, baseret på anerkendte algoritmer, som minimum svarende til SSL 256bit. Alle Wifi-forbindelser, som anvendes på Famlys kontor og i Driftscentret er sikrede gennem brug af sædvanlig kryptering, i form af WPA eller bedre.

- Famlys Fjernadgang: Når Famlys ansatte tilgår Famlys it-løsning via fjernadgang er sådan forbindelse sikret gennem brug af kryptering, fx i form af VPN. Enhver tilgang til Famlys it-systemer kræver at Famlys ansatte anvender brugernavn og password. Betingelserne i denne databehandleraftale overholdes af Famly, uagtet der måtte anvendes fjernadgang

- Famlys adgangskodepolitik: Alle ansatte i Famly med adgang til Famlys IT løsninger er omfattet af en streng adgangskodepolitik. Adgangskoder skal indeholde mindst 10 karakterer og indeholde følgende: Store bogstaver samt små bogstaver, tal og specialtegn. Adgangskoder ændres mindst hver tredje måned. Adgangskoder kan ikke indeholde navne eller brugernavne.

Organisatorisk sikkerhed

Aktiviteter i it-systemer, der ikke er omfattet af de tildelte autorisationer, skal forhindres.

Lovkravsmæssig definition af godkendelsesmetoden og adgangskontrol samt overvågning og logning af adgang:

a) Autorisationer

- Alle ansatte i Famly, som har adgang til persondata, er autoriserede af Famly. Sådanne autorisationer angiver, hvilken adgang og til hvilke formål den enkelte ansatte har adgang til persondata. Famlys ansatte er alene autoriserede til at tilgå Kundens persondata med driftsmæssige eller tekniske formål for øje. Famlys ansatte har ikke adgang til persondata, som ikke er omfattet af deres autorisation.

- Famly kontrollerer og ajourfører løbende, og mindst halvårligt, alle ansattes autorisationer. Autorisationerne tilpasses eller tilbagekaldes i forbindelse med at ansatte skifter stilling, ansvarsområde eller fratræder.

- Ansatte i Driftscentret er alene autoriserede til at tilgå persondata med driftsmæssige formål. Sådan tilgang logges og autorisationen tilbagekaldes, når den ikke længere er nødvendig under henvisning til det driftsmæssige formål.

- Famlys it-system er sat op således, at Kunden kan autorisere sine ansatte på baggrund af roller. Kunden tildeler sine ansatte autorisationer via det af Famly til rådighed stillede web-modul. Øvrige brugere af Løsningen skal tillige underlægges autorisationer, som giver relevant adgang

- Alle ansatte i Famly med adgang til persondata er informeret om denne databehandleraftale og er forpligtede til at overholde de medarbejderrettede krav i denne databehandleraftale. Ansatte I Famly har ikke adgang til persondata, der ikke er inkluderet I deres autorisation.

- Alle ansatte i Famly med adgang til persondata vil I forbindelse med deres ansættelse blive bedt om at fremvise en straffeattest.

b) Login, brugernavne og adgangskoder

- Alle ansatte i Famly og Driftscenteret har unikke brugernavne og adgangskoder. Brugernavne og adgangskoder oprettes og ændres efter alment anerkendte principper, og intet brugernavn genbruges i en periode på mindst 6 måneder fra samme brugernavn sidst har været i brug. Såfremt en ansat i Famly ikke har anvendt sit brugernavn i en periode på 3 måneder suspenderes brugernavnet automatisk.

- Efter gentagne og på hinanden følgende fejlede login-forsøg med samme brugernavn, blokeres login med det pågældende brugernavn, for såvel ansatte hos Kunden som hos Famly. Såfremt de fejlede login-forsøg sker fra samme IP-adresse, blokeres adgang fra den pågældende IP-adresse. Blokering af adgang i de nævnte situationer, medfører intet ansvar for Famly. Såfremt der sker blokering af Famlys ansattes logins foretager Famly snarest opfølgning på dette.

- Der kan ikke ske login i Famlys it-systemer ved brug af anonyme brugerkonti eller gæstekonti.

c) Fortrolighed

- Alle ansatte hos Famly, som kan have adgang til persondata, er i deres ansættelsesaftaler underlagt fortrolighed, ligesom alle ansatte i Driftscenteret er underlagt fortrolighed.

- Fortroligheden opretholdes også ved Famly Aftalens ophør, eller hvor Famlys aftale med underdatabehandleren ophører, ligesom ansatte er omfattet af fortrolighedsforpligtelsen også efter ansættelsens ophør.

Separation af data

Persondata indsamlet med forskelligt formål må behandles separat.

Foranstaltninger til sikring af separat behandling (opbevaring, ændring, sletning, overførsel) af data til forskellige formal:

- Opbevaring af data: I Famly IT-løsningen er alle data gemt i Driftscenteret. Kundens data lagres logisk adskilt fra andre kunders data, for hvem Famly udfører databehandling for. Alle data er mærket med unikke id's, som kan identificere hvilken slutbruger eller kunde dataene tilhører.

2. Integritet (*GDPR artikel 32, stk. 1 litra b)*

Videregivelse af persondata

Aspekter af videregivelse af persondata skal sikres: elektronisk overførsel, datatransport, overførselskontrol mv.

Foranstaltninger til at transportere, overføre og formidle eller gemme data på data medier (manuel eller elektronisk) og til efterfølgende kontrol:

- IT-lagringsmedier: I forbindelse med genbrug, kassering, reparation eller service på lagringsmedier, som er blevet anvendt til lagring af persondata, sikres at tredjemand ikke kan opnå adgang til data på sådanne

medier. Sådan sikring sker enten gennem kryptering eller gennem grundig sletning eller overskrivning, som sikrer at tidligere lagrede persondata ikke kan genskabes, ved brug af en anerkendt standard (fx DOD 5220-22-M).

- Fysiske medier: Alle fysiske medier, som måtte indeholde persondata fra Kundens IT-løsning (fx udskrifter), bliver kasseret på betryggende vis, når det fysiske medie har opfyldt sit formål. Dette kan fx ske gennem makulering eller på anden vis, som sikrer, at der ikke er adgang til persondata.

- Fjernadgang: Når Famlys ansatte tilgår Famlys it-løsning via fjernadgang er sådan forbindelse sikret gennem brug af kryptering, fx i form af VPN. Enhver tilgang til Famlys it-systemer kræver at Famlys ansatte anvender brugernavn og adgangskode.

- Elektronisk signatur: Famly anvender 256-bit SSL certificater til identifikation af ægtheden af Famly overfor slutbrugerne.

- Transport sikkerhed: Famly anvender end-to-end SSL kryptering fra slutbrugerens enheder hele vejen til databasen såvel som mellem interne tjenester på serverne.

Datatilgængelighed

Fuld dokumentation af datahåndtering og vedligeholdelse skal opretholdes.

Foranstaltninger til sikring af kontrol af, hvorvidt data er blevet indtastet, ændret eller fjernet (slettet) og af hvem:

- Enhver tilgang til persondata i forbindelse med brug af Famlys it-løsning logges automatisk ("Anvendelseslog"). Ved logningen registreres tidspunkt, brugernavn, type af anvendelse samt den person som oplysningerne vedrører, eller det anvendte søgekriterium. Loggen opbevares i mindst 6 måneder og slettes efter maksimalt 7 måneder.

- Kunden kan efter særlig anmodning få adgang til oplysninger i Anvendelsesloggen.

- Såfremt der sker tilgang til Famlys it-løsning i teknisk øjemed, fx i forbindelse med support, fejlretning eller af anden teknisk årsag, logges sådan adgang i særlige logs. Hvor der i sådanne tilfælde sker anvendelse af Famlys it-løsning på tilsvarende vis, som andre brugere, sker der logning i Anvendelsesloggen.

3. Tilgængelighed og fleksibilitet (GDPR artikel 32, stk. 1 litra b og litra c)

Tilgængelighedskontrol

Data skal beskyttes mod utilsigtet destruktion eller tab.

Foranstaltninger til sikring af datasikkerhed (fysisk / logisk):

- Brand, strømafbrydelser mv.: Famlys kontor og Driftscentret er sikret på sædvanlig vis mod brand. Driftscentret er tillige sikret, således at driften kan forsætte, også ved strømafbrydelser af en vis varighed, ligesom der er etableret sikring mod tab af kommunikationsforbindelser til Driftscentret.

- Backup: Famly sikrer data lagret i Famlys it-løsning ved løbende og flere gange dagligt at foretage backup af lagrede data. Backup foretages som en blanding af fuld og trinvis (hvorved ændringer gemmes) backup. Famly foretager jævnligt restore-tests af tidligere gennemførte backups, således at det sikres, at

backuprutiner fungerer som tiltænkt. Backups er også duplikerede og lagret i et andet datacenter fra den samme udbyder i samme land og region.

- Uafbrydelig strømforsyning (UPS): Datacenteret elektriske systemer er designet til at være fuldstændigt uafhængig og vedligeholdt uden indvirkning på operationer, 24 timer i døgnet og 7 dage om ugen. UPS-enheder (Uninterruptible Power Supply) giver backup-effekt i tilfælde af elektrisk fejl for kritiske og væsentlige belastninger i anlægget. Datacentres generatorer genererer backup-strøm til hele anlægget.

- Klima og temperatur: Klimakontrol er nødvendigt for opretholdelse af en konstant temperatur i servere og andet hardware, hvilket forhindrer overophedning og reducerer muligheden for tekniske udfald. Datacentre er betinget af at opretholde atmosfæriske forhold på optimale niveauer. Personale og systemer overvåger og styrer temperatur og fugtighed på passende niveauer. Elektriske, mekaniske og livsstøttesystemer og udstyr overvåges, så alle problemer identificeres straks. Forebyggende vedligeholdelse udføres for at opretholde udstyrets fortsatte drift.

Genopretning ved nedbrud:

I tilfælde af en hændelse har Famly mulighed for hurtigt at gendanne adgang til personlige data ved at genoprette de seneste sikkerhedskopierede filer på andre servere. Dette kan ske inden for få minutter og sikrer, at enhver potentiel nedbrudstid minimeres.

4. *Procedurer for regelmæssig afprøvning, vurdering og evaluering (GDPR artikel 32, stk. 1, litra d and artikel 25, stk. 1, GDPR)*

Sikkerhedsbrud:

Procedure ved sikkerhedsbrud:

- Såfremt Famly måtte blive bekendt med et sikkerhedsbrud eller en trussel herom i forbindelse med Famlys it-løsning, vil Famly snarest mulig søge at lokalisere og identificere sådan brud eller trussel samt omfanget deraf, søge at begrænse potentiel eller opstået skade i videst muligt omfang, søge at hindre sådant sikkerhedsbrud i fremtiden, samt i det omfang det er muligt reetablere eventuelt mistede data.

- Famly vil i tilfælde af sikkerhedsbrud, hvor uautoriserede personer har fået adgang til Kundens data eller hvor der er opstået et datatab, når det er muligt, orientere Kunden skriftligt om sikkerhedsbruddet. Sådan orientering vil indeholde oplysning om hvilke data, der efter Famlys opfattelse er opnået uautoriseret adgang til, om Famly har iværksat særlige forholdsregler, ligesom orienteringen vil oplyse om Kunden efter Famlys opfattelse skal tage særlige forholdsregler.

Kontraktkontrol

Famly har indgået standardiserede GDPR-databehandleraftaler med leverandører for at leve op til betingelserne i denne kontrakt.

Revision

Famly vil mindst én gang årligt anvende ekstern revisor til verificering af overholdelse af procedurerne i denne aftale.