Forenede
Fordi der er forskel

Forenede A/S
Borupvang 5E
2750 Ballerup
(+45) 39 69 50 50
forenede.dk
CVR: 19710742

FORENEDES POLITIK FOR DATAETIK

Dataetik vedrører databeskyttelsesforordningen (GDPR) og databeskyttelsesloven, men dataetik handler ikke kun om at overholde love. Forenedes politik for dataetik er derfor forankret i vores tre værdier, og enhver form for databehandling- og indsamling skal foretages på måder, der afspejler dem:

- Ansvar
- Engagement
- Omtanke

Mere konkret vil det sige, at Forenede tager ansvar og handler med omtanke over for medarbejdere, kunder og de borgere, vi hjælper. Vi er derfor også engagerede i dataetik.

Politikkens formål

I forbindelse med Forenedes serviceydelser og kommunikation med relevante myndigheder foretages dataindsamling på forskellige områder. Formålet med nærværende politik er at redegøre for Forenedes generelle dataindsamling- og anvendelse med henblik på at sikre transparens.

Denne politik for dataetik suppleres af Forenedes persondatapolitik, der er tilgængelig på Politikker - Forenede DK, og evalueres årligt af koncernledelsen. Nedenfor beskrives konkret, hvordan vi griber dataetik an generelt og dernæst specifikt går til dataetik i vores forskellige samarbejdsrelationer.

Generelt om persondata

Forenede søger, at alle nye systemer konfigureres med Single Sign-on for nem on- og offboarding. Dette sikrer, at medarbejdere og brugere bliver fjernet fra systemer med persondata, når disse bliver offboardet i vores HR-systemer. Systemerne følger reglerne opsat i vores generelle IT-sikkerhedspolitik, som alle medarbejdere undervises i. Al ekstern adgang til vores systemer er opsat med multifaktorvalidering som et ekstra sikkerhedslag. Medarbejdere undervises i sikker håndtering af persondata via vores awareness-system.

Data om medarbejdere

Medarbejdernes personoplysninger behandles, for at virksomheden kan håndtere ansættelsen og opfylde forpligtelserne over for medarbejderen. For en vis behandling kræves et særligt samtykke fra medarbejderen.

I tilfælde af ansættelsesforholdets ophør opbevares kun personoplysninger vedrørende faktuelle oplysninger såsom årsagen til ansættelsesforholdets ophør, lønklasser, tjenestebeviser, personoplysninger til administrative formål og for at kunne give referencer.

I tilfælde af en anmodning fra den registrerede om at blive slettet, opbevares kun de personoplysninger, som virksomheden har ret til eller er forpligtet til at gøre i overensstemmelse med ufravigelig lovgivning eller juridisk forpligtelse i henhold til den generelle databeskyttelsesforordning.

Alle oplysninger ligger i HR-systemerne Sympa, HRM samt Quinyx og TimePlan, som bruges til tidsregistrering.

Data om kunder

Kundedata, der indeholder personoplysninger, slettes, når kundeforholdet er ophørt, og ethvert tidspunkt for reklamationsret, fortrydelsesret eller lignende er udløbet.

Kontaktoplysninger kan opbevares til markedsføringsformål baseret på en interesseafvejning. Modtageren af markedsføringen har dog altid ret til at framelde sig, hvilket så naturligvis respekteres.

I tilfælde af at virksomheden fungerer som databehandler på vegne af en kunde, slettes data i overensstemmelse med instruktioner fra kunden.

Alle kundedata ligger i hhv. Hubspot CRM samt i vores kontraktsystemer i Navision.

Data om leverandører

Personoplysninger fra leverandører opbevares på grundlag af kontrakten. Formålet er at kunne håndtere, modtage, klage eller fortryde f.eks. et køb af et produkt eller en ydelse. Derudover opbevares oplysningerne kun i det omfang, det kræves af ufravigelig lovgivning eller retlig forpligtelse i henhold til databeskyttelsesforordningen.

Leverandørdata lagres som kontrakter i SharePoint samt vores kontraktstyringssystem.

Data om patienter og beboere

Patienter og beboere i vores Care-forretninger lagres og journaliseres i dertilhørende omsorgssystemer. I Sverige anvendes primært Sekoia til dette, hvis der ikke er indgået aftale med kommunen om anvendelse af deres journalsystem.

I Danmark anvendes primært Nexus på egne lokationer og på kommunale tilbud anvendes kommunernes systemer.

Alle systemerne er ift. håndtering af persondata omfattet af de nationale lovgivninger på området.

Dataetisk Råds 10 principper og værdier er retningsgivende for Forenedes datahåndtering:

1) **Velfærd**
   Behandling af data skal ske med respekt for og hensyn til sociale forhold, samfund og demokrati.
2) **Værdighed**
   Behandling af data må ikke anvendes til at skade det enkelte menneske, og mennesker bør have den primære gavn af databehandlingen. Det vil sige, at mennesker skal prioriteres før kommercielle og institutionelle interesser.
3) **Privatliv**
   Behandling af data skal ske med respekt for privatliv og under beskyttelse af personlige oplysninger. Det bør altid overvejes, hvilke data der er nødvendige, fra hvilke kilder data skal indhentes, og hvor følsomme disse data anses for at være. Indhold, omfang og deling af borgernes personlige data bør begrænses mest muligt og ikke opbevares i længere tid end højst nødvendigt.

4) **Selvbestemmelse**
   Behandling af data skal støtte mennesket i at træffe oplyste og selvstændige valg. Det skal ikke mindske, begrænse eller vildlede menneskets selvbestemmelse. Det enkelte menneske bør have kontrol over egne data, herunder kontrol med hvilke data, der indsamles, hvad de anvendes til og i hvilke sammenhænge.
5) **Lighed**
   Behandling af data må ikke diskriminere på baggrund af etnicitet, seksualitet, køn, socioøkonomisk baggrund, politiske meninger, religion, fagforeningsmedlemskab, genetiske data, biometriske data, handicap eller andre sundhedsrelaterede data. Behandling af data må ikke reproducere fordomme, der marginaliserer og stigmatiserer befolkningsgrupper. Der bør målrettet arbejdes for, at ressourcesvage og udsatte borgere får gavn af den teknologiske udvikling. Der skal sikres mangfoldighed og diversitet i udvikling og anvendelse af ny teknologi ved for eksempel inddragelse af relevante faggrupper, brugergrupper og organisationer.
6) **Frihed**
   Behandling af data skal ske med respekt for grundlæggende frihedsrettigheder i et demokratisk samfund. Herunder ytrings-, informations-, religions-, forsamlings- og foreningsfrihed.
7) **Retssikkerhed**
   Behandling af data skal støtte mennesket i at træffe oplyste og selvstændige valg. Det skal ikke mindske, begrænse eller vildlede menneskets selvbestemmelse. Det enkelte menneske bør have kontrol over egne data, herunder kontrol med hvilke data, der indsamles, hvad de anvendes til og i hvilke sammenhænge.
8) **Gennemsigtighed**
   Behandling af data skal være tilstrækkelig gennemsigtig. Der skal være adgang til indsigt i egne data. Der skal informeres klart og forståeligt om behandlingen af data, databehandlingens formål, funktion, sikkerhed og begrænsninger. Bagvedliggende mønstre skal kunne forklares og retfærdiggøres.
9) **Sikkerhed**
   Behandling af data skal være tilstrækkelig sikker, robust og pålidelig. Der skal sikres sikkerhed i opbevaring og deling af data, således at data ikke utilsigtet bliver tilgængelige for uvedkommende personer. Det skal være muligt at overvåge og udøve effektivt tilsyn og kontrol, så fejl og potentielle negative sociale eller etiske konsekvenser kan identificeres, evalueres, dokumenteres og minimeres.
10) **Ansvarlighed**
   Det skal være muligt at stille mennesker til ansvar. Det skal i alle led være klart hvem, der er ansvarlig for konsekvenserne for udvikling og anvendelse af data. Det gælder blandt andet udviklere, anvendere, myndigheder, virksomheder, samarbejdspartnere og tredjeparter.