Databeskyttelsespolitik for Ulandshjælp fra Folk til Folk-Humana People to People (UFF-Humana)

Oversigt:

1. Generelt

Denne data- og privatlivspolitik er gældende for de persondata, som du giver til UFF-Humana og/eller som vi indsamler om dig, når du deltager i en aktivitet, er bidragyder, medlem, jobsøgende, kunde, leverandør, ansat i en myndighed eller som bruger af vores tjenester, herunder ved færden på vores hjemmeside. I politikken kan du læse mere om, hvilke persondata vi indsamler, hvordan vi håndterer dine data og hvor længe, vi opbevarer data om dig.

2. Formål

Databeskyttelsespolitikken beskriver det ledelsesgodkendte niveau for datasikkerhed i UFF-Humana og indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af UFF-Humanas datasikkerhedshåndbog med de underliggende retningslinjer og forretningsgange.

De retningslinjer, der udformes for at understøtte databeskyttelsespolitikkens hovedmålsætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til sikkerhed i behandlingen af personoplysninger i det daglige arbejde.

Databeskyttelsespolitikken er især formuleret med henblik på beskyttelse af personoplysninger, men den finder tilsvarende anvendelse på økonomiske- og andre data.

UFF-Humana ser det vigtige i et højt sikkerhedsniveau for at kunne overholde lov- og myndighedskrav, men også som en kvalitet i at kunne tilbyde en sikkerhed for alle, som henvender sig eller indgår et samarbejde med os.

Datasikkerhed er derfor en nøgleværdi, og den er en naturlig del af UFF-Humanas databehandling af oplysninger, herunder især personoplysninger.

3. Omfang

Databeskyttelsespolitikken er gældende for alle ansatte hos UFF-Humana.

Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til UFF-Humanas systemer, data og oplysninger skal gøres bekendt med politikken og følge den.

Databeskyttelsespolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af UFF-Humanas automatiske databehandlingssystemer samt manuelle arkiver og registre.

4. Hovedmålsætninger og sikkerhedsniveau

UFF-Humana har følgende sikkerhedsmålsætning:

"UFF-Humana har et passende og tilstrækkelig teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data ved hel eller delvis anvendelse af automatisk databehandling, samt for behandling af manuelle dokumenter."

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene gennemfører UFF-Humana passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Et passende og tilstrækkeligt databeskyttelsesniveau (som beskrevet i Databeskyttelsesforordningen artikel 32) opnås igennem tekniske og organisatoriske foranstaltninger, der sikrer:

- ***vedvarende fortrolighed, integritet, tilgængelighed og robusthed*** af UFF-Humanas behandlingssystemer og be-handlingstjenester i forhold til den risikovurdering, der er gennemført for de enkelte systemer og data.
- anvendelse af ***kryptering,*** hvor det er relevant, herunder ved dataudveksling med databehandlere og eksterne parter og offentlige myndigheder
- evnen til rettidigt at ***genoprette tilgængelighed*** af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse
- en procedure for regelmæssig ***afprøvning, vurdering og evaluering*** af databeskyttelsessikkerheden
- beskyttelse af UFF-Humanas it-aktiver, oplysninger og data i UFF-Humanas varetægt.

Et tilstrækkeligt sikkerhedsniveau ***fastholdes*** ved:

- at der ***vedvarende*** forefindes ***retningslinjer og forretningsgange***, som sikrer, at datasikkerheden er en integreret del af UFF-Humanas drift og daglige arbejde.
  Målet er, at sikre en kontinuerlig forbedringsproces, der løbende vedligeholder og optimerer databeskyttelsespolitikken, retningslinjer og forretningsgange.
- *at det* igennem ***kontrakt- og leverandørstyring*** sikres, at brugen af eksterne leverandører, konsulenter og samarbejdspartnere lever op til den gældende databeskyttelseslovgivning og UFF-Humanas databeskyttelsesniveau.
- at der i forbindelse med indførelse af ***nye IT-systemer*** gennemføres:
  - passede tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er ***nødvendige*** behandles
  - en evt. analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, hvis det skønnes nødvendigt (***Konsekvensanalyse***)
- **UFF-Humana** følger op på datasikkerheden igennem løbende vedligeholdelse og optimering af databeskyttelses-politikken og de dertilhørende retningslinjer og forretningsgange.

5. Organisation og ansvar

Sikkerhedsmålsætning:

"Alle ansatte har ansvar for datasikkerheden. De er bekendte med og efterlever UFF-Humanas databeskyttelses-politik, retningslinjer og forretningsgange, der er beskrevet i datasikkerhedshåndbogen."

Planlægning, implementering og kontrol af datasikkerheden er defineret af **UFF-Humanas** ledelse, der også er ansvarlig for implementering og vedligeholdelse af databeskyttelsessikkerhedssystemet og er ansvarlig for opfølgning på sikkerhedshændelser.

UFF-Humanas ledelse fastsætter i en ***datasikkerhedshåndbog, hvem der har ansvaret*** for hver af institutionens, ***automatiske og manuelle databehandlingssystemer***, styring af ***systemadgang og netværksadgang***, tildeling af rettigheder, indgåelse af ***IT-kontrakter og andre kontrakter***, ***Indkøb af hardware og installation af software,*** behandling af ***henvendelser fra de registrerede, o***psamling og styring af ***anmeldelse af brud på persondatasikkerheden*** til Datatilsynet og de registrerede, der er berørt af bruddet.

Databeskyttelsespolitikken revurderes og godkendes én gang årligt, eller i forbindelse med eventuelle situationer, der nødvendiggør det.

Ledere og ansatte er ansvarlige for at efterleve retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Ansatte, der konstaterer eller oplever brud på datasikkerheden, skal anmelde det hurtigst muligt til dataansvarlig.

Den nødvendige viden og kompetence om datasikkerhed kommunikeres til alle ansatte, og der bliver løbende arbejdet med holdninger og viden omkring datasikkerhed.

Ledelsen er ansvarlig for, at databeskyttelsespolitikken overholdes.

6. Datasikkerhedshåndbogen

Databeskyttelsespolitikken uddybes af ledelsen i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabspolitik, forretningsgange og datasikkerhedshåndbogen, der inddeles i følgende hovedområder

1. Retningslinjer for ***ansattes håndtering af sikkerhed***.
   - Fokus på, at personoplysninger altid behandles fortroligt.
   - Regler for login og password.
   - Regler for anvendelse af mobilt udstyr, PC'er, USB-nøgler, mobiltelefoner mv.
   - Regler for anvendelse af private PC'er til brug til arbejdsopgaver som indebærer behandling af personoplysninger
   - Regler for anvendelse af internettet.
   - Regler for anvendelse af mails, herunder sikker mail, og privat anvendelse af UFF-Humanas *firmamail*.
   - Regler for eller forbud mod download af IT-programmer, spil, billeder mv.
2. Retningslinjer for ***adgangsstyring.***
3. Retningslinjer for behandling af ***data på mobile enheder.***

4. Retningslinjer for anvendelse af ***sikker mail*** ved kommunikation, som indeholder persondata med kunder, samarbejdspartnere, kommuner og andre offentlige myndigheder.
5. Retningslinjer for ***netværksstyring***, herunder trådløse netværk.
6. Retningslinjer for ***styring af sikkerhedshændelser***, herunder
   - Anmeldelse af brud på persondatasikkerheden til Datatilsynet og de registrerede, herunder procedurer, kontakt til databehandler og indhold i anmeldelsen.
   - Forretningsgange for behandling, reetablering og rettelser af data.
7. Principper og forretningsgange for ***behandling af personoplysninger*** som beskrevet nedenfor i afsnit 7.
8. Retningslinjer for ***styring af leverandører og databehandlere.***
   - Databehandleraftaler
   - Databehandlerens sikkerhedsniveau og håndtering af sikkerhed

7. Behandling og opbevaring af personoplysninger

UFF-Humana opbevarer og behandler kun dine personoplysninger, så længe det er nødvendigt i forhold til det fastsatte formål med behandlingen. Når formålet med behandlingen ikke længere er til stede, vil dine personoplysninger blive slettet, anonymiseret eller overført til arkiv efter reglerne i arkivlovgivningen.

Ledelsen fastsætter principper og forretningsgange for UFF-Humanas behandling af personoplysninger, der sikrer overholdelse af Databeskyttelsesforordningen og Databeskyttelsesloven. Forretningsgangene og procedurer, der ***dokumenteres***, omfatter

- ***Principper for behandling af personoplysninger.***
- Anvendelse af ***samtykke*** som grundlag for behandling af personoplysninger.
- Procedurer for udøvelse af den ***registreredes rettigheder,*** herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling.
- ***Fortegnelser udarbejdet over behandlingsaktiviteter*** med personoplysninger.

8. Risikovurdering og klassifikation af data

8.1 Risikovurdering

UFF- Humana ønsker at være bevidst om enhver risiko, og ud fra en risikovurdering opnå at et passende og tilstrækkeligt sikkerhedsniveau bliver etableret både elektronisk og fysisk.

Ledelsen deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici ved automatisk og manuel databehandling.

Det tages op i ledelsen en gang om året om risikovurderingen skal revurderes, samt ved eventuelle større ændringer i opgaver, leverandører, databehandlingssystemer.

8.2 Klassifikation

For at sikre, at systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, integritet (pålidelighed) og fortrolighed.

8.2.1 Tilgængelighed

I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Det er for UFF-Humana især vigtigt med høj tilgængelighed til data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med:

- Personer som donerer til UFF-Humana
- Kunder som køber tøj af UFF-Humana
- Personer som er vært for en eller flere UFF-Humana containere
- Samarbejdspartnere
- Udsendelser til vores kunder og medlemmer
- Personaleadministration

Tilgængeligheden sikres først og fremmest igennem bestemmelser i de IT-kontrakter og/eller databehandleraftaler, der indgås med leverandørerne.

8.2.2 Integritet/Pålidelighed

I integritet/pålidelighed ligger, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.

Det er for UFF-Humana især vigtigt med høj integritet/pålidelighed i data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med behandlinger, hvor persondata indgår.

Integritet/pålidelighed sikres først og fremmest gennem den kvalitetskontrol, der finder sted under de fastlagte forretningsgange for behandling af sagerne.

8.2.3 Fortrolighed

Med ***fortrolighed*** menes der, at kun autoriserede personer har ret til at tilgå oplysningerne, og oplysningerne skal kun være tilgængelige for autoriserede personer.

Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse har hjemmel i lovgivningen.

I Datasikkerhedshåndbogen angives det, hvem der har adgang til hvilke personoplysninger. Vi stræber efter at begrænse denne adgang til personer, som er afhængige af denne adgang til at udføre deres arbejdsopgaver.

9. Overtrædelse af databeskyttelsespolitikken

Alle ansatte i UFF-Humana er forpligtet til at efterleve den til enhver tid gældende datasikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle ansatte modtager ved deres tiltræden af stillingen en kopi af de vigtigste bestemmelser om data- og persondata-sikkerhed rettet til medarbejderne og skriver under på, at de vil overholde UFF-Humanas datasikkerhedspolitik.

En overtrædelse af datasikkerhedsbestemmelser eller regler for behandling af personoplysninger kan efter omstændighederne medføre ansættelsesretlige konsekvenser.

10. Afvigelser

Hvis der opstår situationer, hvor kravene i Databeskyttelsespolitikken ikke kan efterleves, skal det godkendes af ledelsen og dokumenteres, og der indføres alternative sikringsforanstaltninger.

11. Udarbejdelse, dataansvarlig og ikrafttrædelse

Denne version af Databeskyttelsespolitikken er godkendt den 21.10.2019, og træder i kraft den 01.11.2019

UFF-Humana har udnævnt Else Hanne Henriksen som dataansvarlig. Hvis du har spørgsmål omkring vores data-beskyttelses politik, kan du henvende dig til:

E-mail: elsehanne@uff.dk
Telefon: 23 34 42 98

Adresse:
Ulandshjælp fra Folk til Folk – Humana People to People
Kildebrogårdsvej 11K
4622 Havdrup

Bilag 1: Begreber og definitioner

Begreb	Definition
Fortrolighed	Kun autoriserede personer har ret til at behandle oplysningerne, der kun skal være tilgængelige for autoriserede personer.
Integritet	Det er muligt at validere, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige. Herunder sikring af Backup og eller systemdublering
Tilgængelighed	Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
Robusthed	Behandlingssystemers- og tjenesters tekniske og organisatoriske modstandsdygtighed, der beskytter dem mod skadelige hændelser. Dette kan f.eks. være sikring mod udfald ved dublering, køling, nødstrømsanlæg, brandslukning mv.
Pseudonymisering	Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, der opbevares separat og sikkert.
Kryptering	En proces, der omdanner de oprindelige oplysninger til oplysninger, der er ulæselig for en tredjepart.
Vedvarende	Evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester er en løbende teknisk og organisatorisk forpligtelse
Databeskyttelsespolitik	Databeskyttelsespolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som besluttes af ledelsen, og som udstikker de overordnede krav og målsætninger, som opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser, der findes i Datasikkerhedshåndbogen.
Retningslinjer	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Retningslinjerne fungerer på et overordnet niveau og indeholder ikke tekniske og systemrelaterede beskrivelser.
Forretningsgange og instrukser	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
Sikkerhedsforhold	Med sikkerhedsforhold menes alle de forhold, som kan påvirke oplysningers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
Sikkerhedshændelser	Begrebet forstås bredt som alle de hændelser, der påvirker databeskyttelsessikkerheden, herunder brud på sikkerheden