

Vejledning til de dataansvarlige til brug for de komplementerende kontroller under gældende ISAE3000 erklæring.

Vedr. ansvar ved brug af løsningen, herunder indtastning af personoplysninger benævnt i bilag A.

Svar: Denne vejledning omhandler de mellem XFlow (herefter "databehandleren") og den dataansvarlige aftalte bestemmelser, hvad angår behandlingens omfang og karakter. Dette er specifikt benævnt i databehandleraftalens bilag A.

Fra bilag A kan det udledes, at behandlingen udelukkende må omfatte de registrerede og kategorier af personoplysninger, som fremgår heraf. Eftersom databehandlerens løsning(er) giver den dataansvarlige mulighed for at tilføje enhver personoplysning om alle kategorier af registrerede, skal den dataansvarlige, forinden indtastning af sådanne oplysninger til løsningen, sikre at de indtastede oplysninger ikke afviger fra de aftalte oplysninger i databehandleraftalens bilag A. Databehandleren kan ikke med rimelighed føre kontrol med alle dets kunder for at sikre overholdelse af de aftalte bestemmelser, hvorfor det forventes, at den enkelte dataansvarlige selv påtager sig denne forpligtelse.

Databehandleren anerkender at visse omstændigheder kan medføre, at den dataansvarliges behov løbende ændrer sig således, at behandlingen af andre registrerede eller andre kategorier af personoplysninger er nødvendig, og derfor afviger fra gældende bilag A. Såfremt dette er tilfældet, opfordres den dataansvarlige til at indgå en opdateret databehandleraftale eller underskrive et tillæg til den allerede eksisterende.

Vedr. ansvar ved supportanmodninger

Svar: Denne vejledning vedrører forholdet mellem XFlow (herefter "databehandleren") og den dataansvarlige, når den dataansvarlige fremsætter en anmodning om support. Efter det er blevet fastslået at den dataansvarliges henvendelse vedrører support og dermed ikke en fejlkorrektion, skal den dataansvarlige sikre, at databehandleren udelukkende bliver tildelt adgang til eller opnår indsigt i de oplysninger, deriblandt personoplysninger, som er nødvendige for at databehandleren kan bistå med supportanmodningen. Det er således op til den dataansvarlige at vurdere, hvilke oplysninger der er relevante i supportsammenhænge. Oftest vil sådanne henvendelser kunne løses uden involvering af personoplysninger omhandlende enkelte data subjekter med kyndig vejledning fra vores supportteam.

Såfremt I som dataansvarlige fortsat er i tvivl om, hvorvidt der er tale om en fejl eller om support er påkrævet, henledes opmærksomheden på afsnit 3 i gældende Abonnementsvilkår. Her fremgår en nærmere beskrivelse af dette forhold.

Vedr. adgange og rettigheder

Systemet indeholder funktioner til at understøtte denne kontrol som en administrator hos kunden vil kunne tilgå:

Brugerlisterapport

Systemet kan generere fuldt udtræk over alle bruger samt hvilke roller de er tildelt. De givne roller en bruger er tildelt, vil give et antal rettigheder, alt efter hvordan kunden har opsat rolle-rettighedstilknytningen.

Automatisering

Der mulighed for at lave fuld automatisering af rolle- og rettighedsstyringen ved sammenkobling med den dataansvarliges egen bruger-database med XFlow. Dette kan se via login-claims eller en decideret brugerimport/brugersynkronisering via kundens IDM systemet eller via XFlows REST API.

Vedr. ansvar for instruks

Svar: Denne vejledning har til formål klarlægge ansvarsfordelingen mellem XFlow (herefter "databehandleren") og den dataansvarlige, hvad angår lovligheden af behandlingen, herunder den dataansvarliges instruks specifikt benævnt i databehandleraftalens præambelbetragtning 4 og gældende bilag C.

Eftersom databehandlerens løsning(er) giver den dataansvarlige mulighed for at tilføje enhver personoplysning om alle typer af registrerede, skal den dataansvarlige, forinden indtastning af sådanne oplysninger til løsningen, sikre at der foreligger et tilstrækkeligt hjemmelsgrundlag. Her henvises der til Databeskyttelsesforordningens art. 6 og 9 afhængig af kategorien af personoplysninger. Endvidere er det den dataansvarliges ansvar at sikre, at brugen af databehandlerens løsning udelukkende sker i henhold til de øvrige bestemmelser i Databehandleraftalen. Vi, som databehandler, behandler udelukkende personoplysninger i det omfang I, som dataansvarlige, har instrueret herom. Af denne grund er det således alene den dataansvarlige, der skal sikre, at den angivne instruks er lovlig på ethvert tidspunkt af behandlingens varighed. Vi står altid til rådighed, hvis I har nogle spørgsmål til ovenstående.

Vedr. kryptering

Alt netværkstrafik i systemet er krypteret og overholder gældende anbefalinger fra Datatilsynet, for nu fastsat som TLS 1.2 eller højere. Dette gælder både trafik til og fra systemet fra eksterne kilder, samt kommunikation mellem interne komponenter i systemet.

Vedr. Sletning i løsningen

XFlow indeholder mulighed for at den dataansvarlige selv kan slette data i løsningen. Alt data som bliver indtastet eller uploadet til løsningen kan efterfølgende slettes. Den dataansvarlige, bliver som en del af undervisning og implementering af løsningen, informeret om disse muligheder.

Indberetninger kan slettes ved at tilgå søgesiden med korrekte brugerrettigheder, herefter kan man via flueben vælge den/de indberetninger som skal slettes.

Ligeledes kan brugere slettes når de ikke længere har indberetninger i systemet.

Vedr. XFlow og de registreredes rettigheder

XFlow platformen understøtter at I som dataansvarlige kan imødekomme udøvelse af jeres kunders/brugeres (som registrerede) håndhævelse af deres rettigheder efter Databeskyttelsesforordningen.

I den forbindelse antager vi, at I er bevidste om de begrænsninger og undtagelser der gælder for imødekommelse af de registreredes håndhævelse af deres rettigheder, hvorfor disse ikke behandles i nedenstående, som netop forudsætter, at I imødekommer den registreredes anmodninger.

Via XFlow platformen har I mulighed for, at:

1. give indsigt i den registreredes personoplysninger (artikel 15),

Efter artikel 15, har den registrerede ret til at vide om den dataansvarlige behandler personoplysninger om den pågældende. Den registrerede har ligeledes ret til at få indsigt i de personoplysninger, som den dataansvarlige behandler om den pågældende. Indsigt kan gives ved at udlevere en kopi af de originale personoplysninger eller på anden lignende måde, så længe den registrerede får en egentlig kopi af personoplysningerne.

Nedenstående i kursiv er et eksempel på at give indsigt i den registreredes personoplysninger:

Der kan via fritekstsøgning, f.eks. på et navn, et CPR-nummer eller lign., fremsøges alle indberetninger som indeholder informationer om dette. Der kan ligeledes søges direkte på alle indberetninger oprettet af en konkret bruger i systemet.

Den registrerede kan altid logge ind og se alle egne indberetninger, som ikke er blevet slettet via automatiserede slettefrister.

2. berigtige personoplysninger efter den registreredes anmodning (artikel 16),

Efter artikel 16, har den registrerede, uden unødigt forsinkelse, ret til at få urigtige (forkerte) personoplysninger om sig selv berigtiget, ligesom den registrerede, uden unødigt forsinkelse, har ret til at få fuldstændiggjort ufuldstændige personoplysninger, under hensyntagen til formålene med behandlingen. Såfremt der ikke er enighed mellem parterne om hvorvidt oplysningerne er rigtige, er den dataansvarlige ikke forpligtet til at slette oplysningerne, men skal sørge for at dokumentere den registreredes holdning til personoplysningerne. Uanset artikel 16, skal den dataansvarlige dog altid sørge for at berigtige personoplysninger, hvis denne skulle blive opmærksom på at personoplysningerne er forkerte.

Nedenstående i kursiv er et eksempel på hvordan personoplysninger kan berigtiges:

Hvis login foregår via NemID/MitID, vil stamdata om egen bruger opdateres automatisk med data herfra. Dette gælder navn, adresse og CPR-nummer – disse data kan som udgangspunkt ikke rettes i systemet, men skal rettes i stamdatasystemet, her CPR-registret. Det er muligt at rette den tilknyttede mailadresse.

3. slette personoplysninger på den registrerede, såfremt der findes grundlag herfor (artikel 17), Såfremt mindst en af forholdene i artikel 17, litra a-f (grundlaget) er opfyldt, har den registrerede, uden unødigt forsinkelse, ret til at få personoplysninger om sig selv slettet. Den dataansvarlige har ligeledes pligt til at slette oplysningerne, hvis et af forholdene i art. 17, litra a-f er opfyldt, men den dataansvarlige har også, uanset art. 17, pligt til at slette personoplysninger når det ikke længere er nødvendigt for denne at have dem af hensyn til de formål, hvormed oplysningerne behandles.

Nedenstående i kursiv er et eksempel på at slette personoplysninger om den registrerede:
Anmodninger om at få slettet alle personoplysninger vil kunne imødekommes.

Det er muligt både at fremsøge og efterfølgende slette en indberetning fra en registreret, samt at slette den registreret fra systemet, så snart der ikke ligger flere indberetning fra den registrerede i systemet.

Den enkelte organisation kan fastsætte faste slettepolitikker i forhold til automatiseret sletning af data, efter variable parametre. Dette kan fastsættes ud fra de enkelte indberetningstyper.

4. begrænse behandlingen af personoplysninger på den registrerede (artikel 18),

Såfremt mindst en af betingelserne i artikel 18, litra a-d er opfyldt, har den registrerede ret til at få begrænset behandlingen af sine personoplysninger, således at oplysningerne ikke må underlægges andre behandlinger end opbevaring. I praksis kan behandling af personoplysninger begrænses bl.a. ved, at oplysningerne gøres utilgængelige for brugerne af den dataansvarliges system. Det bør i den forbindelse tydeligt angives i systemet, at oplysningerne er blevet begrænset, så brugeren bliver informeret.

5. udtrække personoplysninger på den registrerede i XFlow platformen (artikel 19).

Efter artikel 19, har den dataansvarlige efter enhver berigtigelse, sletning eller begrænsning der er udført i henhold til artikel 16, 17, stk. 1 og 18, stk. 1, pligt til at underrette alle modtagere som de berigtigede, slettede eller begrænsede personoplysninger måtte være videregivet til. Dette gør sig dog ikke gældende såfremt det viser sig umuligt, eller er uforholdsmæssigt vanskeligt.

Nedenstående i kursiv er et eksempel på beskrivelse af udtrækning af personoplysninger på den registrerede:

Der er fuld sporbarhed på hvilke handlinger der er blevet foretaget af systemet på den enkelte indberetning, herunder hvilke dataafleveringer som er sket, som har videregivet personoplysninger ud af systemet. Denne information kan herefter bruges til at underrette eventuelle modtagere.

Sporbarhed ophører hvis indberetningen er blevet slettet i henhold til den slettepolitik som er sat op for indberetningstypen.