Danmarks Miljøportal

Data om miljøet i Danmark

Brugeradministrationsaftale

Denne aftale (herefter Aftalen) indgås mellem parterne

Danmarks Miljøportal, Fællesoffentligt Partnerskab mellem Miljø- og Fødevareministeriet, KL og Danske Regioner, Haraldsgade 53, 2100 København Ø, CVR. Nr. 29776938, EAN nr. 5798000871007 (herefter kaldet DMP)

Og *(indsæt oplysninger)*

Navn/Virksomhed/Organisation:

Vej, nr.:

Postnr., by:

CVR nr.:

EAN nr.:

Kontaktperson:

(herefter kaldet Organisationen).

1. Formål

Danmarks Miljøportal (DMP) udbyder en lang række fællesoffentlige databaser (fagsystemer) via miljoeportalen.dk (Miljøportalen).

Adgangen til databaserne kontrolleres via DMP's brugeradministrationssystem for at beskytte data. DMP's brugeradministrationssystem har til formål at administrere brugernes adgange og rettigheder til databaser i Miljøportalen. Brugeradministrationssystemet håndterer brugere fra mange forskellige organisationer, herunder brugere fra offentlige myndigheder, laboratorier samt konsulenters, forskeres og privates adgange til Miljøportalen.

Brugeradministrationssystemet bygger på tildeling af adgange til Miljøportalen via foruddefinerede roller. Rollerne er designet efter, hvad brugeren skal bruge databaserne til; nogle skal kunne læse fagdata, mens andre skal kunne indtaste og redigere i data eller godkende data indlæst af laboratorier.

Brugeradministrationen varetages af den enkelte Organisation (brugerorganisation), der selv administrerer egne brugeres adgange til Miljøportalens databaser. Organisationen kan vælge enten at have en central opkobling til brugeradministrationssystemet via login fra DMP's servere, eller Organisationen kan have en decentral opkobling til brugeradministrationssystemet via føderation, hvor login sker via sammenhængende log-in.

Aftalen regulerer to overordnede forhold i den forbindelse:

a) DMP behandler data om Organisationens medarbejdere (brugernavn, e-mail adresse, oplysninger om certifikat, tildelte roller etc.). I persondatalovens forstand er Danmarks Miljøportal her databehandler for Organisationen (brugerorganisationen), som er dataansvarlig. I bilag 1 til Aftalen findes en standardinstruks, hvor Organisationen instruerer Danmarks Miljøportal vedr. denne behandling.

b) Organisationens medarbejdere får adgang til fagdata via Miljøportalen, når Organisationens brugeradministrator tildeler dem roller. Med henblik på at sikre en hensigtsmæssig håndtering af disse data skal Organisationen overholde en række sikkerhedskrav defineret af DMP. Disse krav er afspejlet i afsnit 2 - 20 nedenfor.

2. Miljøportalens instruktioner

DMP har udarbejdet en række instruktioner (vejledninger og adgangspolitikker) til Organisationerne om DMP's brugeradministrationssystem. Organisationens brugeradministratorer skal anvende instruktionerne ved tildeling af adgangsrettigheder (roller) til brugere inden for egen organisation til de databaser, der udstilles på Miljøportalen.

Vejledninger, adgangspolitikker og DMP's FAQ, der indeholder løsningsforslag på hyppige spørgsmål vedrørende installation mm., er tilgængelige på www.miljoeportal.dk angående inddatering af data / digitale løsninger.

3. Generelle sikkerhedsbestemmelser

Begge parter skal som hhv. databehandlere og dataansvarlige for data ved administration af brugere og miljøfaglig data o.l. overholde reglerne i gældende lovgivning vedr. krav til såvel digital som fysisk sikkerhed, i henhold til sikkerhedsbekendtgørelsen (BEK nr. 528 af 15/06/2000 med senere ændringer).

Begge parter skal desuden have etableret egne sikkerhedspolitikker fx i overensstemmelse med DS484 eller ISO 27001 med senere ændringer/versioner eller baseret på andre af parterne valgte principper, som sikrer en tilfredsstillende sikkerhed.

Parterne skal fastlægge nærmere interne bestemmelser om sikkerhedsforanstaltninger til uddybning af reglerne i sikkerhedsbekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationer samt kontrol med autorisationer. Parterne skal endvidere hver især fastsætte instrukser, der beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af it- udstyr. Desuden skal parterne hver især fastsætte retningslinjer for tilsyn med, at sikkerhedsforanstaltningerne overholdes.

Parterne skal desuden hver især sikre, at data eller filer, som udveksles via løsningen, er beskyttet mod virus mv. ved anvendelse af gængse og opdaterede antivirusprogrammer og lignende foranstaltninger. Parterne skal til stadighed overholde god it-sikkerhedspolitik, som fastlagt ved sædvane eller gældende standarder.

4. Organisatoriske krav hos Organisationen ved brug af brugeradministrationssystemet

Med henblik på, at sikre en forsvarlig administration af adgangskontrolordninger og autorisationer i forbindelse med Organisationens anvendelse af DMP's brugeradministrationssystem, skal Organisationen etablere processer for brugeradministration i egen organisation inkl. oprettelse, nedlæggelse, identifikation og autentifikation. Processerne skal tage højde for, at brugeres rettigheder til Miljøportalen tildeles i overensstemmelse med DMP's adgangspolitik, samt at de løbende holdes ajour, når brugerens arbejdsopgaver ophører eller ændres - eller når adgangspolitikken revideres.

Organisationen må alene oprette brugere i Miljøportalens brugeradministrationssystem, der har et berettiget formål med at få adgang til de databaser, der er tilkoblet brugeradministrationssystemet.

Organisationen skal instruere sine lokale brugeradministratorer om at overholde DMP's instruktioner hvad angår brugeradministration.

Organisationen skal opretholde den tekniske sikkerhed i egne systemer, herunder særligt beskyttelse af private nøgler, der anvendes som adgangs-token, samt systemer hvori rettighedsoplysninger administreres samt lagres.

I det omfang Organisationen har behov for at lade eksterne brugere udføre aktiviteter i databaserne på vegne af Organisationen, er Organisationen ansvarlig for de eksterne brugeres aktiviteter, og Organisationen forpligter sig til særligt at sikre, at disse eksterne brugere følger og overholder de samme retningslinjer, der er gældende for Organisationen.

Organisationen har ansvaret for at holde alle informationer, der er relateret til brugerens identitet (dvs. brugerattributter) og rolletildelinger, opdaterede. Organisationen har herunder ansvar for uden ugrundet ophold, at låse brugerkonti for brugere, der ikke længere arbejder hos - eller på vegne - af Organisationen.

Organisationen skal årligt gennemgå egne adgangspolitikker og instrukser med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i Organisationen og efterlever kravene fra DMP angående brugeradministration.

I bilag 2 er vedhæftet en vejledende tjekliste til brug for interne kontrolprocesser.

5. Tekniske standarder

Parterne skal anvende de til enhver tid gældende offentlige standarder i forbindelse med kommunikation om udstedelse af adgangs-token, herunder OIOSAML og OIO Basic Privilege Profile.

Såfremt Organisationen anvender den centrale opkobling til DMP's servere vil de tekniske krav til kommunikation om udstedelse af adgangs-token og deres autenticitetssikringsniveau automatisk være opfyldt.

6. DMP's logning

DMP logger alle Organisationens brugerdata i brugeradministrationssystemet, herunder personoplysninger og sikkerhedsrelaterede hændelser, afvigelser og brugeraktiviteter.

DMP logger ligeledes afviste adgangsforsøg baseret på afviste adgangs-token. En afvisning af et adgangs-token kan fx skyldes udløbet af et adgangs-token, en forkert signatur, manglende rettigheder osv.

DMP registrerer i loggen en unik nøgle til identifikation af brugeren, der anvender et adgangs-token til at tilgå data i de (fag)systemer, der kan tilgås via Miljøportalen. Det skal muliggøre samstilling af data med Organisationens log af brugerens aktiviteter i Miljøportalen.

DMP opbevarer af efterforskningsmæssige hensyn en transaktionslog i en periode på fem år fra seneste loghændelse(r).

7. Organisationens logning

7.1.Decentral logning

Organisationer, der indgår samarbejde om sammenhængende log-in i form af føderation med DMP via en lokal Identity Provider, skal i egne systemer logge udstedelse af alle adgangs-token, herunder hvilket akkreditiv, som blev anvendt til log-in. Loggen skal anvendes til konstatering af afviste adgangsforsøg, til at identificere brugerne og til opfølgning af sikkerheden (fx DS484, ISO 27001 med senere ændringer og versioner eller baseret på andre af parterne valgte principper, som sikrer en tilfredsstillende sikkerhed), samt til generel overholdelse af DMP's instruktioner. Organisationer skal i loggen registrere en unik nøgle til identifikation af brugerens adgangs-token. Det skal muliggøre samstilling af data med DMP's log.

Loggen skal omfatte oplysninger om, hvem der har tildelt rettigheder (administrator-id), hvilke medarbejdere der har fået rettigheden, hvornår den træder i kraft, samt hvornår den ophører. Det må ikke være muligt at tildele rettigheder uden at dette registreres i loggen.

Organisationen er forpligtet til at gemme alle hændelser i loggen samt opbevare disse data på en sikker og betryggende måde i seks måneder fra loghændelsen, hvorefter disse hændelser skal slettes af Organisationen.

7.2.Central logning

Organisationen kan vælge ikke at indgå samarbejde om sammenhængende log-in i form af føderation, men i stedet anvende DMP's centrale løsning, hvor logdata så vil blive etableret på DMP's servere.

Organisationen er desuagtet fortsat forpligtet til at foretage de samme gennemsyn af logdata, som hvis brugerdata var blevet lagret decentralt i egne servere i Organisationen.

Organisationen er således forpligtet til at overvåge alle væsentlige informationer i relation til identitetsinteraktioner (dvs. log-in og log-out-hændelser, passwordskift) og administrative aktiviteter (dvs. brugeradministrationsaktiviteter, loghændelser) i seks måneder fra loghændelsen.

Bemærk, at backup og sletning af logfiler i den centrale opkobling påhviler DMP.

8. Revision

Organisationens udstedelse af adgangs-token og efterlevelse af DMP's adgangspolitik indgår i Organisationens ordinære it-revision på linje med it-revision af adgangspolitikker, brugerrettighedsstyring og teknisk sikkerhed i interne it-systemer mv. Såfremt en it-revision viser, at Organisationen ikke kan leve op til kravene om sikkerhed og adgangspolitikker, skal dette straks meddeles til DMP med plan for afhjælpning.

9. Servicemål og support

Driften af brugeradministrationssystemet varetages på vegne af DMP af en driftsleverandør. Systemets oppetid er 99% på arbejdsdage i tidsrummet fra 8-17.

Organisationen varetager selv 1st level support direkte til dennes egne brugere. DMP tilbyder support i forbindelse med login på arbejdsdage i tidsrummet 9-14 via DMP's help-desk. Desuden tilbyder DMP 2nd level support til Organisationen i relevant omfang.

10. Samarbejde

Organisationen skal via funktionerne i DMP's brugeradministrationssystem oplyse, hvem der er den ansvarlige brugeradministrator i Organisationen. DMP kan til en til enhver tid kontakte brugeradministratoren vedr. sikkerhedsmæssige forhold.

Kontaktperson fra DMP om Miljøportalens brugeradministration oplyses af DMP's support via mail miljoeportal@miljoeportal.dk samt via telefon 7254 5454.

Hver part er forpligtet til at sikre den løbende opdatering af kontaktoplysningerne.

11. Tavshedspligt

Parternes administratorer, herunder dennes medarbejdere og eksterne brugere på vegne af Organisationen, der evt. arbejder med personhenførbare eller fortrolige data via Miljøportalen, er undergivet sædvanlig tavshedspligt.

12. Rettigheder

Aftalen medfører ikke nogen overdragelse af ejendoms- eller ophavsret til Miljøportalens databaser eller til Brugeradministrationssystemet til Organisationen.

Ansvaret for kvaliteten af brugerdata og fagdata, der inddateres af Organisationen i Miljøportalen samt, dokumentation og ajourføring heraf bæres af Organisationen.

DMP har ubetinget ret til at behandle og genanvende indberettet data i overensstemmelse med gældende lovgivning.

Såfremt Organisationen anvender værktøjer eller programmer til indlæsning og ajourføring af data og filer via Miljøportalen, skal Organisationen sikre, at denne besidder de nødvendige tilladelser og rettigheder hertil.

13. Opfølgning på brud på sikkerhed

Parterne har pligt til straks at underrette hinanden ved sikkerhedshændelser, som kan påvirke modparten. Parterne har pligt til uden forsinkelse at medvirke ved afdækning samt afhjælpning af sikkerhedshændelser, fx ved at gennemgå logs.

Såfremt Organisationens administratorer eller brugere forårsager sikkerhedsbrud, er Organisationen forpligtet til at rette alle fejl og mangler i relation til sikkerhedsbruddet uden ugrundet ophold efter disse er konstateret.

Parterne skal aktivt tage skridt til at sikre, at sikkerhedsbrud ikke kan gentages.

14. Ændringer og opgraderinger

DMP opgraderer løbende DMP's brugeradministrationssystem og/eller ændrer den tekniske eller organisatoriske infrastruktur i Miljøportalen i hhv. databaserne og/eller fagapplikationerne.

Større ændringer hos en eller begge parter som følge af væsentlige organisatoriske ændringer, der berører brugernes rettigheder, teknologiske opgraderinger, certifikatfornyelser, ændring DMP's adgangspolitik eller lignede, skal varsles mindst 90 dage inden ændringer foretages, således at den anden part kan afse ressourcer til at foretage eventuelle nødvendige ændringer.

Hver part er forpligtet til at afholde evt. egne udgifter i forbindelse med ændringer og tilpasninger af eget(egne) system(er) ved ændringer.

DMP påtager sig intet ansvar for eventuelle tab, meromkostninger o.l. hos Organisationen som følge af opgraderinger og/eller tekniske og organisatoriske ændringer.

Mindre ændringer kan ske med 30 dages varsel.

Varslinger om ændringer annonceres på DMP's hjemmeside, www.miljoeportalen.dk.

I det omfang DMP vurderer, der er behov for direkte ændring eller supplering af Aftalens vilkår som følge af tekniske, organisatoriske eller lovgivningsmæssige forhold, vil dette dog ske ved skriftlig henvendelse direkte til Organisationen.

15. Misligholdelse og ansvar

Parterne er hver især ansvarlige for overholdelsen af nærværende Aftale. Dansk rets almindelige regler om misligholdelse og misligholdelsesbeføjelser finder anvendelse for Aftalen.

I det omfang Organisationen udøver skade på brugeradministrationssystemet eller tilkoblede databaser, misbruger brugerdata eller indholdsdata og som forårsager et tab herved, er Organisationen forpligtet til at holde DMP skadesløs for enhver omkostning i forbindelse med det direkte tab, som DMP måtte have i forbindelse med udbedring af disse forhold. Erstatning ved direkte tab er begrænset til 5 mio. kr.

Der kan ikke kræves erstatning fra nogen af parterne for indirekte tab og følgeskader, såsom driftstab, tabt fortjeneste, rentetab og mistede besparelser. Tab af data anses for indirekte tab, bortset fra tilfælde, hvor dette skyldes Organisationens misbrug af adgangspolitikker og sikkerhedskrav eller anden datahåndtering, hvor dette er omfattet af Aftalen.

Foranstående begrænsninger gælder kun, såfremt tabet ikke kan henføres til grov uagtsomhed eller forsætlige forhold hos den skadevoldende part.

16. Ophævelse

Såfremt en part væsentligt misligholder sine forpligtelser, og ikke ophører hermed senest 10 dage efter skriftligt at være anmodet herom, kan den anden part skriftligt og uden varsel hæve Aftalen.

I tilfælde af alvorlige sikkerhedsbrud skal DMP træffe nødvendige foranstaltninger, fx ved straks at lukke for Organisationens adgangs-token samt eventuelt politianmelde væsentlige sikkerhedsbrud.

17. Overdragelse

Organisationen er ikke berettiget til at overdrage eller på anden måde overføre rettigheder og forpligtelser i henhold til Aftalen til tredjemand, uden skriftlig tilladelse fra DMP.

DMP kan overdrage rettigheder og forpligtelser til en anden organisation eller til tredjepart.

18. Lovvalg og tvister

Aftalen er undergivet dansk ret, og hvor ikke andet er anført gælder dansk rets almindelige regler i parternes indbyrdes forhold.

Såfremt der opstår en uoverensstemmelse mellem parterne i forbindelse med Aftalen, skal parterne med en positiv, samarbejdende og ansvarlig holdning søge at løse tvisten, evt. ved inddragelse af mediation.

Kan tvisten herefter fortsat ikke kan løses, er hver af parterne berettiget til at kræve tvisten løst endeligt ved de almindelige domstole.

19. Ikrafttræden og varighed

Aftalen er gældende ved begge parters underskrifter. Aftalen kan opsiges af begge parter med 6 måneders varsel.

Organisationen tilslutter sig hermed Aftalen med DMP med henblik på at få adgang til databaserne via Miljøportalens brugeradministrationssystem. Aftalen erstatter evt. tidligere aftaler indgået mellem parterne om adgang til Miljøportalens databaser via brugeradministrationssystemet.

Parternes underskrifter

Dato:	Dato:
Sekretariatsleder Nils Høgsted Danmarks Miljøportal	Underskriftsberettiget for Organisationen (juridisk ansvarlig)
	(Angiv underskriverens navn og stilling med blokbogstaver)

Bilagsfortegnelse:

Bilag 1: Instruks fra Organisationen (dataansvarlig) til Danmarks Miljøportal (databehandler).

Bilag 2: Tjekliste ved interne kontroller af de angivne processer og procedurer i Aftalen om anvendelse af Danmarks Miljøportals brugeradministrationssystem.

Bilag 1: Instruks fra Organisationen til Danmarks Miljøportal vedr. behandling af persondata

Danmarks Miljøportal handler alene efter instruks fra den dataansvarlige Organisation (brugerorganisation) vedr. behandlingen af personoplysninger om Organisationens medarbejdere. Behandlingen sker alene med henblik på, at Organisationens medarbejdere kan få adgang til databaser på Danmarks Miljøportal.

Danmarks Miljøportal skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger. DMP skal på den dataansvarliges anmodning give den dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

Danmarks Miljøportal skal ved behandlingen påse, at sikkerhedsbekendtgørelsen overholdes (jf. BEK. nr. 528 af 15/6 2000 med senere ændringer).

Bilag 2: Tjekliste

Tjekliste ved interne kontroller af de angivne processer og procedurer i Aftalen om anvendelse af Danmarks Miljøportals brugeradministrationssystem.	Relevant for Organisationen med decentral opkobling via sammenhængende login	Relevant for Organisationen med central opkobling til DMP's brugerkatalog (*)	Sæt X for opfyldt
1. At Organisationen har gennemgået og kommunikeret i egen organisation vedr. brugen af Danmarks Miljøportals skriftlige instruktioner (vejledninger og adgangspolitik/rollebeskrivelser mm) inden Organisationens anvendelse af Danmarks Miljøportals brugeradministrationssystem, se www.miljoeportalen.dk.	X	x	
2. At en sikkerhedspolitik - ex DS484/ISO 27001 eller baseret på andre af parterne valgte principper, som sikrer en tilfredsstillende sikkerhed - er vedtaget og implementeret.	x	x	
3. At adgangs-token kun udstedes til de personer, som autoriseres hertil.	x	x	
4. At Danmarks Miljøportals krav til adgangs-token overholdes herunder, at der angives et korrekt autenticitetssikringsniveau (mål for hvor sikkert medarbejderen er autentificeret), og at rettigheder kun optræder i billetten, hvis de er tildelt af en brugeradministrator.	x		
5. At rettigheder til Danmarks Miljøportals databaser tildeles til brugere i overensstemmelse med den adgangspolitik (rollebeskrivelse) som er defineret for fagsystemet.	x	x	
6. At der er fastlagt procedurer for, at brugere ved jobændring får opdateret deres rettigheder til Miljøportalens databaser.	x	X	
7. At logfiler er beskyttet mod uautoriseret adgang - herunder sletning og ændring af indhold, samt at der jævnligt tages backup af logfiler.	x		
8. At it-systemer, som udsteder adgangs-token eller anvendes til brugeradministration, er beskyttet mod uautoriseret adgang.	x		
9. At der er etableret en procedure om omgående alarmering af Danmarks Miljøportal, hvis der opstår tegn på misbrug, brud på sikkerhed eller andre forhold, der kan lede til uautoriseret adgang til Danmarks Miljøportals databaser, herunder	x	x	

afviste adgangsforsøg.			
10. At alle systemer involveret i udstedelse af adgangs-token indgår i listen over systemer, der underkastes en årlig it-revision.	x		
11. At egne adgangspolitikker og instrukser gennemgås en gang årligt med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i Organisationen.	x	x	
12. At logfilerne slettes løbende af Organisationen efter 6 måneder hos Organisationen	x		
13. At logfilerne skal slettes løbende af Danmarks Miljøportal efter 5 år.		x	

(*) Bemærk, at såfremt Organisationen anvender den centrale opkobling vil de tekniske krav til adgangs-token og deres autenticitetssikringsniveau automatisk være opfyldt. Desuden vil backup og sletning af logfiler påhvile DMP.