**DATABEHANDLERAFTALE**

Mellem

Kunden

CVR. nr.:

(herefter ”Kunden”)

Underskrivers navn:

Underskrivers e-mail:

og

Væksthus Syddanmark

Forskerparken 10

5230 Odense

CVR. nr.: 30089448

(herefter ”Leverandøren”)

er der indgået nedenstående databehandleraftale (herefter ”Databehandleraftalen”) om Leverandørens behandling af personoplysninger på vegne af kunden (dataansvarlige) ved brug af *Væksthusenes fælles CRM-system* (ESCRM):

# Generelt

* 1. Leverandøren og Kunden har indgået en aftale om Kundens adgang til Leverandørens ESCRM-system. Dette indebærer, at Leverandøren behandler personoplysninger på vegne af Kunden. Denne databehandleraftale skal regulere de persondataretlige konsekvenser af dette samarbejde.
	2. Databehandleraftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:
1. Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).
2. Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).
	1. Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at databehandleraftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.
	2. I Databehandleraftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.
	3. Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse, i det omfang andet ikke fremgår af Databehandleraftalen.
	4. Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
3. **Formål**
	1. ESCRM er ejet af Væksthusene i Danmark og kan anvendes af erhvervsfremmeaktører i regi af Væksthusene, kommuner, regioner, lokal erhvervsservice mv. til at registrere og udveksle informationer om virksomheder, som er i kontakt med erhvervsfremmesystemet.

Systemet er udviklet med sigte på fællesskab, samarbejde og ensartethed i erhvervsfremmeindsatsen og er skræddersyet til erhvervsservicesystemet. Det er et mål, at systemet kan understøtte koordinering af det virksomhedsopsøgende arbejde på tværs af erhvervsfremmeaktører.

Registreringer i systemet danner grundlag for effektmåling af erhvervsfremme systemet og data kan udleveres til Erhvervsstyrelsen, Kommunernes Landsforening og Danmarks Statistik. Udleveret data anvendes udelukkende til statistik og må kun publiceres i agregeret form. Der udleveres ikke detaljeret data.

I CRM-systemet registreres virksomhedskontakter, hvilket giver overblik og mulighed for at lave relevante udtræk om brugerne af erhvervsfremme. Ligeledes muliggør ESCRM en registrering af medarbejdernes timer og kørsel, der kan eksporteres til økonomisystemer.

Derudover er ESCRM tilsluttet *Den fælleskommunale Virksomhedskontaktdatabase* (FVDB).

Formålet med databasen er at understøtte virksomhedsindsatsen på tværs af kommuner, væksthuse og erhvervscentre mv., så mødet med virksomhederne bliver mere koordineret og mere professionelt.

Databasen består af en løsning der gør det muligt for kommunerne at udveksle relevante oplysninger om virksomhedskontakt og -besøg på tværs af kommuner og på tværs af jobcentre, væksthuse og erhvervscentre. Løsningen vil digitalt understøtte en koordineret virksomhedskontakt på tværs af kommune- og organisationsgrænser og dermed skabe grundlag for at pro-fessionalisere indsatsen.

# Kundens rettigheder og forpligtelser

* 1. Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle i ESCRM.
	2. Kunden har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Databehandleraftalens pkt. 1.1 og 1.2.
	3. Kunden er forpligtiget til løbende at være bekendt med nyeste version af bilag 4 og 5 DPO Orienteringsark og Admin Orienteringsark. De opdatere versioner af bilagne kan findes på blog.escrm.dk.

# Leverandørens forpligtelser

* 1. Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kunden, jf. pkt. 6 og bilag 3.
	2. Leverandøren behandler alene de overladte personoplysninger efter instruks fra den dataansvarlige (Kunden), jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af formålet med ESCRM.
	3. Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.
	4. Leverandøren skal på opfordring fra Kunden hjælpe med at opfylde Kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra individuelle personer om indsigt i egne oplysninger, udlevering af dennes oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af personens oplysninger, samt Kundens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
	5. Leverandøren skal fra 25. maj 2018 hjælpe Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.
	6. Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

# Underleverandør (underdatabehandler)

* 1. Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kunden.
	2. Leverandøren har ret til at anvende andre underdatabehandlere end dem, som er angivet i bilag 2, til at behandle de personoplysninger, som Kunden har overladt til Leverandøren i medfør af Hovedaftalen. Leverandøren skal ajourføre oplysninger om underdatabehandlere i bilag 2 ved enhver ændring. Kunden har ret til at gøre indsigelse mod brugen af en underleverandør inden 7 dage efter ajourføringen.
	3. Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
	4. Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Databehandleraftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
	5. Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.
	6. Kunden kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kunden.

# Instrukser

* 1. Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks.

* 1. Leverandøren giver fra 25. maj 2018 omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

# Tekniske og organisatoriske sikkerhedsforanstaltninger

* 1. Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:
1. tilintetgøres, mistes, ændres eller forringes,
2. kommer til uvedkommendes kendskab eller misbruges, eller
3. i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1
	1. Leverandøren skal iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
	2. Leverandøren er forpligtet til indenfor 72 timer at underrette Kunden om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

# Overførsler til andre lande

* 1. Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, kræver de dataansvarliges forudgående accept.
	2. Ved overførsel til tredjelande er Leverandøren og Kunden i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.
	3. Hvis Kundens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes, såfremt den anden medlemsstats regler finder anvendelse.

# Tavshedspligt og fortrolighed

* 1. Leverandøren er – under og efter aftalens ophør – pålagt fuld tavshedspligt om alle oplysninger, denne bliver bekendt med gennem samarbejdet. Underdatabehandleraftalen indebærer, at tavshedspligtbestemmelserne i straffelovens §§152-152f, jf. straffelovens § 152a, finder anvendelse.
	2. Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af Databehandleraftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

# Kontroller og erklæringer

* 1. Leverandøren er forpligtet til uden ugrundet ophold at give Kunden nødvendige oplysninger til, at Kunden til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne Databehanlderaftale, når Kunden anmoder om dette.
	2. Kunden, en repræsentant for Kunden eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Databehandleraftale.
	3. I tilfælde af, at Kunden og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og Leverandørens underleverandører at stille tid og ressourcer til rådighed herfor. Leverandøren kan kræve et rimeligt vederlag herfor, der skal dække Leverandørens omkostninger

# Ændringer i Databehandleraftalen

* 1. Ændringer i aftalen sker ved enighed mellem parterne. Ændringer skal være skriftlige og fremgå af et tillæg til denne databehandleraftale, medmindre andet aftales.
	2. Aftalen ændres ved enighed.

# Sletning af data

* 1. Kundens data slettes efter ophør af Hovedaftalen. Dog bliver stamdata om virksomheder og deres kontraktpersoner i ESCRM ikke slettet, da denne stamdata også deles med andre brugere af ESCRM. Disse stamdata er opmfattet af systemets automatiske og manulle oprydningsrutiner.
	2. Leverandøren sletter alle data, i form af noter, filer og projektnoter natten efter aftalens udløb. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever sletning.
	3. Leverandøren har ret til at anonymisere data omhandlet af aftalen. Leverandøren ejer denne anonymiserede data og kan dele den med andre.

1. **Ikrafttræden og varighed**
	1. Databehandleraftalen træder i kraft ved begge Parters underskrift.
2. **Underskrift**
	1. Databehandleraftalen skal foreligge skriftligt hos Kunden og Leverandøren.

For Kunden For Væksthus Syddanmark

Dato Dato: 07.03.2018

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Jani Lykke Methmann

**Bilag:**

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

Bilag 3 – Instruks

Bilag 4 – DPO Orienteringsark

Bilag 5 – Administrator Orienteringsark

Bilag 1 – Sikkerhed

# Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

# Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

* tilintetgøres, mistes, ændres eller forringes,
* kommer til uvedkommendes kendskab eller misbruges,
* eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

**Generelle sikkerhedsforanstaltninger**

Leverandøren, herunder underdatabehandleren (ID Solutions), har tilrettelagt databehandlingen som følgende:

* + Databehandlingen finder sted på servere ejet af ID Solutions, som fysisk befinder sig i et hostingcenter i Danmark (adressen fremgår af bilag 2)
	+ Adgang til hostingcentret er begrænset til særligt betroede teknikere
	+ Hostingcentret har brandsikring, videoovervågning og nødstrøm
	+ Data lagres på spejlede diske, og der tages dagligt backup.
	+ Daglig administration af servere finder sted på ID Solutions kontor (adressen fremgår af bilag 2), som kommunikerer med hostingcentret via VPN.
	+ ID Solutions administratorer kan endvidere oprettte VPN-forbindelse til servere fra andre lokationer med henblik på akut fejlretning.
	+ Udvikling af systemet finder sted på ID Solutions kontor (adressen fremgår af bilag 2) eller via fjernadgang, hvorved der ikke lagres data på udviklers lokale PC.
	+ Der benyttes en udviklingsdatabase, hvori data er en obfuskeret version af driftsdata
	+ Administration af servere finder sted ved fjernadgang, hvorved der ikke lagres data på administratorers lokale PC.
	+ Ved udskiftning af diske slettes data enten ved overskrivning af samtlige sektorer eller ved fysisk destruktion.
	+ ID Solutions instruerer sine administratorer om generelle sikkerhedsforanstaltninger og fortrolighed af data.

**Autorisation og adgangskontrol**

ID Solutions:

* + Administratorer er de eneste hos ID Solutions, som har nogen form for adgang til systemet og dets data. ID Solutions udfører ingen manuel databehandling.
	+ Kun særligt betroede medarbejdere kan godkendes som administratorer
	+ Administratorernes adgang sikres ved en kombination af VPN-certifikat og server-password
	+ Login på servere logføres, både når de lykkedes og når de afvises.

**Inddatamateriale som indeholder personoplysninger**

Systemet anvender ikke inddatamateriale i fysisk form. For så vidt angår inddata i elektronisk form er sikkerhedsforanstaltningerne oven- og nedenfor.

**Uddatamateriale som indeholder personoplysninger**

Systemet anvender ikke uddatamateriale i fysisk form. For så vidt angår uddata i elektronisk form er sikkerhedsforanstaltningerne oven- og nedenfor.

**Eksterne kommunikationsforbindelser**

*[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om eksterne kommunikationsforbindelser. Hjælp til udfyldelse kan findes i Datatilsynets it-sikkerhedstekster:* [*https://www.datatilsynet.dk/publikationer/it-sikkerhedstekster/*](https://www.datatilsynet.dk/publikationer/it-sikkerhedstekster/)*]*

* + Systemet anvender internettet som databærer for VPN mellem hostingcenter og ID Solutions.
	+ Til VPN benyttes et standardsystem (OpenVPN)
	+ VPN kræver autorisation i form af et særligt certifikat, og al kommunikation foregår krypteret.
	+ Servere er beskyttet af en firewall, som kun har nødvendige porte åbne.

**Kontrol med afviste adgangsforsøg**

Afviste adgangforsøg undersøges reaktivt.

**Logning**

Logning finder sted mhp. fejlfinding.

**Hjemmearbejdspladser**

Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser [*Leverandøren udfylder*]:

◼ Ja

🞏 Nej

ID Solutions anvender undtagelsesvist hjemmearbejdspladser til systemadministration. Dette sker under samme iagttagelse af sikkerhedsforskrifter som gælder på kontoret.

#  Sikkerhedskrav fra 25. maj 2018 [*Se kommentarer*]

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk

2. Implementeringsomkostningerne

3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)

4. Konsekvenserne for registrerede ved et sikkerhedsbrud

5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:

a) tilintetgørelse af oplysningerne

b) tab af oplysningerne

c) ændring af oplysningerne

d) uautoriseret videregivelse af oplysningerne

e) uautoriseret adgang til oplysningerne

ID Solutions iagttager sikkehedsforanstaltninger som nævnt ovenfor.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. **Lokation(er) for behandlingen**

ID SOLUTIONS ApS

Vandtårnsvej 62 A

2860 Søborg

CVR.nr. 27555373

ID Solutions hostingscenteradresse:

ID Solutions ApS hostingcenteradresse:

v/ Rackhsting ApS

Hørskætten 6 C

2630 Taastrup

Bilag 3 – Instruks

**Instruks**

Kunden herefter (”Kunden”) instruerer hermed Leverandøren om at foretage behandling af Kundens oplysninger til brug for drift af løsningen, Væksthusenes fælles CRM-system samt udveksling med Fælleskommunal Virksomhedskontaktdatabase (FVDB).

**Behandlingens formål**

Behandling af Kundens oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

**Generel beskrivelse af behandlingen**

Systemets navn er "Væksthusenes fælles CRM-system" (ESCRM)

Formålet med systemet er, at registrere og udveksle informationer om virksomheder, som er i kontakt med erhvervsfremmesystemet. I systemet registreres virksomhedskontakter, hvilket giver overblik og mulighed for at lave relevante udtræk om brugerne af erhvervsfremme. Ligeledes muliggør CRM en registrering af medarbejdernes timer og kørsel, der kan eksporteres til økonomisystemer.

Derudover udveksler systemet informationer med den ”Fælleskommunale Virksomhedskontakt Database” (FVDB). Formålet med denne udveksling er at understøtte virksomhedsindsatsen på tværs af kommuner og på tværs af væksthuse, jobcentre og erhvervscentre.

Underdatabehandleren (ID Solutions) varetager alene driften af servere og opdatering af systemerne hvorpå systemet hostes. Derudover foretages support og udvikling alene efter instruks/specifikation fra Leverandøren.

**Typen af personoplysninger**

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier.Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1*.*

**ESCRM er beregnet til almindelige personoplysninger**, jf. Databeskyttelsesforordningens artikel 6 og cpr-numre (personumre). Såfremt Kunden ønsker behandling af andre typer af oplysninger, skal han indgå en tillægsaftale til denne databehandleraftale.

* 1. **Kategorier af registrerede**

Der behandles typisk oplysninger om følgende kategorier af registrerede:

A) Kontaktpersoner i virksomheder

B) Iværksættere

C) Konsulenter i væksthuse, erhvervscentre og jobcentre

**Tredjelande (ikke EU-medlemslande)**

Leverandøren skal indhente forudgående accept, inden der kan foretages en tredjelandsoverførsel, medmindre overførslen er påkrævet efter gældende ret.

Bilag 4 – DPO Orienteringsark

Du modtager denne info da du er udpeget som DPO for din enhed, i relation til ESCRM. I dette dokument finder du oplysninger om hvad du konkret skal gøre i relation til jeres arbejde og dataregistreringer i ESCRM. Om din enhed har brug for en formel DPO der lever op til DPO kravene i GDPR eller ej, det forholder vi os ikke til i dette dokument.

**DPO forpligtigelser i forbindelse med ESCRM:**

Uanset om din rolle som DPO er formel eller uformel skal du sikre, at enheden overholder de forpligtelser som forordningen beskriver i arbejdet med systemet.

Disse forpligtelser omfatter:

* sikre at registreringer der foretages i ESCRM, af brugere i din enhed, er i overensstemmelse med GDPR.
* holde dig ajour med opdateringer vedrørende denne rolle. Find den seneste version af dette dokument på bloggen. (http://blog.escrm.dk)
* sikre at personer som enheden behandler data for, i ESCRM, er behørigt orienteret og/eller et samtykke/kontrakt er udfyldt.
* orientere ESCRM v/Væksthus Syddanmark, om eventuel systematisk registrering af følsomme data, således at vi er bekendt med denne praksis. Dette er især relevant i forhold til datalæk.
* i samarbejde med administrator sikre, at felter på stamdata og i projektnoter er klassificeret korrekt. Klassifikation sker indenfor følgende kategorier; almindelige data, enhedsvæsentlige data (= almindelige data i forhold til forordningen), CPR-nummer, personhenførbare og følsomme data.
* i samarbejde med administrator sikre, at felter på stamdata og i projektnoter har korrekt anonymiseringsindstilling. Dette skal sikre at man ikke, heller ikke sammen med andre informationer, kan regne ud hvem en anonymiseret person var.
* informere brugerne, i enheden, omkring, hvorledes man korrekt angiver udløbsindstillinger på noter og dokumenter, samt hvilke kriterier der bør overvejes i forbindelse med indstilling af udløbet.
* informere brugerne om hvornår data er personhenførbart og/eller følsomt.
* informere brugerne om hvordan man registrerer, at en note eller en fil indeholder følsomme oplysninger.
* sikre, sammen med administrator, at brugere har personligt login. Dette er et krav i forhold til at sikre korrekt logning.

**Personfølsomt data:**

Det er enhedens ansvar at være bekendt med karakteren af de behandlede data, b.la. hvorvidt der, jf. persondatalovens § 7, er tale om personfølsomme oplysninger eller ikke-personfølsomme oplysninger. Er der tale om personfølsomme oplysninger vil det betyde et skærpet fokus på beskyttelsen samt håndteringen af disse data. Dette sikres i ESCRM via opsætning som enhedens administratorer kan foretage efter instruks fra dig. Globale felter er klassificeret af ESCRM, denne klassifikation kan ikke ændres i enheden.

Definitionen på personfølsomme data er, jf. persondataloven § 7; racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold. Denne opregning er udtømmende.

CPR-nummer er teknisk set ikke personfølsomme oplysninger, men det tillægges, jf. persondatalovens § 11, stor sikkerhed og der findes derfor tilsvarende strenge krav i forhold til databehandling af CPR, som der gør med personfølsomme oplysninger. Der er i ESCRM oprettet en særskilt klassifikation af CPR-numre.

Når en bruger vil læse følsomt data i ESCRM vil brugeren fremover blive mødt med en information om at denne læsning vil blive logget. Her kan brugeren acceptere og se data, eller afvise og data vil være skjult. Loggen opbevares i ESCRM så længe som den person/virksomhed informationen er gemt på behandles i systemet. Dvs. først når en kontakt anonymiseres slettes logningen. Læsning af følsomme data skal oplyses såfremt en person beder om indsigt i registreringer på deres person.

**Anonymisering:**

DPO skal sikre at alle felter er opsat med korrekt anonymiseringsindstilling, det er i praksis administrator som opsætter indstillingen. ESCRM vil løbende foretage en automatisk anonymisering af kontakter, virksomheder og projektnoter registreret i systemet. For at det kan lade sig gøre er det en nødvendighed, at alle data indstilles med korrekte indstillinger for at denne proces kan fungere. Ligeledes er det et krav at alle udløb er opsat korrekt. Herefter vil alt data, der kan henføres til en bestemt person i systemet, blive slettet eller erstattet – mens data, der ikke er personhenførbart, vil blive tilbage, f.eks. postnummer og by. Dette er i fuld overensstemmelse med forordningen, og sikrer at enheden stadig kan lave statistikker der kører mange år tilbage. Eksempelvis, hvis en given person har været i et givent vækstforløb, vil der stå tilbage at der engang har været en – nu anonymiseret person – i dette forløb – alt data og øvrige kommentarer om forløbet står stadig tilbage – bare intet om den pågældende person.

Klassifikationen, som sker på feltniveau i Projektnoter og på stamdata, kan sættes til almindelige data, enhedsvæsentlige data, CPR-nummer, personhenførbare data eller følsomme data. Ved anonymisering ryddes eller erstattes indholdet i felter markeret med CPR, personhenførbar og følsom. Andre steder er det hele registreringen, f.eks. noter og dokumenter, der klassificeres. Disse registreringer kan ikke anonymiseres og skal enten slettes eller beholdes, de klassificeres som enten indeholdende eller ikke indeholdende persondata og som følsomme eller ikke følsomme data. Bemærk indeholder noter eller filer persondata eller følsomme data, så skal registreringen slettes når det ikke længere er relevant at behandle disse data.

**Formel beskrivelse vedrørende DPO-rolle klippet fra forordningen.**

DPO-forpligtelser for enheder der er omfattet af GDPR artikel 37, punkt 1-3:

Enheder der, jf. artikel 37, er omfattet af følgende kategorier, skal udpege en DPO der lever op til GDPR’s forventninger af en DPO. Disse enheder omfatter følgende:

a) Enheder der kan kategoriseres som værende en offentlig myndighed eller et offentligt organ1.

b) Enheder hvor den primære aktivitet af databehandler eller dataansvarlig inkluderer jævnlig og systematisk overvågning af dataenheder på en stor skala; eller

c) Enheder hvor den primære aktivitet af databehandler eller dataansvarlig inkluderer bearbejdning af store mængder af personfølsomt data.

Krav for DPO’er, jf. GDPR – Artikel 39.

Stk. 1. Databeskyttelsesrådgiveren har som minimum følgende opgaver:

at underrette og rådgive den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til denne forordning og anden EU-ret eller national ret i medlemsstaterne om databeskyttelse.

at overvåge overholdelsen af denne forordning, af anden EU-ret eller national ret i medlemsstaterne om databeskyttelse og af den dataansvarliges eller databehandlerens politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteter, og de tilhørende revisioner.

at rådgive, når der anmodes herom, med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til artikel 35.

at samarbejde med tilsynsmyndigheden.

at fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.

Stk. 2. Databeskyttelsesrådgiveren tager under udførelsen af sine opgaver behørigt hensyn til den risiko, der er forbundet med behandlingsaktiviteter, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål.

Bilag 5 – Admin Orienteringsark

Du modtager denne info da du er opsat som Administrator for din enhed i ESCRM. I dette
dokument finder du oplysninger om hvad du konkret skal gøre i relation til jeres arbejde og dataregistreringer i ESCRM, særdeles i forhold til GDPR. I din enhed har I ligeledes udpeget, eller skal udpege, en DPO. DPO skal sikre at der leves op til kravene i GDPR, det forholder vi os ikke til i dette dokument, da DPO’en har eller vil modtage særskilt orientering. Der kan i enheden være flere administratorer, men kun en DPO.

**Administrator-forpligtigelser i forbindelse med ESCRM:**
Som administrator i ESCRM er der en række forpligtigelser som du skal efterleve.

Disse forpligtigelser omfatter:

* sikre at brugere har personligt login. Dette er et krav i forhold til at sikre korrekt logning.
* sikre nedlæggelse af brugerne når de stopper i organisationen.
* i samarbejde med DPO sikre, at felter på stamdata og i projektnoter er klassificeret korrekt.
DPO’en er ansvarlig for klassifikationen, i overensstemmelse med GDPR, men har måske
ikke selv administrator adgang og kan derfor (måske) ikke selv sætte klassifikationen.
* sikre at positivlisten på enhedsvæsentlige felter er korrekt opsat
* i samarbejde med DPO sikre, at felter på stamdata og i projektnoter har korrekt
anonymiseringsindstilling. Alle felter som indeholder CPR-nummer, personhenførbare data eller følsomme data skal have angivet en anonymiseringsindstilling. Dette skal sikre at man ikke, heller ikke sammen med andre informationer, kan regne ud hvem en anonymiseret person var.
* informere brugerne, i enheden, omkring, hvordan man angiver udløbsindstillinger på noter og dokumenter.
* informere brugerne om hvordan man registrerer, at en note eller en fil indeholder
følsomme oplysninger.
* sikre at rollen som administrator overdrages til en kollega hvis din ansættelse/rolle ændrer sig, i en sådan grad at det er nødvendigt, i forhold til enhedens arbejde med ESCRM. Kun relevant såfremt enheden kun har en administrator.

**Klassifikation og anonymiserings indstillinger:**
Det er administratorens rolle, at markere og kategorisere de data enheden systematisk
bearbejder. Dette foregår i feltdesigneren, enten for stamdata eller projektnoter. Her kan felter
markeres som indeholdende henholdsvis; ”alm. data”, ”enhedsvæsentlig”, ”personhenførbar”,
”CPR” og ”følsom”.

Almindelige data er data som ikke kan benyttes til at identificere en person og ikke er klassificeret i en af de øvrige klassifikationer. Enhedsvæsentlige data er data som i natur er almindelige data, men har en værdi for enheden der gør at virksomheder og personer med disse data ikke anonymiseres. Her skal vedligeholdes en positivliste over indhold som forhindre anonymisering. Eksempelvis kunne et rullegardin/dropdown-felt ”medlems status” været opsat som enhedsvæsentligt med mulighederne ”ikke medlem” og ”aktivt medlem”, her skal kun ”aktivt medlem” være på positivlisten. CPR-nummer er til markering af felter der indeholder CPRnummer, læsning af disse informationer logges og skal udleveres når en person benytter retten til indsigt. Personhenførbare data er oplysninger der kan benyttes til at identificere en person og disse skal slettes eller ændres når kontaktpersoner anonymiseres. Følsom angiver at adgang til data skal logges, der skelnes ikke mellem personfølsom og virksomhedsfølsom i opsætningen.

**Anonymisering:**
I forhold til henvendelser fra personer, der ønsker anonymisering, då skal administratorer forsøge at anonymisere via knappen i systemet. Hvor administrator ikke kan anonymisere personen, grundet f.eks. låst data, som kan opstå ved brugerevalueringer eller projektdeltagelse i andre enheder. I disse tilfælde vil systemet kompilere en meddelelse med årsagen til at den pågældende ikke kan anonymiseres, samt hvornår det eventuelle udløb for fastlåsningen er. Ligeledes vil angivelse af enheder med låsen fremgå, således personen kan henvende sig hos enheden med eventuelle spørgsmål i forhold til låsen. Derfor er det meget vigtigt at DPO har informeret grundigt om hvornår man kan angive et udløb med lås.