Regionshuset
Viborg

Regionssekretariatet
Skottenborg 26
Postboks 21
DK-8800 Viborg
Tel. +45 8728 5000
kontakt@rm.dk
www.rm.dk

Vejledning til skabelonen "Databehandleraftale_feb2015"

Skabelonen "Databehandleraftale_feb2015" er opbygget på den måde, at man skriver egen tekst i stedet for den eksisterende, hvor denne er markeret med gult. Man skal med andre ord slette den eksisterende tekst i de felter, der udfyldes.

Ordlyden i punkterne 2-11 og 13-14 må ikke ændres. Hvis det er nødvendigt at supplere standardformuleringerne i disse punkter, skal dette beskrives i pkt. 15, inden den redigerede databehandleraftale underskrives.

Notatet anvender følgende systematik:

A. Felter der skal udfyldes eller ændres
B. Felter der ikke skal udfyldes eller ændres

Nedenfor redegøres først for de felter, der skal udfyldes (A). Dernæst beskrives baggrunden for de felter, der ikke må ændres ved (B).

A. FELTER DER SKAL UDFYLDES ELLER ÆNDRES

0. Forsiden (præamblen)

"Journalnummer"
Journalnummeret er det nummer i ESDH eller tilsvarende elektronisk journalsystem, der gør det muligt at identificere sagen entydigt og hvor det øvrige kontraktkompleks (alle dokumenter, der har relevans for aftalen) journaliseres.

"Projektnavn/titel/system og beskrivelse"
Projektets navn skal gøre det muligt på en entydig måde at identificere projektet. Formålet er at skabe genkendelighed uden nødvendigvis først at skulle slå op i ESDH.

"Navn, e-mail, dato"
Navn og e-mail skal henvise til den person, der har udfyldt databehandleraftalen.

Datoangivelsen skal angive den dato, hvor databehandleraftalen er blevet udarbejdet.

"Afdeling"
Navnet på den afdeling eller delorganisation i Region Midtjylland, der er ansvarlig for kontraktindgåelsen med den eksterne leverandør.

Formålet er at sikre, at man på et senere tidspunkt kan finde ud af, hvilken afdeling der har journaliseret aftalekomplekset. Dette kan eksempelvis være relevant i forbindelse med et tilsyn fra Datatilsynet.

"Firmanavn, adresse, CVR-nummer" m.v.
Ud fra disse oplysninger skal det være muligt at identificere leverandøren entydigt. Derfor er det en fordel at angive CVR-nummer – se evt. www.cvr.dk, hvis der er tale om et dansk selskab.

Man kan med fordel henvise til leverandørens underafdeling eller kontaktperson i denne forbindelse.

"Aftale af xx. xxxxxx 201x om leverance af …"
Her skal der henvises til den kontrakt (hoveddokumentet), der regulerer regionens indkøb. Grunden til at der skal henvises til denne kontrakt er, at den udgør det mest centrale dokument i det aftalegrundlag, som databehandleraftalen er et supplement til.

Det er meget vigtigt at henvise til det samlede aftalekompleks på en entydig måde (angivelse af dato for aftalens indgåelse hjælper eksempelvis). Brug derfor helst ordret den samme beskrivelse af kontrakten, som den selv anvender.

Databehandleraftalen bør ideelt set indgå som et bilag til hovedkontrakten. Dette er med til at tydeliggøre samhørigheden mellem de to dokumenter.

1. Databehandlerens opgave

I dette felt skal databehandlerens ydelse kort beskrives. De fire punkter er alene en inspiration til udformning en løbende tekst. Det er dog vigtigt at understrege, at beskrivelsen af databehandlers opgave typisk ikke vil være tilstrækkeligt præcis, hvis man ikke har beskrevet følgende fire punkter i et eller andet omfang:

1) Databehandlerens opgave, herunder formålet med databehandlingen
2) Kategorier af registrerede borgere, som databehandlingen omfatter
3) Kategorier af oplysninger, som databehandlingen omfatter.
4) Hvor data opbevares [fysisk placering af data/servere]

Ad 1. Regionen og vores databehandlere må kun behandle data i overensstemmelse med det formål, de er indsamlede til. Derfor skal det beskrives, hvordan databehandleren bidrager til dette formål.

Ad 2. Med "kategorier af borgere" menes en generel beskrivelse af de borgere, man har indsamlet data om – eksempelvis at de er 60-70 år, at de frivilligt har valgt at udfylde spørgeskema, at de er udvalgt på baggrund af en bestemt diagnosekode eller lignende.

Ad 3. Når der tales om "kategorier af oplysninger", tænkes der på de kategorier, som persondataloven beskriver. Det vil sige følgende:

a. racemæssig eller etnisk baggrund,
b. politisk, religiøs eller filosofisk overbevisning,
c. fagforeningsmæssige tilhørsforhold
d. helbredsmæssige og seksuelle forhold
e. strafbare forhold
f. væsentlige sociale problemer
g. andre rent private forhold (f.eks. ulykkestilfælde med væsentlige personlige eller sociale konsekvenser, selvmord og forsøg derpå, familiestridigheder, separations- og skilsmissebegæringer, adoptionsforhold, oplysninger om en medarbejders positive alkohol- eller narkotikatest samt om afvisning, hjemsendelse eller bortvisning fra en arbejdsplads).
h. CPR-numre, og
i. almindelige personoplysninger (der ikke er omfattet af pkt. a-h)

Ad 4. For at regionen skal kunne kontrollere Databehandlers aktiviteter (evt. ved en senere audit), er det nødvendigt at beskrive, hvor data fysisk opbevares.

Et eksempel på en beskrivelse af databehandlers opgave kunne være følgende:

"Formålet med projektet er statistisk at undersøge sammenhængen mellem anvendelsen af lægemiddel X og patienternes oplevelse af behandlingsforløbet på afdeling Y. I denne forbindelse bidrager konsulentvirksomhed Z med vikarer (som beskrevet i kontrakten), der skal hjælpe med at inddatere og kategorisere de indkomne besvarelser, som respondenterne har indleveret via spørgeskemaerne.

Undersøgelsen omfatter alle patienter, der har været indlagt på afdeling Y og som frivilligt har valgt at deltage. Der vil i forbindelse med undersøgelsen blive behandlet CPR-numre, helbredsoplysninger og almindelige personoplysninger såsom alder og køn.

Serveren er fysisk placeret ved Region Midtjylland (Olof Palmes Allé 19, lokale L207). Databehandler har alene adgang til serverne fra computere, som regionen stiller til rådighed på adressen.

Punkterne 2-11
Se nedenfor.

12. Underskrifter
Region Midtjylland har besluttet, at Kenneth Becker (CISO) underskriver alle regionens databehandleraftaler.

Den fysiske person der skriver under på vegne af Databehandleren skal være tegningsberettiget for det selskab, forening el.lign., som vedkommende binder kontraktuelt.

Databehandleren har formentlig sine egne retningslinjer der fastslår, hvem der er tegningsberettiget. Før vedkommende underskriver databehandleraftalen har den projektansvarlige (ansat ved Region Midtjylland) pligt til at undersøge, om vedkommende har ret til at indgå aftaler på vegne af Databehandleren.

Punkterne 13-14
Se nedenfor

15. Ændringer til punkterne 2-11 og 13-14
Hvis det er tvingende nødvendigt at ændre punkterne 2-11 eller 13-14, skal ændringerne beskrives her. Det vil i disse tilfælde være formuleringerne i pkt. 15, der regulerer aftaleforholdet mellem den Dataansvarlige og Databehandleren.

Med punkt 15 anerkender regionen, at der kan være individuelle forhold, der medfører behov for en særlig bestemmelse i databehandleraftalen. Dette kunne eksempelvis være en bestemmelse om revisionserklæringer

som alternativ eller supplement til audits (se punkt 7) eller en bestemmelse om fastsættelse af bod.

Hvis man beskriver fravigelser fra punkter 2-11 eller 13-14 i punkt 15, skal man indsende den endelige databehandleraftale til Juridisk Kontor, der så har mulighed for at komme med en udtalelse om ændringerne inden den endelige aftale underskrives.

Om it-revisionserklæringer:
Hvorvidt regionen skal kræve årlige revisionserklæringer vil være en individuel vurdering. Der skal i hvert enkelt tilfælde foretages en konkret vurdering af hvilke kontrolforanstaltninger der må anses for nødvendige.

Det følger af vejledningen til sikkerhedsbekendtgørelsen, at Region Midtjylland som dataansvarlig aktivt skal sikre, at de krævede sikkerhedsforanstaltninger overholdes hos databehandleren, og at det i den sammenhæng kan være relevant at indhente en årlig revisionserklæring fra en uafhængig tredjepart.

It-revisionserklæringer udarbejdes af en uafhængig tredjepart, hvilket afspejles i projekternes omkostningsniveau. Regionen har derfor en økonomisk interesse i kun at kræve revisionserklæringer, når der er behov for disse. Et sådant behov vil der eksempelvis være, når der er tale om store systemer med høj grad af følsomhed.

Det bemærkes i denne sammenhæng, at det kan være vanskeligt at stille omkostningstunge krav til it-systemer, der allerede er indkøbt og som er i drift. It-revision er dyrt og leverandøren vil sjældent tilbyde det omkostningsfrit. Derfor er det en fordel at beskrive krav herom i udbudsmaterialet, hvis dette er muligt.

Det skal understreges, at ved særligt kritiske it-systemer bør regionen stille krav om indlevering af regelmæssige it-revisionserklæringer.

Om bod
I forbindelse med indgåelse af særligt kritiske it-systemer vil det være en fordel at inkludere en bodsbestemmelse i den egentlige kontrakt, der knytter sig til it-sikkerheden. Det kan muligvis fordyre det endelige indkøb, men vil sikre databehandler et økonomisk incitament til at sikre sig mere grundigt mod ulovlig behandling af personoplysninger.

Som et alternativ til en bodsbestemmelse i selve kontrakten, kan bodsbestemmelsen beskrives i databehandleraftalens pkt. 15.

Man kan tage udgangspunkt i følgende ordlyd:

"Bod
Såfremt databehandler tilsidesætter sine forpligtelser i medfør af de bestemmelser, der er oplistet i databehandleraftalen og dette bevirker, at

personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven og dertilhørende bekendtgørelser og vejledninger, skal databehandler betale en bod på kr. XX.XXX til den dataansvarlige."

B. FELTER DER IKKE SKAL UDFYLDES ELLER ÆNDRES

Nedenfor beskrives baggrunden for de punkter i skabelonen, som ikke må ændres eller redigeres forud for indgåelsen af databehandleraftalen.

Formålet med denne beskrivelse er alene at redegøre for de enkelte afsnits baggrund, således at det fremstår mere klart, om det kan lade sig gøre at fravige punkterne ved at beskrive en undtagelse hertil i pkt. 15.

2. Lovbestemmelser og ISO 27001

Databehandleren agerer på vegne af den Dataansvarlige og skal derfor overholde lovgivning der regulerer såvel private virksomheder som offentlige myndigheder. Særligt relevant er det eksempelvis at henvise til reglerne om tavshedspligt[1] og sikkerhedsbekendtgørelsen[2].

ISO 27001 er en international standard, der stiller krav til et "Ledelsessystem for informationssikkerhed", også kaldet et ISMS. Idet organisationer er forskellige, vil et ISMS altid opbygges individuelt til at håndtere den konkrete organisations sikkerhedsbehov. Standarden stiller derfor ikke direkte krav til konkrete sikringsforanstaltninger.

Når der henvises til principperne og anbefalingerne i ISO 27001 skal dette derfor ses i sammenhæng med eksempelvis informationssikkerhedshåndbogen. Det vil sige at man ved tvivlstilfælde kan kigge i standardens tekst.

Ved en eventuel misligholdelse kan ISO 27001 anvendes som et fortolkningsbidrag til det samlede kontraktkompleks.

3. Databehandlerens ansvar

Ved at henvise til bilagene i pkt. 13 tillægges disse værdi i relation til aftalen mellem den Dataansvarlige og Databehandleren. Dermed skal Databehandleren agere i overensstemmelse med eksempelvis informationssikkerhedshåndbogen, hvis virksomheden vil være sikker på ikke at misligholde aftalen.

Desuden understreger henvisningen til den Dataansvarliges interne dokumenter, at Databehandler alene agerer på vegne af den Dataansvarlige og således ikke selv kan tage beslutninger, der vedrører de personoplysninger, som virksomheden har overladt til behandling efter instruks fra den Dataansvarlige.

---

[1] Se forvaltningslovens § 27 og straffelovens § 152 ff.

[2] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for den offentlige forvaltning med senere ændringer.

4. Databehandlers brug af underleverandører
Det er den Dataansvarliges ansvar, at personoplysningerne bliver opbevaret og behandlet i overensstemmelse med gældende regulering på området. Dette ansvar gælder også, når den Dataansvarlige overlader behandlingen til eksterne parter, hvilket både omfatter Databehandleren og dennes underleverandører.

For at sikre sig, at Databehandlerens underleverandører også efterlever den regulering, som gælder for den Dataansvarlige, har den Dataansvarlige behov for at kunne kontrollere hvilke oplysninger og processer, som Databehandleren overlader til underleverandører.

Hvis Databehandleren anvender underleverandører, som befinder sig i usikre tredjelande, skal både den Dataansvarlige og Databehandleren være særligt opmærksomme på, at kravene til lovlig behandling af personoplysninger efterleves. Dette kan blandt andet sikres, ved at Databehandleren indgår en kontrakt med underleverandøren, som baserer sig på Kommissionens skabelon til databehandleraftaler med aktører i usikre tredjelande.

5. Ad hoc arbejdspladser
Som anført ovenfor er både Databehandler og dennes underleverandører omfattet af en række love og bekendtgørelser i forbindelse med databehandlingen, herunder sikkerhedsbekendtgørelsen.

Idet sikkerhedsbekendtgørelsen som nævnt stiller en række krav til kryptering, autorisation, logning m.v., skal Databehandleren beskrive hvorledes anvendelsen af hjemmearbejdspladser el.lign. teknisk er sat op, således at sikkerhedsbekendtgørelsens bestemmelser efterleves.

Såfremt den Dataansvarlige ikke er klar over, at Databehandler anvender ad hoc arbejdspladser, er det ikke muligt for den Dataansvarlige effektivt at kontrollere det arbejde, som Databehandler udfører.

6. Samarbejde med tilsynsmyndigheder
Den Dataansvarlige 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 persondataloven.

For at sikre sig, at Databehandleren også agerer inden for lovens rammer og i overensstemmelse med den Dataansvarliges instruks, er det nødvendigt for den Dataansvarlige at kunne udføre kontrol med Databehandler.

Derfor skal Databehandler samarbejde med den Dataansvarlige i forbindelse med audits, uanset om sådanne audits sker efter den Dataansvarliges eget initiativ eller efter en henvendelse fra en tilsynsmyndighed (Datatilsynet).

7. Underretningspligt
For at den Dataansvarlige kan dokumentere eventuelle sikkerhedsbrud har Databehandleren en forpligtelse til skriftligt at meddele den Dataansvarlige om sådanne. Dette skyldes at den Dataansvarlige stadig er ansvarlig for behandlingen af personoplysningerne, selv om dette sker ved en ekstern part og derfor er nødt til at blive informeret ved sikkerhedsbrud, således at man kan undersøge omstændighederne ved disse og forhindre dem fremadrettet.

8. Håndtering af data efter aftalens ophør
Det følger af persondataloven, at personoplysninger alene må opbevares så længe der er et lovligt formål med opbevaringen og behandling af oplysningerne. Derfor er det beskrevet, hvorledes data skal slettes ved aftalens ophør.

Såfremt virksomheden går konkurs, er det vigtigt for Region Midtjylland at få data tilbageført, således at man kan behandle dem selv eller overlade dem til en ny databehandler.

Hvis du har udfordringer med at få udleveret sine data fra et konkursbo el.lign., bør du kontakte Juridisk Kontor.

9. Misligholdelse
Det er en meget central del af databehandleraftalen, at det anses som en væsentlig misligholdelse af det i præamblen anførte aftaleforhold, såfremt Databehandler ikke overholder de krav, der er oplistet i pkt. 9.

Ved en sådan misligholdelse kan det være muligt for den Dataansvarlige at hæve hele kontrakten og/eller kræve erstatning af leverandøren.

Når den Dataansvarlige har mulighed for at anvende misligholdelsesbeføjelser, vil det ofte være lettere at forhandle med leverandøren om, hvorledes denne kan efterleve gældende regulering. Hvis dette ikke kan lade sig gøre, kan den Dataansvarlige være forpligtet til at hæve kontrakten og finde en anden databehandler.

Hvis du erfarer, at en leverandør ikke efterlever databehandleraftalen med dertilhørende bilag, bør du kontakte Juridisk Kontor.

10. Aftalens ikrafttræden og varighed
Dette punkt er med til at sammenkæde databehandleraftalen med kontraktkomplekset, der er nævnt i præamblen.

Det skal understreges, at databehandleraftalen ikke er en selvstændig aftale, der kan indgås eller opsiges uafhængigt af det øvrige kontraktkompleks. Den er et dokument, som den Dataansvarlige er forpligtet til at indgå som en del af aftaleforholdet, når man indgår kontrakt med en databehandler.

11. Tavshedspligt
Idet Databehandler er omfattet af den samme regulering som den Dataansvarlige og agerer på dennes vegne, skal Databehandlers ansatte iagttage de samme tavshedspligtregler som den Dataansvarliges ansatte.

12. Underskrifter
Se ovenfor.

13. Bilag
Som bilag til databehandleraftalen skal en række dokumenter altid vedlægges som bilag. Det drejer sig om følgende:

1. Databehandlerinstruks
2. Retningslinjer tilknyttet databehandlerinstruksens § 9, stk. 1.3., herunder
    a. "Vejledning til adgang til Region Midts netværk og systemer",
    b. "It-sikkerhedsfunktionens overordnede principper for eksterne leverandørs remote support adgang til Region Midt".
3. Dataansvarliges informationssikkerhedspolitik
4. Dataansvarliges informationssikkerhedshåndbog.

Ad 1. Databehandlerinstruksen opsummerer de krav, som Region Midtjylland opstiller for eksterne databehandlere. Der er tale om mere tekniske krav end de beskrivelser, der fremgår af selve databehandleraftalen. Kravene tager udgangspunkt i sikkerhedsbekendtgørelsen og vejledningen til denne. Dette gælder eksempelvis kravene om kontrol af afviste adgangsforsøg og logning.

Ad 2. Retningslinjerne tilknyttet databehandlerinstruksen beskriver mere detaljeret de krav, Region Midtjylland stiller til eksterne leverandører.

Eksempelvis beskrives det i retningslinjerne, at det ved hver enkelt ekstern leverandørs ønske om etablering af "remote support" skal undersøges, hvorvidt dette sker i overensstemmelse med reglerne om overførsel til tredjelande.

Ad 3. Informationssikkerhedspolitikken er den overordnede ramme for informationssikkerheden i Region Midtjylland, og er vedtaget af Regionsrådet. Dokumentet har ikke til formål at regulere aftaleforhold direkte, men danner rammen for udarbejdelsen af Informationssikkerhedshåndbogen og er derfor et relevant bilag.

Ad 4. Informationssikkerhedshåndbogen beskriver og samler de retningslinjer, som Region Midtjylland skal følge for at sikre, at det ønskede sikkerhedsniveau efterleves.

Både instruksen, retningslinjerne og håndbogen består delvist af faste krav fra relevant lovgivning og dertilhørende bekendtgørelse, men dokumenterne indeholder også ledelsesmæssige beslutninger, der fastlægger rammerne for det niveau af informationssikkerhed, som regionen ønsker at have.

Ved at anvende disse dokumenter direkte sikres det, at man både lever op til gældende regulering og til de instruktionsbeføjelser, som ledelsen har i medfør af den enkeltes ansættelsesforhold i Region Midtjylland.

14. Øvrige henvisninger

Dette punkt henviser til en række offentligt tilgængelige dokumenter, der ikke udgør en bindende del af aftaleforholdet. Der er dog tale om lovgivning, bekendtgørelser, vejledninger eller standard, der alle har relevans i forhold til den Dataansvarliges og Databehandlers pligter og rettigheder.

15. Ændringer til punkterne 2-11 og 13-14

Se ovenfor.