

Tilsynserklæring vedrørende vejman.dk/Tilladelser og Vinterman til erstatning for fysisk eller andet tilsyn

1. maj 2019

Ledelsens udtalelse

IT-området i Vejdirektoratet kan i henhold til Databehandleraftale af 25. maj 2018 med vejman.dk/Tilladelser eller Vinterman erklære:

- at de i Databehandleraftalen og -bilag krævede skriftlige forretningsgange og kontroller har været etableret og efterlevet for perioden 25/5 2018 - 24/5 2019,
- at forretningsgangene og de etablerede systemer overholder de i Databehandleraftalen med bilag opstillede krav,
- at Vejdirektoratet har udarbejdet og bekræfter overholdelse af vedlagte kontrolmål for vejman.dk/Tilladelser og Vinterman
- at vedlagte "Definitioner og uddybende sikkerhedsoplysninger vedr. vejman.dk, Vinterman og kommuner" overholdes

Vejdirektoratet den 1. maj 2019



Hanne Sommerfelt, områdechef IT-området

Systembeskrivelse og uddybende sikkerhedsoplysninger

Ved vejman.dk forstås Vejdirektoratets internet baserede system med brugeruniverser og diverse specialmoduler, som er til brug for både kommune- og statsveje.

Al brugerprogrammel og data er installeret på centrale servere i Vejdirektoratet. Kommunerne har adgang via internettet til brugerprogrammel og data.

Kommunen tildeler og styrer personlige og fortrolige adgangskoder for kommunens relevante medarbejdere, der skal have adgang til brugerprogrammet.

Data i vejman.dk er primært tekniske data, dog er der brugeroplysninger og tilladelsesmodulet indeholder data om ansøgere og entreprenører. Vinterman kan indeholde telefonoplysninger til brug for udkald.

Databehandleraftalen omfatter ikke uheldsdata. Hvis Kommunerne anvender uheldsdata, sker det ved en dataoverdragelse, jf. kontraktens bilag 4.

Alle persondata i vejman.dk er almindelige persondata jvf. GDPR art. 6

Vejdirektoratets databehandling omfatter alene opbevaring af data for kommunerne, da øvrig databehandling foretages af kommunernes egne medarbejdere.

Kommunernes data opbevares og sikres på lige fod med Vejdirektoratets egne data:

- Der er dublerede datakommunikationsforbindelser til internettet med firewall beskyttelse.
- Serverrum med adgangskontrol ved hjælp af adgangskort, som kun giver adgang for godkendt IT-personale.
- Vinduer til serverrum er sikret med stålskotter.
- Der er 24/7 timers overvågning af servere med tilsvarende servicetilkald.
- Servere har redundant disksystemer eller tilsluttet redundant SAN disksystem.
- Servere er forsynede med redundante strømforsyninger og netværksforbindelser.
- Der tages daglig backup
- Backup opbevares adskilt fra serverrum

Grundlaget for Vejdirektoratets informationspolitik er gældende lovgivning på vejområdet samt ISO 27001, som er den standard, staten har besluttet at anvende for styring af informationssikkerhed. Sikkerhedsniveauet er desuden baseret på en årlig risikovurdering.

Informationssikkerhedspolitikken er gældende for

- alle medarbejdere i Vejdirektoratet
- alle leverandører og samarbejdspartnere, som har fysisk eller elektronisk adgang til Vejdirektoratets infrastruktur, systemer, data og informationer
- alle, der indsamler data for Vejdirektoratet

Informationssikkerhedspolitikken omfatter alle informationer i Vejdirektoratet uanset hvilken form og placering, disse måtte have.

Informationssikkerhed opnås ved at implementere, overvåge, revurdere og løbende ajourføre et passende sæt af foranstaltninger bestående af politikker, regler, procedurer, organisatoriske tiltag og tekniske funktioner.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A			
Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.		Vejdirektoratets databehandling for kommuner omfatter alene opbevaring af data, da den egentlige databehandling foretages af kommunens medarbejdere. Instruksen vedr. opbevaring fremgår af aftalegrundlaget med Vejdirektoratet. Aftalerundlaget mellem parterne vurderes jævnligt, minimum en gang årligt i forbindelse med fakturering.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.		Vejdirektoratet foretager kun opbevaring af data (hosting) for kommunerne. Serverne er opbevares i Vejdirektoratets videoovervågede serverrum.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.		Vejdirektoratet foretager kun opbevaring af data (hosting) for kommunerne.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret.	Kommunernes data opbevares og sikres på lige fod med Vejdirektoratets egne data: <ul style="list-style-type: none"> • Der er dublerede datakommunikationsforbindelser til internettet med firewall beskyttelse. • Serverrum med adgangskontrol ved hjælp af adgangskort, som kun giver adgang for godkendt IT-personale. • Vinduer til serverrum er sikret med stålskotter. • Der er 24/7 timers overvågning af servere med tilsvarende servicetilkald.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvaluering</i>
			<ul style="list-style-type: none"> • Servere har redundant disksystemer eller tilsluttet redundant SAN disksystem. • Servere er forsynede med redundante strømforsyninger og netværksforbindelser. • Der tages daglig backup • Backup opbevares adskilt fra serverrum
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.	Vejdirektoratet gennemfører årligt risikovurderinger af vejman.dk og vinterman.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Vejdirektoratets driftsleverandør opdaterer som minimum hver måned servere med nye antivirusprogrammer. Der udgiver opdateringsrapport hver måned.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.		Alle Vejdirektoratets systemer er beskyttet af firewall
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vejdirektoratets netværk er inddelt i 3 niveauer: VDNET (beskyttet af firewall), DMZ (hvor webserverne står) og VDextra (som er en ekstra sikkerhedszone mellem VDNET og DMZ).
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger.	Begrænsning af brugernes adgang til personoplysninger styres gennem applikationernes brugerstyring.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
B.7	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:</p> <ul style="list-style-type: none"> • Vejman.dk • Vinterman 	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Der er etableret overvågning med værktøjer til de nævnte systemer. I tilfælde af nedbrud udsendes servicemeddelelser til kommunerne
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.		Da der ikke opbevares fortrolige og følsomme personoplysninger i vejman.dk/tilladelser og Vinterman, anvendes der ikke i denne sammenhæng kryptering.
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk <p>Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.</p>		Vejdirektoratet udfører ikke logning på almindelige persondata i vejman.dk og vinterman.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.		vejman.dk/tilladelser og Vinterman benytter testdatabaser, som kan indeholde almindelige personoplysninger. Der arbejdes i vejman.dk/tilladelser på at udarbejde rutiner, der kan anonymisere disse.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	<p>Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests.</p> <p>Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.</p>	Vejdirektoratet har gennemført stikprøvevis penetrationstest på udvalgt udstyr.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
		ger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.	Vejdirektoratet har formaliserede patch procedurer der sikrer, at de forskellige systemer er opdateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.		For hver kommune findes der en lokaladministrator, som Vejdirektoratet tildeler brugeradgang på vegne af kommunen. Lokaladministratoren tildeler og overvåger kommunens øvrige brugere. I vejman.dk ophører brugeradgangene såfremt de pågældende brugere ikke har anvendt systemet i 3 måneder. I Vinterman afbrydes alle brugere årligt, inaktive brugere fjernes, og aktive brugere tildeles adgang på ny.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.		Ikke relevant for vejman.dk/tilladelser og vinterman
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vejdirektoratet har etableret serverrum med adgangskontrol ved hjælp af adgangskort, som kun giver adgang for godkendt IT-personale.

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vejdirektoratet har indført it-sikkerhedspolitik på baggrund af ISO27001. Sikkerhedspolitikken opdateres årligt.

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.		Informationssikkerhedspolitikken lever op til de indgåede databehandleraftaler.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser 	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vejdirektoratet har formaliseret ansættelsesprocedure, som efterprøves i relevant omfang. Indhentelse af straffeattest foretages efter individuel vurdering.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.		Fortrolighedserklæringen er en del af ansættelsesaftalen. Alle nye medarbejdere skal gennemgå introduktion til Vejdirektoratets informationssikkerhedspolitik.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.		Ved fratrædelse er der procedurer der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører og at aktiver som adgangskort, pc, mobiltelefon etc. Inddrages.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.		Nye medarbejdere informeres om deres tavshedspligt i ansættelsesbrevet.

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Vejdirektoratet tilbyder alle medarbejdere e-læring gennem de løsninger der stilles til rådighed af Moderniseringsstyrelsen. Der har været gennemført omfattende GDPR-kampagner i hele Vejdirektoratet i 2018/2019, rettet dels mod medarbejdere og dels mod ledere. Vejdirektoratets intranet opdateres løbende om GDPR

Kontrolmål D			
Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.		Vejdirektoratet opbevarer data for kommunerne, det er kommunernes eget ansvar at slette.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: <ul style="list-style-type: none"> • [indsæt beskrivelse af konkrete forhold] 		Vejdirektoratet opbevarer data for kommunerne, det er kommunernes eget ansvar at slette.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: <ul style="list-style-type: none"> • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning. 		Data registreret i vejman.dk/tilladelser og Vinterman kan ved kontraktens ophør udleveres til kommunerne jf. kontrakten.

Kontrolmål E			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurene skal opdateres.		Vejdirektoratet opbevarer alene de persondata, som kommunerne registrerer i vejman.dk/tilladelser og vinterman.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder	Det fremgår af aftalegrundlaget, hvor databehandlingen finder sted, pt. hos Vejdirektoratet, Guldalderen 12, 2640 Hedehusene. Vejdirektoratet har behandlingsfortegnelse for de aktiviteter der involverer persondata, som behandles for kommunerne.

Kontrolmål F			
Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvaluering</i>
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vejdirektoratet anvender ikke underdatabehandlere der ikke er nævnt i databehandleraftalen. Proceduren fremgår af databehandleraftalens bilag B
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.	De dataansvarlige har via databehandleraftalen godkendt de af Vejdirektoratet benyttede underdatabehandlere. Oversigten fremgår af databehandleraftalens bilag B
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Proceduren fremgår af databehandleraftalen. Proceduren fremgår af databehandleraftalens bilag B
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.	Vejdirektoratet anvender Datatilsynets databehandlerkabelon overfor sine underdatabehandlere.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: <ul style="list-style-type: none"> • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen 	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Oversigt over anvendte underdatabehandlere, herunder oplysninger om underdatabehandleren, fremgår af databehandleraftalens bilag B.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabe-	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.	Vejdirektoratet fører jævnlige tilsyn (skriftligt eller fysisk) med sine underdatabehandlere. Underdatabehandlere er alene konsulenter, der udfører deres assistance på Vejdirektoratets lokation. Data opbevares alene hos Vejdirekto-

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
	handleren.		ratet

Kontrolmål G			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.		Vejdirektoratet overfører hverken egne persondata eller persondata på vegne af kommunerne til udlandet.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.		Vejdirektoratet overfører hverken egne persondata eller persondata på vegne af kommunerne til udlandet.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.		Vejdirektoratet overfører hverken egne persondata eller persondata på vegne af kommunerne til udlandet.

Kontrolmål H			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvevaluering</i>
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreres rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.		Det fremgår af databehandleraftalen at Vejdirektoratet skal bistå kommunerne i relation til de registreres rettigheder. Vejdirektoratet er ved at udarbejde rutiner, som kommunerne kan anvende for at fremfinde persondata.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	Det er kommunernes eget ansvar at håndtere de nævnte procedurer. Vejdirektoratet bistår kommunerne via Vejdirektoratets brugerservicecenter med de nævnte procedurer, jf. vejman.dk aftalens bilag 2 Vejdirektoratet er ved at udarbejde rutiner, som kommunerne kan anvende for at fremfinde persondata.

Kontrolmål I			
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Selvevaluering</i>	<i>Resultat af selvaluering</i>
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at proceduren er opdateret.</p>	<p>Vejdirektoratet har formaliserede procedurer til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Proceduren opdateres årligt.</p>
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger 	<p>Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p>	<p>Der findes vejledning på Vejdirektoratets intranet vedr. databrud og der er udarbejdet procedure for indmelding</p>
I.3	<p>Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.</p>	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p>	<p>Vejdirektoratet har et system til dokumentation af sikkerhedshændelser.</p> <p>p.t. (marts 2019) har der ikke været sikkerhedsbrud, der har krævet underretning af den dataansvarlige.</p>
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	<p>Vejdirektoratet har procedure tilgængelig på intranettet. Proceduren kan forevises for kommunerne hvis det ønskes</p>