Endelig afrapportering om Statens Serum Instituts databeskyttelsesretlige compliance ved forsknings-samarbejder

KØBENHAVN
VESTER FARIMAGSGADE 23
DK-1606 KØBENHAVN V

AARHUS
ÅBOULEVARDEN 49
DK-8000 AARHUS C

T +45 33 15 20 10
@ MAIL@KAMMERADVOKATEN.DK
W WWW.KAMMERADVOKATEN.DK

Indhold

RESUME

Som det fremgår af Kammeradvokatens foreløbige vurdering af Statens Serum Instituts (SSI's) databeskyttelsesretlige compliance ved forskningssamarbejder, der blev offentliggjort i juni 2020, var det vores vurdering, at sikringen af overholdelse af databeskyttelsesreglerne på SSI havde lidt under betydelige mangler, og at behandlingen på en række punkter ikke havde været i overensstemmelse med de databeskyttelsesretlige regler. SSI har også selv i begyndelsen af 2020 gennemført en kortlægning af områder, hvor der er behov for at forbedre procedurer, udbedre gaps mv.

På den baggrund har SSI allerede iværksat en række initiativer med henblik på at forbedre den databeskyttelsesretlige compliance på SSI.

Denne endelige afrapportering indeholder en plan for, hvorledes SSI bliver en moden organisation i databeskyttelsesretlig henseende, således at compliancearbejdet bliver en naturlig del af arbejdsprocesserne på SSI og understøttes af hensigtsmæssige it-løsninger. Planen, som er udarbejdet i fællesskab mellem Kammeradvokaten og SSI, skal være gennemført ved udgangen af 2022. Der opstilles i rapporten fire deadlines for processen frem mod dette slutmål. Prioriteringen af gennemførelsen af projekter er blandt andet foretaget ud fra, hvilke forhold det af hensyn til sikringen af beskyttelsen af personoplysninger haster mest at få rettet op på.

1. INDLEDNING

1.1 Baggrund og grundlag for den endelige afrapportering

I december 2019 iværksatte Sundheds- og Ældreministeriet en advokatundersøgelse af Statens Serum Institut (SSI). Undersøgelsen skulle blandt andet omhandle instituttets behandling af personoplysninger til forskningsbrug i forbindelse med forskningssamarbejder. Den 22. juni 2020 offentliggjorde Sundheds- og Ældreministeriet Kammeradvokatens foreløbige vurdering af databeskyttelsesretlig compliance ved SSI.[1]

Nærværende rapport tager udgangspunkt i konklusionerne fra den foreløbige vurdering. Endvidere baserer rapporten sig på møder mellem Kammeradvokaten og afdelingen ved SSI for Quality Assurance & Compliance (QA & Compliance), ligesom der har været afholdt en række møder mellem Kammeradvokaten, SSI og Sundheds- og Ældreministeriet, herunder i regi af en styregruppe for arbejdet med deltagelse

[1] Kammeradvokatens rapport "Foreløbig vurdering af Statens Serum Instituts databeskyttelsesretlige compliance ved forskningssamarbejder", offentliggjort af Sundheds- og Ældreministeriet den 22. juni 2020

af Kammeradvokaten, SSI, Sundheds- og Ældreministeriet samt Sundheds- og Ældreministeriets koncernfælles DPO. Nærmere bestemt har der været afholdt følgende møder:

- Møde den 26. juni 2020 med SSI
- Møde den 10. august 2020 med SSI
- Møde den 13. august 2020 med styregruppen
- Møde den 20. august 2020 med QA & Compliance ved SSI
- Møde den 3. september 2020 med QA & Compliance ved SSI
- Møde den 8. september 2020 med styregruppen
- Møde den 18. september 2020 med QA & Compliance
- Møde den 22. september 2020 med SSI
- Møde den 29. september 2020 med direktionen ved SSI
- Møde den 20. oktober 2020 med Afdelingen for Epidemiologisk Forskning ved SSI
- Møde den 22. oktober 2020 med afdelingscheferne ved SSI
- Informationsmøder den 10., 12. og 13. november 2020 med afdelingschefer og sektionsledere ved SSI

Desuden har vi modtaget yderligere dokumenter fra SSI til brug for nærværende rapport, herunder dokumenter vedrørende en gennemført compliance gap-analyse (se afsnit 1.3 nedenfor), værktøjer til etablering af compliance på relevante områder ved SSI mv.

Den 9. oktober 2020 modtog SSI et brev fra Datatilsynet[2] om instituttets behandling af personoplysninger, som tager udgangspunkt i den foreløbige vurdering. Ved brevet anmoder Datatilsynet blandt andet SSI om inden den 1. januar 2021 at sende en redegørelse til Datatilsynet, hvori SSI påviser, at SSI i sine forskningssamarbejder har indgået de fornødne databehandleraftaler, har indhentet de fornødne tilladelser fra Datatilsynet og besidder det fornødne grundlag for overførsler til tredjelande. Med samme frist skal SSI aflevere en redegørelse til Datatilsynet, hvorved SSI påviser, at SSI har gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til kortlagte risici. Endelig beder Datatilsynet om senest den 1. januar 2021 at modtage en kopi af SSI's interne retningslinjer, procedurer og politikker om behandling af personoplysninger. Generelt angår Datatilsynets henvendelse SSI's forskningsprojekter. Datatilsynet har efterfølgende accepteret en udsættelse af fristen til den 1. marts 2021.

Hvor den første rapport fra Kammeradvokaten indeholdt en vurdering af den databeskyttelsesretlige compliance ved SSI, indeholder denne endelige rapport overvejelser om og en plan for, hvorledes man fremadrettet kan sikre databeskyttelsesretlig compliance på SSI. Dette skal blandt andet ses i lyset af,

[2] Datatilsynets brev til SSI af 9. oktober 2020.

at der på SSI har været en erkendelse af behovet for at styrke den persondataretlige compliance, hvilket blandt andet har bevirket en ny og fokuseret organisering samt forøgelse af antallet af medarbejdere på SSI, der beskæftiger sig med databeskyttelse, ligesom der allerede er iværksat en lang række initiativer. Denne rapport bygger blandt andet oven på disse initiativer.

Ved udarbejdelsen af rapporten har vi taget højde for det nævnte brev fra Datatilsynet, ligesom der er taget højde for det arbejde, som QA & Compliance ved SSI har iværksat med henblik på at sikre compliance generelt på SSI, dvs. compliance også på andre områder end det databeskyttelsesretlige.

1.2 Konklusioner fra den foreløbige vurdering

Til brug for undersøgelsen i den foreløbige vurdering af databeskyttelsesretlige forhold ved SSI blev der blandt andet taget udgangspunkt i en gennemgang af 14 forskningsprojekter, hvoraf syv projekter potentielt omfattede overførsel af personoplysninger til (usikre) tredjelande. De relevante projekter blev identificeret ud fra en dialog med instituttet og udvalgt fra instituttets forskerfortegnelse, således som fortegnelsen var ajourført i foråret 2020 (hvor der på tidspunktet for udvælgelse i marts 2020 var anført 328 forskningsprojekter). Endvidere blev SSI's interne retningslinjer, procedurer og politikker om behandling af personoplysninger gennemgået.

Det var ikke hensigten, at der ved gennemgangen af projekterne skulle foretages en udtømmende vurdering af samtlige databeskyttelsesretlige forhold, men derimod en gennemgang med fokus på de væsentligste forhold. Dette omfattede identificering af de forskellige aktørers roller som henholdsvis dataansvarlig og/eller databehandler, sikkerhedsforanstaltninger, tilsyn, behandlings- og overførselsgrundlag samt Datatilsynets tilladelse til videregivelse.

Vi konkluderede i den foreløbige vurdering, at sikringen af overholdelse af databeskyttelsesreglerne på SSI havde lidt under betydelige mangler, og at behandlingen på en række punkter ikke havde været i overensstemmelse med de databeskyttelsesretlige regler.

Vi konkluderede endvidere, at der var en række tilfælde, hvor der i forskningssamarbejder ikke var indgået de påkrævede aftaler eller de rette aftaler (overførselsgrundlag og/eller databehandleraftaler), ligesom der var tilfælde, hvor der ikke var indhentet de fornødne tilladelser fra Datatilsynet. Endvidere var der ikke forud for iværksættelsen af projekterne foretaget en tydelig og på skrift dokumenteret vurdering af, hvilken rolle de forskellige involverede parter havde i databeskyttelsesretlig henseende. Der forelå ikke dokumenterede risikovurderinger, og der var gennemgående ikke fastsat tilstrækkelige sikkerhedsforanstaltninger internt eller i forhold til modtagere af personoplysninger. Der forelå ligeledes ikke dokumentation for gennemførte tilsyn med SSI's databehandlere. Endelig havde SSI ikke systematisk forholdt sig til sit eget (lovlige) behandlingsgrundlag.

Det blev desuden helt overordnet vurderet, at SSI's interne retningslinjer, procedurer og politikker manglede ajourføring. Endvidere blev det vurderet, at adgangen til SSI's interne retningslinjer, procedurer og politikker burde gøres mere tilgængelig for relevante medarbejdere, og at SSI burde sikre sig, at retningslinjer mv. via awareness-kampagner, uddannelse og lignende tiltag blev formidlet til disse.

For en nærmere beskrivelse af den foreløbige vurdering, se afsnit 2.2.1 nedenfor.

1.3 Øvrige erfaringer

SSI har i en længere periode arbejdet med compliance og med en mere systematisk og grundlæggende forankring af arbejdet med at sikre overholdelse af regler, standarder mv., herunder både af databeskyttelsesretlige regler, men også af andre regler, som er centrale for den virksomhed, SSI driver.

I den anledning har SSI den 1. januar 2020 oprettet afdelingen QA & Compliance. QA & Compliance har som øverste (strategiske) retningslinje udarbejdet en fælles Kvalitets- & Compliancemanual, som overordnet beskriver SSI's profil og myndighedskrav til SSI, governance og organisatorisk ramme, kvalitets- og compliancepolitik samt design af et fælles ledelsessystem for SSI (kaldet Quality Management System (QMS)) med henblik på at sikre den løbende understøttelse af arbejdet med kvalitet og compliance i forhold til blandt andet GxP ("good practice"), ISO17025 og øvrige relevante ISO-standarder og databeskyttelsesretlige regler (herunder ISO27001 og ISO27701).

Til brug for sit arbejde har QA & Compliance blandt andet gennemført en såkaldt gap-analyse, hvorved afdelingen har kortlagt, på hvilke områder der er behov for at forbedre procedurer og udbedre gaps mv. med henblik på at sikre overholdelse af regler, standarder mv. Dette arbejde er blandt andet blevet understøttet af konsulentfirmaet Devoteam og har ud over mapning i forhold til lovgivning, krav og guidelines omfattet workshops med repræsentative medarbejdere ved SSI. SSI har oplyst, at der blev afholdt i alt fire workshops med fokus på 1) persondatabeskyttelse, 2) informationssikkerhed generelt, inklusive it-sikkerhed, 3) fysisk sikkerhed og tilhørende it-understøttelse, inklusive rundtur på campus og i Biobanken samt 4) GxP it compliance.

Gaps afdækket i dette arbejde er i relevant omfang inkluderet i nærværende beskrivelse af det fremadrettede arbejde med databeskyttelsesretlig compliance ved SSI. Der er i vidt omfang sammenfald mellem de problemer, der blev afdækket ved vores undersøgelser, og de databeskyttelsesretlige gaps, som SSI's egen analyse afdækkede. Se nærmere afsnit 2.2.2.

1.4 Rapportens opbygning

Som nævnt i afsnit 1.1 har denne rapport til formål at understøtte de konkrete tiltag, der er nødvendige for fremadrettet at sikre compliance på databeskyttelsesområdet på SSI. Hvor den første rapport indeholdt en vurdering af den databeskyttelsesretlige compliance ved SSI, indeholder indeværende endelige rapport overvejelser om og en plan for, hvorledes man fremadrettet kan sikre databeskyttelsesretlig compliance på SSI.

Rapporten har to hovedelementer. For det første beskrives i afsnit 2 de forhold, der efter vores opfattelse skal arbejdes med for at sikre databeskyttelsesretlig compliance. For det andet indeholder afsnit 3 et udkast til en plan for gennemførelse af tiltag med henblik på at sikre databeskyttelsesretlig compliance. Planen vil indebære, at SSI ved udgangen af 2022 har etableret databeskyttelsesretlig compliance, således at det fra dette tidspunkt handler om løbende drift samt vedligeholdelse og opdatering af compliancearbejdet.

2. BRUTTOKATALOG OVER FORHOLD ("GAPS")

2.1 Generelle forhold

At sikre databeskyttelsesretlig compliance handler – ligesom compliancearbejde i almindelighed – om meget mere end blot at sikre overholdelse af reglerne. Hvis man skal sikre langsigtet og holdbar compliance, handler det også om at etablere de rette rammer rundt om compliancearbejdet, således at der er en *organisering*, som løbende understøtter regeloverholdelse, ligesom der skal være den tilstrækkelige *viden* om (og fornemmelse for) databeskyttelsesretlige forhold. SSI behandler rigtigt mange personoplysninger, herunder i forbindelse med den forskning som bedrives på SSI, og hertil kommer, at der ofte er tale om følsomme personoplysninger i form af helbredsoplysninger.

Når der har været visse databeskyttelsesretlige problemer på SSI, skyldes det ikke en modvilje mod reglerne fra de enkelte medarbejdere, men derimod at der ikke har været den tilstrækkelige compliancemæssige understøttelse, og det er en ledelsesopgave at etablere en sådan understøttelse.

SSI har oplyst, at det i 2019 stod klart for SSI's ledelse, at området skulle organiseres bedre og styrkes yderligere, hvis SSI skulle opnå et tilfredsstillende complianceniveau i forhold til databeskyttelse og informationssikkerhed generelt. På den baggrund blev der i andet halvår af 2019 arbejdet på forskellige oplæg til reorganisering. Dette arbejde resulterede i en beslutning fra SSI's direktion om at samle og styrke de funktioner, der arbejder med databeskyttelse (herunder DPA-funktionen) og informationssikkerhed (herunder CISO-funktionen) i en ny compliancesektion i SSI's eksisterende kvalitetssikringsafdeling (QA), som herefter fik navnet QA & Compliance. Beslutningen om bemandingen af afdelingen blev

endeligt truffet den 17. december 2019. Organisering af afdelingen og ansættelse af yderligere medarbejdere (ud over de to persondatabeskyttelsesjurister og en CISO, der var ansat på daværende tidspunkt) blev påbegyndt herefter.

Beslutningen blev ifølge SSI truffet på baggrund af et ønske om at kunne leve op til databeskyttelsesforordningens krav ved blandt andet at etablere et samlet ledelsessystem inden for privatlivsbeskyttelse (PIMS), informationssikkerhed (ISMS) og kvalitetssikring (QMS), et ønske om at kunne servicere forretningen uden, at der opstår flaskehalse, samt en erkendelse af et behov for at gennemgå SSI's eksisterende behandlingsaktiviteter og sikre, at også behandlingsaktiviteterne overholder databeskyttelsesforordningens krav.

Det første hold af nye medarbejdere blev rekrutteret ved udgangen af februar 2020 med ansættelse den 1. april 2020. Nedlukningen af samfundet på grund af COVID-19 betød, at de nye medarbejdere – ligesom resten af landet – var hjemsendt og dermed ikke fysisk kunne starte på SSI. Herudover kontraherede SSI med Kammeradvokaten, og otte jurister derfra hjalp med COVID-19-aktiviteter og det løbende compliancearbejde.

SSI har i dag følgende interne ressourcer allokeret til områderne for databeskyttelse og informationssikkerhed:

- En sektionsleder for SSI Compliance, CISO
- Tre jurister med speciale i databeskyttelse, herunder en DPA og en person, der starter 1. december 2020
- To juridiske fuldmægtige
- Yderligere en jurist under rekruttering til ansættelse den 1. januar 2021
- Fire jurastuderende, heraf starter en person den 1. januar 2021
- En risk manager (jurist)
- To informationssikkerhedsspecialister under rekruttering til start 1. december 2020 (Rollen varetages på nuværende tidspunkt af en ekstern konsulent.)
- En projektleder til at drive compliance-projektprogrammet vedrørende databeskyttelse og informationssikkerhed
- En it-compliance-koordinator, hvis opgave er at sikre, at nye it-systemer opfylder en række lovkrav og standarder, herunder i forhold til databeskyttelse
- En QMS-compliance-specialist til at drive etablering og vedligehold af et PIMS/ISMS-ledelsessystem (retningslinjer og instruktioner)

SSI her derudover seks medarbejdere ansat til at varetage opgaver inden for kvalitetssikring (GxP) i SSI's QA-sektion, som også bidrager med varetagelse af tværfaglige complianceopgaver, herunder leverandørstyring, eksterne og interne audits og tilsyn samt etablering af retningslinjer.

Som nævnt ovenfor forudsætter sikring af databeskyttelsesretlig compliance den rette organisering og den rette viden. Det vil vi uddybe i det følgende.

2.1.1 Organisering

Det er relevant at overveje organisering i to tempi. For det første skal der sikres den rette organisering frem til udgangen af 2022, der er den planlagte tidshorisont for etablering af databeskyttelsesretlig compliance. For det andet skal der sikres den rette organisering i den efterfølgende periode, hvor man så at sige går "i drift", og hvor det således ikke længere handler om etablering, men om løbende vedligeholdelse af den databeskyttelsesretlige compliance.

For begge perioder gør det sig gældende, at man kun lykkes med compliance, hvis der er den tilstrækkelige ledelsesmæssige opbakning. Der skal med andre ord være den rette "tone from the top". Ledelsen skal prioritere arbejdet dermed, og den skal ved sine handlinger reelt vise, at overholdelsen af reglerne er vigtig. Medarbejdere vil altid primært orientere sig mod, hvad en ledelse gør, og ikke mod, hvad den siger, og ledelsen bør signalere, at overholdelsen af de databeskyttelsesretlige regler grundlæggende er en "license to operate".

For så vidt angår perioden frem til udgangen af 2022, bør der etableres en projektorganisering med en styregruppe med deltagelse af såvel ledelsen på SSI som repræsentation fra Sundheds- og Ældreministeriets departement. Det er således vigtigt, at opgaven ikke blot bliver placeret i QA & Compliance, men at både SSI's ledelse og departement løbende engagerer sig i og får viden om fremdriften i arbejdet med henblik på, at der kan iværksættes yderligere initiativer, hvis arbejdet ikke skrider planmæssigt frem.

For så vidt angår perioden derefter, vil arbejdet i videre omfang kunne forankres i QA & Compliance, men det er vigtigt, at ledelsen stadig løbende bliver orienteret om den databeskyttelsesretlige compliance. Der bør således etableres relevante målepunkter, som kan bruges til at udarbejde ledelsesinformation, så SSI's ledelse fortsat modtager oplysninger om status for det løbende compliancearbejde. Ledelsesinformationen kan passende integreres med ledelsesinformation om det øvrige compliancearbejde. Desuden bør QA & Compliance have en direkte og nem adgang til at give oplysninger og eskalering til ledelsen om databeskyttelsesretlige problemer.

SSI har oplyst, at ledelsesinformation og målepunkter for persondatabeskyttelse inkorporeres i konceptet for den årlige "Topledelsesevaluering", som allerede eksisterer inden for kvalitetssikring (GxP og ISO17025) på SSI.

Endelig er det vigtig, at der løbende sker inddragelse af relevante medarbejdere og medarbejdergrupper, herunder af de relevante forskere. Den gensidige udveksling af erfaringer, viden mv. er en forudsætning for et vellykket compliancearbejde.

Det er i øvrigt vores vurdering, at den opnormering af medarbejdere, der på SSI beskæftiger sig med databeskyttelse, se afsnit 2.1 ovenfor, er hensigtsmæssig og formentlig kan sikre den rette understøttelse af compliancearbejdet.

2.1.2 Viden

En forudsætning for databeskyttelsesretlig compliance er, at de relevante medarbejdere har tilstrækkelig viden – ikke nødvendigvis til at løse alle databeskyttelsesretlige problemstillinger, men nok til at overholde basale databeskyttelsesretlige krav, nok til at løse simple problemstillinger og nok til at identificere mere vanskelige problemstillinger, hvor de i givet fald skal have hjælp fra mere specialiserede medarbejdere. Det er ikke nødvendigvis en forudsætning, at medarbejderne er klare over, at de ved bestemte handlinger overholder databeskyttelsesretten. Typisk sikres compliance bedst ved, at der indarbejdes bestemte måder at agere på eller bestemte procedurer, man følger, i en organisation, således at regeloverholdelse sikres, uden medarbejderne selv er bevidste om, at de derved sikrer regeloverholdelse. Derimod kan de være motiverede af andre forhold, f.eks. at handlemåden eller proceduren sikrer dokumentation af, hvorledes der er handlet, hvilket også kan understøtte dokumentation i forskningsmæssig henseende.

Som nævnt under afsnit 1.2 ovenfor blev det helt overordnet vurderet i vores foreløbige vurdering af SSI's databeskyttelsesretlige compliance ved forskningssamarbejder, at SSI's interne retningslinjer, procedurer og politikker manglede ajourføring. Endvidere blev det vurderet, at adgangen til SSI's interne retningslinjer, procedurer og politikker burde gøres mere tilgængelig for relevante medarbejdere, og at SSI burde sikre sig, at retningslinjer mv. via awareness-kampagner, uddannelse og lignende tiltag formidles til disse.

Det er essentielt for sikring af velfungerende databeskyttelsesretlig compliance ved SSI, at der etableres faste, opdaterede og tilgængelige procedurer, som følges, og som sikrer dels overholdelsen af de databeskyttelsesretlige regler, dels dokumentation for at reglerne er overholdt.

Det forudsætter blandt andet, at SSI's interne retningslinjer, procedurer og politikker ajourføres. Denne ajourføring skal blandt andet medvirke til, at databeskyttelsesforordningen og de nye krav, som denne

indeholder (f.eks. om "Privacy by Design", "Privacy by Default" og udarbejdelse af konsekvensanalyser), bliver integreret i SSI's arbejdsgange og it-systemer.

Det forudsætter ligeledes, at procedurerne reelt følges. Det er derfor væsentligt, at medarbejdere ved SSI får en basal viden om databeskyttelsesretten, og at der sikres nem adgang til at dokumentere efterlevelsen af reglerne. Det forudsætter blandt andet, at den rette træning og løbende uddannelse af medarbejderne er etableret. Træning og løbende uddannelse kan antage mange former, herunder skriftligt undervisningsmateriale, kurser, e-learning, gamification mv. Det er ikke afgørende, hvilket format der vælges, men der bør vælges et format, som er tilpasset modtagerne, herunder i forhold til hvilken tidsmæssig indsats de pågældende medarbejdere reelt kan levere.

I forbindelse med den gennemgang, som lå til grund for vores foreløbige vurdering af SSI's databeskyttelsesretlige compliance ved forskningssamarbejder, konstaterede vi, at dokumentationen for overholdelsen af reglerne, herunder dokumentationen for f.eks. indgåelsen af de nødvendige aftaler, til tider manglede og til tider var af varierende kvalitet. Det vil lette og understøtte arbejdet med databeskyttelsesretlig compliance i betragteligt omfang, hvis der etableres ensartede og hensigtsmæssige procedurer for dokumentation. Der bør i den forbindelse også sikres en it-mæssig understøttelse af dokumentationen i et såkaldt dokumentstyringssystem (EDMS) med tilhørende træningsmodul. Derudover bør efterlevelse af complianceprocesser sikres ved, at flows defineres og følges ved it-understøttelse (EQMS).

2.2 Konkrete databeskyttelsesretlige forhold

I det følgende gennemgås mere detaljeret de problematiske databeskyttelsesretlige forhold, som blev konstateret i den foreløbige vurdering (afsnit 2.2.1), ligesom de problematiske forhold, som SSI selv har konstateret, gennemgås (afsnit 2.2.2).

2.2.1 Kammeradvokatens foreløbige vurdering

2.2.1.1 Vurdering af tredjelandssamarbejder

I den foreløbige vurdering af SSI's databeskyttelsesretlige compliance ved forskningssamarbejder af juni 2020 blev der udledt en række konkrete og tværgående konklusioner baseret på gennemgangen af syv udvalgte forskningsprojekter med potentielle overførsler af personoplysninger til tredjelande.

For det første kunne vi konstatere, at SSI i almindelighed ikke i tilstrækkeligt omfang havde undersøgt og beskrevet samarbejdspartneres *databeskyttelsesretlige roller*. Det var således gennemgående, at SSI i det for os foreliggende materiale kun i begrænset omfang havde beskrevet, hvordan SSI var kommet frem til vurderingerne af dataansvarlige og databehandlere i forbindelse med forskningsprojekter med

tredjelandsoverførsler. Forinden behandlingsaktiviteterne begyndte i forskningsprojekterne, burde SSI have afklaret og dokumenteret projektets ansvars-, opgave- og rollefordeling.

For det andet kunne vi konstatere, at SSI i alle syv projekter ikke havde indgået *databehandleraftaler* med samarbejdspartnere uden for EU/EØS (som SSI anså for databehandlere), der levede op til kravene i databeskyttelsesforordningens artikel 28. Dette skal ses i lyset af, at SSI hidtil havde været af den opfattelse, at EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger fra en dataansvarlig inden for EU/EØS til en databehandler uden for EU/EØS kunne udgøre en databehandleraftale. Det er imidlertid vores vurdering, at standardkontraktbestemmelserne ikke i almindelighed, efter databeskyttelsesforordningen har fået virkning, fuldt ud lever op til minimumskravene til databehandleraftaler i databeskyttelsesforordningens artikel 28.

For det tredje kunne vi konstatere, at SSI ikke i tilstrækkeligt omfang havde beskrevet eller fastsat passende tekniske og organisatoriske sikkerhedsforanstaltninger, som krævet i databeskyttelsesforordningens artikel 32, i forbindelse med behandlingen af personoplysninger for samarbejdspartnere uden for EU/EØS. Efter det oplyste havde SSI ikke foretaget skriftlige *risikovurderinger* samt fastsat sikkerhedsforanstaltninger og tilsyn med samarbejdspartnere på baggrund af sådanne risikovurderinger.

For det fjerde sås der ikke på baggrund af det for os foreliggende materiale i nogen af projekterne at være ført *tilsyn* med de samarbejdspartnere uden for EU/EØS, som SSI anså for databehandlere.

For det femte kunne man ikke af det for os foreliggende materiale se, at SSI havde forholdt sig til behandlingsgrundlaget. På det foreliggende grundlag var det dog vores vurdering, at der var *hjemmel* til at foretage behandlingsaktiviteterne i forskningsprojekterne.

SSI havde umiddelbart et *overførselsgrundlag* i fem ud af de syv forskningsprojekter i form af EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger fra en dataansvarlig i et land inden for EU/EØS til en databehandler i et land uden for EU/EØS. I tre af forskningsprojekterne var det imidlertid – for det sjette – vores vurdering, at mest talte for, at samarbejdspartneren ikke blot var databehandler for SSI, men handlede som dataansvarlig, hvorfor der burde have været anvendt en anden udgave af standardkontraktbestemmelserne.

Det kunne for det syvende konstateres, at SSI i ingen af projekterne havde indhentet Datatilsynets forudgående tilladelse til videregivelse af personoplysninger efter databeskyttelseslovens § 10, stk. 3, og den tidligere gældende persondatalovs § 10, stk. 3.

For så vidt angår de databeskyttelsesretlige roller – som har stor betydning for indholdet af de øvrige databeskyttelsesretlige krav – bemærkes det, at man fremadrettet kan vælge at organisere arbejdet på

anden måde end hidtil med henblik på at indtage nye databeskyttelsesretlige roller. F.eks. kan man ved at sikre et instruktionsforhold mellem SSI og en samarbejdspartner i et tredjeland etablere en "dataansvarlig-databehandler-relation", selvom der i mangel af en sådan mulighed for instruktion på nuværende tidspunkt må siges at være tale om en "dataansvarlig-dataansvarlig relation". Det fremadrettede arbejde kan således tage udgangspunkt i, hvilket samarbejde man ønsker at etablere, og dermed hvilke roller parterne indtager i et sådant arbejde, snarere end at tage udgangspunkt i, hvorledes samarbejdet historisk har været organiseret. Det er imidlertid vigtigt, at man ved de enkelte forskningsprojekter forholder sig til spørgsmålet om databeskyttelsesretlige roller.

2.2.1.2 Vurdering af udvalgte samarbejder inden for EU/EØS

Ved den foreløbige vurdering af SSI's databeskyttelsesretlige compliance ved forskningssamarbejder af juni 2020 udledte vi en række konkrete og nogle tværgående konklusioner på baggrund af gennemgangen af syv udvalgte, forskelligartede forskningsprojekter med videregivelser eller overladelser inden for EU/EØS.

Det bemærkes, at de syv forskningsprojekter udgjorde en meget lille andel af det samlede antal forskningsprojekter, og nedenstående opsamling skal læses i det lys.

For det første var det kendetegnende for projekterne, at der som oftest ikke forud for iværksættelsen af projekterne var foretaget en tydelig og på skrift dokumenteret vurdering af, hvilke *databeskyttelsesretlige roller* de forskellige involverede parter havde.

For det andet konstaterede vi, at der i ingen af forskningsprojekterne forelå en samlet skriftlig *risikovurdering*, og at der samlet set alene syntes at være foretaget risikovurderinger i meget begrænset omfang. For de få ikke-skriftlige risikovurderinger, der lod til at være foretaget, sås ikke at være foretaget en opdatering heraf i forbindelse med ændringer af projekter, hvilket ellers også foreskrives i SSI's interne retningslinjer.

For det tredje var der kun i et enkelt tilfælde dokumentation for gennemførte *tilsyn* med databehandlere. Der var i varierende grad på kontraktligt grundlag sikret adgang til at gennemføre tilsyn.

For det fjerde var det et gennemgående træk, at man ikke af det for os tilgængelige materiale kunne se, at SSI havde forholdt sig til *behandlingsgrundlaget* bortset fra i et enkelt projekt. Det bemærkes, at det må antages, at der i almindelighed er hjemmel til behandlingerne i forskningsprojekterne.

For det femte var der tilfælde, hvor *databehandleraftaler* ikke var blevet opdateret, efter den nye databeskyttelsesforordning fik virkning den 25. maj 2018.

For det sjette må det antages, at der i hvert fald i visse tilfælde var sket videregivelse af personoplysninger uden fornøden *tilladelse fra Datatilsynet*, men at vurderingen af dette spørgsmål ofte er vanskeliggjort af den manglende fastlæggelse af roller.

Som nævnt i afsnit 2.2.1.1 kan man fremadrettet vælge at organisere arbejdet på anden vis end hidtil med henblik på at indtage nye databeskyttelsesretlige roller.

2.2.2 SSI's egen afdækning af "gaps"

Som nævnt i afsnit 1.3 har QA & Compliance ved SSI blandt andet gennemført en gap-analyse i første kvartal af 2020, hvorved man har kortlagt, på hvilke områder der er behov for at forbedre procedurer, udbedre gaps mv. med henblik på at sikre overholdelse af regler, standarder mv.

I alt 14 projektspor blev identificeret. Projektsporene dækker over områder af varierende størrelse og omfang. Projektsporene er følgende:

1) Regimedesign (Design af QMS, inklusive informationssikkerhed (ISMS) og GDPR (PIMS))
2) Ledelsesgovernance
3) Fortegnelser
4) Leverandørstyring (herunder databehandleraftaler, tilsyn med databehandlere og kontraktstyring)
5) De registreredes rettigheder
6) Datagovernance
7) Awareness
8) Risikostyring
9) Hændelsesstyring
10) It-projektstyring
11) Styring af aktiver
12) It-drift
13) Fysisk adgang
14) Beredskab

Disse projektspor indeholder i et vidt omfang forhold, som er relevante for databeskyttelsesretlig compliance. For den nærmere udskillelse af, hvilke spor der særligt er relevant for den databeskyttelsesretlige compliance, henvises til afsnit 3.1 nedenfor.

1) Regimedesign

Som overordnet og styrende strategisk dokument for det fælles ledelsessystem har SSI vurderet, at der var behov for at etablere en kvalitets- og compliancemanual, som omfatter krav til diagnostik (ISO17025) samt udvikling, produktion og distribution af vacciner (GxP). Dette er sket, og manualen omfatter nu også compliancekrav til forskning og overvågning i forhold til informationssikkerhed og persondatabeskyttelse. Manualen beskriver opbygningen af et fælles ledelsessystem (kaldet Quality Management System (QMS)) og har referencer til de lovkrav, SSI er underlagt.

SSI har desuden etableret en liste over identificerede procedurer og instruktioner, som enten skal genbesøges eller udarbejdes på ny i forhold til i højere grad at inkorporere informationssikkerhed og persondatabeskyttelse. Som eksempler kan nævnes SOP (Standard Operating Procedure) for god dokumentation i praksis, dokumentstyring og arkivering, som blandt andet skal forholde sig både til krav om at gemme data og at slette data og krav til læsbarhed og tilgængelighed i hele dataenes levetid. SOP for dataklassifikation på SSI skal ligeledes genbesøges. Processen for overvågning af nye myndighedskrav og guideline "Compliance Intelligence" skal opdateres til ud over GxP at inkludere informationssikkerhed og persondatabeskyttelse. Genbesøg og etablering af processer og procedurer er derudover indeholdt i samtlige projektspor.

Som it-understøttelse etableres et dokumentstyringssystem (EDMS) til erstatning af det eksisterende system, som ud over håndtering af SOP'er og instruktioner samt automatiseret styring af træning og awareness også indeholder it-understøttelse af kvalitets- og complianceprocesser (EQMS), som f.eks. hændelsesstyring, risikostyring, leverandørstyring mv.

2) Ledelsesgovernance

SSI har siden etablering af afdelingen QA & Compliance arbejdet med ledelsesgovernance. Kvalitets- og compliancemanualen for SSI beskriver nu ledelsesgovernance, herunder governance-fora, roller og ansvar for ledere og medarbejdere (f.eks. roller som DPA og CISO).

Der anvendes tre governance niveauer inden for SSI's kvalitets- og compliance-governance:

- Topledelsesniveau
- Kvalitets- og complianceudvalg drevet af chefen for QA & Compliance
- It-sikkerhedsudvalg med repræsentanter fra de forskellige afdelinger drevet af SSI's CISO og DPA

Formål og mandat for de forskellige niveauer er beskrevet i kvalitets- og compliancemanualen. Roller og ansvar skal støttes op med etablering af stillingsbeskrivelser for ledere og (nøgle)personer, som arbejder med informationssikkerhed og databeskyttelse, ligesom der skal etableres en træningspakke for disse personer.

Informationssikkerhed og persondatabeskyttelse bør ifølge SSI endvidere integreres i den eksisterende topledelsesevaluering. Herudover skal kommissoriet for sikkerhedsudvalget genbesøges, herunder deltagerkredsen og sammenhængen med governance-hierarkiet. Der skal ske en opgradering af kompetencer samt ansættelse af nyt personale i SSI Compliance til sikring af it-sikkerhed, fysisk sikkerhed og beredskab.

3) Fortegnelser

Hvad angår SSI's fortegnelse over databehandlingsaktiviteter, har SSI vurderet, at der mangler en formel procedure for førelse af fortegnelser. De eksisterende fortegnelser – forskerfortegnelsen og administrativ fortegnelse – findes ikke fyldestgørende, da de ikke er tilpas detaljerede. De administrative fortegnelser findes at være bedre beskrevet end fortegnelserne på forskningsområdet. SSI finder, at der skal særligt fokus på hjemmelsproblematikken og identificering af databehandler(e), hvor der findes at være en del mangler.

Der er 12 administrative fortegnelser. SSI ønsker at genbesøge disse, da de med fordel kan uddybes, så de bliver mere dækkende for den eksisterende praksis. På sigt skal fortegnelserne fordeles til deres respektive områder ved SSI, men ansvaret for fortegnelserne er endnu ikke delegeret, og det vurderes, at det tidligst bør ske, når fortegnelserne er gennemgået og fuldstændige.

Det er vurderet, at en lang række forskningsprojekter efter SSI's oplysninger skal kvalitetssikres og potentielt ajourføres. Det er ikke klart, i hvilket omfang forskningsprojekterne stadig er aktive. Indholdet af fortegnelserne skal kobles sammen med risikovurderinger, så de rette perioder for genbesøg mv. kan etableres. Endvidere ønskes det, at de tekniske og organisatoriske foranstaltninger uddybes i fortegnelsen.

Det bemærkes, at SSI efter sommerferien var begyndt at indhente oplysninger til og udfylde de nye fortegnelser i overensstemmelse med de ovenfor angive retningslinjer, men at arbejdet er sat i bero med henblik på i første omgang at levere de ting, der efterspørges i Datatilsynets henvendelse af 9. oktober 2020, se hertil også afsnit 3.1.

4) Leverandørstyring

Dette projektspor omfatter blandt andet databehandleraftaler, tilsyn med databehandlere og kontraktstyring.

For så vidt angår *databehandleraftaler*, foreligger der på SSI en proces for indgåelse af databehandleraftaler ved SSI, og skabelonen for databehandleraftaler fra Datatilsynet anvendes. Ansvaret ligger hos den respektive afdelingschef. Dette ansvar skal nedfældes i en SOP for databehandleraftaler. Der mangler et komplet overblik over databehandlere, hvilket skal udarbejdes. Derudover skabes overblik over, hvor SSI selv indgår som databehandler for øvrige dataansvarlige. Nye versioner af databehandleraftaleskabeloner skal kommunikeres i forbindelse med udvidelsen af SOP'en for databehandleraftaler.

Sikring af efterlevelse af SSI's databehandleraftaler, når SSI er databehandler, er ikke formaliseret. Der skal også udarbejdes proces for dette.

Hvad angår *tilsyn med databehandlere*, har SSI oplyst, at der kun er gennemført få fysiske tilsyn og indhentet revisionserklæringer for en række større databehandlere, hvor SSI er dataansvarlig.

SSI har desuden oplyst, at der medio 2020 er udarbejdet en procedure for leverandørstyring og audits, hvor krav til tilsyn af databehandlere og it-leverandører er blevet inkorporeret. Der er desuden udarbejdet en plan for tilsyn for 2021.

Det er vurderet, at der skal etableres proces for audits og tilsyn med databehandlere med udgangspunkt i de tilrettede procedurer. Procedure for "audits of investigational sites" skal også tilrettes, så den inkluderer tilsyn af persondatabeskyttelse. Endvidere skal SOP for selvinspektion tilpasses til at indeholde krav til internt tilsyn for informationssikkerhed og overholdelse af databeskyttelsesretten. Endelig skal der gennemføres tilsyn.

5) De registreredes rettigheder

I SSI's gap-analyse vurderes det, at indsigtsanmodninger fra registrerede håndteres ad hoc. Dette blev på daværende tidspunkt forklaret med, at SSI modtog meget få indsigtsanmodninger. SSI vurderer, at der mangler en procedure for håndtering af indsigtsanmodninger.

Der er nu etableret en proces for borgerhenvendelser, og der sker ugentlig ledelsesopfølgning. Denne proces er nu ved at blive formaliseret i en SOP.

Desuden er der ikke en formaliseret procedure for håndtering af oplysningspligt i den situation, hvor SSI henvender sig direkte til en borger eller borgere. Endvidere findes oplysningspligten på hjemmesiden under emnet "persondatapolitik" ikke tilstrækkelig. Der mangler en formaliseret procedure for sikring af de registreredes ret til berigtigelse, sletning, begrænsning og underretning.

SSI har vurderet, at der skal udarbejdes en beskrivelse af de registreredes rettigheder, herunder ret til underretning, berigtigelse, sletning og begrænsning. Der skal endvidere udarbejdes SOP'er for at sikre de registreredes ret til berigtigelse, sletning, begrænsning og underretning.

Definition af indsigtsanmodning og processen herfor skal udarbejdes. Det skal undersøges, hvor mange indsigtsanmodninger der modtages i forbindelse med forskningsprojekter, vedrørende biobanken osv. Der skal ligeledes etableres en formaliseret proces for håndtering af disse.

Endelig skal en procedure for indhentning og håndtering af *samtykke* etableres og standardiseres, så samme procedure følges i forskellige projekter.

6) Datagovernance

SSI vurderer, at data, herunder forskerdata, visse steder på SSI er placeret på fællesdrev i ikke-pseudonymiseret form.

SSI har vurderet, at "godkendelsesflowet" for *overførsler af personoplysninger* til tredjelande og internationale organisationer skal gennemgås, og at der skal afsættes ressourcer til løbende godkendelser. Det bemærkes, at spørgsmålet om overførsler til (usikre) tredjelande er behandlet i en dom fra EU-Domstolen, som blev afsagt i juli 2020 (C-311/18, Schrems II), og at implikationerne af dommen stadig er under afklaring.

Endvidere skal der udarbejdes procedure for sletning. SSI har oplyst, at arbejdet med at udarbejde procedure for opbevaringsbegrænsning, herunder sletning, er påbegyndt.

7) Awareness

Hvad angår *træning og uddannelse*, har SSI oplyst, at det er et krav, at samtlige ansatte på SSI skal gennemføre e-træning i GDPR-forståelse, og at kurserne afholdes med faste intervaller med henblik på løbende træning. Derudover har SSI oplyst, at man har afholdt awareness-kursus i sikkerhedsbrud og sletning af personoplysninger i mails og lokale drev for samtlige afdelinger.[3]

[3] Kammeradvokatens foreløbige vurdering af SSI's databeskyttelsesretlige compliance, side 86

Herudover har SSI oplyst, at man agter at udarbejde en kommunikationsplan om "kultur, træning og opmærksomhed med GDPR", således at relevante emner gennemgås løbende. Til dette formål vil SSI træne ledere i krav til træning af medarbejdere om nye procedurer samt gennemføre awareness-træning i informationssikkerhed og databeskyttelse. Dette inkluderer f.eks. et nyt interaktivt kursus for laboranter. Endvidere er der taget det initiativ, at træning af personale nu omfatter krav til awareness-træning i informationssikkerhed og GDPR, og der er indarbejdet træningsplan og træningsmatrix, som beskriver, hvilke medarbejdere der skal modtage træning i bestemte procedurer.

8) Risikostyring

Krav til og proces for udarbejdelse af *konsekvensanalyser* er under udarbejdelse. Samtidig skal der udarbejdes en procedure for *risikovurdering*, og risikovurderinger skal foretages.

Udarbejdelse af risikovurderinger er påbegyndt, og i den forbindelse udarbejder SSI en liste over it-systemer, som i almindelighed må betragtes som sikre (en "positivliste") at anvende som understøttelse til forskningsaktiviteter.

9) Hændelsesstyring

SSI har en procedure ved konstateret databrud. Endvidere er der et onlinekursus i databrud. Det er dog af SSI vurderet, at det er vanskeligt for medarbejdere at vurdere, hvornår der skal rapporteres.

Proceduren på intranettet i forhold til databrud indeholder otte spørgsmål, som medarbejderen skal besvare, hvorefter QA & Compliance vurderer, om det skal anmeldes til Datatilsynet i samråd med den koncernfælles DPO.

SSI mener, at tidligere anvendt awareness-kampagne om databrud kan genbruges. Herudover skal den eksisterende proces alignes og samles med øvrige hændelsesprocedurer eller -afvigelser. Proceduren for databrud skal gennemgås, og medarbejdere skal oplyses om, hvad databrud er. Endvidere skal der udarbejdes træning i proces med henblik på at få registreret alle databrud.

13) Fysisk adgang

Der er medio 2020 startet nye tiltag til forbedring af den fysiske sikkerhed på SSI i form af udbud af et nyt adgangskontrolsystem (ADK), herunder tiltag i form af zoneinddeling af Campus. Derudover er der iværksat tiltag til etablering eller forbedring af dataopbevaring og -arkivering, herunder proces for back-up og gendannelse samt gennemførsel af gendannelsesprocesser for kritiske it-systemer.

Hvad angår *den fysiske sikkerhed* ved SSI, har SSI ud fra gap-analysen vurderet, at politikken for fysisk sikkerhed skal genbesøges og tilpasses eventuelle nye krav. Endvidere skal der inkluderes krav til adfærd og færden i kritiske områder. Der skal foretages fysisk sikring af kontorer og kritiske områder.

14) Beredskab

SSI har oplyst, at beredskabsplaner skal genbesøges, herunder for proces for beredskabsplan for SSI, som tager højde for samspillet med Sundhedsdatastyrelsen. Krav til "back-up and restore" skal genbesøges og tilpasses krav til leverandører. Der er udarbejdet et udkast til en SOP for proces for og krav til etablering af nye it-systemer, herunder krav om "Information Security by Design" og "Privacy by Design". SOP skal endvidere indeholde krav til design af log.

3. PLAN FOR ARBEJDET MED GDPR-COMPLIANCE

3.1 Generelle overvejelser om prioriteringer og den overordnede plan

Som nævnt under afsnit 2.2.2 har SSI identificeret en række projektspor, som skal gennemføres for at forbedre compliance på SSI.

Særligt ni af projektsporene omfatter databeskyttelsesrelevante forhold. Flere af projektsporene indeholder også elementer, som sikrer overholdelsen af andre regler, standarder mv., hvilket skyldes hensigtsmæssigheden ved at samle etableringen af compliance i forhold til forskellige regler, standarder mv., hvor der er overlappende krav mv.

Alle projektspor kan ikke gennemføres på én gang – dels er der begrænsede ressourcer, dels er der gensidige afhængigheder mellem de forskellige projektspor. Man bliver nødt til at prioritere. Vi har sammen med SSI foretaget en prioritering og fastlagt en rækkefølge for gennemførelsen af de forskellige projektspor. Ved prioriteringen er der blandt andet lagt vægt på, hvilke forhold det af hensyn til sikringen af beskyttelsen af personoplysninger haster mest at få rettet op på, hvor der er det største behov for forbedring, samt om visse forhold er mere grundlæggende at få på plads end andre. Samtidig er der forhold, som forudsætter f.eks. it-mæssige investeringer mv., og som derfor kan have en længere tidshorisont.

Hertil kommer, at der ved prioriteringen har skullet tages hensyn til den henvendelse fra Datatilsynet, som omtales i afsnit 1.1, hvorved Datatilsynet anmoder SSI om at aflevere en række redegørelser mv. om udbedringen af en række forhold senest den 1. marts 2021. Det bemærkes i den forbindelse, at det f.eks. havde været naturligt at gennemføre arbejdet med forbedringen af SSI's fortegnelser som noget af det første, da dette arbejde kan anvendes i de øvrige projektspor, men henvendelsen fra Datatilsynet har

bevirket, at dette arbejde er sat på pause og først gennemføres efter udbedringen af de forhold, som tilsynet har anmodet SSI om at forholde sig til.

De ni projektspor, der særligt omfatter databeskyttelsesretlige forhold, er følgende:

- Ledelsesgovernance
- Fortegnelser
- Leverandørstyring, der i det følgende underopdeles på databehandleraftaler, tilsyn med databehandlere og kontraktstyring
- Registreredes rettigheder
- Datagovernance
- Awareness
- Risikostyring
- Hændelsesstyring
- It-projektstyring

De fem forhold, som Datatilsynet ønsker, at SSI adresserer i forhold til sine forskningsprojekter, er følgende:

- Databehandleraftaler
- Overførsler til tredjelande
- Tilladelser fra Datatilsynet
- Risikovurderinger (og konsekvensanalyser)
- Interne retningslinjer

På den baggrund har vi i fællesskab med SSI opstillet følgende fire deadlines for etablering af databeskyttelsesretlig compliance:

Deadline 1 (Datatilsynets henvendelse	
- Databehandleraftaler - Overførsler til tredjelande - Tilladelser fra Datatilsynet - Risikovurderinger - Interne retningslinjer	*Forventes implementeret ultimo 2020 (Q4)*

Deadline 2	
- Registreredes rettigheder (i det omfang det ikke er gennemført under Deadline 1) - Databehandleraftaler (i det omfang det ikke er gennemført under Deadline 1) - Tilsyn - Fortegnelser - Ledelsesgovernance	*Forventes implementeret medio 2021 (Q2)*
Deadline 3	
- Awareness - Hændelsesstyring - Risikostyring (i det omfang det ikke er gennemført under Deadline 1) - Datagovernance (i det omfang det ikke er gennemført under Deadline 1)	*Forventes implementeret ved udgangen af 2021 (Q4)*
Deadline 4	
- Kontraktstyring - It-projektstyring	*Forventes implementeret ved udgangen af 2022 (Q4)*

Det bemærkes, at baggrunden for, at de projektspor, der nævnes under Deadline 1, ikke nødvendigvis afsluttes her, er, at Datatilsynets henvendelse alene angik forskningsprojekter, og at arbejdet frem til Deadline 1 derfor koncentrerer sig derom. Det indebærer, at der kan være udeståender i de pågældende projektspor, der først tages hånd om efterfølgende. Endvidere bemærkes det, at skemaet ikke skal forstås således, at man først går i gang med projektsporene under de enkelte deadlines, når projektsporene under de forudgående projektspor er afsluttede. Derimod vil det formentlig for en række projektspors vedkommende være en forudsætning for at overholde den endelige deadline, at arbejdet med projektsporene iværksættes parallelt og meget tidligere. Endelig bemærkes det, at når man når frem til de pågældende deadlines, har SSI ikke nødvendigvis løst alle databeskyttelsesretlige problemer. Ambitionen er derimod, at man på dette tidspunkt er "i drift", forstået således, at der på dette tidspunkt er etableret et system for databeskyttelsesretlig compliance, og at det herefter handler om løbende at vedligeholde systemet og håndtere de problemer, der løbende må opstå.

SSI har oplyst, at for de fleste projektspor og projekters vedkommende har instituttet allerede påbegyndt implementeringen. Det bemærkes i den forbindelse, at selvom ledelsesgovernance er placeret under Deadline 2, så er det essentielt, at arbejdet dermed påbegyndes så tidligt som muligt, og alle ledelsesniveauer ved SSI har da også været inddraget i udarbejdelsen af den plan, der præsenteres her i rapporten. Det er således en forudsætning for vellykket gennemførelse af databeskyttelsesretlig compliance, at der hele vejen igennem forløbet er tilstrækkelig ledelsesmæssig opbakning på alle niveauer i organisationen.

Selvom awareness er placeret under Deadline 3, er det selvklart ligeledes vigtigt, at man på SSI tidligt begynder systematisk at arbejde med medarbejdernes kendskab til og opbakning bag den databeskyttelsesretlige compliance. I den forbindelse skal man selvfølgelig også være opmærksom på, at gennemførelsen af alle de øvrige projektspor selvfølgelig også har som afledt effekt, at kendskabet til (vigtigheden af) databeskyttelsesretten udbredes.

Det bemærkes, at overholdelse som sådan af de databeskyttelsesretlige regler etableres løbende, og at en del af projektsporene (og projekterne under sporene) ikke alene har til formål at sikre basal overholdelse af reglerne, men har til formål at gøre SSI til en moden organisation i databeskyttelsesretlig henseende, hvor den databeskyttelsesretlige compliance er indarbejdet som en naturlig del af arbejdsprocesserne og understøttes af hensigtsmæssige it-løsninger. Det sidstnævnte gør sig blandt andet gældende for de to projektspor under Deadline 4. Gennemførelsen af de to projektspor er således ikke en forudsætning for overholdelsen af reglerne som sådan.

3.2 Planen for gennemførelse af databeskyttelsesretlig compliance

I samarbejde med afdelingen for QA & Compliance ved SSI har vi fastlagt, hvorledes GDPR-compliance-samarbejdet kan koordineres med det øvrige compliancearbejde i overensstemmelse med den prioritering, som er angivet ovenfor under afsnit 3.1. Der er på den baggrund udarbejdet en mere detaljeret drejebog over compliance-opgaverne, der inkluderer databeskyttelsesretlig compliance. Drejebogen er et dynamisk redskab. Hvor de overordnede deadlines bør fastholdes, rummer drejebogen samtidig:

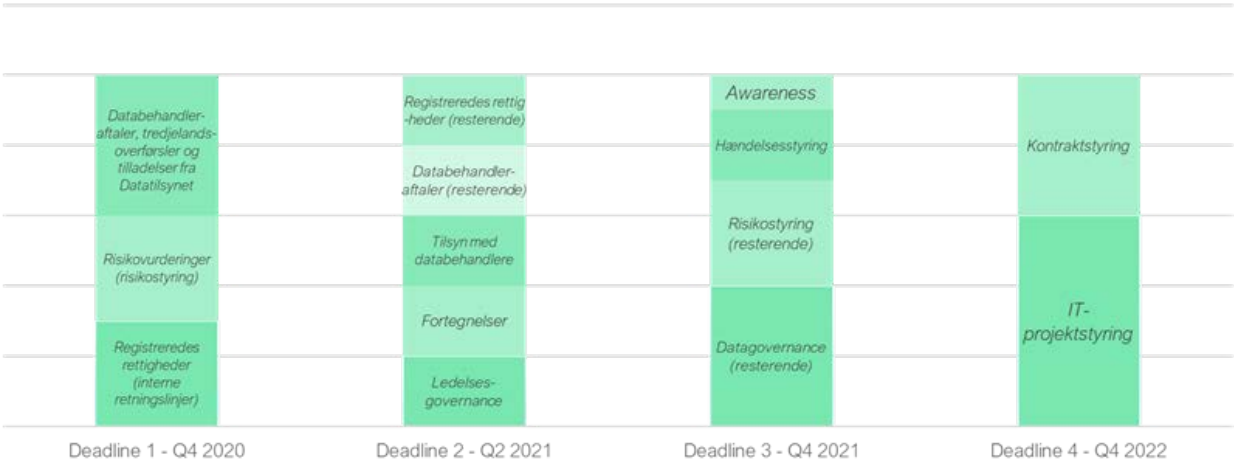
- Overbliksskemaer, hvor der løbende kan indsættes erfaringer fra det hidtidige arbejde og overvejelser om, hvilke næste skridt der skal foretages.
- Mulighed for løbende at indsætte yderligere delprojekter og milepæle

Drejebogen er udarbejdet således, at den kan anvendes til løbende afrapportering over for en styregruppe. Drejebogen vedlægges som bilag 1[4], og dens indhold er i øvrigt nærmere beskrevet nedenfor.

Projektsporene er inddelt i fire deadlines efter den prioritering, som fremgår ovenfor under afsnit 3.1.

[4] Drejebog for GDPR-compliance ved SSI pr. 1. november 2020.

Overblik over projektspor og de fire deadlines:



3.2.1 Deadline 1

Den første deadline omfatter de særlige fokusområder, som Datatilsynet har anmodet SSI om redegørelser for ved sin henvendelse af 9. oktober 2020. Den første deadline omfatter tre projektspor. Det bemærkes, at det også indgik i arbejdet forud for modtagelsen af Datatilsynets henvendelse, at områderne i disse projektspor skulle prioriteres højt, og at det arbejde, som allerede er påbegyndt ved SSI vedrørende udviklingen af disse områder i compliancerегi, understøtter den høje prioritering heraf.

SSI har udarbejdet målsætninger og tidsplaner for hvert projekt og dertilhørende aktiviteter, som sikrer udførelsen heraf. Det bemærkes, at anmodningen fra Datatilsynet har medført et tidspres for SSI, som dog forventes imødekommet ved omprioritering og inddragelse af ekstra ressourcer efter behov.

Hvad angår projektsporet om databehandleraftaler, tredjelandsoverførsler og tilladelser fra Datatilsynet, bemærkes det, at der indtil ultimo 2020 fokuseres på det, som henvendelsen fra Datatilsynet omhandler, dvs. forskningsprojekter og navnlig på at sikre, at de enkelte forskningsprojekter gennemføres i overensstemmelse med databeskyttelsesretten.

Hvad angår databehandleraftaler, vil det samlede projektspor først være afsluttet under Deadline 2. Projektsporet indebærer:

- Etablering af en samlet proces for håndtering af databehandleraftaler
- Etablering af overblik over databehandlere, som SSI på nuværende tidspunkt samarbejder med

- Indgåelse af manglende og opdatering af mangelfulde databehandleraftaler for eksisterende samarbejder. Hvis man ikke ved årsskiftet 2020/21 når i mål dermed, skal der – som en mellemliggende milepæl – som det mindste foreligge en plan for, hvorledes dette mål opnås, eller alternativt hvorledes de pågældende samarbejder afvikles.

Det bemærkes, at det er forventningen, at der er visse databehandlere, som SSI ofte og løbende samarbejder med, og at der derfor vil kunne opnås en stor og hurtig databeskyttelsesretlig effekt ved opdateringen af aftalerne med disse.

Hvad angår tredjelandsoverførsler og tilladelser fra Datatilsynet, indgår disse i projektsporet datagovernance, der først forventes afsluttet ved Deadline 3. Arbejdet hermed forudsætter:

- Etablering af en samlet proces for overførsel af persondata til tredjelande (tredjelandsoverførsler).
- Etablering af overblik over tredjelandsoverførsler, som SSI på nuværende tidspunkt foretager.
- Indgåelse af manglende og opdatering af mangelfulde aftaler. Hvis man ikke ved årsskiftet 2020/21 når i mål dermed, skal der – som en mellemliggende milepæl – som det mindste foreligge en plan for, hvorledes dette mål opnås, eller alternativt hvorledes de pågældende samarbejder afvikles.
- Indhentelse af nødvendige tilladelser fra Datatilsynet efter databeskyttelseslovens § 10, stk. 3.
- Etablering af et samlet overblik over overførsler, som SSI på nuværende tidspunkt foretager, og som kræver Datatilsynets tilladelse. Som en mellemliggende milepæl skal der være ansøgt om alle relevante tilladelser inden udgangen af 2020.

Hvad angår projektsporet om risikovurderinger, som også omfatter konsekvensanalyser (de såkaldte DPIA'er) gælder – som for databehandleraftaler, tredjelandsoverførsler og tilladelser fra Datatilsynet – at der indtil ultimo 2020 fokuseres på det, som henvendelsen fra Datatilsynet omhandler, dvs. forskningsprojekter og navnlig på at sikre, at de enkelte forskningsprojekter gennemføres i overensstemmelse med databeskyttelsesretten. I øvrigt indgår risikovurderinger i projektsporet risikostyring, som forventes afsluttet ved Deadline 3. Arbejdet omfatter en plan for implementeringen af anvendelse og håndtering af risikovurderinger ved SSI, hvilket blandt andet omfatter udarbejdelse af praktisk anvendelige skabeloner for risikovurderinger.

Endelig skal der udarbejdes tilstrækkelige interne retningslinjer, idet det bemærkes, at arbejdet med registreredes rettigheder fortsætter efterfølgende og indgår under Deadline 2. Arbejdet omfatter blandt andet:

- Etablering af en proces for, at oplysningspligten over for de registrerede sikres.
- Etablering af proces for borgerhenvendelser (som det i øvrigt bemærkes, at SSI i 2020 har modtaget et stort antal af, og som det forventes, at SSI fortsat vil modtage mange af), herunder etablering af proces for håndtering af henvendelser om indsigt, sletning, berigtigelse mv.
- Etablering af proces for tilfælde, hvor der skal indsamles samtykke fra den registrerede, samt for en ensrettet håndtering af indhentede samtykker

Inden udgangen af februar 2021 skal der være udfærdiget opdaterede interne retningslinjer på SSI's intranet. Der skal endvidere være udfærdiget en ajourføring af de retningslinjer for registreredes rettigheder, som er tilgængelige eksternt på SSI's hjemmeside.

3.2.2 Deadline 2

Deadline 2 omfatter især fokusområderne for tilsyn, håndtering af fortegnelser samt ledelsesgovernance ved SSI. Desuden omfatter Deadline 2 projektsporene databehandleraftaler og registreredes rettigheder, som er omtalt ovenfor under Deadline 1. Deadline 2 omfatter således i alt fem projektspor, og alle er allerede påbegyndt.

Idet sikring af de registreredes rettigheder er højt prioriteret ved SSI, er det bestemt, at såfremt der foreligger mangler, som vedrører de registreredes rettigheder, men som ikke relaterer sig til etablering eller ajourføring af SSI's retningslinjer herfor (og dermed Datatilsynets anmodning), skal disse håndteres inden for Deadline 1, således at eventuelle udeståender er håndteret medio 2021.

Hvad angår projektsporet om tilsyn, indebærer det etablering af en proces for tilsyn med databehandlere, som SSI på nuværende tidspunkt har. Processen skal blandt andet omfatte håndtering af revisionserklæringer. Endvidere skal der etableres en plan og et program for årlige tilsyn, idet det bemærkes, at der allerede er lavet en plan for 2021. SSI skal inden medio 2021 have gennemført tilsyn med mindst to databehandlere.

Arbejdet med ajourføring af SSI's fortegnelser over databehandlinger er allerede påbegyndt. Som en mellemliggende milepæl skal der inden udgangen af januar 2021 være etableret en proces for håndtering af fortegnelserne. Der skal i den forbindelse etableres proces for sletning. Herudover skal der etableres proces for rolle- og ansvarsdelegering.

Hvis det viser sig, at der mangler eller er mangelfulde oplysninger i fortegnelserne, skal disse indføres eller ajourføres. Samlet set er målet, at eksisterende fortegnelser er fuldt opdateret medio 2021.

Til understøttelse af gennemførelsen af compliance for databeskyttelse er der på området for ledelses-governance udarbejdet en række milepæle, som relaterer sig til det overordnede compliance-arbejde ved SSI. Det er således bestemt, at interessentlandskabet for dette skal være kortlagt inden udgangen af januar 2021. Inden 1. april 2021 skal der endvidere etableres udvalg for henholdsvis Kvalitets- og Compliance, It-sikkerhed samt It-digitalisering.

Hertil kommer, at der inden udgangen af januar 2021 skal identificeres stillingsbeskrivelser og herefter etableres træningsplan og træningspakker for henholdsvis ledere og it-sikkerhedsudvalget inden medio 2021.

Endelig skal der etableres målepunkter (KPI'er) for rapportering og rapportskabelon til SSI's øverste ledelse (i form af Topledelsesevalueringen, som udvides med informationssikkerhed og databeskyttelse).

Projekterne omfattet af Deadline 2 forventes således for alle projektsporenes vedkommende færdiggjort medio 2021.

3.2.3 Deadline 3

Deadline 3 omfatter projektsporene awareness, hændelsesstyring, risikostyring samt datagovernance. Arbejdet med sikring af compliance for alle sporene er allerede påbegyndt.

Awareness om databeskyttelse er højt prioriteret ved SSI, og det er implicit, at alle synlige tiltag vedrørende databeskyttelsesmæssig compliance vil skabe en vis grad af awareness ved institutionen. For at sikre, at der løbende og fremadrettet holdes fokus på databeskyttelse, er det besluttet, at der skal være etableret en proces for løbende awareness-kampagner. Det kommende års awareness-kampagner fastlægges årligt af topledelsen, ligesom effekten af det forudgående års kampagner evalueres en gang årligt af topledelsen.

Hvad angår hændelsesstyring, skal der pr. 1. oktober 2021 være etableret en proces for håndtering af hændelser, *Incident Management*. Endvidere skal der etableres en overordnet proces for hændelsesstyring ved SSI, og der skal specifikt foreligge en proces for håndtering af kritiske databrud.

Hvad angår risikostyring, skal der – som en mellemliggende milepæl – senest 1. oktober 2021 være etableret en overordnet proces for håndtering af risiko, *Risk Management*. Endvidere skal der – som endnu en mellemliggende deadline – senest 1. november 2021 være etableret en overordnet proces for it-sikkerhed.

Herudover skal der som yderligere milepæle ved udgangen af november 2021 være etableret en proces specifikt for rolle- og ansvarsdelegering under Risk Management, og ved udgangen af november 2021 skal der være etableret en proces for udarbejdelse og håndtering af konsekvensanalyser.

Hvad angår projektsporet datagovernance, bør der allerede være gennemført tiltag herom i forbindelse med tidligere deadlines. Der henvises i øvrigt til Deadline 1, for så vidt angår tiltag vedrørende overførsler til tredjelande og tilladelse fra Datatilsynet.

Som en mellemliggende milepæl skal der senest den 1. august 2021 foretages en klassifikation af data og etableres de nødvendige processer. Der skal etableres en overordnet proces for opbevaring af data. Desuden skal der etableres en proces for sletning af data. Herudover skal der etableres en proces for styring af dokumenter/data og arkivering af disse, som dog forventes at være mere omfattende, og derfor først forventes etableret ved udløbet af Deadline 3.

Som en mellemliggende milepæl skal der etableres en proces for videregivelser internt i SSI senest den 1. marts 2021. Herudover skal der etableres proces for videregivelser til og fra Sundheds- og Ældreministeriet. Der skal ligeledes etableres en proces for videregivelser eksternt til samarbejdspartnere.

Projekterne omfattet af Deadline 3 forventes således for alle projekternes vedkommende færdiggjort ved udgangen af 2021.

3.2.4 Deadline 4

Deadline 4 omfatter projektsporene kontraktstyring og it-projektstyring. Der er tale om områder, hvor gennemførelse af compliance påkræver en større tidsramme, hvorfor tidsrammen forventes at løbe til ultimo 2022. Området omfatter således to større projekter, hvortil arbejdet med compliance allerede er påbegyndt. Det er ligeledes områder, der formentlig kræver investeringer af en vis størrelse. Det bemærkes, at det forventes, at SSI skal gennemføre et leverandørskifte i forhold til it på et tidspunkt i 2021, hvilket kan få betydning for gennemførelsen af de to projektspor.

Hvad angår kontraktstyring, skal der ske en identificering, kategorisering og hierarkisering af de kontrakttyper, som SSI på nuværende tidspunkt anvender. Som en mellemliggende milepæl skal dette ske inden 1. marts 2022. Derudover skal der være etableret en overordnet proces for kontraktstyring ved SSI inden udgangen af 2022.

Hvad angår projektsporet it-projektstyring, er det i forhold til implementering af databeskyttelsesforordningens princip om "Privacy by Design" besluttet, at der som en mellemliggende milepæl skal være foretaget en afklaring af projektmodet for SSI og Sundheds- og Ældreministeriet senest den 1. marts 2022.

Projektsporet omfatter i øvrigt:

- Etablering af en proces for alignment af et it-projektmodul, herunder genbesøg af procesbaseret it-flow for godkendelse af projekter
- Etablering af en proces for porteføljestyring

Som en mellemliggende milepæl skal der inden 1. juli 2022 være etableret en proces for *Life Cycle Management* af it-systemer, herunder både for etablering af nye it-systemer og for den løbende drift deraf.

Der skal endvidere – som en mellemliggende milepæl – inden udgangen af februar 2022 være etableret en proces for håndtering og gennemførsel af periodiske review af it-systemer, ligesom der inden den 1. juli 2022 skal være etableret proces for *Data Integrity*.

Projekterne omfattet af Deadline 4 forventes således for alle projekternes vedkommende færdiggjort ved udgangen af 2022.

3.3 Overvejelser om anvendelse af planen mv. på andre forskningsinstitutioner mv.

Den 13. oktober 2020 annoncerede Datatilsynet, at det vil iværksætte en undersøgelse af forskningsområdet. Som det fremgår af Datatilsynets pressemeddelelse, er der i mange forskningsprojekter tale om behandling af store mængder af personoplysninger, herunder følsomme oplysninger. Derfor er det ifølge Datatilsynet afgørende, at reglerne på forskningsområdet overholdes for at kunne varetage hensynet til de enkelte registrerede. Med henblik på at undersøge, om de databeskyttelsesretlige problemstillinger, som blev afdækket ved vores undersøgelse af SSI, ligeledes gør sig gældende ved andre forskningsinstitutioner, har Datatilsynet iværksat et skriftligt tilsyn af en række andre offentlige myndigheder, som udfører forskning. Tilsynene fokuserer på:

- Roller og ansvar (dataansvar)
- Behandlingsgrundlag
- Overførsel af personoplysninger til modtagere i EØS-lande og til modtagere i lande uden for EU
- Tilsyn med databehandlere
- Datatilsynets eventuelle tilladelse til videregivelse
- Fortegnelse
- Politikker/retningslinjer om databeskyttelse i forbindelse med gennemførelse af forskningsprojekter

Endvidere har Datatilsynet besluttet at udarbejde en ny vejledning på forskningsområdet, og med henblik herpå har Datatilsynet indledt et samarbejde med i første omgang Sundheds- og Ældreministeriet.

De erfaringer, som SSI har gjort sig, og de værktøjer mv., som SSI udvikler som led i det compliancearbejde, som denne rapport indeholder en plan for, vil andre forskningsinstitutioner mv. formentlig også kunne drage læring af.

Desuden vil andre forskningsinstitutioner mv. formentlig også kunne drage nytte af selve planen og den til rapporten tilknyttede drejebog. Selvfølgelig vil de enkelte institutioner i første omgang skulle afdække, om tilsvarende problemer gør sig gældende ved dem, hvilket kan have betydning for, hvor lang tid det i givet fald vil tage at blive databeskyttelsesretlig compliant, men grundlæggende vil det være de samme elementer mv., der skal gennemgås.

Behandlingen af personoplysninger på forskningsområdet er på mange måder særlig sammenlignet med behandlingen af personoplysninger på andre områder. Blandt andet er det karakteristisk for forskningsområdet, at formålet med behandlingen og den databeskyttelsesretlige rollefordeling kan udvikle sig hen over forløbet af et forskningsprojekt, blandt andet fordi der er tale om en kreativ proces, hvor de involverede parter løbende udveksler tanker om og idéer til, hvorledes man kan udvikle nye produkter og få nye indsigter ved brugen af de oplysninger, som man har til rådighed. Det medfører, at man ved udførelsen af forskning løbende må gøre sig databeskyttelsesretlige overvejelser. Hvis f.eks. rollefordelingen ændrer sig, eller hvis behandlingsformålet ændrer sig, kan der være behov for at genbesøge sikkerhedsvurderinger, konsekvensanalyser og det grundlæggende databeskyttelsesretlige set-up. Samtidig kan forskningsområdets særlige karakter give anledning til at overveje, om der skal laves særlige regler mv. for området.

Det fremgår af de almindelige bemærkninger til den gældende databeskyttelseslov, jf. pkt. 2.3.6.3 i lovforslag L 68 af 25. oktober 2017, at det blev vurderet hensigtsmæssigt at foretage et eftersyn af den samlede lovgivning på området for forskningsmæssig og statistisk behandling af personoplysninger. Som det fremgår af bemærkningerne, var det således hensigten, at der skulle nedsættes en tværministeriel arbejdsgruppe, som skulle se på lovgivningen med inddragelse af blandt andet Datatilsynet og med den målsætning, at lovgivningen skal være sammenhængende, og at den skal sikre en høj beskyttelse af personoplysningerne, samtidig med at den understøtter behovet for at være let at forstå og anvende for såvel borgere som udøvere af forskning og statistik. Der var således fra lovgivers side en erkendelse af, at området er særligt vanskeligt og kræver særlige overvejelser. Vi er imidlertid ikke bekendt med, at den nævnte arbejdsgruppe blev nedsat.

Det synes på den baggrund hensigtsmæssigt og kun helt naturligt, at Datatilsynet nu tager initiativ til at undersøge området, herunder med bevidstheden om, at lovgivers tidligere erkendelse af behovet for at

efterse området ikke har ledt til iværksættelsen af et konkret initiativ. Der synes at være et behov for etablering af en ensartet databeskyttelsesretlig praksis på området.

Det kan i øvrigt overvejes, om forskningsområdet har sådanne karakteristika, at det kan være hensigtsmæssigt at udvikle en adfærdskodes for området, som kan være med til at bidrage til korrekt anvendelse af databeskyttelsesretten. Databeskyttelsesforordningen indeholder en bestemmelse om adfærdskodekser, jf. artikel 40, men en kodeks vil kunne udvikles både inden for eller uden for rammerne deraf.