Rapport fra Danmarks Statistiks DPO-team vedrørende efterlevelse af GDPR - 2019

Indhold

1. Indledning

Denne rapport er udarbejdet til Direktionen i Danmarks Statistik (DST) af DST's DPO-team (DPO). Rapporten er i udgangspunktet udarbejdet til DST, hvorfor DST alene beslutter, hvorvidt dele eller hele rapporten skal offentliggøres eller på anden måde deles med andre.

DPO er nærmere beskrevet i 'Kommissorium DPO-teamet', der er godkendt af Direktionen i DST. DPO skal bl.a. rådgive om Databeskyttelsesforordningen (GDPR) og overvåge overholdelsen af GDPR i DST. DPO vil årligt udarbejde en rapport til Direktionen i DST, hvor DPO vil redegøre for, hvorledes GDPR er implementeret. DPO vil i denne rapport også komme med forslag til eventuelle forbedringstiltag.

Denne rapport beskriver, hvorledes DST lever op til udvalgte områder af Databeskyttelsesforordningen (GDPR) samt de bestemmelser i Databeskyttelsesloven, der implementerer dele af GDPR i Danmark. Rapporten skal læses i forlængelse af den tilsvarende rapport for 2018. Vægtningen mellem de forskellige artikler er en smule anderledes end rapporten for 2018. Dette skyldes bl.a. de sager vedrørende databeskyttelse, DST har haft, og de områder DST har arbejdet med det seneste år.

Rapporten er bygget op omkring udvalgte artikler i GDPR. Artiklerne vil blive gennemgået i separate afsnit opbygget på følgende måde: 1) Beskrivelse af artikel og dennes relevans. 2) Vurdering af efterlevelse. 3) Vurdering og forslag til evt. forbedringstiltag. Vurderingen af efterlevelsen i punkt 2) vil ske på baggrund af det kendskab DPO har til DST. Punkt 3 vil indeholde forslag til, hvorledes DST kan sikre en bedre efterlevelse af GDPR ift. den konkrete artikel.

Dette er den anden DPO-rapport skrevet til DST i den periode, hvor GDPR har været gældende. Rapporten kan med fordel læses i sammenhæng med den tidligere rapport fra februar 2019. På de områder og afsnit, hvor der ikke er sket udvikling det seneste år, vil rapporten være meget lig den tidligere rapport. I flere afsnit vil der blive kommenteret på, hvorvidt DST har igangsat eller fuldt ud implementeret tiltag på baggrund af den tidligere rapport.

2. Sammenfatning, opfølgning på tidligere anbefalede forbedringstiltag og anbefalinger til forbedringstiltag

DPO finder, at DST lever op til de krav og rettigheder, der fastsættes i GDPR. Konklusionen er derfor, at DST efterlever GDPR.

Opfølgning på sidste års anbefalinger

I februar 2019 anbefalede DPO nedenstående forbedringstiltag. Ved hvert forbedringstiltag er tilføjet, hvorledes DPO mener, der er blevet fulgt op på forbedringstiltaget gennem det seneste år.

- DST behandler oplysninger til statistiske formål, hvilket DST oplyser de registrerede om, når oplysningerne indsamles eller de registrerede henvender sig til DST. Alligevel videregives enkelte oplysninger til AUB, der benytter oplysningerne til administrative formål. DST bør derfor overveje, hvorvidt der er uoverensstemmelse mellem de faktiske forhold, og det DST oplyser til respondenterne?
    - DPO finder det yderst tilfredsstillende, at DST gennem de seneste år har haft og stadig har fokus på formålsbegrænsningen. DPO anerkender det arbejde, DST i samarbejde med UVM har gjort, for at finde en brugbar løsning i forhold til AUB. DPO finder det yderst tilfredsstillende at DST ift. eventuelle nye lovgivninger har arbejdet for løsninger, hvor der tages hensyn til formålsbegrænsningen.
- Det bør gennemgås, hvilken hjemmel der er for de forskellige behandlinger, der sker i DST. Der bør være et særligt fokus på, hvorvidt der er tilstrækkelig og korrekt hjemmel for indsamling af oplysninger i de forskellige dele af DST. Herunder kan det med fordel undersøges, hvorvidt der er hjemmel til indsamling af oplysninger, hvis disse ikke benyttes i DST's statistikproduktion, men alene benyttes i Lovmodellen?
    - DST har gennem det seneste år haft specielt fokus på Lovmodellen. DST har i samarbejde med FM udviklet og er i gang med at implementere en række procedureændringer og processer, der gør, at Lovmodellen i højere grad lever op til kravene i GDPR. Det er DPO's holdning, at de nye procedurer og processer er en klar forbedring af Lovmodellens efterlevelse af GDPR. DPO mener, at skal Lovmodellen sikres mere, skal der kigges på den grundlæggende opbygning af Lovmodellen. En yderligere opstramning i Lovmodellen kunne være, at Lovmodellens medarbejdere med administrationsrettigheder blev flyttet fra finansministeriet til DST.
- DST bør gennemgå, hvorvidt DST lever op til oplysningspligten, når oplysningerne indsamles hos den registrerede.
    - DPO anerkender, at der i DST er fokus på opfyldelse af oplysningspligten. Dette arbejde er dog ikke afsluttet, hvorfor et stadigt fokus er nødvendigt. Der bør være et særligt fokus, når den registrerede ikke er myndig eller tilhører en særlig sårbar gruppe.
- Der udarbejdes en guide om, hvorledes kontrollen med DST's forskellige databehandlere bør foregå? Kontrollen bør med stor sandsynlighed være forskellige fra situation til situation, hvorfor guiden skal fokusere på, hvorledes den korrekte kontrol vælges.
    - DPO er bekendt med, at en guide er udarbejdet og sendt til de relevante aktører i DST.
- Opgaverne i DST Survey gennemgås, så der kommer klarhed over DST's rolle i de enkelte opgaver. Alt efter om DST er dataansvarlig eller databehandler, vil de lovgivningsmæssige krav være

forskellige. En sådan gennemgang og evt. ændringer af praksis vil koste tid og ressourcer. DPO anbefaler dog at det sker.
    - DPO har i samarbejde med DST Survey haft en overordnet gennemgang og analyse af procedurerne i DST Survey. Den overordnede analyse viser, at der er gode procedurer i DST Survey. På enkelte områder kan der med fordel udarbejdes klarere og skriftlige procedurer.
- Der nedskrives overordnede retningslinjer for, hvornår et brud er så alvorligt, at de registrerede bør underrettes?
    - DPO finder, at tilfredsstillende tiltag er gennemført.
- Der laves mere konkrete konsekvensanalyser og risikovurderinger for de enkelte behandlinger. Dette bør særligt gøres, når der igangsættes nye typer af behandlinger.
    - DST har bedt DPO udarbejde retningslinjer til, hvornår og hvorledes der bør udarbejdes risikovurderinger og konsekvensanalyser. DPO finder, at dette er positivt. DPO er bekendt med, at retningslinjer er på vej.

Anbefalinger til forbedringstiltag

I DPO-rapport 2019 kommer DPO med en række anbefalinger til forbedringstiltag. De vigtigste anbefalinger er følgende:

- Der sker en omfattende sletning af mails i Outlook. Da stort set alle mails vil indeholde personoplysninger, fx ansættelsesmæssige oplysninger om afsenderen, vil en sletning sikre dataminimering. Da Outlook ikke er karakteriseret som et sikkert journaliseringssystem, så bør oplysninger, der ikke skal slettes, journaliseres i et sikkert system. Når der træffes beslutning om, hvorvidt en mail og oplysninger skal slettes, skal der tages højde for relevant lovgivning såsom offentlighedsloven.
- Det sikres, at der sker det nødvendige tilsyn med de databehandlere, DST benytter. Det er den enkelte systemejer i DST der er ansvarlig for at føre tilsyn med deres databehandlere. Der kan internt i DST indføres en procedure for, hvorledes det sikres, at den enkelte systemejer har foretaget det nødvendige tilsyn med databehandlere.
- Der rettes fokus mod korrekt efterlevelse af oplysningspligten, når oplysninger indsamles hos de registrerede. Der bør særligt være fokus på oplysningspligten, når der indsamles oplysninger hos ikke-myndige personer eller udsatte borgere.
- Særligt i forbindelse med nye behandlinger kan der med fordel i højere grad udarbejdes konsekvensanalyser, så det sikres, at behandlingerne sker på bedst mulig måde.

3. GDPR artikel 5: Principper for behandling af personoplysninger

I GDPR's artikel 5 listes en række principper, som altid skal efterleves, når der behandles personoplysninger. Fokus i denne rapport vil være på formålsbegrænsning og dataminimering, da disse er vurderet særlig vigtige for DST.

1. b) Formålsbegrænsning

Baggrund

I GDPR artikel 5 paragraf 1 b) fastslås det, at behandling af oplysninger altid skal ske til udtrykkeligt angivne og legitime formål. Yderligere fastsættes det, at oplysninger ikke må viderebehandles til formål, der er uforenelige med det oprindelige formål, hvortil oplysningerne blev indsamlet. Dog vil viderebehandling til statistiske og videnskabelige formål ikke være uforenelige med de oprindelige formål.

Efterlevelse

DST behandler – som institution – oplysninger til flere forskellige formål. DST behandler oplysninger om de ansatte i DST til administrative formål. Dette gøres efter de retningslinjer og lovgivninger, som gælder for alle offentlige institutioner. De registrerede er fuldt oplyste om, at deres oplysninger bliver behandlet, hvad formålet med behandlingen er og deres rettigheder som registreret. Denne information gives til alle medarbejdere i DST.

DST indsamler og behandler også kunde- og kontaktoplysninger. Når disse indsamles, informeres kunderne om, til hvilke formål oplysningerne skal benyttes.

Langt den største del af oplysningerne i DST indsamles og behandles dog udelukkende til statistiske eller videnskabelige formål. Dette gør, at der gælder en række særlige bestemmelser for behandlingen af oplysningerne, og der gælder også undtagelser i forhold til de registreredes rettigheder. Det betyder samtidig, at disse oplysninger i udgangspunktet ikke må videregives til andre formål, f.eks. administrative formål. Mange oplysninger indsamles ikke direkte hos de registrerede, mens andre oplysninger indhentes direkte hos de registrerede.

Når oplysninger indsamles hos respondenterne (de registrerede), oplyses disse om indsamlingernes formål og om deres rettigheder. Respondenterne oplyses om, at deres oplysninger alene vil blive behandlet til statistiske eller videnskabelige formål. Som beskrevet i rapporten fra februar 2019, har DPO konstateret, at i minimum et tilfælde videregiver DST oplysningerne til andre formål. Generelt sker der dog ikke videregivelse, der strider mod formålsbegrænsningen. DST har også været aktiv omkring eventuelle nye lovgivninger, så det sikres, at formålsbegrænsningen overholdes.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST i høj grad lever op reglerne om formålsbegrænsning. Både når det gælder den enkelte ansatte, DST's brugere/kunder og respondenter, oplyses disse om, til hvilke formål deres oplysninger vil blive behandlet. Samtidig sørger DST for, at oplysninger ikke videregives eller behandles til formål, som er uforenelige med formålet, hvortil de oprindeligt blev indsamlet.

DST har i samarbejde med UVM arbejdet for at finde en løsning, der i højere grad skulle gøre videregivelsen af oplysninger til AUB i overensstemmelse med GDPR. På trods af at der ikke er fundet en alternativ løsning, er det yderst positivt, at der har været fokus på problemstillingen.

DPO finder det meget positivt, at DST har været aktiv ift., at evt. nye lovgivninger ikke vil stride mod formålsbegrænsningen. DPO anbefaler, at DST fortsat forsøger at sikre, at ny lovgivning, hvor oplysninger fra DST evt. skal videregives, tager højde for formålsbegrænsningen.

1. c): Dataminimering

Baggrund

I GDPR artikel 5 paragraf 1 c) fastslås det, at behandlingen af personoplysninger skal være tilstrækkelige, relevante og begrænsede (dataminimering). I praksis betyder det, at der ikke skal indhentes flere oplysninger end det til formålet nødvendige. Samtidig bør behandlingen og adgangen til de konkrete oplysninger begrænses til et minimum.

Efterlevelse

Langt de fleste af de oplysninger, der behandles i DST, behandles udelukkende til statistiske eller videnskabelige formål. DST ønsker at påføre respondenterne en så lav indberetningsbyrde som muligt, hvorfor de ikke stilles flere spørgsmål end det er nødvendigt. Dette bidrager til dataminimering, da DST dermed ikke kommer til at have flere oplysninger om de registrerede end der er nødvendige for udarbejdelse af de konkrete statistiske produkter. Dette er med til at sikre, at de indberettede oplysninger bliver så korrekte som muligt, og at respondenterne vil deltage i andre undersøgelser. Ofte vil DST kunne berige oplysningerne om respondenterne med en lang række baggrundsvariable. Dette kræver dog, at DST kender respondenternes cpr-nr. Når DST spørger om respondenternes cpr-nr., er dette faktisk med til at sikre dataminimeringen.

En måde at sikre dataminimering internt i DST er, at så få personer har adgang til så få oplysninger i så kort tid som muligt. DST sikrer dette via halvårlige gennemgange af medarbejdernes adgangstildelinger, der har til formål at sikre, at medarbejderne kun er tildelt aktuelle, arbejdsbetingede rettigheder.

Grundlaget for disse gennemgange er en identifikation af, hvilke data DST anser for fortrolige, og hvem der er ansvarlige for disse. I det efterfølgende er det forudsat, at den dataansvarlige er en personaleansvarlig chef.

Der udtrækkes halvårligt, hvilke medarbejdere der har adgang til hvilke data. Der gennemføres så halvårligt skiftevis opfølgning 1. og opfølgning 2.

1. Hver enkelt kontorchef tager stilling til om dennes medarbejdere fortsat har behov deres adgange til både egne og andres oplysninger.
2. Hver enkelt kontorchef tager stilling til, hvilke medarbejdere i hele DST, der fortsat har brug for adgang til dennes chefs oplysninger.

Opfølgningsoversigterne udarbejdes pr. chef, således at ingen har den fulde oversigt. Hvis der ikke længere er arbejdsbetingede behov for adgang, så skal der ske en fjernelse af adgangen. Resultatet af opfølgningerne dokumenteres, og det rapporteres til Direktionen.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST har en særdeles god praksis ift. dataminimering.

4. GDPR artikel 6: Lovlig behandling

Baggrund

Når oplysninger behandles, er behandlingen lovlig, hvis den opfylder et af følgende forhold:

a) Den registreredes samtykke
b) Kontraktlig forpligtigelse med den registrerede
c) Retlig forpligtigelse som påhviler den dataansvarlige
d) Beskyttelse af personers vitale interesser
e) Offentlig myndighed, der udfører en opgave i samfundets interesse
f) Forfølge legitim interesse, hvis ikke den registreredes grundlæggende rettigheder går forud

Efterlevelse

Når DST behandler personaleoplysninger eller oplysninger om kunder, vil det oftest ske efter enten samtykke eller kontraktlig forpligtigelse (a og b). Dette bliver oplyst til personale og kunder.

Behandling af oplysninger om respondenterne vil ske som offentlig myndighed, der udfører opgave i samfundets interesse (e).

Vurdering og evt. forbedringstiltag

Det er DPO's vurdering, at de behandlinger der foretages af DST er fuldt lovlige. Yderligere er DST bevidst om, hvorfor behandlingerne er lovlige. Det bør dog undersøges nærmere, hvorvidt DST i alle tilfælde informerer de registrerede om, hvorfor behandlingen er lovlig. Det bør klart fremgå af de informationer, DST giver respondenterne, hvorfor behandlingen er lovlig. Der bør være henvisninger til de relevante artikler i GDPR, Lov om Danmarks Statistik, anden relevant national lovgivning og EU-lovgivning.

Udover den normale statistikproduktion tilbyder DST via DST Consulting, DST Survey og Forskningsservice mere specialiserede statistiske ydelser. DPO anbefaler, at det gøres klart, hvilken hjemmel disse ydelser udarbejdes efter. De enkelte opgaver, der løses i forbindelse med disse ydelser, bør ligeledes altid vurderes ift. den konkrete hjemmel, før løsningen af opgaverne påbegyndes.

5. GDPR artikel 7: Betingelser for samtykke

Baggrund

Hvis en behandling er baseret på den registreredes samtykke, skal samtykket påvises. Det skal sikres, at registrerede har forstået, hvad samtykket indebærer, og at samtykket er afgivet frivilligt.

Efterlevelse

Når DST indhenter samtykke, får de registrerede oplyst deres rettigheder.

Vurdering og evt. forbedringstiltag

DPO vurderer, at betingelserne for samtykke opfyldes.

6. GDPR artikel 9: Behandling af særlige kategorier af personoplysninger

Baggrund

Behandling af en række særlige kategorier af personoplysninger er i udgangspunktet forbudt. Dog er der en række undtagelser til dette forbud. Det er bl.a. lovligt at behandle disse særlige kategorier, hvis formålet med behandlingen udelukkende er statistisk eller videnskabeligt.

Efterlevelse

Når DST behandler særlige kategorier af personoplysninger, sker det til statistiske eller videnskabelige formål.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST behandling af særlige kategorier af personoplysninger sker inden for rammerne af GDPR.

7. GDPR artikel 13: Oplysningspligt ved indsamling af personoplysninger hos den registrerede

Baggrund

Når der indsamles oplysninger hos den registrerede, skal den registrerede gives en række informationer. De forskellige forhold der skal gives oplysninger omkring listes i artiklen i GDPR.

Efterlevelse

Det er DPO's vurdering, at DST giver de registrerede de rette informationer, når DST indsamler oplysninger hos de registrerede. DPO er dog bekendt med, at en anden statslig organisation har modtaget alvorlig kritik fra Datatilsynet, da der efter Datatilsynets opfattelse ikke er sket den tilstrækkelige oplysningspligt i forbindelse med en indsamling af oplysninger hos unge under 18 år. Datatilsynet indikerede, at når der indsamles oplysninger hos unge under 18 år, så skal oplysningspligten ske ift. forældrene. Ud fra DPO's oplysninger, så sker der oplysningspligt til forældrene, når DST indsamler oplysninger hos unge under 18 år.

Vurdering og evt. forbedringstiltag

Det er DPO's anbefaling, at DST har et ekstra fokus på området. Når der sker indsamling af oplysninger hos unge under 18 år, ikke-myndige personer eller hos særligt udsatte grupper, så bør DST have et ekstra fokus på, hvorledes oplysningspligten bedst udføres i de enkelte indsamlinger.

8. GDPR artikel 14: Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede

Baggrund

Når personoplysninger ikke indsamles hos den registrerede, skal den registrerede gives en række oplysninger. Dog er der flere tilfælde, hvor der kan undtages ift. denne oplysningspligt. En sådan undtagelse er, hvis oplysningspligten vil kræve en uforholdsmæssig stor indsats, her nævnes bl.a. i forbindelse med behandling til statistiske og videnskabelige formål.

Efterlevelse

Det er DPO's vurdering , at det vil kræve en uforholdsmæssig stor indsats at oplyse registrerede, når DST behandler oplysninger, der ikke er indsamlet hos den registrerede – især når det tages i betragtning, at oplysningerne udelukkende benyttes til statistiske eller videnskabelige formål.

Vurdering og evt. forbedringstiltag

Det vurderes, at DST lever op til kravene i artiklen.

9. GDPR artikel 15-20: Den registreredes rettigheder

Baggrund

Det er den dataansvarliges forpligtigelse at træffe de foranstaltninger, der er nødvendige for at kunne opfylde de registreredes rettigheder. Hvilke rettigheder, der er gældende for den pågældende oplysning, vil afhænge af, til hvilket formål oplysningen indsamles og behandles.

For oplysninger, der udelukkende er indsamlet og behandles til statistiske eller videnskabelige formål, er der i GDPR indskrevet en række undtagelser for de registreredes rettigheder. Yderligere giver artikel 89 paragraf 2 mulighed for at indføre yderligere undtagelser i enten EU-lovgivning eller national lovgivning. I den danske databeskyttelseslov er indskrevet undtagelser for de registreredes rettigheder, hvis oplysningerne udelukkende behandles til statistiske eller videnskabelige formål. Samlet betyder det, at oplysninger, der behandles til statistiske eller videnskabelige formål, er undtaget fra de fleste af de registreredes rettigheder. Vigtigt er det dog at bemærke, at dette ikke er gældende for oplysninger der behandles til andre formål, f.eks. personaleoplysninger eller kundeoplysninger.

Efterlevelse

DST har udarbejdet materiale, hvor de registrerede kan læse om deres rettigheder. Dette kan læses på https://www.dst.dk/da/OmDS/lovgivning/danmarks-statistiks-efterlevelse-af-gdpr. Som beskrevet i ovenstående, er der forskellige rettigheder alt efter behandlingens formål. DST har en procedure for, hvorledes henvendelsen vedrørende indsigt i oplysninger mm. besvares. Der gives ikke indsigt i oplysninger, der behandles til statistiske formål, mens der gives indsigt i oplysninger der behandles til andre formål.

Vurdering og evt. forbedringstiltag

DPO finder, at DST på god vis tager hånd om de registreredes rettigheder og sørger for, at rettighederne efterleves.

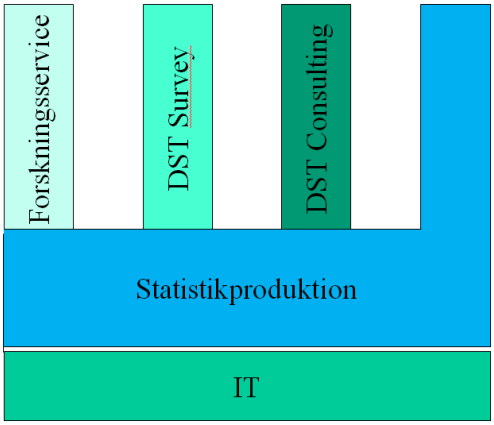
10. GDPR artikel 24: Den dataansvarliges ansvar

Baggrund

I henhold til GDPR artikel 24 skal den dataansvarlige gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer, at oplysningerne behandles i overensstemmelse med behandlingsreglerne i GDPR, herunder sikring af, at oplysningerne ikke behandles til andet end statistiske eller videnskabelige formål for den del af behandlingen, der er omfattet af denne formålsbegrænsning. I den forbindelse bør der bl.a. indføres passende databeskyttelsespolitikker.

Efterlevelse

En overordnet oversigt over Damarks Statistik produktion kan ses i Figur 1.



Figur 1

Danmarks Statistik er opbygget således, at IT servicerer de øvrige afdelinger og kontorer i Danmarks Statistik, så disse kan udarbejde det output, brugerne og kunderne efterspørger. Det er IT, som står for at opbygge og vedligeholde system- og it-værktøjer, herunder de systemer, hvor oplysninger kommer ind i Danmarks Statistik. Arbejdet udføres i et tæt og formaliseret samarbejde med statistikkontorerne

Når oplysninger er indberettet og placeret i de rette systemer, vil medarbejdere i statistikproduktionen have adgang til de for dem nødvendige oplysninger. I statistikproduktionen benyttes oplysninger til at udarbejde de statistiske produkter som kan offentliggøres for Danmarks Statistiks brugere.

Statistikproduktion er betegnelse for de funktioner i Danmarks Statistik, der fremstiller de generelle statistikker til brug for offentligheden, herunder Personstatistik, Erhvervsstatistik og Økonomisk statistik. Samlet set er der mere end 10 kontorer (afdelinger), der medvirker i statistikproduktionen og antallet af medarbejdere er ca. 250.

Yderligere kan brugere også bestille specielle produkter i henholdsvis Forskningsservice, DST Survey og DST Consulting.

Organisatoriske og tekniske sikringsforanstaltninger:

Der er implementeret følgende foranstaltninger:

- Direktionen er ansvarlig for, at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.
- Informationssikkerhedspolitikken revurderes, ajourføres og godkendes en gang om året af Direktionen, eller i forbindelse med eventuelle situationer, der tilsiger det, såsom større ressortændringer.
- DST har nedsat et informationssikkerhedsudvalg med reference til Direktionen. Formand for udvalget er en afdelingsdirektør (for Brugerservice), og de øvrige medlemmer repræsenterer alle afdelinger samt IT.
- DST har en informationssikkerhedskoordinator, som er personalemæssigt placeret i IT, men som i it-sikkerhedsmæssige spørgsmål refererer til formanden for informationssikkerhedsudvalget.
- Det løbende daglige it-sikkerhedsarbejde varetages af IT og it-sikkerhedsgruppen, som understøttes af DST's governancemodel på sikkerhedsområdet.
- DST har udpeget systemejere, som er de fagligt ansvarlige for DST's systemer. Systemejerne er typisk cheferne i IT samt kontorchefer for statistikkontorerne. De skal sikre, at de gældende it-sikkerhedsregler overholdes for deres systemer.
- Risici for kompromittering af data minimeres gennem retningslinjer og instrukser, udarbejdet på grundlag af risikovurderinger samt kontrolaktiviteter formuleret ud fra kontrolmål med reference til databeskyttelsesforordningen og databeskyttelsesloven.
- DST's Infrastruktur og statistikproduktion driftes af DST selv, hvor it-infrastrukturen er opbygget efter stærke og best-practice sikkerhedsprincipper med netværkssegmentering, firewalls, adgangsstyring, logning, backup systemer, nøddrift m.v.
- Et gennemgående princip er, at den enkelte medarbejder kun skal have adgang til de systemer og data, der er nødvendige til udførelse af det daglige arbejde.
- DST efterlever informationssikkerhedsstandarden ISO 27001:2013, hvilket betyder, at DST har etableret et ledelsessystem for informationssikkerheden (ISMS), der løbende vedligeholdes og forbedres i sammenhæng med informationssikkerhedspolitikken og DST Statement of Applicability-dokument (SoA). SoA-dokumentet forstås som en erklæring af, hvilket aktuelt sikkerhedsniveau, som DST har besluttet og som er godkendt af Direktionen. Dokumentet er forudsætningen for ledelsessystemet, der har et særligt fokus på GDPR, databeskyttelsesloven og DST's informationssikkerhedspolitik. Det implementerede kontrolmiljøet følger ISO 27002, som er i overensstemmelse med SoA-dokumentet.

- ISMS'et omfatter en lang række interne procedurer, politikker, vejledninger med videre og tager højde for såvel udefrakommende og interne påvirkninger, der kan give anledning til tilpasninger af ISMS'ets indhold.
- DST har ligeledes et årshjul for informationssikkerhedsarbejdet, som løbende ajourføres.
- It-beredskabsplanen er en del af DST beredskabsplan, og vedligeholdes løbende.
- DST har yderligere udarbejdet og implementeret en datafortrolighedspolitik. Datafortrolighedspolitikken er det sæt af regler og retningslinjer, som DST anvender i håndteringen af de mange data om danskerne og danske virksomheder, der er grundlaget for statistikproduktionen.

Vurdering og evt. forbedringstiltag

DST har ultimo 2019 haft revisionsfirmaet BDO til at gennemgå DST's tekniske og organisatoriske sikringsforanstaltninger med henblik på at få indhentet ISAE 3000 erklæringer for områderne "Statistikproduktionen", "Forskningsservice", DST Survey" og "DST Consulting".

Revisionsfirma konkluderede, at pr. . november 2019 var beskrivelserne af de ovennævnte områder og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, i alle væsentlige henseender retvisende, og at de tekniske og organisatoriske sikkerhedsforanstaltninger i alle væsentligste henseender var hensigtsmæssigt udformet, således som de var implementeret.

DPO finder ikke grund til, at ovenstående revisioner skulle være misvisende, hvorfor DPO mener, at DST lever op til kravene i GDPR.

11. GDPR artikel 25: Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Baggrund

Den dataansvarlige skal under hensyntagen til det aktuelle tekniske niveau gennemføre passende tekniske og organisatoriske foranstaltninger.

Efterlevelse

I ovenstående_afsnit 10 er gennemgået DST's sikkerhedsforanstaltninger. DST mailsystem (Outlook) og arkivering af mails er dog ikke gennemgået.

Mails vil meget ofte indeholde personoplysninger. Det kan være i form af selve indholdet i mailen, men selve mailen vil stort set ofte i sig selv indeholder oplysninger om afsenderen af mailen. Det kan være

oplysninger om bl.a. ansættelsesforhold. Det er DPO's forståelse, at der i DST mange steder benyttes Outlook som arkiveringssystem, og at der ikke er slettefrister for mails i Outlook.

Det er det overordnede princip i GDPR, at oplysninger skal behandles i sikre systemer, og at der skal ske dataminimering, hvorfor oplysninger skal slettes, hvis de ikke længere er nødvendige. Det er vurderingen fra bl.a. Datatilsynet, at Outlook ikke er et sikkert journaliseringssystem. Samtidig skal der tages højde for andre nationale lovgivninger, når der træffes beslutning om, hvilke oplysninger og mails der skal slettes, og hvilke der skal flyttes fra Outlook til et sikkert journaliseringssystem. Det kan krav der stilles i f.eks. regnskabsloven og offentlighedsloven.

Vurdering evt. forbedringstiltag

Det er DPO's vurdering, at DST ikke lever op til GDPR, når det kommer til brugen af Outlook til journalisering. Det er yderligere DPO's vurdering, at der ikke i tilstrækkeligt omfang sker en sletning af oplysninger og mails i Outlook. Det er derfor DPO's anbefaling, at der igangsættes en proces, hvor oplysninger og mails slettes i Outlook. De mails der ikke skal slettes bør derimod journaliseres i et centralt journaliseringssystem, der kan modtage de mails der ikke skal slettes.

12. GDPR artikel 28: Databehandler

Baggrund

Når en dataansvarlig benytter sig af databehandlere, er der en række krav, som skal overholdes. Disse specificeres bl.a. i artikel 28 i GDPR. Der skal indgås en databehandleraftale mellem parterne, og det skal sikres, at parterne overholder deres forpligtigelser. Det er både den dataansvarliges og databehandlerens ansvar, at de nødvendige aftaler udarbejdes, og at forpligtigelserne overholdes.

Efterlevelse

DST optræder i flere tilfælde som databehandler for andre dataansvarlige. DST benytter sig også af databehandlere, når DST er dataansvarlig. På baggrund af Datatilsynets skabelon til databehandleraftaler har DST udarbejdet en skabelon til databehandleraftaler. Efter en udtalelse fra Det europæiske Databeskyttelsesråd reviderede Datatilsynet i december 2019 deres skabelon til databehandleraftaler. Datatilsynet anbefaler, at alle nye databehandleraftaler tager udgangspunkt i den reviderede skabelon. Dog behøves tidligere indgåede databehandleraftaler ikke revideres.

I de tilfælde hvor DST som dataansvarlig benytter databehandlere, erfarer DPO, at der udarbejdes tilfredsstillende databehandleraftaler. En vigtig del af databehandleraftalerne er, at den instruks, DST giver databehandlerne, skal være præcis, hvilket er tilfældet i de indgåede databehandleraftaler. I henhold til databehandleraftalerne skal DST kontrollere, at databehandlerne lever op til de vilkår, der stilles i aftalerne. Der er i DST udarbejdet retningslinjer til, hvorledes kontrollen med de enkelte databehandlere kan foregå.

Af retningslinjerne fremgår det, at det er den enkelte systemejer i DST at træffe beslutning om, hvilken form for kontrol der bør finde sted. Det er den enkelte systemejer der er ansvarlig for, at kontrollen finder sted.

DST optræder i mange situationer som databehandler. Situationerne kan deles op i følgende fire kategorier: Statistikproduktionen, Forskningsservice, DST Consulting og DST Survey.

Statistikproduktionen

I statistikproduktionen er DST databehandler i en række tilfælde. DPO erfarer, at der er indgået de nødvendige databehandleraftaler, og der er klare og konkrete instrukser for databehandlingen. Samtidig stilles en revisionserklæring til rådighed for de dataansvarlige, hvilket gør, at de kan overholde deres tilsynsforpligtigelse.

Forskningsservice

Forskningsservice er opbygget således, at DST er databehandler, mens de enkelte forskere er dataansvarlige for deres projekter. Dette kræver, at der er indgået databehandleraftaler med de enkelte forskere eller disses forskningsinstitutioner. Så vidt DPO er informeret, er langt hovedparten af de nødvendige databehandleraftaler indgået. Samtidig stiller Forskningsservice en revisionserklæring til rådighed for forskerne, hvilket gør, at forskerne kan overholde deres tilsynsforpligtigelse.

DST Consulting

I DST Consulting vil der for løsning af flere af de leverede ydelser skulle indgås databehandlerafter, da DST vil være databehandler for de oplysninger kunderne selv bidrager med ift. de konkrete opgaver. Så vidt DPO er informeret, er der i DST Consulting implementeret en procedure, der sikrer, at alle de nødvendige databehandleraftaler indgås. Samtidig stiller DST Consulting en revisionserklæring til rådighed for kunderne, hvilket gør, at kunderne kan overholde deres tilsynsforpligtigelse.

DST Survey

DST Survey kan optræde både som dataansvarlig og databehandler. Det bør derfor vurderes ift. den konkrete opgave, hvorvidt DST bør være dataansvarlig eller databehandler. Om DST er dataansvarlig eller databehandler på de enkelte opgaver vil have konsekvenser for, hvorledes opgaven kan og skal løses, hvilke oplysninger respondenterne skal have samt hvilke oplysninger der kan udleveres til kunden. Der bør derfor være fuldstændig klarhed over disse forhold, når den konkrete opgave løses.

Så vidt DPO er informeret er de nødvendige databehandleraftaler indgås i DST Survey. DST Survey stiller en revisionserklæring til rådighed for kunderne, hvilket gør, at kunderne kan overholde deres tilsynsforpligtigelse.

Vurdering og evt. forbedringstiltag

Det er DPO's vurdering, at DST i høj grad indgår de nødvendige databehandleraftaler. DPO vurderer også, at de indgåede databehandleraftaler lever op til de krav, der stilles i GDPR. På baggrund af Datatilsynets anbefaling af, at nye databehandleraftaler tager udgangspunkt i Datatilsynets reviderede skabelon, er det DPO's anbefaling, at der udarbejdes en ny skabelon til DST's databehandleraftale. DPO finder det positivt, at DST får udarbejdet revisionserklæringer – ikke mindst fordi det er vigtigt med eksterne eksperters syn på vores standarder vedr. datafortrolighed og informationssikkerhed.

DPO finder det positivt, at er udarbejde retningslinjer for, hvorledes DST skal leve op til tilsynsforpligtigelsen, når DST benytter databehandlere. Det bør sikres, at de enkelte systemejere foretager de tilstrækkelige tilsyn.

13. GDPR artikel 30: Fortegnelse over behandlingsaktiviteter

Baggrund

I henhold til artikel 30 i GDPR skal den dataansvarlige føre fortegnelser over deres behandlinger. I artikel 30 specificeres, hvilke oplysninger fortegnelserne skal indeholde.

Efterlevelse

DST har fortegnelser på de forskellige områder, hvor DST udfører behandlinger. Fortegnelserne indeholder de krævede oplysninger i henhold til artikel 30 i GDPR.

Vurdering og evt. forbedringstiltag

Det er DPO vurdering, at fortegnelserne lever op til de krav, GDPR stiller. DPO anbefaler, at der implementeres en procedure der sikrer, at fortegnelserne opdateres årligt.

14. GDPR artikel 32: Behandlingssikkerhed

Baggrund

I henhold til artikel 32 i GDPR skal den dataansvarlige og databehandleren implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger.

Efterlevelse

Se afsnit 8 omhandlende GDPR artikel 24.

Vurdering og evt. forbedringstiltag

Se afsnit 8 omhandlende GDPR artikel 24.

15. GDPR artikel 33: Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

Baggrund

Brud på persondatasikkerheden skal anmeldes til Datatilsynet inden for 72 timer, hvis det vurderes, at bruddet kan have at have betydning for de registreredes frihedsrettigheder eller rettigheder. Dette følger af artikel 33 i GDPR.

Efterlevelse

DST har it-beredskab som træder i kraft, når der sker informationssikkerhedsmæssige katastrofer og hændelser, såsom længerevarende nedbrud, strømsvigt, brand mv. Yderligere har DST procedurer for, hvorledes evt. brud på persondatasikkerheden skal håndteres internt i DST. En del af disse procedurer er også, hvorledes det vurderes, om bruddet skal anmeldes til Datatilsynet, og hvem der står for denne anmeldelse.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST lever op til kravene i GDPR. DST har anmeldt brud til Datatilsynet. I forbindelse med anmeldelse af disse brud kan det konstateres, at de interne procedurer i DST har fungeret efter hensigten.

16. GDPR artikel 34: Underretning om brud på persondatasikkerheden til den registrerede

Baggrund

Hvis det vurderes, at et sikkerhedsbrud vil have en høj risiko for de registreredes rettigheder eller sikkerhedsrettigheder, så skal den registrerede underrettes, medmindre visse omstændigheder gør sig gældende.

Efterlevelse

DST har procedure for, hvorledes brud anmeldes til Datatilsynet. En del af disse procedurer er også, om der skal ske underretning til den registrerede.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST lever op til kravene i GDPR.

17. GDPR artikel 35: Konsekvensanalyse vedrørende databeskyttelse

Baggrund

I henhold til GDPR artikel 35 foretager den dataansvarlige konsekvensanalyser vedrørende den dataansvarliges behandlinger.

Efterlevelse

DST har foretaget konsekvensanalyser for forskellige typer af behandlinger. Det er i GDPR ikke klart, på hvilket niveau af behandlingen der skal foretages konkrete konsekvensanalyser. De i DST foretagne konsekvensanalyser er på et mere overordnet niveau.

Vurdering og evt. forbedringstiltag

DPO vurderer, at DST's konsekvensanalyser er på et meget overordnet niveau. GDPR er ikke klar ift., hvilket niveau konsekvensanalyser skal være på. Det vurderes derfor, at DST lever op til kravene. Direktionen bør dog overveje, hvorvidt mere specificerede konsekvensanalyser kan være gavnlige. Yderligere anbefaler DPO, at der ved nye typer af behandlinger udarbejdes forudgående konsekvensanalyser.

18. GDPR artikel 36: Forudgående høring

Baggrund

GDPR artikel 36 medfører, at når en konsekvensanalyse viser, at en behandling medfører en høj risiko, så skal den dataansvarlige konsultere Datatilsynet.

Efterlevelse

Da ingen af DST's behandlinger er blevet vurderet til at medføre en høj risiko, har denne artikel har endnu ikke været vurderet relevant for DST.

Vurdering og evt. forbedringstiltag

Ingen kommentarer.

19. Konklusion

Beskyttelse af de registreredes oplysninger og sikring af deres rettigheder vigtige emner. Særligt vigtige er de for en institution som DST, hvis kerneforretning er at behandle oplysninger med henblik på statistiske formål.

DPO har på baggrund af materiale og sit kendskab til DST gennemgået, hvorledes DST lever op til kravene i udvalgte dele af GDPR og dansk lovgivning. Det er DPO's vurdering, at DST sørger for at sikre og beskytte oplysninger, og at DST lever op til at sikre de registreredes rettigheder.

DPO kan konkludere, at DST har en lang række procedurer og forretningsgange, der er med til at sikre, at DST lever op til GDPR. DPO finder, at arbejdet med og opfyldesen af GDPR er en kontinuerlig proces. Det er derfor vigtigt, at DST hele tiden arbejder på at forbedre området. I denne rapport er nævnt en række områder, hvor DST med fordel kan lave tiltag der vil være med til at forbedre sikkerheden.