Rapport fra Danmarks Statistiks DPO-team vedrørende efterlevelse af GDPR

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 interessenter.

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 udarbejder årligt en rapport til direktionen i DST, hvor DPO redegør for, hvorledes GDPR er implementeret. DPO kommer i denne rapport også med forslag til eventuelle forbedringstiltag. At der udarbejdes en årlig rapport i DST, er alene en intern beslutning i DST, da der ikke stilles krav om en sådan i GDPR.

Rapporten beskriver, hvorledes DST lever op til udvalgte områder af GDPR samt de bestemmelser i Databeskyttelsesloven, der implementerer dele af GDPR i Danmark. Rapporten skal læses i forlængelse af de tilsvarende rapporter for 2018 og 2019. Vægtningen mellem de forskellige artikler i denne rapport er en smule anderledes end i rapporterne for 2018 og 2019. Dette skyldes bl.a. de sager vedrørende databeskyttelse, som DST har haft, og de områder DST har arbejdet med de seneste år.

Rapporten er bygget op omkring udvalgte artikler i GDPR. Artiklerne bliver 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.

Rapporten er den tredje skrevet til DST i den periode, hvor GDPR har været gældende. Rapporten kan med fordel læses i sammenhæng med tidligere rapporter. 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 bliver der kommenteret på, hvorvidt DST har igangsat eller fuldt ud implementeret tiltag på baggrund af tidligere rapporter.

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

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

Opfølgning på sidste års anbefalinger

I marts 2020 anbefalede DPO nedenstående forbedringstiltag. Ved hvert forbedringstiltag er tilføjet, hvorledes DPO mener, at der er fulgt op på forbedringstiltaget gennem det seneste år.

- Der sker en omfattende sletning af e-mails i Outlook. Da stort set alle e-mails indeholder personoplysninger, fx ansættelsesmæssige oplysninger om afsenderen, vil en sletning sikre dataminimering.
    - DPO kan konstatere, at DST har gennemført oprydning af mails i funktionspostkasser i Outlook og sletning af funktionspostkasser der ikke længere benyttes. Dette er yderst positivt. DPO kan konstatere, at der dog stadig ikke sker den nødvendige sletning af oplysninger i alle medarbejderes Outlook. DPO kan konstatere, at DST har påbegyndt et projekt der skal sikre, at oplysninger bliver journaliseret i et sikkert journaliseringssystem og i langt højere

grad slettes i Outlook. DPO finder det positivt, at et sådant projekt er startet op, da det kan sikre, at DST i højere grad lever op til GDPR og lovgivning vedr. offentlige myndigheders journaliseringspligt. DPO anbefaler derfor, at projektet prioriteres med tilstrækkelige ressourcer og opmærksomhed.

- Det sikres, at der sker det nødvendige tilsyn med de databehandlere, DST benytter.
    - Der er i DST udarbejdet en vejledning til, hvorledes der føres tilsyn med databehandlere. De enkelte systemejere er ansvarlige for, at der sker det nødvendige tilsyn. Yderligere er det besluttet, at DPO ud fra stikprøver undersøger, om de nødvendige tilsyn er sket. DPO finder, at dette er en god procedure.

- 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 personer under 18 år eller udsatte borgere.
    - DPO kan konstatere, at der på nuværende tidspunkt er tilfredsstillende fokus på oplysningspligten i DST Survey og DST generelt. Yderligere er der ekstra fokus på oplysningspligten, når der er tale om personer under 18 år eller udsatte borgere.

- Særligt i forbindelse med nye behandlinger af personoplysninger kan der med fordel i højere grad udarbejdes konsekvensanalyser for at sikre, at behandlingerne sker på bedst mulig måde.
    - DPO finder, det yderst positivt, at der inden for IT er iværksat sket en proces til på forbedringen af risikostyreingen, hvor GDPR er en integreret del af risikostyringen.

<u>Anbefalinger til forbedringstiltag</u>

- Det anbefales, at implementeringen og udrulningen af et sikkert journaliseringssystem fortsættes og prioriteres, da dette system er forudsætningen for, der kan ske sletning af e-mails i Outlook. Af hensyn til journaliseringspligten skal e-mails først slettes i Outlook, når de er journaliseret i et sikkert journaliseringssystem. Når journaliseringssystemet er implementeret og udrullet i hele DST, og der sker den nødvendige journalisering af e-mails i systemet, anbefales det, at der sker sletning af e-mails i Outlook. Da stort set alle e-mails indeholder personoplysninger, fx ansættelsesmæssige oplysninger om afsenderen, vil en sletning sikre dataminimering.

- Det anbefales, at der sker en juridisk udredning af GDPR artikel 23, stk. 1. Det er DPO's vurdering, at det på nuværende tidspunkt er uklart, hvornår - og i hvilke konkrete situationer - artiklen åbner for, at der via nationale lovgivninger kan ske undtagelser for f.eks. formålsbestemtheden. For DST er det af største vigtighed, at der er klarhed om dette, da det kan have betydning for bl.a. DST mulighed for ubegrænset behandling af data (herunder samkøring) samt at benytte undtagelser i de registreredes rettigheder, såsom indsigtsretten og oplysningspligten. Det anbefales, at en sådan juridisk udredning sker i samarbejde med Datatilsynet samt relevante europæiske organisationer og myndigheder.

- Det anbefales, at DST fortsat har stort fokus på IT-sikkerheden. DST's ISO-certificering bekræfter, at DST har en høj IT-sikkerhed, men fokus på dette område er stadig nødvendigt.

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 vil i denne rapport være på formålsbegrænsning og dataminimering, da disse er vurderet som særligt 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 uforenlige formål, f.eks. administrative formål. Hovedparten af de oplysninger DST indsamler til statistiske formål sker ved, at oplysningerne videregives fra andre nationale myndigheder og institutioner til DST. DST indsamler dog også oplysninger direkte hos de registrerede. Denne indsamling sker bl.a. via DST Survey og Erhvervsindberetning.

I DPO-rapporten fra februar 2019 blev det beskrevet, at i forbindelse med AUB videregiver DST oplysninger til ikke-statistiske formål. Videregivelsen er hjemlet i dansk lovgivning. Yderligere blev 'Lov om tidlig pension' i 2020 vedtaget af det danske Folketing. Loven fastsætter, at Danmarks Statistik på anmodning fra ATP skal videregive en række personoplysninger til ATP. Disse oplysninger skal ATP benytte til at træffe en administrativ afgørelse rettet mod den enkelte registrerede/den enkelte ansøger om tidlig pension, om hvorvidt den enkelte ansøger af tidlig pension kan få bevilget tidlig pension eller ej. ATP's behandling må vurderes at være uforenlig med det formål, hvortil DST har indsamlet oplysningerne. I betænkningerne til lovforslaget gøres opmærksom på dette. I betænkningerne gøres dog også opmærksom på, at der i henhold til GDPR artikel 23, stk.1 kan ske behandling af oplysninger til et andet uforenligt formål end det, oplysningerne er indsamlet til, baseret på national lovgivning som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er fastsat i forordningens artikel 23, stk. 1. I betænkningerne henvises ikke direkte til, hvilken litra/hensyn i GDPR artikel 23, stk. 1 der er begrundelsen for at formålsbegrænsningen kan undtages. Det må dog antages, at det er litra e, der er hjemlen for via den nationale lovgivning at begrænse formålsbegrænsningen af hensyn til:

> *e) andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed*

Det skal i den forbindelse erindres, at så længe DST's behandling udelukkende sker til statistiske eller videnskabelige formål, er der relativt ubegrænsede muligheder for samkøring af data, hvilket er hele grundlaget for statistikproduktionen i DST. Hvis data anvendes eller videregives til andre formål, kan DST's muligheder for samkøring blive draget i tvivl.

Ud over de nævnte eksempler, så sker der generelt ikke videregivelse, der strider mod formålsbegrænsningen.

Vurdering og evt. forbedringstiltag

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

Dog findes der i hvert fald to tilfælde, hvor det via national lovgivning er vedtaget, at DST skal videregive oplysninger indsamlet til statistiske formål til andre uforenlige formål. Når det i Lov om tidlig pension vurderes, at formålsbegrænsningen kan undtages grundet GDPR artikel 23, stk. 1, litra e, kan der stilles spørgsmål ved, i hvilken grad bestemmelsen dermed generelt kan benyttes i kommende national lovgivning, hvor oplysninger indsamlet til statistiske formål ønskes benyttet til administrative formål? Hvis det ikke er tilfældet, så kan det med fordel beskrives, hvad der er begrundelse for, at den netop kan benyttes i Lov om tidlig pension? Bedømmes det derimod, at den generelt kan benyttes, så skal DST overveje, hvilken betydning det har for DST virksomhed, undtagelser etc., der i høj grad bygger på, at de oplysninger DST indsamler ikke sidenhen benyttes og behandles til administrative formål.

DPO finder det vigtigt, at DST forsøger at spille en aktiv rolle ift., at evt. nye lovgivninger ikke strider mod 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 og sikrer, at de indberettede oplysninger er så korrekte som muligt, og at respondenterne vil deltage i andre undersøgelser. DST vil ofte kunne berige oplysningerne om respondenterne med en lang række baggrundsvariabler. Det 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 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 en oversigt over, hvilke medarbejdere der har adgang til hvilke data. Der gennemføres to halvårlige opfølgninger, skiftevis opfølgning 1. og opfølgning 2.

1. Hver enkelt kontorchef tager stilling til om dennes medarbejdere fortsat har behov for adgang 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 arbejdsbetinget behov for adgang, så skal adgangen fjernes. Resultatet af opfølgningerne dokumenteres og 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 kontraktlig forpligtigelse eller som led i DST arbejde som offentlig myndighed (b og e). Personale og kunder bliver oplyst om dette.

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, som DST foretager er lovlige. Yderligere er DST bevidst om, hvorfor behandlingerne er lovlige. Det bør dog undersøges nærmere, hvorvidt DST i alle tilfælde, når oplysningerne indsamles direkte hos den registrerede, informerer de registrerede om, hvorfor behandlingen er lovlig. Det bør klart fremgå af de informationer, DST giver respondenterne, hvorfor behandlingen er lovlig

med henvisninger til de relevante artikler i GDPR, Lov om Danmarks Statistik, anden relevant national lovgivning og EU-lovgivning.

Ud over 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

Er en behandling baseret på den registreredes samtykke, skal samtykket påvises. Det skal sikre, at registrerede har forstået, hvad samtykket indebærer, og at samtykket er afgivet frivilligt. Den dataansvarlige er forpligtet til at kunne påvise dette.

Efterlevelse

Datatilsynet anbefaler, at offentlige myndigheder ikke behandler oplysninger på baggrund af samtykke, hvorfor dette ikke sker i DST.

Vurdering og evt. forbedringstiltag

DPO finder det fornuftigt, at Datatilsynets anbefaling følges.

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, jf. GDPR artikel 9, stk. 2, litra j.

Efterlevelse

Når DST behandler særlige kategorier af personoplysninger, sker det udelukkende 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 modtage en række informationer. De forskellige forhold der skal oplyses om, fremgår af artiklen i GDPR.

Efterlevelse

Det er DPO's vurdering, at DST overordnet giver de registrerede de rette informationer, når DST indsamler oplysninger hos de registrerede.

Vurdering og evt. forbedringstiltag
DPO finder, at DST lever op til oplysningspligten. DPO anbefaler, at DST stadig har fokus på at iagttage særlige forhold omkring oplysningspligten, når der indsamles oplysninger hos unge under 18 år eller hos særligt udsatte grupper.

DST informerer de registrerede om, at oplysningerne udelukkende vil blive behandlet til statistiske og videnskabelige formål. Som beskrevet i afsnit '1. b) Formålsbegrænsning', findes der minimum to nationale lovgivninger, hvor DST er pålagt at videregive oplysninger til administrative formål.

I afsnittet anbefaler DPO, at DST skaber klarhed over, hvorvidt der på sigt kan komme anden national lovgivning, hvor DST vil blive pålagt at videregive oplysninger til administrative formål. Det bør derfor overvejes, om DST fremadrettet kan blive ved med at oplyse de registrerede om, at deres oplysninger behandles til statistiske og videnskabelige formål, hvis det fremadrettet må forudses, at oplysningerne vil blive behandlet til administrative formål.

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

Baggrund
Når personoplysninger ikke indsamles hos den registrerede, skal den registrerede modtage en række oplysninger. Der er flere tilfælde, hvor denne oplysningspligt kan undtages, f.eks. hvis oplysningspligten vil kræve en uforholdsmæssig stor indsats 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 de registrerede, når DST behandler oplysninger, der ikke er indsamlet hos de 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. Som beskrevet i afsnittet om vurdering og evt. forbedringstiltag i afsnit 8, så bør det vurderes, hvorvidt DST stadig og fremadrettet alene indsamler oplysninger udelukkende til statistiske og videnskabelige formål. Kan det ikke garanteres, at DST indsamler oplysningerne udelukkende til statistiske og videnskabelige formål, skal det vurderes, hvorvidt DST skal oplyse de registrerede, når DST indsamler oplysningerne fra f.eks. andre offentlige registre.

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 der indskrevet undtagelser for de registreredes rettigheder, hvis oplysningerne udelukkende behandles til statistiske eller videnskabelige formål. Samlet betyder det, at oplysnin-

ger, der behandles til statistiske eller videnskabelige formål, er undtaget fra de fleste af de registreredes rettigheder. Det er dog vigtigt at bemærke, at dette ikke gælder 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.

DPO finder det vigtigt at holde sig for øje, at ved undtagelser fra de registreredes rettigheder, er disse undtagelser betinget af, at oplysningerne udelukkende behandles til statistiske og videnskabelige formål. Som tidligere nævnt, er der implementeret minimum to nationale lovgivninger, som pålægger DST at videregive oplysninger til administrative formål. Det anbefales at undersøge, hvorvidt de enkelte behandlinger og oplysninger i DST er omfattet af undtagelserne i de registreredes rettigheder, eller om de registreredes rettigheder er gældende for de oplysninger, som DST videregiver til administrative formål. Problemstillingen er allerede aktuel, men hvis det forudses, at yderligere oplysninger fra DST i fremtiden skal videregives til administrative formål, vil aktualiteten af problemstillingen stige.

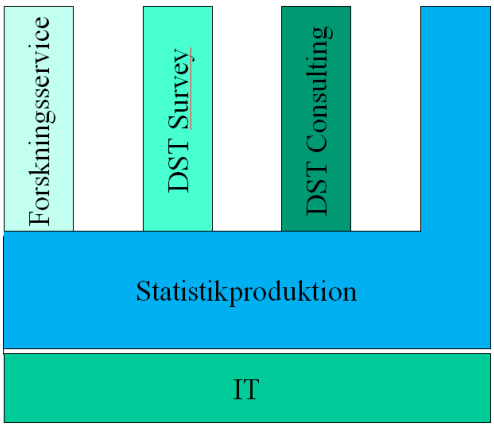
10. GDPR artikel 24: Den dataansvarliges ansvar

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 sikre, 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 de kan udarbejde det output, brugerne og kunderne efterspørger. IT 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 medarbejderne i statistikproduktionen have adgang til de for dem nødvendige oplysninger. I statistikproduktionen benyttes oplysninger til at udarbejde de statistiske produkter, som 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) og ca. 250 medarbejdere, der medvirker i statistikproduktionen.

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 når eventuelle situationer tilsiger det, såsom større ressortændringer.
- DST har nedsat et informationssikkerhedsudvalg med reference til direktionen. Afdelingsdirektøren for Brugerservice er formand for udvalget, og de øvrige medlemmer repræsenterer alle afdelinger samt IT.
- DST har en informationssikkerhedskoordinator, som personalemæssigt er 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 fagligt ansvarlige for DST's systemer. Systemejerne er typisk cheferne i IT samt kontorchefer for statistikkontorerne. Systemejerne skal sikre, at de gældende it-sikkerhedsregler overholdes for deres respektive systemer.
- Risici for kompromittering af data minimeres gennem retningslinjer og instrukser, der er 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 er i 2020 blevet certificeret efter informationssikkerhedsstandarden ISO 27001:2013. Således har DST etableret et ledelsessystem for informationssikkerheden (ISMS), der løbende vedligeholdes og forbedres i sammenhæng med informationssikkerhedspolitikken og DST Statement of Applicabi-

lity-dokument (SoA). SoA-dokumentet forstås som en erklæring af, hvilket aktuelt sikkerhedsniveau, som DST har besluttet og 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 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 2020 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".

Revisionsfirmaet konkluderede, at pr. 30. november 2020 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 afsnit 10 er DST's sikkerhedsforanstaltninger gennemgået. DST's e-mailsystem (Outlook) og arkivering af e-mails er dog ikke gennemgået.

E-mails vil meget ofte indeholde personoplysninger. Det kan være i form af selve indholdet i e-mailen, og e-mailen i sig selv indeholder ofte oplysninger om e-mailens afsender. Det kan være oplysninger om bl.a. ansættelsesforhold. Det er DPO's forståelse, at i DST benyttes Outlook mange steder som arkiveringssystem, og at der ikke er slettefrister for e-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 e-mails der skal slettes, og hvilke der skal flyttes fra Outlook til et sikkert journaliseringssystem. Det kan f.eks. være krav i regnskabsloven og offentlighedsloven.

Vurdering evt. forbedringstiltag

I DPO-rapport 2019 anbefalede DPO, at DST i højere grad sørgede for at slette oplysninger i Outlook. DST har gennemført sletning af mails i funktionspostkasser i Outlook og sletning af funktionspostkasser der ikke længere benyttes. Dette er yderst positivt. 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 e-mails i alle medarbejderes Outlook. DPO kan konstatere, at DST har påbegyndt en proces, hvor der skal udrulles en ny journaliseringspraksis og sletning af e-mails i Outlook i DST. DPO kan kun støtte op om en sådan proces. Det er DPO's vurdering, at det er vigtigt, at der inden for en kort tidshorisont udrulles en praksis, som sikrer at DST kan leve op til kravene i lovgivningen. Her tænkes ikke alene på krav i GDPR, men også på journaliseringskrav i f.eks. offentlighedsloven.

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 forpligtelser. Det er både den dataansvarliges og databehandlerens ansvar, at de nødvendige aftaler udarbejdes, og at forpligtelserne overholdes.

Efterlevelse

DST optræder i flere tilfælde som databehandler for andre dataansvarlige. DST benytter sig også af databehandlere, når DST er dataansvarlig. DST har på baggrund af Datatilsynets skabelon til databehandleraftaler selv udarbejdet en databehandleraftaleskabelon. 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 behøver 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 for, hvorledes kontrollen med de enkelte databehandlere kan foregå. Af retningslinjerne fremgår det, at den enkelte systemejer i DST træffer beslutning om, hvilken form for kontrol der bør finde sted. Den enkelte systemejer 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 tilsynsforpligtelse.

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

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 tilsynsforpligtelse.

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 har konsekvenser for, hvorledes opgaven kan og skal løses, hvilke oplysninger respondenterne skal have samt hvilke oplysninger der kan udleveres til kunden. Der bør være fuldstændig klarhed over disse forhold, når den konkrete opgave løses.

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

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 der er udarbejdet retningslinjer for, hvorledes DST skal leve op til tilsynsforpligtelsen, 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's vurdering, at fortegnelserne lever op til de krav.

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 et 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.

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, skal den registrerede underrettes, medmindre visse omstændigheder gør sig gældende.

Efterlevelse

DST har procedurer 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 overordnede konsekvensanalyser for forskellige typer af behandlinger. I DST's risikostyring er der taget højde for GDPR forstået på den måde, at når der fortages risikoanalyser for it-systemer etc. Systemejere skal i deres risikovurderinger tage højde for, hvorvidt behandlingen omfatter personoplysninger, og hvor dette sker, skal der foretages konsekvensanalyser.

Vurdering og evt. forbedringstiltag

Det vurderes derfor, at DST lever op til kravene

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 er vigtige emner. De er særligt vigtige 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, DST lever op til GDPR. 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 iværksætte tiltag der forbedrer sikkerheden.