Vejledning til tilsyn med databehandlere

Referencer:

Datatilsynets Vejledende tekst om tilsyn med databehandlere og underdatabehandlere

Baggrund for tilsyn

Organisationer der er dataansvarlig, skal som følge af databeskyttelsesforordningen og databeskyttelsesloven indgå databehandleraftaler med eventuelle databehandlere. Databehandleraftalen skal sikre, at oplysningerne kun bliver behandlet efter instruks fra den dataansvarlige og, at databehandleren benytter sig af passende teknisk og organisatorisk sikkerhed i forhold til de risici, som er forbundet med de personoplysninger, som databehandleren foretager behandling af. Disse sikkerhedsforanstaltninger skal fremgå af databehandleraftalen og udarbejdes på baggrund af den risikovurdering de dataansvarlige har foretaget for behandlingen af personoplysningerne.

Selvom det ikke udtrykkeligt er nævnt i databeskyttelsesforordningen, har den dataansvarlige pligt til at føre tilsyn med sine databehandlere således, at kravet om ansvarlighed kan efterleves. Tilsynet skal sikre at databehandleren efterlever de krav der fremgår af databehandleraftalen, både i forhold til sikkerhedsforanstaltninger, men også i forhold til behandling til andre formål, sletning, videregivelse og opbevaringssted.

Det er den dataansvarliges ansvar at føre tilsyn med sine databehandlere og sikre, at disse overholder de indgåede databehandleraftaler. Denne opgave kan dog også overdrages til en ekstern og uafhængig tredjemand, som fx en revisor, eller databehandleren kan få udarbejdet en relevant revisorerklæring som fx en ISAE3000 erklæring.

Hvad er et tilsyn?

Et tilsyn er en kontrol med at databehandleren efterlever databehandleraftalen, databeskyttelsesforordningen og databeskyttelsesloven.

Hvordan foretages tilsyn?

Der kan føres tilsyn med en databehandler på flere forskellige måder. De mest almindelige er enten et fysisk tilsyn eller et skriftligt tilsyn. Ved begge typer tilsyn stiller den dataansvarlige en række spørgsmål, som skal besvares af databehandleren, hvorved der indsamles informationer om overholdelse af databehandleraftalen gennem en række spørgsmål.

Et tilsyn med en databehandler kan også gøres via en uafhængig tredjepart, der laver et fysisk eller skriftligt tilsyn med databehandleren, eller det kan gøres gennem brugen af revisorerklæringer eller certificeringer. Her er det eksempelvis en revisor der laver en kontrol med databehandlerens overholdelse af forordningens regler, og udarbejder en erklæring på baggrund af den kontrol. Denne erklæring vil i de fleste tilfælde kunne stå i stedet for et tilsyn fra den dataansvarlige.

Valget af tilsynsform afhænger af den identificerede risiko, som skal være udarbejdet inden behandlingen af personoplysninger begynder.

Lav risiko	Ved lav risiko kan man eksempelvis stille databehandleren en række spørgsmål, som vil kunne afdække, om databehandleren efterlever de krav der er stillet i aftalen. Hvilke spørgsmål, der kan stilles, afhænger af behandlingen og risikovurderingen.
Høj risiko	Hvis risikoen for de registreredes rettigheder er høj, kan det være nødvendigt at foretage fysisk tilsyn med databehandleren. Elementer i risikovurderingen, som kan tale for et fysisk tilsyn er blandt andet delegation og brug af administrative rettigheder, adgangen til personoplysninger, pålagte sletteregler m.fl.

Alle dataansvarlige bør i sine politikker begrunde, hvor ofte, man vil føre tilsyn med sine databehandlere, samt hvordan dette vil ske. Dermed skabes den løbende dokumentation af efterlevelse af forordningens krav om ansvarlighed.

Hvor ofte skal man påse behandlingssikkerheden hos sine databehandlere?

Frekvensen af, hvor ofte der skal foretages tilsyn med databehandleren, afhænger af risikovurderingen, jo større risiko, des oftere bør tilsyn føres.

Lav risiko	Hvis risikoen er lav, kan den dataansvarlige nøjes med at føre tilsyn med databehandleren med en lav frekvens. Datatilsynet kommer dog ikke med nærmere præcisering af, hvad "lavere frekvens" indebærer.
Høj risiko	Hvis risikoen er høj, kan det være nødvendigt at foretage fysisk tilsyn med databehandleren halvårligt eller oftere.

Hvordan føres tilsyn hos eventuelle underdatabehandlere?

Det følger af databeskyttelsesforordningen, at eventuelle databehandlere er ansvarlige for at pålægge underdatabehandlere mindst samme forpligtelser, som databehandleren har over for den dataansvarlige.

Databehandleren er tillige over for den dataansvarlige ansvarlig for underdatabehandlerens aktiviteter. Det er databehandleren, der skal føre tilsyn med en eventuel underdatabehandler, men den dataansvarlige er forpligtet til at sikre, at databehandleren rent faktisk fører det aftalte tilsyn med sin underdatabehandler, dette vil ofte ske ved udlevering af dokumentation for tilsynet.

Et skriftligt tilsyn kan fx ske i form af løbende afrapporteringer fra databehandleren i forhold til de parametre, som med risikovurderingen er vurderet som værende påkrævede. Disse afrapporteringer kan fx være baseret på udvalgte kontroller fra SANS Critical Security Controls, ISO27007 eller andre typer af kontroller, der kan rapporteres omkring. Der kan også foretages stikprøver og temakontroller over de kontrolregimer, der måtte afspejle den dataansvarliges risikovurdering.

Hvordan udføres et tilsyn?

Efter den dataansvarlige har fastsat en metode og en frekvens for tilsynet, skal det faktiske tilsyn udføres. Dette gøres i praksis ved, at den dataansvarlige udvælger en eller flere områder, og udfærdiger en række spørgsmål, der skal belyse databehandlerens efterlevelse af reglerne inden for de områder.

Dette kan fx være 10 spørgsmål om databehandleraftaler, 10 spørgsmål om behandlingssikkerheden og 5 spørgsmål om de generelle principper inden for behandlingen af personoplysninger. Dette afhænger af, om man ønsker at fokusere på et eller flere områder, eller om man ønsker en mere bred besvarelse på flere områder. Antallet af spørgsmål og hvilke emner man bør fokusere på afhænger af risikovurderingen.

Disse spørgsmål kan den dataansvarlige så enten selv tage ud til databehandleren for at få besvaret og samtidig med egne øjne for bekræftet svarenes validitet. Alternativt kan den dataansvarlige sende disse spørgsmål til databehandleren og bede denne om at besvare dem. Det fysiske tilsyn vil derfor oftest være en mere sikker indikator for den faktiske situation i forhold til efterlevelse af forordningens regler.

I bilag 1 til dette dokument, findes en liste med forskellige spørgsmål, som kan bruges til tilsyn eller til inspiration til udarbejdelse af egne spørgsmål til tilsyn.

Det rent praktiske

Arbejdet for forordningen, risici og tilsyn er, uanset hvordan dette dokument måtte få det til at fremstå, ikke nogen let eller enkelt sag. Det anbefales derfor, at spørgsmålene udvælges i et samarbejde mellem de system eller procesansvarlige samt organisationens databeskyttelsesrådgiver, og muligvis også organisationens informationssikkerhedsfunktion.

Yderligere bør alle svar sendes til organisationens databeskyttelsesrådgiver og organisationens informationssikkerhedsfunktion, således at disse kan vurdere, om yderligere tiltag skal foretages, eller om svarene er fornuftige og tilsynet kan dokumenteres, journaliseres og afsluttes.

Bilag 1: Liste over mulige spørgsmål til databehandleren

Overblik over personoplysninger

1. Er der skabt et overblik over organisationens behandlinger af personoplysninger, som gør det muligt at udpege personoplysninger herunder fortrolige og følsomme oplysninger?
2. Hvis ja, vedlæg venligst
3. Er processer og systemer der behandler personoplysninger identificeret?
4. Hvis ja, vedlæg venligst
5. Er system- og risikoejere defineret?
6. Bliver det løbende arbejde med databeskyttelsesforordningen dokumenteret og foreligger tilgængeligt, fx politikker, procedure, compliancedokumenter, GAP-analyser, handlingsplaner, eller dagsordener fra styregrupper?
7. Hvis ja, vedlæg venligst
8. Forefindes en metode, skabelon og vejledning for udarbejdelse af en fortegnelse over behandlingsaktiviteter?
9. Er der udpeget en databeskyttelsesrådgiver for organisationen?

Fortegnelsen

10. Er der udarbejdet en fortegnelse for organisationens behandlingsaktiviteter?
11. Hvis ja, vedlæg venligst
12. Er der en klar ansvarsfordeling for opdatering og kvalitetskontrol af fortegnelsen?
13. Er der tilstrækkelig IT understøttelse af fortegnelsesarbejdet?
14. Er fortegnelsen kommunikeret til relevante medarbejdere?
15. Er fortegnelsen opdateret og afspejler den aktuelle sagsgange?
16. Tilføjer organisationen ændringer til fortegnelsen? Hvor ofte?
17. Opdateres fortegnelsen minimum én gang årligt og altid i forbindelse med større ændringer?
18. Kan der fremvises en fortegnelse, som er opdateret inden for det sidste år?
19. Hvornår har organisationens databeskyttelsesrådgiver sidst gennemgået fortegnelsen?

Databeskyttelsespolitik, vurdér herunder i hvilket omfang at:

20. En godkendt databeskyttelsespolitik foreligger og er kommunikeret til medarbejderne og relevante eksterne parter.
21. Hvis ja, vedlæg venligst
22. Foreligger der dokumentation for, at politikken følges i praksis, som kan forevises fx i forbindelse med revision eller tilsyn.

23. Hvis ja, vedlæg venligst
24. Opdateres databeskyttelsespolitikken som minimum én gang årligt, eller ved ændringer af relevans for politikken.

Awareness

25. Har organisationen sikret awareness af databeskyttelsesforordningen?
26. Er roller og ansvar beskrevet og tilpasset organisationens behov og prioritering fsva. arbejdet med databeskyttelsesforordningen?
27. Er der fastsat en operationel ramme for databeskyttelsesforordningens retningslinjer og procedurer (fx i kvalitetsledelsessystem eller intranet), som er tilgængelig for medarbejdere?
28. Hvad har organisationen gjort for at uddanne medarbejdere i korrekt behandling af personoplysninger?
29. Er der holdt oplæg om databeskyttelsesforordningen for medarbejdere fx fra databeskyttelsesrådgiveren?
30. Hvor ofte er der awareness aktiviteter vedrørende databeskyttelsesforordningen?
31. Er der udsendt e-læring evt. med quiz og opfølgning/måling af medarbejdere
32. Har medarbejdere deltaget i kurser om databeskyttelsesforordningen?
33. Hvilke medarbejdere har deltaget i disse kurser?
34. Hvilke kurser er der tale om?
35. Er der udarbejdet pixibøger, plakater og undervisningsmateriale i organisationen?
36. Er der udarbejdet instruktion til medarbejdere og ledere om, hvordan de overholder databeskyttelsesforordningen i dagligdagen?
37. Er der indtænkt awareness i forbindelse med ansættelse af nye medarbejdere og hvordan?
38. Orienteres nye medarbejdere om ansvar og opgaver vedr. behandling af personoplysninger og om konsekvenser ved overtrædelse af reglerne?
39. Orienteres medarbejdere om ansvar og opgaver vedr. behandling af personoplysninger og om konsekvenser ved overtrædelse af reglerne?
40. Har organisationen en procedure/vejledning for brug af sikker mail?
41. Foreligger dokumentation for at procedurerne følges i praksis, som kan forevises fx ifm. revision eller tilsyn?
42. Hvornår er der iværksat oprydninger i Outlook og af fildrev?
43. Hvordan er denne oprydning iværksat?
44. Er der udført kontrol med efterlevelse af oprydningen?

Risikovurderinger og styring:

45. Foretages der løbende vurderinger af sikkerhedsrisici internt og hos centrale underdatabehandlere, herunder risikovurdering i forbindelse med underdatabehandleraftalens indgåelse?
46. Hvordan sikres det at relevante krav indskrives i databehandleraftalen?
47. Hvordan sikres det at principperne for leverandørstyring er godkendt af topledelsen?
48. Anvendes den koncernfællesskabelon på intranettet for en databehandleraftale?
49. Hvis nej, vedlæg eksempel på den skabelon, der anvendes

Opbevaringsbegrænsning

50. Hvordan sikres det at oplysninger ikke gemmes længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles?
51. Sker sletning af personoplysninger manuel eller automatisk?
52. Har organisationen en politik for opbevaring og sletning af data?

IT-løsninger

53. Har organisationen skabt et overblik over alle it-systemer, fysiske it-faciliteter, outsourcing, cloud-løsninger mv., hvor organisationen opbevarer personoplysninger?
54. Er der tænkt og dokumenteret databeskyttelse gennem design og standardindstillinger ind i nye systemer?
55. Hvis ja, beskriv Hvordan?
56. Hvilke hensyn og kriterier har organisationen ladet indgå i den risikobaserede tilgang til behandlingssikkerhed, som databeskyttelsesforordningens artikel 32 er udtryk for?
57. Anvender organisationen andre kommunikationsplatforme, IT-systemer, apps og services på internettet, som ikke er anvist af IT-afdelingen?
58. Hvis ja, oplys venligst hvilke IT-systemer, apps, services mv. som anvendes lokalt, og som IT ikke har anvist.
59. Hvis ja, hvilke tekniske og organisatoriske foranstaltninger er så sikret/implementeret?
60. Foreligger procedurer for at sikre korrekt behandling af personoplysninger ved ansættelsesforholdets ændring eller ophør?

Sociale medier

61. Anvender organisationen sociale medier?
62. Hvis ja, beskriv hvorledes oplysningspligten opfyldes.
63. Hvis ja, hvilke tekniske og organisatoriske foranstaltninger er så implementeret?
64. Hvis ja, er der indgået databehandleraftale?

Overførsel af oplysninger til tredjelande

65. Overfører organisationen personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med kapitel V i databeskyttelsesforordningen?
66. Overfører organisationen personoplysninger til sikre eller usikre tredjelande?

Oplysningspligten

67. Hvordan har organisationens dokumenteret, at oplysningspligten er givet?
68. Har organisationen givet oplysningspligt til medarbejdere, om hvordan organisationen behandler deres personoplysninger?
69. Vedlæg gerne et eksempel på eller et link til et sted, hvor oplysningspligten opfyldes.

De registreredes rettigheder

70. Forefindes der procedurer for håndtering af anmodninger fra registrerede om indsigt, sletning, begrænsning, indsigelser og berigtigelse af oplysninger jf. databeskyttelsesforordningens artikel 15, 16, 17, 18 og 21?
71. Hvor mange antal anmodninger om indsigt, sletning, begrænsning, indsigelser og berigtigelse har organisationen modtaget jf. databeskyttelsesforordningens artikel 15, 16, 17, 18 og 21?
72. Hvor mange anmodninger er besvaret indenfor 1 måned efter modtagelsen af anmodningen jf. databeskyttelsesforordningens artikel 12?
73. Hvad er årsagen til, at organisationen ikke har svaret indenfor 1 måneden?
74. Hvor mange henvendelser er svaret indenfor 3 måneder?
75. Hvad er årsagen til at, organisationen har svaret indenfor 3 måneder?
76. Hvor mange henvendelser er svaret efter 3 måneder og hvad er begrundelsen herfor?
77. Har organisationen underrettet den registrerede om, at der sker forlængelse af svarfristen senest 1 måned efter modtagelsen af henvendelsen sammen med begrundelsen for forsinkelsen?
78. Hvis nej, hvorfor ikke?
79. Vedlæg to anonymiserede eksempler på en indsigtsbegæring efter databeskyttelsesforordningens artikel 15, som er blevet givet til den registrerede inden for det seneste år (dato bedes fremgå).
80. Har organisationen meddelt afslag på en anmodning om indsigt, sletning, begrænsning, indsigelser og berigtigelse af oplysninger?
81. Hvis ja: Vedlæg venligst to anonymiserede eksempler på afslaget (dato bedes fremgå).

Brud på persondatasikkerheden jf. databeskyttelsesforordningens artikel 33

82. Foreligger der en procesbeskrivelse af, hvordan brud på persondatasikkerheden håndteres i organisationen inkl. stillingtagen til ansvarsfordeling, vurdering, håndtering, evaluering og forbedring?

83. Hvis ja, vedlæg venligst
84. Foreligger der en procesbeskrivelse af hvordan der foretages anmeldelse af brud til Datatilsynet?
85. Hvis ja, vedlæg venligst
86. Foreligger der en procesbeskrivelse af hvordan registreredes underrettes?
87. Hvis ja, vedlæg venligst
88. Registreres alle brud på persondatasikkerheden?
89. Hvor mange brud på persondatasikkerheden har der været i organisationen fra 25. maj 2018 til dags dato?
90. Hvilke kriterier indgår i organisationens vurdering af, om der er sket et brud på persondatasikkerheden?
91. Hvor mange brud er anmeldt indenfor 72 timer til Datatilsynet?
92. Hvor mange brud er anmeldt til Datatilsynet efter 72 timer?
93. Hvad er begrundelsen for, at bruddene ikke er anmeldt indenfor 72 timer?
94. Hvor mange brud er registreret men ikke anmeldt til Datatilsynet?
95. Hvad er begrundelsen for, at bruddene ikke er anmeldt til Datatilsynet?
96. Foreligger redegørelser for tilfælde af manglende rapportering til Datatilsynet?
97. Har organisationen underrettet de registrerede om brud jf. databeskyttelsesforordningens artikel 34?
98. Hvis nej, hvorfor?
99. Bliver databeskyttelsesrådgiveren underrettet om brud på persondatasikkerheden?
100. Hvis nej, hvorfor?
101. Hvem hos organisationen foretager vurderingen af, om der er sket et brud på persondatasikkerheden?
102. Hvem hos organisationen vurderer, om et brud på persondatasikkerheden skal anmeldes til Datatilsynet?
103. Hvilke kriterier indgår i organisationens vurdering af, om et brud på persondatasikkerheden skal anmeldes til Datatilsynet?
104. Hvis svarene på ovenstående spørgsmål findes i organisationens politikker, procedurer, vejledninger, mv. anmodes organisationen om, at lave henvisninger hertil.
105. Hvordan er organisationens medarbejdere blevet orienteret om og instrueret i at opdage og håndtere et brud på persondatasikkerheden?
106. Hvornår er organisationens medarbejdere blevet orienteret og instrueret i at opdage og håndtere et brud på persondatasikkerheden?
107. Hvor ofte bliver organisationens medarbejdere orienteret og instrueret i at opdage og håndtere et brud på persondatasikkerheden?
108. Hvis organisationen er i besiddelse af skriftligt materiale, der omhandler ovenstående, anmodes om at modtage en kopi af materialet.

Beredskab

109. I hvilken grad styrer og vedligeholder organisationen et passende beredskab for persondatasikkerhed?
110. Er der etableret og implementeret en godkendt beredskabsplan, som løbende vedligeholdes og som beskriver de forskellige processer, roller og procedurer, der indgår i en beredskabssituation?
111. Er beredskabsplanen tilgængelig for relevante personer i organisationen?
112. Gør beredskabsplanen i tilstrækkeligt omfang det muligt at vurdere, om der er tale om et brud på persondatasikkerheden?

Underdatabehandlere

113. Er der udarbejdet en liste over jeres underdatabehandlere?
114. Har organisationen udarbejdet underdatabehandleraftale med alle underdatabehandlere, som direkte eller indirekte håndterer personoplysninger?
115. Hvor mange underdatabehandleraftaler er der udarbejdet siden databeskyttelsesforordningen den 25. maj 2018 fandt anvendelse?
116. Hvor mange underdatabehandleraftaler mangler at blive udarbejdet?
117. Hvad er begrundelse for, at organisationen ikke har udarbejdet underdatabehandleraftaler med organisationens underdatabehandlere?
118. Er der udarbejdet en liste over dem, som er vurderet til ikke at være underdatabehandlere? Vedlæg venligst listen.
119. Har organisationens ført tilsyn med jeres underdatabehandlere?
120. Hvordan sikres det, at organisationens fører tilsyn med underdatabehandlere?