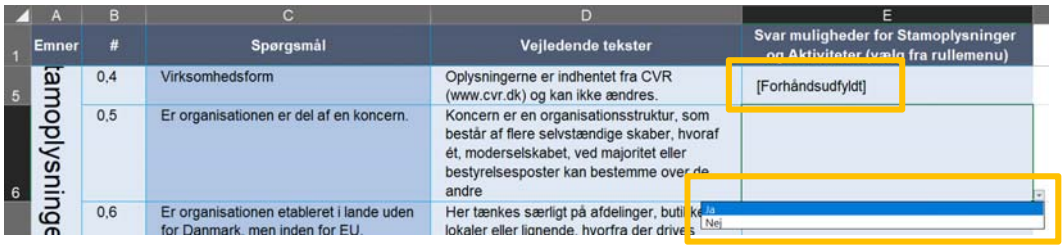
DATATILSYNET

Bilag 1 – Vejledning til udfyldelse af tilsynsskema

1. Introduktion

I det vedhæftede tilsynsskema præsenteres jeres organisation for en række spørgsmål fordelt på udvalgte fagområder, som Datatilsynet finder relevante for overholdelsen af databeskyttelsesreglerne.

Skemaets første del – 'Indledende spørgsmål' – indeholder en række stamoplysninger og indledende spørgsmål til jeres aktiviteter. Nogle stamoplysninger er indhentet fra CVR og er forhåndsudfyldt. Ved andre spørgsmål er det kun muligt at vælge bestemte og standardiserede svarmuligheder. I bedes vælge det mest retvisende svar.



Størstedelen af spørgsmålene er Ja/Nej spørgsmål. I nogle tilfælde skal I forholde jer til talintervaller. Et enkelt spørgsmål vedrører ansvarsplacering, hvor der er mulighed for at vælge én angivet jobfunktion.

Tilsynsskemaets anden og tredje del – 'Emnespørgsmål' – indeholder spørgsmål om organisationens tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med jeres behandling af personoplysninger. Spørgsmålene er så vidt muligt opdelt efter emne og farve for at give jer et bedre overblik.

Hvert spørgsmål er tildelt et unikt ID-nummer, som I kan henvise til i tilfælde af, at der er behov for at kontakte Datatilsynet. Ydermere, findes der for hvert spørgsmål vejledende tekster og referencer til relevante standarder og lovgivning, som kan bidrage til forståelsen af spørgsmålene.

Der er ikke fra Datatilsynets side et krav eller en forventning om, at jeres organisation nødvendigvis skal følge alle de angivne standarder. Omvendt er overholdelse af eksempelvis ISO standarder heller ikke en garanti for overholdelse af alle regler i databeskyttelsesforordningen og databeskyttelsesloven.

2. Besvarelse

Når I besvarer hvert spørgsmål bedes I forholde jer til følgende tre parametre:

1) hvorvidt der er taget stilling til et konkret krav

2) hvorvidt der foreligger dokumentation for stillingtagen
3) hvor hurtigt den pågældende dokumentation kan fremsendes

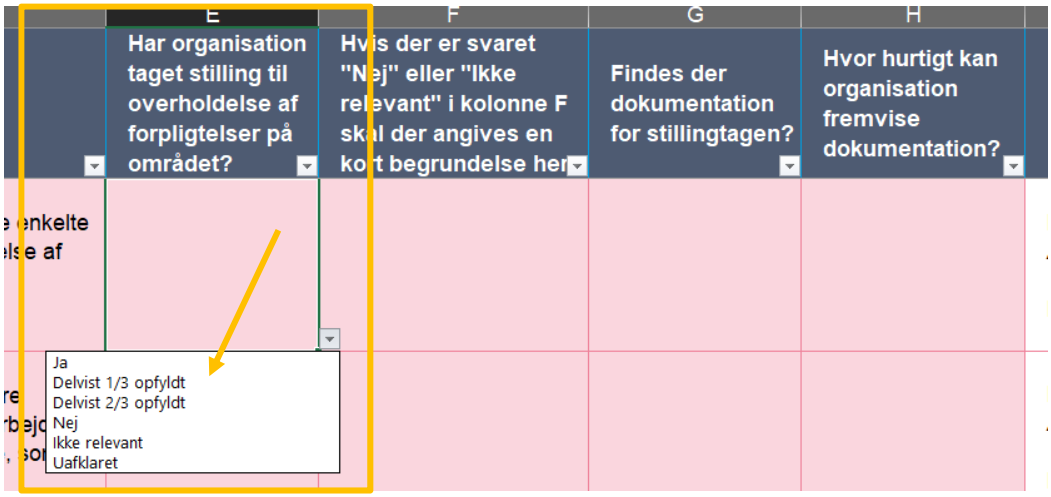
Datatilsynet vil nedenfor forklare, hvorledes disse tre parametre skal besvares.

2.1. Stillingtagen

Tilsynsskemaet har til formål at evaluere jeres organisations modenhedsniveau. Derfor bliver I for hvert spørgsmål bedt om at tage stilling til, i hvilket omfang jeres organisation overholder et konkret krav.

Ved besvarelse af emnespørgsmål kan der vælges mellem seks muligheder:

1. Ja
2. Delvist 1/3 opfyldt
3. Delvist 2/3 opfyldt
4. Nej
5. Ikke relevant
6. Uafklaret

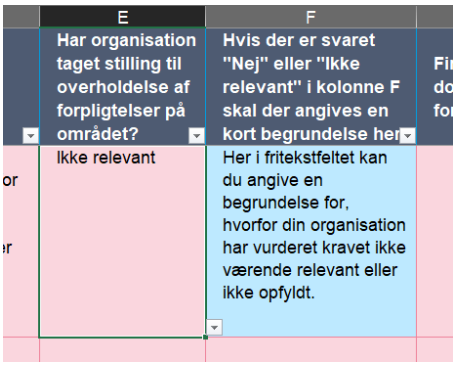


Jeres organisation skal vælge 'Ja', hvis kravet anses for opfyldt på baggrund af det af organisationen fastsatte sikkerhedsniveau og ud fra de krav, som er beskrevet i tilsynsskemaets vejledende tekster. Der kan eksempelvis henvises til spørgsmål 1,11 om *"organisationen har udarbejdet en fortegnelse (oversigt) over behandlingsaktiviteter"*. Her kan I svare 'Ja', hvis kravet om en skriftlig, elektronisk og fyldestgørende oversigt over behandlingsaktiviteter, jf. databeskyttelsesforordningens artikel 30, stk. 1, anses for opfyldt.

Om 'delvist' skal Datatilsynet oplyse, at svarmuligheden bør vælges, når I har påbegyndt, men ikke færdiggjort det pågældende arbejde. Af ord og begreber som kan uddybe 'delvist' kan fx nævnes undervejs og under behandling. Eksempelvis i spørgsmål 1,11 om *"organisationen har udarbejdet en fortegnelse (oversigt) over behandlingsaktiviteter"* kan organisationen bl.a. svare "*delvist 1/3 opfyldt*" og "*delvist 2/3 opfyldt*". I bedes dermed vurdere, hvor langt I er med en fortegnelse, og hvor tæt I er på at have udarbejdet en reel fortegnelse.

I de tilfælde, hvor personer, som svarer på dette tilsynsskema mangler kompetence til at svare på spørgsmål og/eller ikke har mulighed for at inddrage relevante medarbejdere, der kan svare på spørgsmålet, kan der svares 'Uafklaret'.

I de tilfælde, hvor der svares 'Nej' eller 'Ikke relevant', skal Datatilsynet anmode om, at det begrundes med en kort forklaring i kolonne F, hvor der er mulighed for at skrive fritekst.



Datatilsynet skal bemærke, at det ikke er tilsynets forventning, at jeres organisation er i stand til at svare 'Ja' til alle spørgsmål.

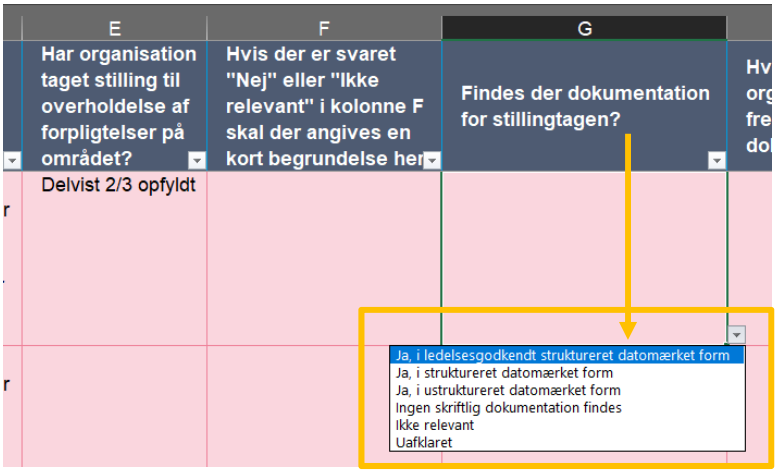
I de tilfælde, hvor I svarer 'Nej' og 'Ikke relevant', skal tilsynet anmode om, at I fortsat besvarer spørgsmålene i kolonne G (dokumentation) og H (fremsendelse) således, at ingen celler i skemaet er tomme.

2.2. Dokumentation for stillingtagen

Efter I har taget stilling til, hvorvidt kravet er opfyldt, spørges I til dokumentation herfor. I bedes alene forholde jer til opfyldelsen af dokumentationskravene. I skal således ikke vedhæfte eventuel dokumentation.

Af spørgsmålet følger 6 svarmuligheder:

1. Ja, i ledelsesgodkendt struktureret datomærket form
2. Ja, i struktureret datomærket form
3. Ja, i ustruktureret datomærket form
4. Ingen skriftlige dokumentation findes
5. Ikke relevant
6. Uafklaret



Ved 'ledelsesgodkendt' dokumentation forstås, at beslutninger har været diskuteret på et ledelsesniveau, og det fremgår tydeligt, at resten af organisatoren agerer ud fra disse beslutninger. I forlængelse hertil, kan det siges, at ledelsesgodkendelse fx kan fremgå af selve politikken, hvis den indeholder dateret underskrift fra relevant ledelsesniveau, eller af anden

dokumentation, hvor det kan påvises, at ledelsen har godkendt dokumentationen, fx e-mail korrespondance, mødereferat eller lign. hvor det tydeligt fremgår, hvad der bliver godkendt og af hvem.

Om 'struktureret' og 'ustruktureret' form for dokumentation skal Datatilsynet oplyse, at for at dokumentation kan anses for at foreligge i 'struktureret' form kræver det, at dokumentationen er organiseret, sorteret og til at finde for relevante medarbejdere. Dette kan eksempelvis opnås ved at samle dokumentation under én politik med tydelige referencer og henvisninger til konkrete procedurer og vejledninger.

Ved 'ustruktureret' skriftlig form forstås, at organisationen har taget udtrykkelig stilling til eventuelle krav, men beslutninger og dokumentation kan være spredt, eksempelvis på forskellige procedurer, vejledninger, Power Point præsentationer, årshjul, medarbejdertræning materiale, mailkorrespondance og anden form for skriftlig dokumentation uden tydelige henvisninger og dermed være ukendt eller svær at fremfinde for øvrige medarbejdere.

Hvis jeres organisation – på baggrund af organisationens egen opfattelse af kompleksitet og risikoprofil – har taget udtrykkelig stilling til, at noget dokumentation ikke anses for at være nødvendigt, er det muligt at svare 'Ikke relevant'.

I de tilfælde, hvor personer, som svarer på dette tilsynsskema mangler kompetence til at svare på spørgsmål og/eller ikke har mulighed for at inddrage øvrige medarbejdere, der kan svare på spørgsmålet, bør der svares 'Uafklaret'.

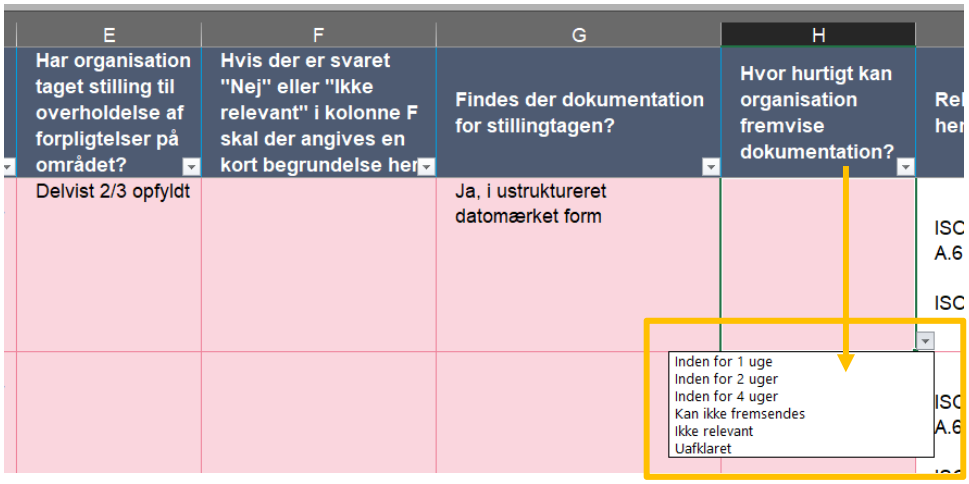
2.3. Fremsendelse af skriftlig dokumentation

Afslutningsvis anmodes jeres organisation om at anføre, hvor hurtigt den pågældende dokumentation kan sendes til Datatilsynet. Som beskrevet ovenfor, kan Datatilsynet i forlængelse af dette tilsyn stille uddybende spørgsmål og/eller anmode om eventuel dokumentation.

Jeres organisation anmodes derfor om en stillingtagen til, hvor hurtigt denne dokumentation eventuelt kan fremsendes til Datatilsynet.

I den forbindelse gives 6 svarmuligheder:

1. Inden for 1 uge
2. Inden for 2 uger
3. Inden for 4 uger
4. Kan ikke fremsendes
5. Ikke relevant
6. Uafklaret



Afhængig af organisationens kompleksitet og opbygning af dokumentationsstruktur, kan tidsintervallet variere. Hvis dokumentation findes i ustruktureret format, vil det som udgangspunkt tage længere tid at fremfinde den relevante dokumentation. Spørgsmålet sigter således ikke mod forsinkelser grundet eksempelvis ferie eller sygdom, men udelukkende til om og hvornår eventuel dokumentation kan leveres.

I tilfælde af, at jeres organisation har gennemført sikkerhedsforanstaltninger, men ikke har skriftlig dokumentation herfor, bedes I vælge 'Kan ikke fremsendes'.

I tilfælde af, at nogle af kravene ikke anses for at være relevant for jeres organisation, bedes I vælge 'Ikke relevant'.

I de tilfælde, hvor personer, som svarer på dette tilsynsskema mangler kompetence til at svare på spørgsmål og/eller ikke har mulighed for at inddrage relevante medarbejdere, der kan svare på spørgsmålet, bør der svares 'Uafklaret'.

3. Afhængigheder

Enkelte af skemaets spørgsmål afhænger af hinanden. For eksempel spørgsmål 4,1 om sikkerhedsbrud, hvor der spørges til, om "*organisationen har udarbejdet procedurer for håndtering af brud på persondatasikkerheden*". Spørgsmål 4,2 spørger herefter til om "*en eventuel procedure for håndtering af brud på persondatasikkerheden indeholder en beskrivelse af hvordan og hvornår der skal ske anmeldelse til Datatilsynet*". Hvis I svarer 'Nej' til spørgsmål 4,1, vil I således ikke kunne svare på det efterfølgende spørgsmål 4,2.

Et andet eksempel på sammenhængende spørgsmål er nr. 17,2 om backup, hvor der spørges til, om organisationen "*i praksis løbende tager backup af data med passende mellemrum*". Spørgsmål 17,4 spørger herefter om "*fører organisationen en skriftlig oversigt (log) over de pågældende backups*". Hvis I svarer 'Nej' til spørgsmål 17,2, vil I således ikke kunne svare på det efterfølgende spørgsmål 17,4.

I sådanne tilfælde skal der svares 'Ikke relevant' til de sidstnævnte spørgsmål, i eksemplerne oven for nr. 4,2 og 17,4.

4. Afsluttende bemærkninger til vejledning

Afslutningsvis skal Datatilsynet bemærke, at jeres organisation skal udfylde alle celler i spørgeskemaet. Således også i tilfælde hvor spørgsmålet og efterfølgende afhængige spørgsmål heraf besvares med 'Ikke relevant'. Jeres organisation skal tage udtrykkelig stilling til alle spørgsmål.

I tilfælde, hvor Datatilsynet modtager besvarelser med ikke udfyldte celler, vil tilsynet foretager en yderligere høring hos jer.

Hvis ovenstående giver anledning til spørgsmål, er I velkomne til at kontakte tilsynet telefonisk.

Med venlig hilsen

Datatilsynet