Vejledning om tilsyn med databehandlere

Pointskala og seks tilsynskoncepter

Oktober 2021

DATATILSYNET

Indhold

Forord 3

1. Start med at skabe overblik 5

1.1 Hvilke databehandlere har du? 5

1.2 Risiko og tilsyn 5

2. Hvordan kan jeg føre tilsyn? (En vejledende model) 6

2.1 Pointskala og tilsynskoncepter 6

2.2 Praktisk anvendelse af pointskalaen 6

2.3 Parametre for de enkelte point (A + B + C + D) 7

A. Hvor mange personer? 7

B. Særlige kategorier af personoplysninger? (Følsomme personoplysninger) 8

C. Andre personoplysninger af beskyttelsesværdig karakter? (Fortrolige oplysninger) 9

D. Særlige behandlinger? 10

3. Hvad skal jeg føre tilsyn med? 12

3.1 Kravene i databehandleraftalen 12

4. Seks vejledende tilsynskoncepter 13

4.1 De seks tilsynskoncepter 13

4.2 Kombination af koncepterne 13

5. Hvor ofte skal jeg føre tilsyn? 22

6. Hvem skal føre tilsyn med underdatabehandlere? 24

Vejledning om tilsyn med databehandlere

Denne vejledning er tænkt som en hjælp til, hvordan du som dataansvarlig kan føre et passende tilsyn med dine databehandlere. Vejledningen indeholder en vejledende model med en pointskala og seks tilsynskoncepter, der eksemplificerer, hvordan du kan gennemføre et passende tilsyn med dine databehandlere.

Når du som privat virksomhed, offentlig myndighed eller institution behandler personoplysninger, har du – som dataansvarlig – et ansvar for, at behandlingen sker på en forsvarlig måde. Behandling af personoplysninger skal bl.a. ske på et lovligt grundlag, der skal være etableret en passende sikkerhed, og du skal være i stand til at sikre overholdelsen af de registreredes rettigheder.

I mange tilfælde vil du som dataansvarlig også have behov for at overlade personoplysninger til eksterne leverandører – såkaldte databehandlere – der på dine vegne og efter dine instrukser behandler de pågældende oplysninger. I sådanne situationer har du også et ansvar for, at dine databehandlere – på samme måde som dig selv – behandler oplysningerne forsvarligt.

Når du gør brug af databehandlere, skal du for det første sikre dig, at der er indgået en såkaldt databehandleraftale mellem dig og databehandleren, og du skal for det andet føre en passende kontrol (tilsyn) med databehandleren.

Denne vejledning er tænkt som en hjælp til, hvordan du kan føre et sådant passende tilsyn med dine databehandlere.

Hvad er en personoplysning?

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selvom personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Personoplysninger kan for eksempel være personnumre, registreringsnumre, et billede, en e-mailadresse, et telefonnummer, et fingeraftryk, en stemmeoptagelse, lægejournaler eller biologisk materiale, når det er muligt at identificere en person ud fra oplysningerne eller ved at sammenholde med andre personoplysninger. Man siger, at oplysningen er "personhenførbar".

Læs mere om hvad personoplysninger er her.

Hvad er behandling af personoplysninger?

En behandling af personoplysninger kan have mange former. En behandling omfatter efter databeskyttelsesforordningen enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Finder blot en af de nævnte former for håndtering af personoplysninger sted, vil der være tale om en behandling, som er omfattet af databeskyttelsesreglerne.

En behandling af personoplysninger kan således godt finde sted, selvom du ikke har læst eller aktivt anvendt de pågældende personoplysninger, f.eks. hvis du alene opbevarer personoplysningerne.

Find mere information om, hvornår du behandler personoplysninger her.

1. Start med at skabe overblik

1.1 Hvilke databehandlere har du?

Hvilke andre virksomheder mv. behandler personoplysninger på dine vegne? Det kan f.eks. være et lønbureau, som står for din lønadministration og derfor håndterer bl.a. lønoplysninger om dine ansatte. En databehandler kan også være et firma, der leverer og drifter dit kundehåndteringssystem (CRM) og derved behandler personoplysninger om f.eks. dine kunders varekøb, betalingsoplysninger, privatadresser, e-mailadresser osv.

Databehandleraftale

Hvis du f.eks. er i tvivl om, hvorvidt dine leverandører er databehandlere for dig, bør du kontakte dem for at få det afklaret. Spørg f.eks. om de normalt indgår databehandleraftaler. Se vejledningen om dataansvarlige og databehandlere for yderligere information om rollefordelingen.

Hvis du ikke har indgået databehandleraftaler med de virksomheder, som behandler personoplysninger på dine vegne, skal du kontakte virksomhederne, så I sammen kan få dette på plads.

Du kan med fordel have et fast tidspunkt hvert år, hvor du gennemgår, hvilke databehandlere du har, og hvem det er tid til at føre tilsyn med.

1.2 Risiko og tilsyn

Generelt kan man sige, at jo mere der kan gå galt ved behandlingen hos databehandleren (stor risiko), jo større krav stilles der til dit tilsyn med databehandleren. Her skal du være opmærksom på, at når det handler om databeskyttelse, er det ikke risikoen for, at du (som virksomhed eller som myndighed) kommer galt afsted. Det er derimod risikoen for de registrerede (f.eks. medarbejderne, kunderne og borgerne), du skal have for øje. Hvor sandsynligt er det, at noget går galt? Hvad er konsekvenserne, hvis det rent faktisk går galt?

Som tommelfingerregel kan du regne med, at kravene til tilsynet med databehandlere stiger i takt med:

- At databehandleren behandler **flere** personoplysninger.
- At oplysninger får en mere **fortrolig** eller **følsom** karakter.
- At behandlingen bliver mere **indgribende.**

Den vejledende model, som er beskrevet i denne vejledning, tager højde for det forhold, at jo større risici der er ved behandlingen hos databehandleren, jo større krav stilles der til dit tilsyn med databehandleren.

I kapitel 2 og 3 kan du se konkrete eksempler på dette.

2. Hvordan kan jeg føre tilsyn?

(En vejledende model)

2.1 Pointskala og tilsynskoncepter

Det kan være svært at finde det helt rigtige niveau for et tilsyn – hvornår gør man for lidt, og hvornår gør man for meget? Nedenfor er en vejledende model, som du kan støtte dig til, når du skal vurdere, hvordan du gennemfører et passende tilsyn med dine databehandlere.

Den vejledende model består af en vejledende pointskala, som kan give dig en fornemmelse af, hvor risikofyldt behandlingen af personoplysninger er. I tilknytning hertil er der seks tilsyns-koncepter, som gradvist stiller større og større krav til din gennemførelse af tilsynet – dvs. koncept 1 er det **mindst** ressourcekrævende, og koncept 5 og 6 vil normalt være de **mest** ressourcekrævende.

Kort sagt; større risiko giver flere point, og flere point betyder, at der stilles flere krav til dit tilsyn med databehandleren.

I de følgende afsnit kan du læse mere om, hvordan du kommer frem til det antal point, som passer bedst på din situation, og du kan læse mere om de forskellige tilsynskoncepter.

2.2 Praktisk anvendelse af pointskalaen

Når du anvender pointskalaen, er det for det første afgørende for antallet af point, hvor mange personer du overlader oplysninger om til din databehandler. Herefter kan det give flere point afhængigt af, hvilke typer af personoplysninger databehandleren behandler på dine vegne, og hvilken slags behandling der er tale om.

2.3 Parametre for de enkelte point (A + B + C + D)

A. Hvor mange personer?

Overlader du oplysninger om under 1.000 personer: **1 point**

Overlader du oplysninger om 1.000-10.000 personer: **2 point**

Overlader du oplysninger om mere end 10.000 personer: **3 point**

Jo flere personer du overlader oplysninger om til din databehandler, jo større vil risikoen for personerne oftest også være. Det skyldes bl.a., at gevinsten for kriminelle ved at misbruge oplysningerne til f.eks. identitetstyveri er højere, når der er tale om mange personer. Hvis der behandles oplysninger om et stort antal personer og dermed mange data, kan det desuden være sværere at få ryddet op og overholde slettefrister. Derfor stiger kravene til dine tilsyn med databehandleren i takt med antallet af personer.

Herudover er det typisk sådan, at jo flere forskellige personer der behandles oplysninger om, desto flere individuelle forskelligheder vil der være omkring risikoniveauet for den enkelte. Eksempelvis er en oplysning om en privatadresse relativt harmløs for de fleste personer, men hvis enkelte har adressebeskyttelse kan en eksponering af adressen indebære en betydelig risiko for den pågældende, og jo flere registrerede der er, desto flere vil antageligt have adressebeskyttelse.

A. Eksempel

Hvis du f.eks. overlader oplysninger til et lønbureau (databehandler A), som administrerer alle dine 250 medarbejderes løn, f.eks. ved beregning af løn og udsendelse af lønsedler mv., vil det være afgørende, hvor mange ansatte du har. Du vil derfor skulle medregne **1 point** (færre end 1.000 personer), når du vurderer, hvordan du skal føre tilsyn med databehandler A.

Antallet af dine kunder er i denne sammenhæng uinteressant.

A. Eksempel

Hvis du derimod overlader oplysninger til en virksomhed (databehandler B), som løbende analyserer alle dine 8.500 kunders indkøbsmønstre, er det alene antallet af kunder, som er afgørende, og du skal i denne situation medregne **2 point** (flere end 1.000, men færre end 10.000 personer), når du vurderer, hvordan du skal føre tilsyn med databehandler B.

Antallet af ansatte er i denne sammenhæng uinteressant.

B. Særlige kategorier af personoplysninger? (Følsomme personoplysninger)

Behandler din databehandler særlige kategorier af personoplysninger på dine vegne?
Hvis ja: **3 point**

De særlige kategorier af personoplysninger er udtrykkeligt afgrænset i databeskyttelsesforordningens artikel 9 og er oplysninger om:

- Race og etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering

Kun de oplysninger, der er nævnt ovenfor, er særlige kategorier af personoplysninger.

B. Eksempel

En fagforening (dataansvarlig) får en virksomhed (databehandler) til at sende nyhedsmails til fagforeningens medlemmer. Virksomheden registrerer i den forbindelse e-mailadresser på de medlemmer, som har tilmeldt sig nyhedsbrevet. Da

nyhedsbrevene alene sendes til medlemmer af fagforeningen, behandler virksomheden også oplysninger om fagforeningsmæssigt tilhørsforhold på vegne af fagforeningen.

Fagforeningen skal dermed medregne **3 point**, når fagforeningen vurderer, hvordan der skal føres tilsyn med databehandleren.

B. Eksempel

En virksomhed (dataansvarlig) bruger et HR-system, som driftes af et eksternt firma (databehandler). I HR-systemet er der også oplysninger om ansattes eventuelle sygdomme. Det eksterne firma behandler dermed helbredsoplysninger på vegne af virksomheden.

Den dataansvarlige virksomhed skal dermed medregne **3 point**, når virksomheden vurderer, hvordan der skal føres tilsyn med databehandleren.

C. Andre personoplysninger af beskyttelsesværdig karakter? (Fortrolige oplysninger)

Behandler din databehandler andre personoplysninger af beskyttelsesværdig karakter på dine vegne? **Hvis ja: 2 point**

Andre personoplysninger af beskyttelsesværdig karakter er en kategori af oplysninger, der ikke er nævnt udtrykkeligt i databeskyttelsesreglerne, men hvor særlige beskyttelsesbehov kan have betydning ved anvendelsen af databeskyttelsesreglerne.

Det kan være lidt svært at vurdere, om oplysninger har en sådan beskyttelsesværdig karakter. Det afgørende er, om oplysningerne efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab[1]. Det vil sige, at du efter bedste evne skal forsøge at vurdere, om de fleste borgere i Danmark vil synes, at det er ubehageligt, hvis andre bliver bekendt med de pågældende oplysninger. Det kunne være fordi, at der er en risiko for, at andre vil kigge skævt til én, hvis de blev bekendt med oplysningerne. Det kan også være fordi, at der er risiko for, at oplysningerne vil kunne misbruges til f.eks. identitetstyveri, hvis de falder i de forkertes hænder.

Eksempler på andre personoplysninger af beskyttelsesværdig karakter er bl.a. oplysninger om væsentlige sociale problemer, personnumre, beskyttede navne og adresser, eksamenskarakterer, disciplinære foranstaltninger (f.eks. en skriftlig advarsel fra arbejdsgiveren), personlighedstest, selvmordsforsøg, langtidsledighed, oplysninger om at man er registreret som dårlig betaler, samt oplysninger om at man modtager førtidspension. Oplysninger om strafbare forhold skal også medregnes til denne kategori af oplysninger.

[1] Jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27.

Sådanne andre personoplysninger af beskyttelsesværdig karakter tæller kun med i pointoptællingen, hvis du typisk overlader sådanne oplysninger, f.eks. personnumre, til din databehandler som led i din virksomhed.

Du skal dog ikke medregne pointene, hvis et personnummer undtagelsesvis bliver overladt til databehandleren, f.eks. fordi en kunde uopfordret oplyser det.

C. Eksempel

En detailvirksomhed (dataansvarlig) har en kundeklub og bruger et firma (databehandler) til at håndtere denne klub. Firmaet behandler i den forbindelse oplysninger om de enkelte kunder, f.eks. navne og adresser på kunderne. Da nogle af kunderne har navne- og adressebeskyttelse, behandler firmaet andre personoplysninger af beskyttelsesværdig karakter på vegne af detailvirksomheden.

Detailvirksomheden skal derfor medregne **2 point** ved vurderingen af, hvilket tilsyn der skal gennemføres.

C. Eksempel

En selvejende institution (dataansvarlig) – som er et bosted for socialt udsatte unge – anvender et særligt system til at registrere oplysninger om de unge. Systemet driftes af et eksternt firma (databehandler). Det er en oplysning af beskyttelsesværdig karakter, at en person bor på et bosted for socialt udsatte unge.

Den selvejende institution skal derfor medregne **2 point** ved vurderingen af, hvilket tilsyn der skal gennemføres**.**

D. Særlige behandlinger?

Går selve behandlingen af oplysninger tæt på folks privatliv? **Hvis ja: 2 point**

Overlader du oplysninger til en databehandler, og går selve behandlingen af oplysninger tæt på folks privatliv, skal du være ekstra opmærksom, da dette i sig selv kan være indgribende, og det vil typisk også medføre en større risiko for de registrerede personer.

Hvor fokus oven for under afsnit B (særlige kategorier af personoplysninger) og afsnit C (andre personoplysninger af beskyttelsesværdig karakter) var på selve oplysningerne, er fokus her på det, som du (eller din databehandler) gør med oplysningerne.

Det kan eksempelvis være relativt uproblematisk, hvis en detailbutik registrerer oplysninger om kunders køb for at kunne yde support ved den senere anvendelse af produkterne. Hvis detailbutikken derimod bruger de samme købsoplysninger for at udarbejde særlige kundeprofiler (profilering) og måske endda supplerer med oplysninger om de enkelte kunders adfærd

på butikkens hjemmeside eller fysiske butikker, begynder det at få en mere indgribende karakter. Det gør sig særligt gældende, hvis det sker for at kunne målrette detailbutikkens markedsføring over for den enkelte kunde og i øvrigt påvirke kundens (ubevidste) købsadfærd.

Ligesom det kan være lidt svært at vurdere, om udvalgte oplysninger har særlig beskyttelsesværdig karakter (afsnit C ovenfor), kan det også være svært at vurdere, hvornår en behandling i sig selv bliver indgribende. På samme måde som ovenfor må du efter bedste evne forsøge at vurdere, om de fleste borgere i Danmark vil synes, at det vil være en indgribende behandling af oplysninger.

Som eksempler på sådanne mere indgribende behandlinger kan nævnes:

- Behandling af lokationsdata med henblik på at kortlægge eller følge personers adfærd.
- Systematisk overvågning af personer med henblik på at kontrollere dem.
- Profilering, hvor f.eks. relativt harmløse oplysninger anvendes til at give meget præcise oplysninger om personers (aktuelle eller fremtidige) behov, adfærd eller personlighed.
- Afgørelser, der alene er baseret på automatisk behandling, herunder profilering, og som har retsvirkning eller på tilsvarende vis betydeligt påvirker personer.
- Samkøring af datasæt med henblik på at tilvejebringe nye oplysninger, som ligger ud over, hvad de registrerede personer med rimelighed kan forvente.

Der er til en vis grad sammenfald mellem disse mere indgribende behandlinger, og hvornår man som dataansvarlig skal foretage en konsekvensanalyse. Du kan derfor også skæve til Datatilsynets liste over behandlingstyper, der er underlagt kravet om konsekvensanalyse.

3. Hvad skal jeg føre tilsyn med?

3.1 Kravene i databehandleraftalen

Det er som udgangspunkt databehandleraftalen, der danner rammerne for, hvad du skal føre tilsyn med hos din databehandler. Kravene til databehandleraftalens indhold fremgår af databeskyttelsesforordningens artikel 28 (Se artikel 28, vejledningen om dataansvarlige og databehandlere og Datatilsynets skabelon til en databehandleraftale).

Databehandleraftalen skal bl.a. indeholde krav om:

- ✓ At databehandlerens medarbejdere, der behandler personoplysninger, har underskrevet en fortrolighedsaftale eller er underlagt en passende lovbestemt tavshedspligt.
- ✓ At databehandleren – i forhold til den behandling af personoplysninger, som databehandleren foretager på dine vegne – gennemfører passende tekniske og organisatoriske sikkerhedsforanstaltninger med fokus på risikoen for de registrerede samt gennemfører eventuelle særlige aftalte sikkerhedskrav.
- ✓ At databehandleren ikke gør brug af en underdatabehandler uden din godkendelse.
- ✓ At databehandleren pålægger eventuelle underdatabehandlere samme forpligtelser som i databehandleraftalen mellem dig og databehandleren, herunder at databehandleren fører tilsyn med eventuelle underdatabehandlere.
- ✓ At databehandleren så vidt muligt bistår dig ved hjælp af passende tekniske og organisatoriske foranstaltninger, så du kan opfylde din forpligtelse til at besvare anmodninger om at udøve de registreredes rettigheder.
- ✓ At databehandleren bistår dig f.eks. i forhold til din forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet, herunder at databehandleren underretter dig uden unødig forsinkelse om brud på persondatasikkeheden, som berører den behandling, som databehandleren foretager på dine vegne.
- ✓ At databehandleren sletter eller tilbageleverer alle personoplysninger til dig, når databehandlerens service til dig ophører.
- ✓ At databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i databehandleraftalen, til rådighed for dig, og at databehandleren giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af dig eller en anden revisor, som er bemyndiget af dig.

4. Seks vejledende tilsynskoncepter

4.1 De seks tilsynskoncepter

Du kan fokusere på de koncepter, som er relevante for dig og din organisation ud fra, hvor mange point du har fået efter pointskalaen (forklaret i kapitel 2).

Uanset hvor mange point du har fået, skal du være sikker på, at du har en databehandleraftale med din databehandler, der lever op til minimumskravene i databeskyttelsesforordningen (se artikel 28, vejledningen om dataansvarlige og databehandlere og Datatilsynets skabelon til en databehandleraftale).

4.2 Kombination af koncepterne

Der er ikke noget til hinder for, at du inden for rammerne af pointsystemet skifter mellem tilsynskoncepterne, eller at to eller flere koncepter supplerer hinanden.

Det kan være, at du har vurderet, at du skal bruge koncept 5 hvert andet år, men at du – for at have en fornemmelse for udviklingen hos databehandleren – supplerer med et tilsyn de øvrige år efter koncept 3.

Som det ses på de lave point-niveauer, kan du vælge mellem flere koncepter, og altså også gå højere end forventet. Du kan f.eks. vælge at basere valget af koncept på de aktuelle omstændigheder, f.eks. hvis der i det forgangne år er oplevet sikkerhedsbrud hos databehandleren, som kan indikere, at der ikke er tilstrækkelig styr på sikkerheden.

Det kan også være nødvendigt at gå til et højere niveau, fordi databehandleren ikke tilbyder det, som kræves af konceptet. Hvis du i princippet kunne nøjes med at følge koncept 3 – hvor du kan forholde dig til en årlig status fra databehandleren – men en sådan årlig status ikke tilbydes af databehandleren, må du enten kræve dette, eller alternativt benytte et koncept på et højere niveau.

Koncept 1

Koncept 1

- Du skal ikke gøre noget, med mindre du bliver opmærksom på, at der er noget galt hos databehandleren.

Hvis du benytter en troværdig og seriøs databehandler, kan du forventeligt stole på, at vedkommende overholder databehandleraftalen. Du skal altså i den situation ikke gøre noget, med mindre du bliver opmærksom på, at der er noget galt hos databehandleren.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

Eksempel: En frisør bruger et online bookingsystem

Point
En frisør (dataansvarlig) bruger et onlinebookingsystem leveret af en it-virksomhed (databehandler).

I onlinebookingsystemet er registreret kunders telefonnumre og mailadresser. Der er oplysninger om under 1.000 personer registreret i systemet.

Eksempel på brug af koncept 1

Frisøren foretager sig ikke noget særligt i forhold til at føre tilsyn med it-virksomheden, men sikrer sig, at der er en lovpligtig databehandleraftale.

En dag er alle tidsbestillingerne pludselig forsvundet, og frisøren kontakter it-virksomheden og beder om en forklaring på, hvad der er sket, samt oplysning om, hvorvidt kundernes oplysninger er blevet slettet eller gjort utilgængelige (krypteret). Frisøren beder om hjælp til at håndtere situationen korrekt.[2]

Koncept 2

Koncept 2

- Databehandleren bekræfter – helst skriftligt – over for dig, at alle krav i databehandleraftalen stadig efterleves.

Hvis du benytter en troværdig og seriøs databehandler, kan du nøjes med at få en bekræftelse fra databehandleren på, at alle krav i databehandleraftalen stadig efterleves.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

[2] Databehandleren skal bistå dig med at sikre overholdelse af dine forpligtelser i forbindelse med bl.a. brud på persondatasikkerheden. Det skal følge af databehandleraftalen, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra f.

Eksempel: En webshop med betalingsløsning til håndtering af betalingskort

Point

Webshoppen 'Det Glade Garnnøgle' (dataansvarlig) bruger betalingsløsningen 'eBetaling' (virksomheden bag løsningen er dermed databehandler) til betalinger med betalingskort.

eBetaling registrerer kortoplysninger – som er andre oplysninger af beskyttelsesværdig karakter – på vegne af Det Glade Garnnøgle. Kortoplysningerne slettes efter købet.

eBetaling opbevarer derfor ikke personoplysninger på vegne af webshoppen men behandler oplysningerne i forbindelse med betaling. Det Glade Garnnøgle har under 1.000 aktive kunder, men da nye kunder kommer til jævnligt, har der over tid været behandlet kortoplysninger om ca. 3.000 personer hos eBetaling.

Eksempel på brug af koncept 2

Eftersom Det Glade Garnnøgle ikke har oplevet problemer med den service, som eBetaling leverer, vælger Det Glade Garnnøgle kun at udføre tilsyn hvert andet år. Ved tilsynet bliver eBetaling bedt om skriftligt at bekræfte, at samtlige krav i databehandleraftalen stadig efterleves. Det Glade Garnnøgle gemmer bekræftelsen til dokumentation.

Koncept 3

Koncept 3

- Databehandleren giver dig årligt – enten direkte eller via sin hjemmeside – en skriftlig status på forhold, der er omfattet af databehandleraftalen, og andre relevante områder (f.eks. organisatoriske eller produktmæssige ændringer).

Du skal sikre, at ovennævnte status dækker alle behandlinger, som databehandleren (enten selv eller via underdatabehandlere) foretager på dine vegne.

Databehandleren kan f.eks. offentliggøre egne rapporter på dennes hjemmeside for at vise kunder og potentielle kunder, hvordan databehandleren efterlever databehandleraftalerne. Databehandleren kan også vælge at sende disse rapporter uopfordret til kunderne (de dataansvarlige), ligesom det kan være, at databehandleren vælger kun at sende en rapport, hvis kunden specifikt beder om at få den at se. Uanset hvad, skal du udnytte dine eventuelle muligheder for at få disse rapporter, forholde dig til dem og gemme dem hos dig selv.

Den årlige status skal også omfatte eventuelle særlige aftalte krav i databehandleraftalen, f.eks. hvis der er konkrete krav til kryptering af al kommunikation mellem dig og din databehandler eller tidspunkter for sletning af testdata. Hvis de særlige aftalte krav ikke fremgår af databehandlerens årlige status, skal du spørge til, hvordan databehandleren overholder disse

krav og eventuelt bede om dokumentation eller foretage stikprøver for at bekræfte svaret – især hvis du ikke får klare, utvetydige svar.

Du skal også bede databehandleren oplyse, hvilke brud på persondatasikkerheden som databehandleren har haft siden dit sidste tilsyn.

Hvad er et brud på persondatasikkerheden?

Et brud på persondatasikkerheden er et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Det betyder f.eks., at hvis der har været adgang til personoplysninger for uautoriserede personer, så har der været et brud – uanset om de uautoriserede personer har anvendt adgangen eller ej.

En anden type brud er, hvis personoplysninger har været eller er blevet utilgængelige pga. systemnedbrud eller hackerangreb. Når du spørger til brud, skal du sikre dig, at databehandleren forstår, hvad det omfatter.

Du skal alene spørge ind til brud på persondatasikkerheden, som kan have berørt databehandlerens behandling af personoplysninger på dine vegne[3] Spørg herefter databehandleren, om databehandleren har forholdt sig til eventuelle problemstillinger, der er knyttet til sikkerhedsbruddene.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

[3] Det kan være, du allerede har modtaget den information, idet databehandleren faktisk skal underrette dig uden unødig forsinkelse, når databehandleren er blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Hvis du konstaterer, at databehandleren ikke har orienteret dig om brud på persondatasikkerheden uden unødig forsinkelse, skal du sikre dig, at databehandleren gør det fremadrettet, så du kan overholde din forpligtelse til bl.a. uden unødig forsinkelse at anmelde brud på persondatasikkerheden til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. Du kan læse mere om brud på persondatasikkerheden i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden.

Eksempel: En statslig myndighed bruger et HR-system driftet af et eksternt HR-bureau

Point
En statslig myndighed (dataansvarlig) bruger et HR-system, som er hostet og drevet af et HR-bureau (databehandler).

Myndigheden har omkring 200 ansatte, hvor navn, adresse, personnummer, ansættelsesdato og evt. sygdomme, fremgår af registreringerne.

Eksempel på brug af koncept 3

Myndigheden forholder sig til den årlige status fra HR-bureauet på forhold, der er omfattet af databehandleraftalen og andre relevante områder. Myndigheden kontrollerer om denne status også dækker de særlige aftalte krav, som er i databehandleraftalen, og om den dækker underdatabehandlere. Hvis ikke, eller hvis rapporten ikke umiddelbart er forståelig, beder myndigheden om en uddybning.

Myndigheden beder desuden HR-bureauet oplyse, hvilke brud på persondatasikkerheden bureauet har haft siden myndighedens sidste tilsyn. Idet den årlige statusrapport m.v. ikke nævner bekymrende problemer, gør myndigheden ikke yderligere.

Koncept 4

Koncept 4

- Databehandleren har en relevant og opdateret certificering eller følger et såkaldt adfærdskodeks, som er relevant for dine behandlingsaktiviteter.

Databehandleren skal skriftligt dokumentere, at behandling af personoplysninger på dine vegne sker i henhold til en opdateret certificering, jf. databeskyttelsesforordningens artikel 42, eller at databehandleren følger et godkendt adfærdskodeks, jf. databeskyttelsesforordningens artikel 40. Se mere på Datatilsynets hjemmeside om certificeringsordninger og adfærdskodekser.

Du skal være opmærksom på, om certificeringen eller adfærdskodekset afspejler alle de krav, der er til databehandleraftalen. Du skal også være opmærksom på, om evt. særlige aftalte krav i databehandleraftalen er dækket af certificeringen eller adfærdskodekset, f.eks. hvis der er konkrete krav til kryptering af al kommunikation mellem dig og din databehandler eller tidspunkter for sletning af testdata. Hvis de ovennævnte krav ikke er dækket, skal du spørge til, hvordan databehandleren overholder disse krav og eventuel bede om dokumentation eller foretage stikprøver for at bekræfte svaret – især hvis du ikke får klare, utvetydige svar.

Du skal også bede databehandleren oplyse, hvilke brud på persondatasikkerheden som databehandleren har haft siden dit sidste tilsyn.

Hvad er et brud på persondatasikkerheden?

Et brud på persondatasikkerheden er et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Det betyder f.eks., at hvis der har været adgang til personoplysninger for uautoriserede personer, så har der været et brud – uanset om de uautoriserede personer har anvendt adgangen eller ej.

En anden type brud er, hvis personoplysninger har været eller er blevet utilgængelige pga. systemnedbrud eller hackerangreb. Når du spørger til brud, skal du sikre dig, at databehandleren forstår, hvad det omfatter.

Du skal alene spørge ind til brud på persondatasikkerheden, som kan have berørt databehandlerens behandling af personoplysninger på dine vegne[4]. Spørg herefter databehandleren, om databehandleren har forholdt sig til eventuelle problemstillinger, der er knyttet til sikkerhedsbruddene.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

Eksempel: Oplysninger fra beacons i en butik håndteres af en it-virksomhed med en certificering

Point
En butik (dataansvarlig) indsamler oplysninger om sine kunders ophold i fysiske butikker ved hjælp af 'beacons'. Omkring 15.000 kunder har butikkens app installeret, og denne app indsamler oplysninger fra 'beacons', og oplysningerne kombineres med kundens navn og e-mail-adresse.

[4] Det kan være, du allerede har modtaget den information, idet databehandleren faktisk skal underrette dig uden unødig forsinkelse, når databehandleren er blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Hvis du konstaterer, at databehandleren ikke har orienteret dig om brud på persondatasikkerheden uden unødig forsinkelse, skal du sikre dig, at databehandleren gør det fremadrettet, så du kan overholde din forpligtelse til bl.a. uden unødig forsinkelse at anmelde brud på persondatasikkerheden til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. Du kan læse mere om brud på persondatasikkerheden i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden.

Eksempel på brug af koncept 4

En it-virksomhed (databehandler) behandler oplysningerne for butikken. It-virksomheden har tilsluttet sig en certificeringsordning for sine behandlingsaktiviteter.

Butikken modtager dokumentation på, at certificeringen stadig er gyldig, at den sikrer it-virksomhedens efterlevelse af krav i databeskyttelsesforordningen, og at certificeringen dækker alle krav til en databehandleraftale. Herudover beder butikken om bekræftelse på efterlevelse af særlige aftalte krav i databehandleraftalen (hvis efterlevelse ikke kan læses af certificeringen). Butikken beder desuden it-virksomheden om at oplyse om brud på persondatasikkerheden siden sidste tilsyn.

Butikken har benyttet samme databehandler gennem flere år uden at opleve problemer i form af alvorlige brud på persondatasikkerheden, og certificeringen har været uafbrudt i samme årrække. På den baggrund vælger butikken kun at udføre dette tilsyn hvert andet år.

Koncept 5

Koncept 5

- En uafhængig tredjepart har ført et dokumenteret tilsyn med databehandleren på et område, som også dækker dine behandlingsaktiviteter.

Du kan basere din kontrol på erklæringer lavet af en uafhængig tredjepart. Et eksempel er en revisionserklæring, f.eks. en ISAE 3000-revisionserklæring. I sådanne tilfælde skal du ved behandlinger, som giver 7-10 point, vælge den revisionserklæring, der etablerer ”Høj grad af sikkerhed”.

En anden mulighed er at anvende en anden parts tilsyn, f.eks. en brancheforening, der fører tilsyn på vegne af medlemmerne, eller en myndighed, der fører tilsyn på vegne af flere myndigheder. Du kan også vælge sammen med andre dataansvarlige at bemyndige en uafhængig tredjepart til at udføre et tilsyn på vegne af alle de dataansvarlige.

Uanset hvilken model du vælger, skal du sikre dig følgende:

- ✓ Tilsynet dækker dine behandlingsaktiviteter hos databehandleren.
- ✓ Tilsynet omhandler overholdelse af databehandleraftalen.
- ✓ Tilsynet dækker eventuelle særlige aftalte krav i databehandleraftalen – f.eks. hvis der er konkrete krav til kryptering af al kommunikation mellem dig og din databehandler eller tidspunkter for sletning af testdata.
- ✓ Tilsynet har også fokus på, om databehandleren sikrer efterlevelse af krav hos eventuelle underdatabehandlere (databehandlernes leverandører).

✓ Den part, som udfører tilsynet, er uafhængig i forhold til især databehandleren. Det kan f.eks. være et problem, hvis den der udfører tilsynet er del af samme virksomhed som databehandleren (datterselskab/moderselskab), eller at de på anden vis har økonomiske interesser hos hinanden.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

Eksempel: En praktiserende læges journalsystem hostes og driftes af en ekstern it-virksomhed

Point
En praktiserende læge (dataansvarlig), der behandler oplysninger om mere end 1.000 patienter, vælger at skifte til et nyt journalsystem. Journalsystemet hostes og driftes hos en it-virksomhed (databehandler)

Eksempel på anvendelsen af koncept 5

Samme journalsystem bruges allerede af andre læger, og en brancheforening fører årligt tilsyn med behandlingerne hos it-virksomheden. Lægen finder, at der er indgået enslydende databehandleraftaler, og tilsynet udført af brancheforeningen kan dermed dække lægens behov for tilsyn med den nye databehandler. Lægen modtager, forholder sig til og gemmer tilsynsrapporterne.

Koncept 6

Koncept 6

- Du fører selv – eller sammen med andre – et dokumenteret tilsyn med databehandleren.

Hvad du skal føre tilsyn med, og hvor omfangsrigt dit tilsyn skal være, skal du finde ud af ved at lave en vurdering af de risici, behandlingerne af personoplysninger udgør for de registrerede personer. Du skal derfor først vurdere, hvor databehandlerens behandling af oplysninger (på dine vegne) kan gå galt, og herefter vurdere, hvad og hvor meget der skal kontrolleres for at minimere disse risici. Du skal med tilsynet få afdækket, hvordan databehandleren opfylder sine forpligtelser efter databehandleraftalen, f.eks. angående underdatabehandlere, underretning

af dig ved brud på persondatasikkerheden, behandlingssikkerhed, særlige aftalte krav i databehandleraftalen (f.eks. krav til kryptering af al kommunikation mellem dig og din databehandler eller tidspunkter for sletning af testdata) mv. Se vejledningens afsnit 5 for en uddybning af, hvad der er relevant at føre tilsyn med. Du kan f.eks. føre tilsyn ved at fremsende et skriftligt spørgeskema til databehandleren og følge op på svarene.

Via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, kan du evt. få indtryk af problemer hos databehandleren, og så bør du tage kontakt til databehandleren for at finde en løsning. Gem altid din korrespondance med databehandleren.

Eksempel: En kommune anvender en privat virksomhed til at håndtere byggesager

Point
En kommune (dataansvarlig) bruger et firma (databehandler) til at håndtere byggesager. Firmaet behandler derfor oplysninger om sager tilknyttet ca. 30.000 borgere i kommunen, f.eks. borgernes navne, adresser (herunder hemmelige adresser) og oplysninger om handikap.

Eksempel på anvendelsen af koncept 6

Kommunen sætter sig sammen med andre kommuner og vurderer risici ved behandlingen og undersøger ligheder/forskelle i anvendelsen af samme databehandler. På denne baggrund beslutter kommunerne et fælles tilsyn, der også omfatter særlige krav, som kun nogle af kommunerne har i deres databehandleraftale. Resultatet af dette tilsyn distribueres og vurderes af hver kommune. Eventulle reaktioner over for databehandleren sker også i fællesskab.

5. Hvor ofte skal jeg føre tilsyn?

Jo mere kritisk behandlingen er for de personer, som du behandler oplysninger om, jo mere intensiv kontrol skal du føre med dine databehandlere. I nogle tilfælde kan det derfor være nødvendigt at føre tilsyn hos dine databehandlere årligt. Ligesom det – alt efter omstændighederne – kan være tilstrækkeligt, hvis risikoen er lav, at føre tilsyn med en lavere frekvens.

Eksempler på elementer der taler for en høj frekvens:

- Databehandleren har haft problemer med at overholde aftaler (ikke bare databehandleraftalen).
- Databehandleren har oplevet flere alvorlige sikkerhedsbrud, herunder brud på persondatasikkerheden.
    - Dette kræver naturligvis, at du bliver informeret om dette, men i nogle tilfælde vil du opdage det, f.eks. fordi bruddet afbryder den service, du får som kunde, og derfor er det måske nødvendigt at forlange en forklaring på afbrydelsen af en service. Dermed kan databehandleren ikke skjule årsagen eller alvoren af et brud.
    - Når det kommer til brud på persondatasikkerheden[5], er det et lovkrav, at databehandleren informerer dig om disse, uden unødig forsinkelse.
- Der skiftes ofte underdatabehandler(e).
- Der sker ofte ejerskifte, opkøb, fusion eller gennemgribende ændringer i strategien hos databehandleren.
    - Den slags vil du ofte bemærke som kunde. Ejerskifte/fusion kan umiddelbart fremstå ligegyldigt, når databehandleraftalen stadig gælder, men den slags kan ændre markant på et firmas strategi og dermed ændrede prioriteringer, der påvirker behandlingssikkerheden. Ejerskifte kan også medføre, at der i skifteprocessen tabes fokus på beskyttelsen af visse dele af it-miljøet, både i forhold til administrationen af miljøet og den fysiske flytning, udskiftning eller kassering.

Eksempler på elementer, der kan indikere et behov for et ekstra tilsyn uden for den normale frekvens:

- Ejerskifte, fusion eller gennemgribende ændringer i strategien hos databehandleren.
- En pandemi ændrer på den måde der arbejdes på, og på tilgangen til personoplysninger (flere hjemmearbejdspladser).

[5] Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet – altså de personoplysninger databehandleren behandler på dine vegne.

Eksempler på elementer der taler for en lav frekvens:

- Lang tids erfaring med databehandlerne (databehandler og underdatabehandlere) viser en stabil service og ingen eller få ikke-alvorlige sikkerhedsbrud.

6. Hvem skal føre tilsyn med underdatabehandlere?

En databehandler må ikke bruge en anden databehandler – en såkaldt underdatabehandler – uden forudgående specifik eller generel skriftlig godkendelse fra dig.

Bruger din databehandler (efter godkendelse fra dig) en underdatabehandler, skal din databehandler sørge for at pålægge underdatabehandleren de samme databeskyttelseskrav som dem, der fremgår af databehandleraftalen med dig. Det vil databehandleren skulle gøre i en underdatabehandleraftale.

Det er også databehandleren, der skal sikre, at underdatabehandleren lever op til dennes databeskyttelsesforpligtelser. Det vil sige, at databehandleren skal føre tilsyn med underdatabehandlerens behandling. Du skal som dataansvarlig imidlertid sikre dig, at databehandleren fører tilsyn med underdatabehandleren, f.eks. ved at databehandleren sender dokumentation for afholdte tilsyn til dig.

En underdatabehandler vil ikke nødvendigvis ligge samme sted på pointskalaen som databehandleren, da den del af behandlingen, som er overladt til underdatabehandleren, kan være mindre omfangsrig og indgribende end databehandlerens behandling.

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk