# Valg af tilsynskoncept – Vurdering:

Sikkerhedsniveauet skal afspejle behandlingens omfang og karakter. **Vurdering skal gemmes sammen med databehandleraftalen.**

Behandlingen omfatter følgende antal registrerede:

1-100

100-1000

1000-5000

Over 5000

Behandlingen omfatter behandling af følgende type personoplysninger:

**Almindelige personoplysninger**

**Fortrolige oplysninger/** **Andre beskyttelsesværdige oplysninger** = oplysninger der efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, f.eks. fordi der er en risiko for, at andre vil kigge skævt til en eller risiko for identitetstyveri:

* Personnummer
* Eksempler: væsentlige sociale problemer, navne- og adressebeskyttelse, eksamenskarakterer, disciplinære foranstaltninger, personlighedstest, selvmordsforsøg, langtidsledighed, dårlig betaler, modtager af førtidspension.

**Oplysninger om strafbare forhold**

**Følsomme personoplysninger**

* Helbredsoplysninger
* Seksuelle forhold eller seksuel orientering
* Race eller etnisk oprindelse
* Politisk, religiøs eller filosofisk overbevisning
* Fagforeningsmæssigt tilhørsforhold
* Genetiske eller biometriske data

**Særlige behandlinger** = behandlinger af oplysninger, som går tæt på folks privatliv, hvilket i sig selv kan være indgribende - fokus er på, *hvad* det bliver gjort med oplysningerne.

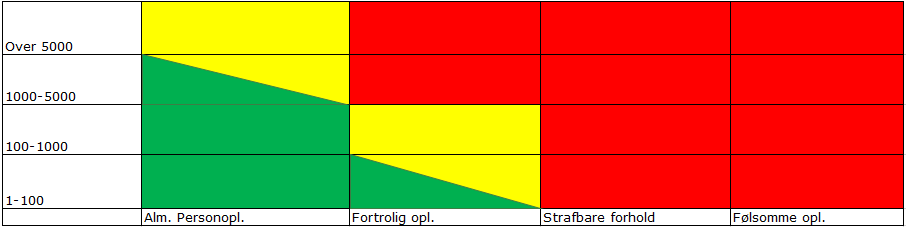
* Vurder efter bedste evne, om de fleste borgere i Danmark vil synes, at det vil være indgribende behandling af personoplysninger.

Omfanget af et tilsyn stiger i takt med (kommer mere hen i gul eller rød kategori):

* At databehandlere behandler flere personoplysninger.
* At oplysninger får en mere fortrolig eller følsom karakter.
* At behandlingen bliver mere indgribende (særlige behandlinger).

Flere personer betyder som oftest større risiko, bl.a. fordi:

* Gevinsten for kriminelle er højere (ved f.eks. identitetstyveri), når der er tale om mange personer
* Det kan være sværere at få ryddet op og overholde slettefrister ved mange data
* Jo flere personer der behandles oplysninger om, desto flere individuelle forskelligheder vil der være omkring risikoniveauet for den enkelte. (eksempel: Adresse er for de fleste harmløs. Ved adressebeskyttelse er risikoen højere, og jo flere personer jo flere med adressebeskyttelse)



På baggrund af ovenstående beskrivelse af behandlingens omfang og karakter etableres et af flg. sikkerhedsniveau:

|  |  |  |
| --- | --- | --- |
| **Lavt** | **Middelhøjt** | **Højt** |
| **Grøn** | **Gul** | **Rød** |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **GRØN** | **GUL** | **RØD** |
| Almindelige personoplysninger & Interne informationer | Fortrolige personoplysninger & Fortrolige informationer | Følsomme personoplysninger |
| Lavt sikkerhedsniveau | Middelhøjt sikkerhedsniveau | Højt sikkerhedsniveau |
|  |  |  |
| ISO27001 / ISO27002 | ISO27001 / ISO27002 | ISO27001 / ISO27002 |

# Valg af tilsynskoncept – Tilsynskoncepter

Valg af tilsynskoncept tager udgangspunkt i vurderingen ovenfor. Kopier tekst og sæt ind i databehandleraftalen (*Bilag C.7 – Procedurer for den dataansvarliges revisioner...*):

Ved middelhøjt til højt risikoniveau (Gul og Rød)

Databehandleren skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen skal være af typen ISAE 3000 GDPR type 2 med høj grad af sikkerhed udarbejdet efter helhedsmetoden, dækkende kravene beskrevet i denne databehandleraftale. Revisionserklæringen fremsendes til den dataansvarlige.

Den dataansvarlige kan fravige den aftalte tilsynsform, såfremt den dataansvarlige vurderer, at databehandleren på anden vis vil kunne dokumentere overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

Baseret på resultaterne af tilsynet er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige, har endvidere ret til at foretage inspektioner af databehandlerens fysiske faciliteter, hvor der behandles personoplysninger, og systemer, der anvendes og har relation til behandlingen, samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt databehandleren har truffet de sikkerhedsforanstaltninger, der følger af disse Bestemmelser samt gældende databeskyttelsesret. Den dataansvarlige indhenter en erklæring om fortrolighed fra den uafhængige revisor.

Den dataansvarlige kan anfægte rammerne for de foretagne kontrolforanstaltninger og kan i sådanne tilfælde anmode om en (ny) revisionserklæring og/eller (ny) inspektion under andre rammer og/eller under anvendelse af anden metode.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndigheden.

Ved lavt til middel-lavt risikoniveau (Grøn til Gul)

Databehandleren skal årligt[[1]](#footnote-1) for egen regning afgive en erklæring angående databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

Såfremt den dataansvarlige vurderer, at den fremsendte erklæring ikke på tilstrækkelig vis godtgør databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag, skal databehandleren på den dataansvarliges anmodning og for databehandlerens regning fremsende den nødvendige dokumentation til påvisning af overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag

Den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige, har endvidere ret til med rimeligt varsel at foretage inspektioner af databehandlerens fysiske faciliteter, hvor der behandles personoplysninger, og systemer, der anvendes og har relation til behandlingen, samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt databehandleren har truffet de sikkerhedsforanstaltninger, der følger af disse Bestemmelser samt gældende databeskyttelsesret. Det kan eksempelvis være tilfældet, hvis en konkret omstændighed, f.eks. et sikkerhedsbrud, giver anledning til tvivl om beskyttelsen af personoplysningerne hos databehandleren. Den dataansvarlige indhenter en erklæring om fortrolighed fra den uafhængige revisor.

Den dataansvarlige kan anfægte rammerne for de foretagne kontrolforanstaltninger og anmode om supplerende dokumentation af databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag

Baseret på resultaterne af kontrolforanstaltningerne, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere tilstrækkelige foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndigheden.

1. Ved lavt risikoniveau kan hvert andet år vælges. [↑](#footnote-ref-1)