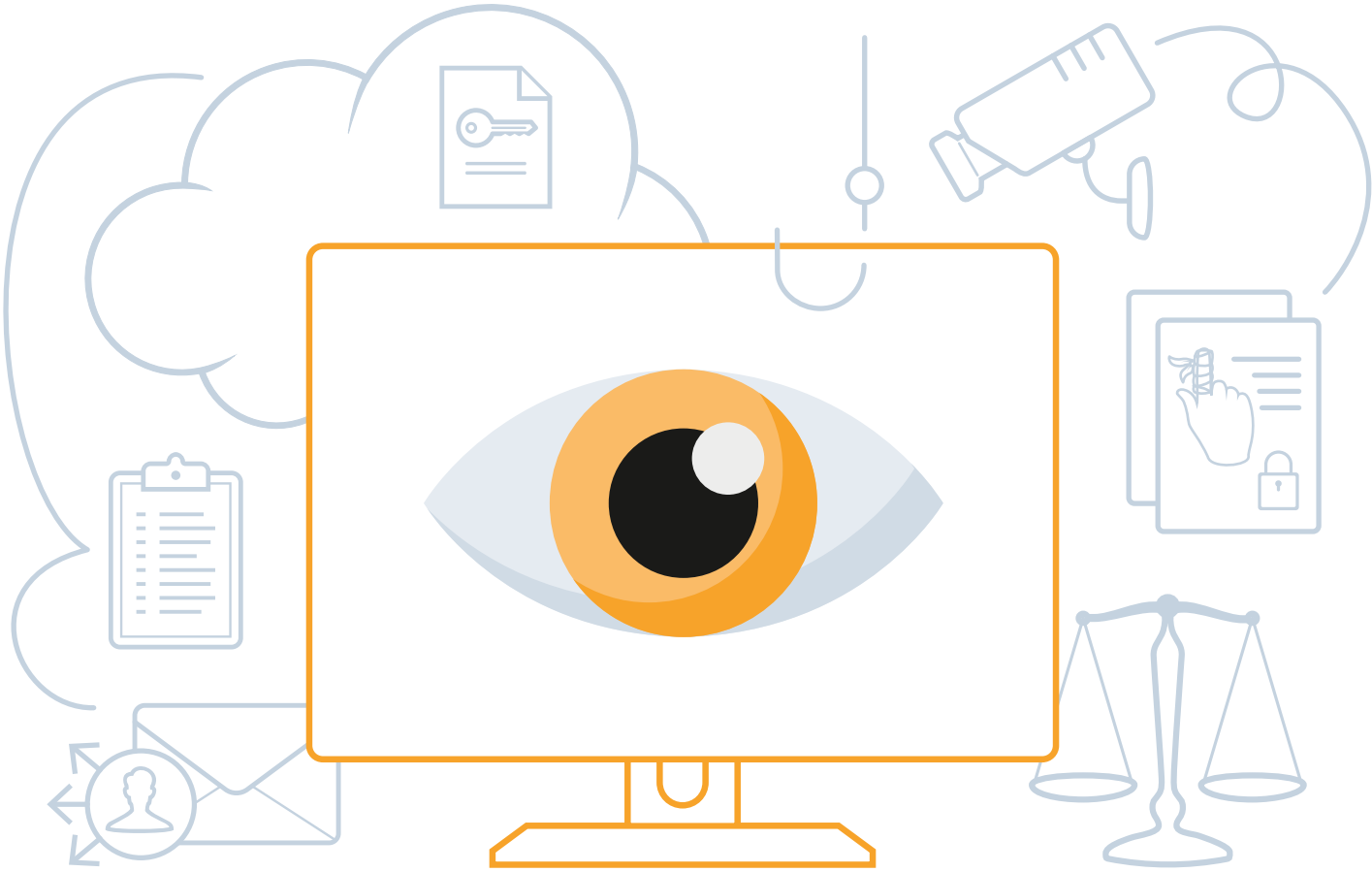


De 10 GDPR-bud

– sådan undgår du Datatilsynets rampelys

Der er ingen vej uden om GDPR. Skrækscenariet ved at ignorere GDPR og omgås persondata lemfældigt er at ende med store bøder. Og de færreste vil næppe heller være stolte af påbud eller forbud fra Datatilsynet.

Den gode nyhed er, at du ved at følge de 10 GDPR-bud er godt på vej til at vige uden om problemerne og undgå rampelyset.

Måske når du ikke i mål med det hele så hurtigt, som du drømmer om. Men det allervigtigste er at være i gang.

VISMA | DataLøn

Her er de vigtigste GDPR-bud til dig, der håndterer persondata i det daglige:

1. Du må ikke forsømme jeres fortegnelse

På GDPR'sk er en fortegnelse en kortlægning af jeres behandlingsaktivitet. På almindelig dansk er det et dokument, der giver jer det gyldne overblik. Det er her, I nøje skriver op, hvilke persondata I opbevarer og bruger, og med hvilket specifikt formål I gør det.

I en fortegnelse kan der for eksempel stå, at I indsamler GPS-data på jeres servicevogne (og dermed chauffører) med det formål at drifte optimalt.

I kan med fordel stille jeres fortegnelse op som et skema eller en matrix for at skabe overblik og gøre det nemt at opdatere den.

2. Du må ikke glemme at slette data

Datatilsynet går meget op i, at I har helt klare regler for, hvornår forskellige personoplysninger skal slettes. Og I skal selvfølgelig overholde reglerne – eller politikkerne som det kaldes inden for GDPR.

En af de svære opgaver i den sammenhæng kan være at få alle medarbejdere, der har persondata mellem hænderne, til at huske sletteregler. Det er en god idé at gøre det til en rutine at minde om, at der skal ryddes op i diverse arkiver og mails. I kan for eksempel lægge det ind i som en fast opgave i den enkelte medarbejders kalender.

3. Du må ikke ignorere hændelsesloggen

En hændelseslog er GDPR's ord for synderegister. Og modsat hvad mange tror, synder selv den bedste. Der sker faktisk brud på datasikkerheden i stort set alle virksomheder – brud der kan være mere eller mindre alvorlige. Men hver gang en medarbejder kommer til at lave en fejl i sin omgang med persondata, skal vedkommende råbe op, og det skal skrives ned i hændelsesloggen. Hvad skete der og hvorfor; hvordan rettede I op på fejlen; og hvordan vil I forsøge at undgå, at det sker igen?

Husk hændelsesloggen!

Eksempler på hvornår hændelsesloggen skal ajourføres:

- En fil med persondata er sendt til forkert modtager
- Jeres system er blevet hacket
- En medarbejder glemmer sin taske med papirer i toget
- Skabet med personalemapper er blevet efterladt ulåst
- I har ikke fået slettet persondata, I ikke længere skal bruge
- I er gået til frokost uden at låse jeres computer

Populært sagt kan I blive tilgivet for meget, så længe I bekender jeres synder i hændelsesloggen - de store såvel som de helt små. Men I skal til enhver tid kunne fremvise loggen til Datatilsynet.

4. Du må ikke negligere medarbejdernes forståelse af GDPR

Kun når medarbejderne ved, hvad et brud på persondatasikkerheden er, kan de bekende deres GDPR-synder. Derfor skal I gøre en dyd ud af (løbende) at lære alle medarbejdere, der håndterer persondata, at forstå GDPR på et grundlæggende niveau. Så de bliver i stand til at genkende og opdage sikkerhedsbrud – hvad enten det er egne eller andres. Og de skal vide, hvor vigtigt det er, at de siger til, når det sker.

5. Du skal holde din oplysningspligt hellig

Datatilsynet støder jævnligt på virksomheder, der ikke overholder deres såkaldte oplysningspligt. Når du arbejder med løn og personale, handler din oplysningspligt om, at du altid skal informere dine medarbejdere (eller for eksempel jobansøgere) om, hvilke af deres persondata du bruger, til hvad – og hvorfor.

Og det skal være fuldstændig klart, på skrift og nemt at finde for den enkelte. Først da vil Datatilsynet give dig ret i, at du opfylder oplysningspligten, som GDPR foreskriver det.

Du skal egentlig tage ordet oplysning ret bogstaveligt: Du skal kaste lys over land (mand) og skabe klarhed.

6. Du må ikke skalte og valte med helbredsoplysninger

Alt hvad der handler om folks helbred, er følsomme personoplysninger. GDPR – og dermed Datatilsynet – ser med ekstra strenge øjne på det, hvis I ikke har en helt særlig, specifik og nødvendig grund til at indsamle og opbevare helbredsoplysninger på jeres medarbejdere eller for eksempel jobansøgere. På samme måde skal I være særligt opmærksomme på at slette oplysningerne igen, så snart de ikke er relevante længere.

Hvis en medarbejder for eksempel melder sig syg med influenza, må du kun fortælle andre, at vedkommende er syg, hvis det er strengt nødvendigt for dem at vide. Og du må under ingen omstændigheder fortælle eller notere, at det drejer sig om influenza.

Til gengæld må du gerne registrere, hvis du har en medarbejder, der er fraværende på grund af en graviditetsbetinget sygdom. For her kan I få sygedagpengerefusion. Du skal selvfølgelig huske at slette oplysningen igen, så snart du har fået refusionen. For nu er oplysningen ikke længere nødvendig og relevant at opbevare.

7. Du må ikke lægge bevisbyrden fra dig

Nej, du skal løfte den. Modsat andre juridiske sammenhænge skal I kunne bevise jeres uskyld. Helt konkret betyder det, at I skal have nedfældet politikker for, hvordan I rent faktisk overholder GDPR. Altså beskrivelser af hvordan I håndterer diverse persondata.

Det kan for eksempel være en beskrivelse af, hvordan I gør brug af krypterede mails, eller hvor ofte I sletter jeres CV-database eller personalemapperne på tidligere ansatte.

8. Du må ikke undervurdere mængden af persondata

Arbejder du i en virksomhed, der håndterer store mængder af persondata, holder Datatilsynet ekstra skarpt øje med jer. Det er ikke det samme som, at små fisk bare ryger gennem nettet. Men alt andet lige er det værre, når mange menneskers data risikerer at blive kompromitteret, end når det er færre.

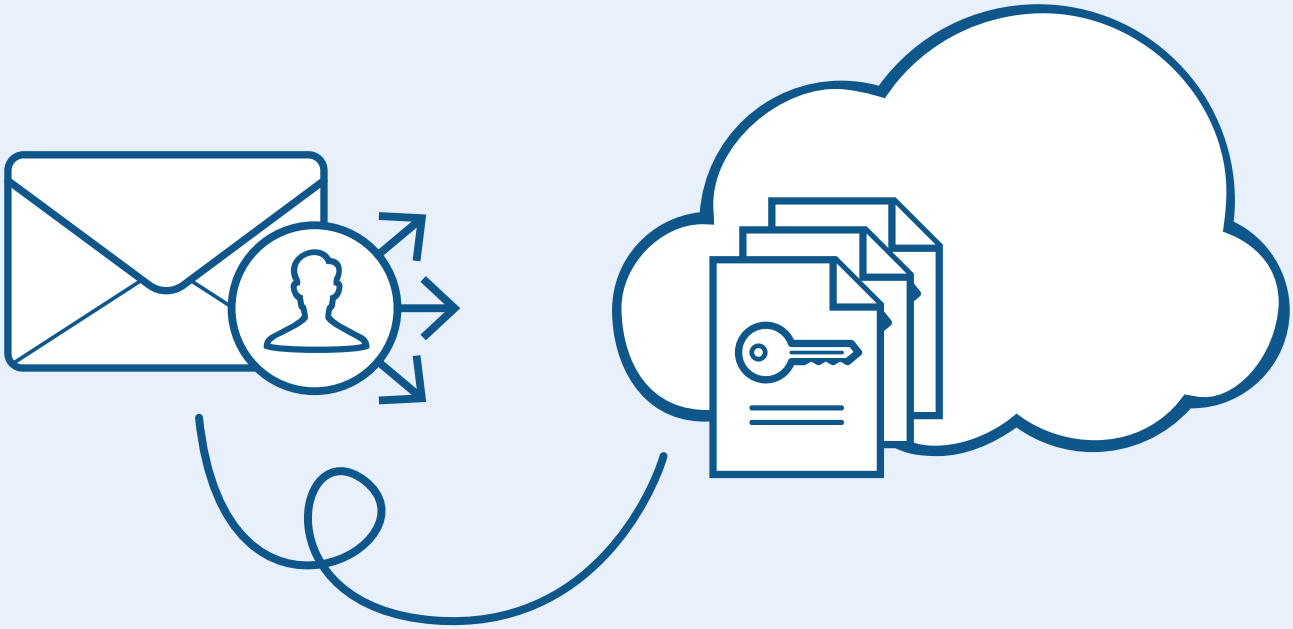
9. Du må ikke dele med hvem som helst

Størstedelen af de brud på GDPR, som Datatilsynet kender til, bunder i, at nogen kommer til at dele personoplysninger med andre, som det ikke er relevant for. Måske får en medarbejder valgt en forkert modtager af en mail, eller måske får du delt en personoplysning med en kollega, som slet ikke har nogen arbejdsmæssig grund til at kende oplysningen.

Det er kun menneskeligt at fejle. Men netop derfor har I jeres hændelseslog, som er så vigtig at bruge hver gang, der går noget galt. Det er en god start i forhold til Datatilsynet og eventuelle konsekvenser af de nærmest uundgåelige fejltrin.

10. Du må ikke følge andre databeskyttelsesforordninger end GDPR

Og så er det heldigt, at der kun findes den samme…



Vil du vide mere og have hjælp med virksomhedens GDPR-arbejde, kan du kontakte vores juridiske GDPR-specialister på 72 27 90 16.

Du kan finde aktuelle GDPR-webinarer på dataløn.dk/gdpr-webinar

VISMA | DataLøn