Datatilsynets fokusområder # 2

Martin Folke Vasehus

CEO og it-advokat, ComplyCloud

Husk at slå din mikrofon og kamera fra

Vi starter kl. 12

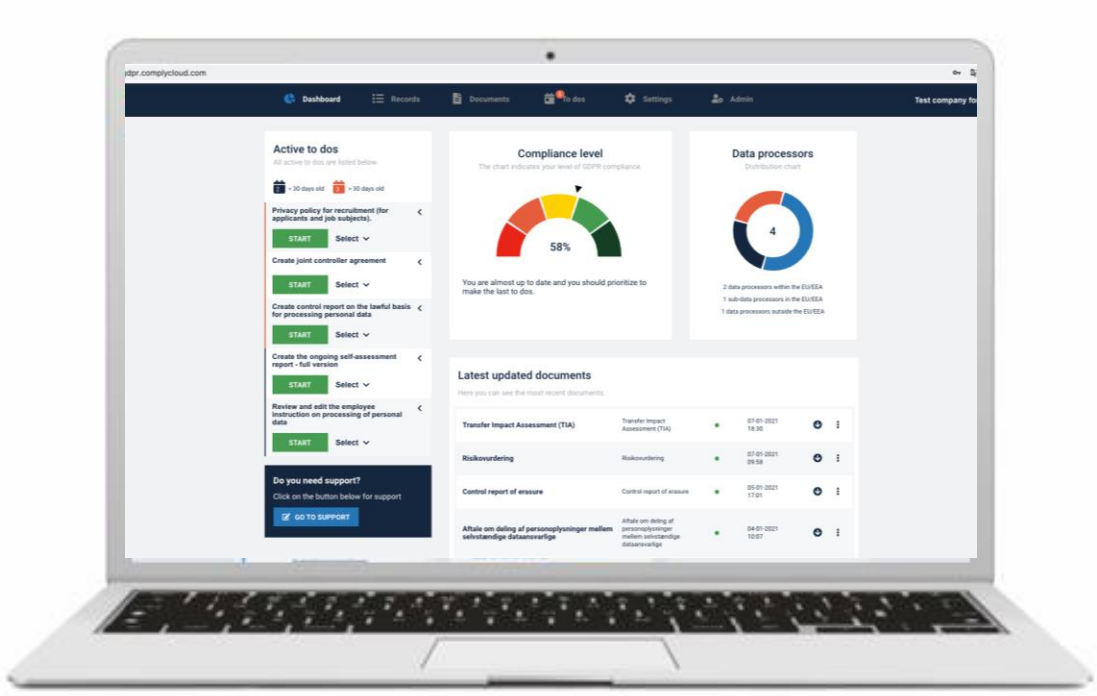
17. februar 2021

Martin Folke Vasehus
Certificeret IT-advokat og CEO
ComplyCloud & CIT

Praktik

- Webinaret bliver optaget.
- Alle kan løbende stille spørgsmål i chatten.
- Hold mikrofon og kamera slukket.
- Kopi af præsentation og video deles med dem, der har samtykket til at modtage direkte henvendelse fra os.
- Hjælp os med at blive bedre ved at udfylde spørgeskema efter webinaret.
- Sæt dig godt til rette med din frokost eller kaffe.

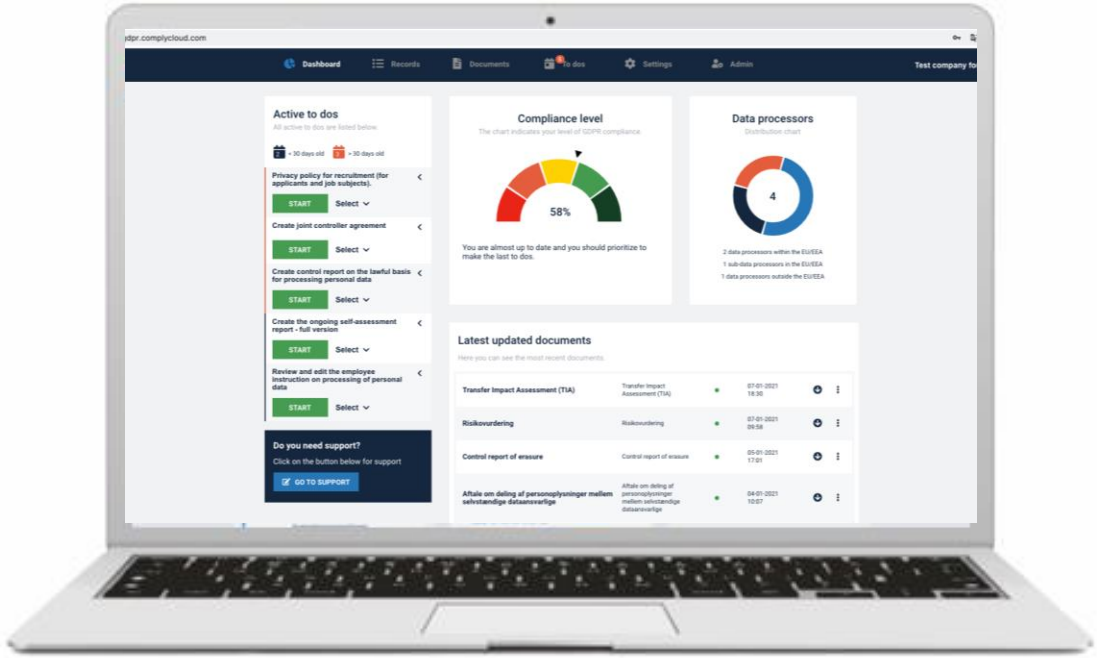
1. Intro
2. De sidste 7 fokusområder
3. Q&A



1 Intro

2 De sidste 7 fokusområder

3 Q&A



DATATILSYNET

DATATILSYNET

Datatilsynet udmelding:

"I 2021 lyder overskrifterne på de særlige fokusområder således:

1. *Kreditoplysningsbureauer, advarselsregistre og spærrelister*
2. *Inkassobureauers oplysningspligt og sletning*
3. *Pengeinstitutters procedure for indsigtsanmodninger*
4. *Tv-overvågning*
5. *Myndigheders videregivelse af personnumre til borgere*
6. *Forskning*
7. *Behandling af personoplysninger om hjemmesidebesøgende (cookies)*
8. *Persondatasikkerhed, inkl. brud på persondatasikkerheden*
9. *Kontrol med databehandlere*
10. *Overførsel af personoplysninger til tredjelande*
11. *Behandling af personoplysninger i fælleseuropæiske informationssystemer*
12. *PNR-loven*
13. *Retshåndhævelsesloven*

DATATILSYNET

Datatilsynet udmelding:

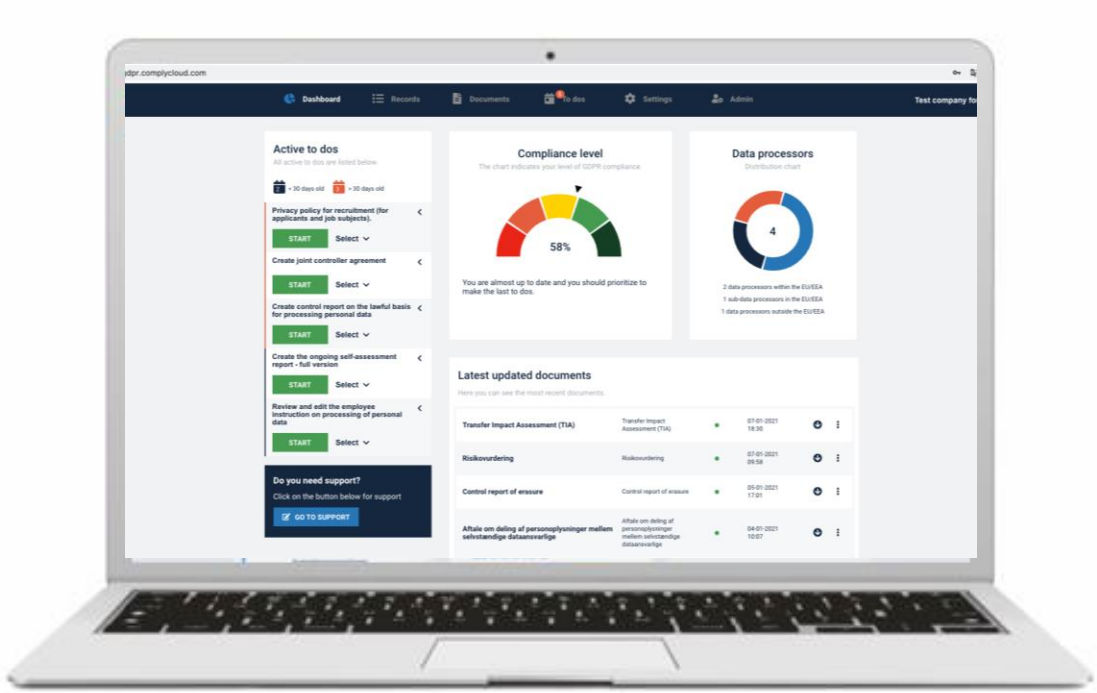
"I 2021 lyder overskrifterne på de særlige fokusområder således:

1. *Kreditoplysningsbureauer, advarselsregistre og spærrelister*
2. *Inkassobureauers oplysningspligt og sletning*
3. *Pengeinstitutters procedure for indsigtsanmodninger*
4. *Tv-overvågning*
5. *Myndigheders videregivelse af personnumre til borgere*
6. *Forskning*
7. *Behandling af personoplysninger om hjemmesidebesøgende (cookies)*
8. *Persondatasikkerhed, inkl. brud på persondatasikkerheden*
9. *Kontrol med databehandlere*
10. *Overførsel af personoplysninger til tredjelande*
11. *Behandling af personoplysninger i fælleseuropæiske informationssystemer*
12. *PNR-loven*
13. *Retshåndhævelsesloven*

1 Intro

2 De sidste 7 fokusområder

3 Q&A



7 Behandling af personoplysninger om hjemmesidebesøgende (cookies)

7 Behandling af personoplysninger om hjemmesidebesøgende (cookies)

Forpligtelserne

- For at overholde **oplysningspligten**, skal oplysningerne gives til den hjemmesidebesøgende i sammenhæng med de brugerhandlinger, den hjemmesidebesøgende foretager sig, jf. afgørelsen om Fynbus.

- Det relevante **behandlingsgrundlag** for behandling af personoplysninger om hjemmesidebesøgende vil ofte være samtykke.

- Samtykket skal blandt andet leve op til følgende krav:
  - Det skal være et aktivt tilvalg, når en besøgende på din hjemmeside giver lov til, at vedkommendes oplysninger behandles.
  - Det skal være klart, hvilke forskellige formål du gerne vil behandle oplysningerne til.
  - Det skal være let for den besøgende at give samtykke til nogle formål og ikke give samtykke til andre.
  - Det skal være nemt ikke at give samtykke - også rent visuelt.
  - Desuden skal du kunne dokumentere, hvad en besøgende har givet samtykke til - og hvordan samtykket er indhentet.

GOLF.dk

GOLF.dk

Sagens baggrund

- Sagen udsprang af en klage over DGU Erhverv A/S' (herefter "DGU") fra en hjemmesidebesøgende på www.golf.dk, som DGU anvendte til at indsamle og behandle personoplysninger. Formålet med behandlingen var bl.a. markedsføring, og behandlingen skete på baggrund af den hjemmesidebesøgendes samtykke.

- Samtykket blev indhentet ved hjælp af en samtykkeløsning, hvorved den hjemmesidebesøgende indledningsvis fik præsenteret information om behandlingsaktiviteterne på www.golf.dk, hvorefter den hjemmesidebesøgende kunne trykke "Tillad alle cookies". Det var ikke muligt for den hjemmesidebesøgende at undlade at give samtykke til behandlingsaktiviteterne. Det fremgik endvidere, at den hjemmesidebesøgendes fortsatte brug af www.golf.dk også ville blive anset som et samtykke.

- DGU ændrede senere sin samtykkeløsning til en løsning, som Datatilsynet også tog delvist stilling til.

GOLF.dk

Sagens baggrund

- Den nye løsning tilbød den hjemmesidebesøgende at vælge mellem ”Kun nødvendige” og ”Jeg accepterer”, og indeholder følgende information til den hjemmesidebesøgende:
    - ”*Efterfølgende behandling sker på grundlag af dit samtykke og i særlige tilfælde på grundlag af legitim interesse*.”
- Ved at klikke på ”cookie indstillinger” i den nye samtykkeløsning blev den hjemmesidebesøgende præsenteret for muligheden for at gøre indsigelse mod hjemmesidens legitime interesser i forhold til statistik og markedsføring.
- Datatilsynet opfordrede DGU til at genoverveje denne nye løsning.

Datatilsynets afgørelse

✕ Datatilsynet udtalte **alvorlig kritik** af, at DGU’s behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 6, stk. 1, litra a (samtykke som behandlingsgrundlag).

GOLF.dk

Vores bemærkninger

- Kravet om granularitet forudsætter, at den registrerede ved flere behandlingsformål frit kan vælge mellem disse.
- Kravet om en utvetydig viljestilkendegivelse forudsætter en aktiv handling, og at bl.a. tavshed eller inaktivitet ikke kan udgøre et gyldigt samtykke.
- Der bør ikke i forbindelse med indhentelse af den hjemmesidebesøgendes samtykke gives information om, at personoplysningerne vil blive behandlet på baggrund af samtykke eller legitime interesser. Dette er efter Datatilsynets opfattelse ikke gennemsigtigt og letforståeligt for den hjemmesidebesøgende.
- Ej heller bør den hjemmesidebesøgende blive præsenteret for muligheden for at gøre indsigelse mod den dataansvarliges behandling på baggrund af legitime interesser i forbindelse med en samtykkeløsning, da det skaber forvirring om behandlingsgrundlaget.

8 Persondatasikkerhed, inkl. brud på persondatasikkerheden

8 Persondatasikkerhed, inkl. brud på persondatasikkerheden

Forpligtelserne

- Man er både som dataansvarlig og databehandler forpligtet til at etablere et passende sikkerhedsniveau under hensyntagen til de implicerede risici, når man behandler personoplysninger.
- Opstår der et brud, er man først og fremmest forpligtet til at anmelde dette til Datatilsynet inden for en bestemt tidsfrist (72 timer). Som databehandler skal man sørge for at underrette den dataansvarlige. I visse tilfælde skal man ligeledes underrette de registrerede.
- Risikovurderingen er et centralt element i arbejdet med datasikkerhed.
- Artikel 32 indebærer, at du skal tilvejebringe et tilstrækkeligt sikkerhedsniveau ud fra en samlet risikovurdering. Dit sikkerhedsniveau skal altså modsvare implicerede risici.
- Risikovurderingen består ifølge Datatilsynet af to dele:
  1. Kortlægning af risici og kategorisering heraf.
  2. Vurdering af passende tekniske og organisatoriske foranstaltninger.

8 Persondatasikkerhed, inkl. brud på persondatasikkerheden

- Datatilsynet modtog i 2020 knap 9.000 anmeldelser om brud på persondatasikkerheden. Datatilsynet har på baggrund af anmeldelserne identificeret fire områder, som er forbundet med stor risiko for manglende efterlevelse af databeskyttelsesreglerne.

  1. Adgangs- og rettighedsstyring.

  2. Anvendelse af personoplysninger i forbindelse med it-udvikling og test.

  3. Håndtering af personoplysninger, som "tages ud af" dertil indrettede it-systemer, f.eks. på bærbare elektroniske medier eller på papir mv. (uddatamateriale).

  4. Om brud på persondatasikkerheden håndteres og anmeldes i overensstemmelse med reglerne herom.


ZOO
KØBENHAVN

Sagens baggrund

- Zoologiske Have i København (ZOO) havde anmeldt et brud på persondatasikkerheden hos Datatilsynet, efter en softwareingeniør via et selvudviklet script havde tilegnet sig adgang til årskortsholderes konti og personoplysninger hos ZOO. Softwareingeniøren havde ikke misbrugt oplysningerne men alene gjort ZOO opmærksom på, hvor let det var at få adgang til brugeroplysningerne.

- Dette gav Datatilsynet lejlighed til at udtale sig om ZOO's tekniske foranstaltninger for adgang til den registreredes personoplysninger og ZOO's håndtering af bruddet herunder den information, som blev givet til den registrerede i forbindelse hermed.

- Sikkerhedsniveauet var ikke højt nok, fordi adgang til loginsiden alene var beskyttet med en 4-cifret kode, og fordi brugerkontiene ikke var beskyttet ved andre foranstaltninger såsom en "spær konto ved tre fejlslagende forsøg"-funktion.

- I forløbet havde ZOO ikke oplyst alle de berørte registrerede og havde heller ikke oplyst disse retvisende.

Datatilsynets afgørelse

- Datatilsynet udtalte **alvorlig kritik** af, at ZOO´s behandling af personoplysninger ikke havde efterlevet databeskyttelsesforordningens artikel 32, stk. 1 og 2 (Behandlingssikkerhed), artikel 33, stk. 3, litra d (Anmeldelse af brud på persondatasikkerhed), artikel 34, stk. 1 og 2 (Underretning om brud til den registrerede), og artikel 5, stk. 1, litra a (Lovlighed, rimelighed og gennemsigtighed).

- Datatilsynet meddelte Zoo **påbud** om at underrette alle registrerede, hvor der foreligger en høj risiko for disses rettigheder. Påbuddet blev givet i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra e.

- Datatilsynet meddelte Zoo **påbud** om at bringe behandlingen af personoplysninger i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a, ved at berigtige den tidligere givne information således at den afspejlede de vurderinger af risikoen som Datatilsynet har redegjort for i afgørelsen, dette skulle gøres i forhold til alle berørte registrerede. Påbuddet blev givet i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Vores bemærkninger

- Når der registreres et databrud, skal det vurderes, om der med en vis sandsynlighed sket misbrug af personoplysninger.

- Når en Dataansvarlig skal undersøge, om der foreligger en misbrugssituation, kan en konstatering af, at brugeradfærden er normal, ikke tages til indtægt for, at der ikke foreligger en misbrugssituation.

- Adgang til en brugerflade, hvor der er personoplysninger, skal beskyttes mod uautoriseret adgang. Dette kan gøres ved:
  - At adgangskoden skal være af en vis længde og kombinationer som besværliggør uretmæssig adgang.
  - At der skal være foranstaltninger som modvirker, at computerprogrammer får adgang til loginsider. Disse foranstaltninger kan konkret være funktionen "jeg er ikke en robot", eller funktionen som spærrer login ved tre fejlslagende forsøg.
  - At man som dataansvarlig, har en procedure for regelmæssig afprøvning og evaluering af den tekniske sikkerhed.

- Er du i tvivl om, hvordan de tekniske foranstaltninger vedrørende adgangskoder skal udformes, er Center for Cybersikkerheds passwordvejledning en god rettesnor.

Vores bemærkninger (fortsat)

- Underretning i forbindelse med brud skal ske til alle registrerede, der er berørt. Denne underretning skal indeholde information om, hvilke følger bruddet kan have i værst tænkelige tilfælde, og hvilke typer oplysninger der kan have være eksponeret for den uvedkommende adgang.

- Uautoriseret adgang til e-mailadresser samt kortnumre på folks brugerprofil udgør en risiko for den registrerede, da oplysningerne kan bruges til at snyde den registrerede, eftersom vedkommende vil antage, at det kun er den dataansvarlige, der har adgang til disse informationer. På den baggrund vil en hacker kunne udgive sig for at være den dataansvarlige over for den registrerede.

- Hemmelige adresser er en personoplysning, der skal udvises en høj grad af fortrolighed over for. Derfor er det vigtigt at overveje, om sådanne oplysninger er omfattet af eventuelle brud.

Randers Kommune

Sagens baggrund

- En person havde klaget over, at Randers Kommune den 15. november 2019 ved en fejl sendte en påtænkt opsigelse af borgeren indeholdende oplysninger om navn og adresse, fagforeningsmæssigt tilhørsforhold og helbredsoplysninger til en anden af kommunens medarbejdere.

- Medarbejderen, som fejlagtigt modtog oplysningerne om klager, var klagers kollega på daværende tidspunkt, og vedkommende sad ikke i en særligt betroet stilling og var ikke vant til at håndtere personoplysninger om kommunens ansatte.

Datatilsynets afgørelse

✕ Datatilsynet udtalte **kritik** af, at Randers Kommunes behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1 (sikkerhed), artikel 33, stk. 1 (anmeldelse af brud til Datatilsynet) og artikel 34 (underretning om brud til den registrerede).

Randers Kommune

Vores bemærkninger

- Afgørelsen står i kontrast til et eksempel i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden, hvor en HR-medarbejder ved en fejl sender lønsedler og ansættelseskontrakt til en forkert medarbejder i virksomheden, og hvor det aftales, at den pågældende medarbejder sletter de modtagne dokumenter med det samme efter at være blevet opmærksom på fejlen. Det fremgår i vejledningen, at der i et sådant tilfælde ikke nødvendigvis skal ske anmeldelse af bruddet til Datatilsynet, og at virksomheden kan vurdere, at bruddet ikke indebærer en risiko for den registrerede henset til, at der er tale om et "internt" brud, og at virksomheden har stor tillid til den pågældende medarbejder.

- Selvom der i denne afgørelse også var tale om et internt brud, skulle det alligevel anmeldes til Datatilsynet, selvom der er tale om et internt brud. Det skyldes, at Datatilsynet lagde vægt på (i) dokumentets fortrolige personalemæssige karakter, (ii) at dokumentet indeholdt oplysninger om klagers helbred og fagforeningsmæssige tilhørsforhold, og (iii) at der derfor havde været en særlig risiko for tab af omdømme og fortrolighed for klager i forbindelse med, at opsigelsen blev sendt til en anden medarbejder på arbejdspladsen.

9 Kontrol med databehandlere

9 Kontrol med databehandlere

Forpligtelsen

- Som dataansvarlig er du forpligtet til at føre kontrol med dine databehandlere og sikre, at de generelt efterlever databeskyttelsesforordningens regler og konkret behandler personoplysningerne på dine vegne i overensstemmelse med den instruks, du har givet.

- Forpligtelsen udspringer af samme bestemmelse, som opstiller kravet om, at der indgås en databehandleraftale mellem dig som dataansvarlig og dine databehandlere. Det er i sagens natur nødvendigt regelmæssigt at kontrollere, at behandlingen lever op til de aftalte krav.

VIBORG
KOMMUNE

VIBORG KOMMUNE

Sagens baggrund

- Viborg Kommune var blandt de myndigheder, som Datatilsynet i 2018 havde udvalgt til tilsyn. Tilsynene fokuserede navnlig på kommunernes efterlevelse af de krav, som knytter sig til anvendelse af databehandlere.

Datatilsynets afgørelse

✕ Datatilsynet fandt samlet set grundlag for at udtale **alvorlig kritik** af, at Viborg Kommune ikke havde efterlevet databeskyttelsesforordningens krav i forbindelse med brugen af databehandlere, jf. databeskyttelsesforordningens artikel 28, stk. 3, og artikel 5, stk. 2, jf. artikel 5, stk.1, fordi; (i) kommunen ikke havde indgået databehandleraftaler med alle databehandlere; (ii) de databehandleraftaler der var genstand for stikprøvekontrol ikke overholdt de indholdsmæssige krav hertil; og (iii) kommunen ikke havde ført tilsyn med sine databehandlere og underdatabehandlere.

✕ Datatilsynet fandt grundlag for at meddele Viborg Kommune **påbud** om at indgå databehandleraftaler, som lever op til kravene i forordningens artikel 28, stk. 3, med fem databehandlere. Datatilsynet anmodede kommunen om en redegørelse for de databeskyttelsesretlige overvejelser, som kommunen havde gjort sig på baggrund af tilsynsbesøget, samt en konkret og detaljeret plan for, hvordan kommunen fremadrettet vil føre det nødvendige tilsyn med kommunens databehandlere og underdatabehandlere.

VIBORG KOMMUNE

Bemærkninger

- Ved valget af sanktion fandt Datatilsynet det tilsyneladende formildende, at de fem databehandleraftaler, som Viborg Kommune – på tidspunktet for tilsynsbesøget – ikke havde nået at indgå, alene udgjorde en lille del af kommunens samlede antal på omkring 130 databehandleraftaler. Dette princip bør formentlig kunne anvendes på lige fod af andre aktører med mange databehandlere og underdatabehandlere.

- Afgørelsen indeholder nogle citater fra en databehandleraftale med "Databehandler 3", som tilsyneladende er Microsoft, idet de anførte citater er enslydende med indholdet i de på det tidspunkt gældende standardvilkår fra Microsoft. Datatilsynet anfører i den forbindelse, at den dokumenterede instruks i standardvilkårene er for uklar og ikke overholder databeskyttelsesforordningens artikel 28, stk. 3.

10 Overførsel af personoplysninger til tredjelande

10 Overførsel af personoplysninger til tredjelande

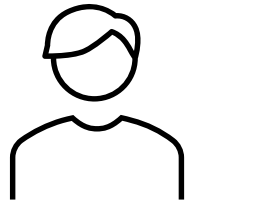
Forpligtelsen

- Ud over generelt at skulle følge forordningens regler, stiller kapitel 5 særlige krav til tredjelandsoverførsler, navnlig at de kun må finde sted med en særlig hjemmel.
- Denne hjemmel kan bl.a. være:
  - En afgørelse fra Kommissionen om, at et land sikrer samme databeskyttelse som i EU (adequacy decision)
  - Behandlingen er omfattet af fornødne garantier (standardkontraktbestemmelser, bindende virksomhedsregler samt godkendte adfærdskodekser og certificeringsmekanismer)
  - Undtagelsessituationer, hvor den registrerede har givet sit udtrykkelige samtykke til overførslen, m.fl.
- Schrems II-afgørelsen gør det klart, at den dataansvarlige skal sikre et beskyttelsesniveau i tredjelandet, der essentielt svarer til det i EU/EØS. Ud over at sikre et overførselsgrundlag kan dette også indebære at iværksætte supplerende foranstaltninger, hvilket navnlig er et krav ift. USA.

One to rule them all…

facebook

An Coimisiún um Chosaint Sonraí
Data Protection Commission



Max Schrems


Herning
Kommune


servicenow

Sagens baggrund

- Herning Kommune brugte en dansk leverandør og databehandler til at drifte og vedligeholde et økonomisystem ejet af 10 kommuner og to regioner. Den danske leverandør brugte en underleverandør, der leverede Service Desk til økonomisystemet.

- Herning Kommune anmeldte et brud på persondatasikkerheden, fordi den anvendte underleverandør af Service Desk ikke var en godkendt leverandør. Leverandøren, som databehandleren overførte personoplysninger til, behandlede oplysningerne i ikke sikre tredjelande.

Datatilsynets afgørelse

✕ Datatilsynet udtalte **alvorlig kritik** af den danske leverandør (EG A/S), fordi ServiceNow – som leverede Service Desk Systemet – ikke var godkendt som underdatabehandler i aftalen med Herning Kommune (eller med de øvrige parter), og dette var den danske leverandørs ansvar, da de ikke havde oplyst om brug af denne.

✕ Datatilsynet udtalte derudover **alvorlig kritik** af, at ServiceNow som led i leverancen af Service Desk Systsmet overfører personoplysninger, herunder personnumre, til tredjelande uden for instruks.

Citater

- ”*For at sikre, at personoplysningerne ikke overføres til ServiceNows kontorer uden for EU, har EG deaktiveret en såkaldt ”follow the sun”-supportfunktion. ServiceNow oplyste i den forbindelse EG om, at når denne supportfunktion var deaktiveret, ville personoplysninger ikke blive behandlet af ServiceNows kontorer i tredjelande*.”

- ”*Den 12. august 2019 oplyser ServiceNow til EG, at ServiceNow, til trods for deaktiveringen af ”follow the sun”-supportfunktionen, ikke kan garantere, at personoplysninger ikke behandles i tredjelande, da ServiceNows medarbejdere i f.eks. Indien kan være ansvarlige for at implementere globale sikkerhedsopdateringer til Service Desk Systemet.*”

Bemærkninger

- Ifølge sagens involverede parter var den potentielle adgang fra ServiceNow's tredjelande kun en adgang til applikationslaget og ikke til datalaget.
- Derudover var ServiceNow skrevet ind i den kommercielle kontrakt mellem parterne, men havde blot glemt at få dem skrevet ind i databehandleraftalen, som var bilag.
- Datatilsynet lægger uden videre til grund, at dette indebærer en overførsel af personoplysninger til tredjelande.
- Hvis den manglende garanti eller blot et forbehold for adgang til applikationslaget i tredjelande ifølge Datatilsynet betyder de facto tredjelandsoverførsel, har alle kunder til Microsoft, AWS, Oracle, SalesForce osv. formentlig et problem med tredjelandsoverførsel.

11 Behandling af personoplysninger i fælleseuropæiske informationssystemer

11 Behandling af personoplysninger i fælleseuropæiske informationssystemer

Hvem rammer det?

- Området fokuserer på de myndigheder, der har adgang til de fælleseuropæiske informationssystemer, som bl.a. er:
- Schengen-informationssystemet (SIS),
- Visuminformationssystemet (VIS),
- EU-fingeraftryksregisteret (Eurodac),
- Toldinformationssystemet (CIS) og
- Informationssystemet for det indre marked (IMI).

- De dataansvarlige myndigheder er forpligtede til at give indsigt i oplysningerne i systemerne/registrene til de registrerede, ligesom at myndighederne i nogle tilfælde skal give de registrerede besked om, at personoplysninger om dem behandles.
-
- De dataansvarlige med adgang til systemerne/registrene skal desuden leve op til visse sikkerhedskrav for at få og beholde adgangen.

ComplyCloud

12 PNR-loven

12

PNR-loven

Hvem rammer det?

- Loven giver hjemmel til oprettelsen af en afdeling i Rigspolitiet, som arbejder med Passagerlisteoplysninger. Området henvender sig derfor primært til denne PNR-enhed, men i øvrigt også de retshåndhævende myndigheder, der modtager passagerlisteoplysninger.
-
- Datatilsynet er udpeget til at føre tilsyn med PNR-enheden.

- Loven opstiller nogle særlige krav til behandlingssikkerheden hos de myndigheder, der modtager og behandler passagerlisteoplysningerne.
-
- Desuden følger det af loven, at listerne kun må opbevares i 5 år, at der skal ske maskering af oplysninger efter 6 måneder og at visse krav skal opfyldes, før der må ske afmaskering igen.

13 Retshåndhævelsesloven

13 Retshåndhævelsesloven

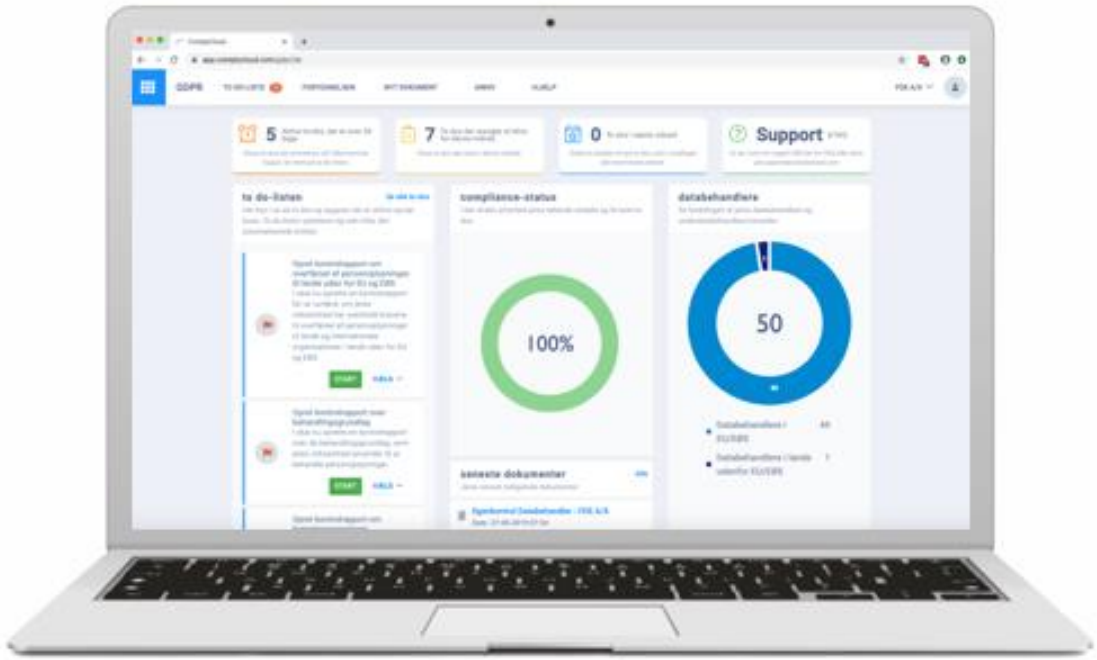
Hvem rammer det?

- Området henvender sig til retshåndhævende myndigheder, der behandler personoplysninger på det strafferetlige område. Det drejer sig om politiet, anklagemyndigheden, kriminalforsorgen, Den Uafhængige Politiklagemyndighed og domstolene.

Forpligtelserne

- Der er i høj grad sammenfald mellem reglerne i retshåndhævelsesloven og databeskyttelsesforordningen.
- De væsentlige forskelle, der består, er de registreredes rettigheder ift. at blive oplyst om, at der sker behandling af personoplysninger, og at opnå indsigt i behandlingerne. Efter retshåndhævelsesloven kan myndighederne nemlig undlade at informere om en behandling og afvise at give indsigt til en registreret, hvis den registreredes interesse i at få indsigt i oplysningerne findes at burde vige for hensynet til private eller offentlige interesser, f.eks. af hensyn til en konkret igangværende efterforskning eller politiets arbejdsmetoder mv.
- På den måde kan myndighederne udføre deres retshåndhævende arbejde og for eksempel føre en efterforskning uden at skulle informere de mistænkte om det – det er ikke helt dumt.

Afslutning og Q&A



Mens I overvejer spørgsmål:

- I modtager en video af en bruger, der udfylder en TIA i ComplyCloud.
- Der er whitepaper klar om blandt andet de nye SCC.
- Der er nye whitepapers på vej om:

(i) Datatilsynets 13 fokusområder (udvidet) og
(ii) pædagogisk redegørelse for FISA 702 og EO 12.333.

- Tjek også vores mange nye webinarer.
- Skriv dig op til nyheder på https://complycloud.com/nyheder

Afslutning og sidste spørgsmål

Få flere faglige nyheder, Casebooks mv. her: https://complycloud.com/nyheder

Martin Folke Vasehus
E: martinvasehus@citlaw.dk
M: 52307597