Forebyggelse & risikovurderinger

v. databeskyttelsesrådgiver og GDPR-jurist
Lill-Jana Vandmose Larsen

GapSolutions
WE FIX IT

CHROMEBOOKSAG

MED ALLAN FRANK 16.08.22

HVAD GIK DER GALT I HELSINGØR KOMMUNENS ARBEJDE MED RISIKOVURDERINGER?

GRAPHIC RECORDING JULIA SOMMER

DEN DATAANSVARLIGE ER NØDT TIL AT FORHOLDE SIG TIL HELE BEHANDLINGSAKTIVITETEN I SIN RISIKOVURDERING!

ART. 5, STK. 2.

ART. 5, STK. 1, LITRA D.

ART. 24, STK. 1

ART. 28, STK. 1.

ART. 35, STK. 1.

DET SOM GIK GALT FOR KOMMUNEN ER, AT DEN UDELUKKENDE HAR RISIKOVURDERET PÅ DELE AF DEN BEHANDLING, SOM FOREGÅR I APPS, MEN HAR IKKE FORHOLDT SIG TIL METADATA I APPS, BROWSER, O.S. OG SELVE CHROMEBOOK DEVICE.

1.1 APPS BRUGERDATA

KOMMUNEN HAR RISIKOVURDERET PÅ BEHANDLINGSAKTIVITETER VED BRUG AF APPS OG FANDT FREM TIL AT RISICI ER LAVE.

DATATILSYNET HAR KONSTATERET AT RISICI ER HØJE OG AT BEHANDLINGEN IKKE LEVER OP TIL KRAVENE I GDPR I PÅ FLERE PUNKTER.

PERSONOPLYSNINGER OVERFØRES TIL USA ER TILGÆNGELIGE FOR GOOGLE LLC I KLARTEKST, FORDI GOOGLE HAR NØGLEN TIL AT DEKRYPTERE PERSONOPLYSNINGER

KOMMUNEN KAN IKKE VÆLGE FRA AT SUPPORT KAN SKE FRA 3.-LANDE, NÅR GOOGLE ER DATABEHANDLER.

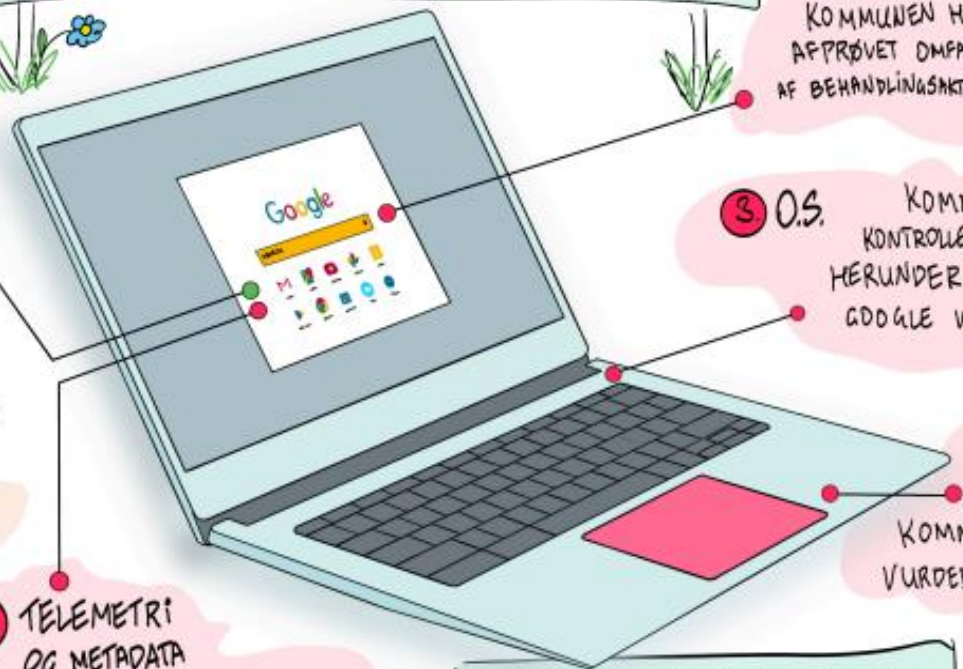
DER SKER BEHANDLING AF SÆRLIGE KATEGORIER AF PERSONOPLYSNINGER (ART. 9.)

2. BROWSER

KOMMUNEN HAR IKKE TILSTRÆKKELIGT AFPRØVET OMFANG OG VIRKEMÅDE AF BEHANDLINGSAKTIVITETER I BROWSER.

3. O.S.

KOMMUNEN KUNNE IKKE DOKUMENTERE, HVORDAN DEN KONTROLLERER GOOGLE'S ADGANG TIL PERSONOPLYSNINGER, HERUNDER SÆRLIGT PÅ OS-NIVEAU OG I INTERAKTION MELLEM GOOGLE WORKSPACES OG GOOGLE BACKEND.



4. FYSISK CHROMEBOOK DEVICE

KOMMUNEN HAR IKKE TILSTRÆKKELIGT VURDERET RISICI PÅ HARDWARE-NIVEAUET.

DER KAN OVERFØRES OPLYSNINGER TIL 3.-LANDE VED YDELSE AF SUPPORT UDEN FORNØDNE SIKKERHEDSNIVEAU.

1.2 TELEMETRI OG METADATA

KOMMUNEN HAR IKKE TAGET STILLING TIL, AT GOOGLE HAR PÅTAGET DATAANSVAR OVER BEHANDLING AF TELEMETRI OG METADATA I APPS, OG AGERER DERFOR IKKE EFTER INSTRUKS FRA KOMMUNEN.

KOMMUNENS TILLID TIL, AT LEVERANDØR GENERELT OVERHOLDER AFTALEN, IKKE UDGØR EN FORNØDEN NEDBRINGELSE AF RISICI.

FORHOLD I PUNKT 1.2, 2, 3 OG 4 KAN IFØLGE GOOGLE FØRST FIXES I 2024 VED AT ÆNDRE KONTRAKTFORHOLD MELLEM GOOGLE OG KOMMUNEN.

Fælles forståelse

Vi er alle lidt på gyngende grund her!

Løsning:

- At forholde sig ansvarligt og gerne at ville databeskyttelsen!
- Start, hvor det giver bedst mening!
- Spis elefanten i små bidder!

Grundig forberedelse
=
Risikovurdering

- Al GDPR bygger på en risikobaseret tilgangsvinkel til behandling af oplysninger, jf. GDPR art. 24.
- **Centrum for risikovurderinger er den enkelte registrerede og deres rettigheder**
- Risikovurderinger = sikkerhedsforanstaltninger
- Afhænger af den enkelte virksomhed/organisation (One Size doesn't Fit All, derfor Chromebooksagen)

Hvad siger lovgivningen?

*”Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige **passende tekniske og organisatoriske foranstaltninger** for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.”*

Hvad betyder det?

- Kortlæg data **hele vejen rundt** ”fra vugge til grav”.
- Udvis **ansvarlighed** og vær i stand til at kunne **dokumentere** det.
- Vedligehold og **ajourfør**.
- Husk, I er også ansvarlige for jeres **databehandleres** håndtering
- Vær **ærlig** i jeres vurdering.
- Hvis risikoen er høj, skal der tillige laves en **DPIA**.
- Risikovurderinger skal laves**, *inden*** man påbegynder behandlingen”

1) Hvad skal der risikovurderes på?
(trusler & beskrivelse)

Tab af

- Tilgængelighed
- Fortrolighed
- Integritet

IT-systemer = Ondsindede mennesker

- Hacking
- Medarbejdermisbrug
- Tyveri mv.

Menneskelige fejl = Alle arbejdsprocesser

- Sendes til forkert modtager
- Oplysninger slettes ikke
- Oplysninger slettes ved en fejl
- Adgangsstyring til oplysningerne
- Forkert opbevaring
- Manglende sletning
- Lukning af adgang til systemer
- Fysisk opbevaring

Generelle risici, eks.

- Fjernarbejdspladser
- Tyveri af IT-udstyr
- Organisatoriske foranstaltninger
- Fysiske skader

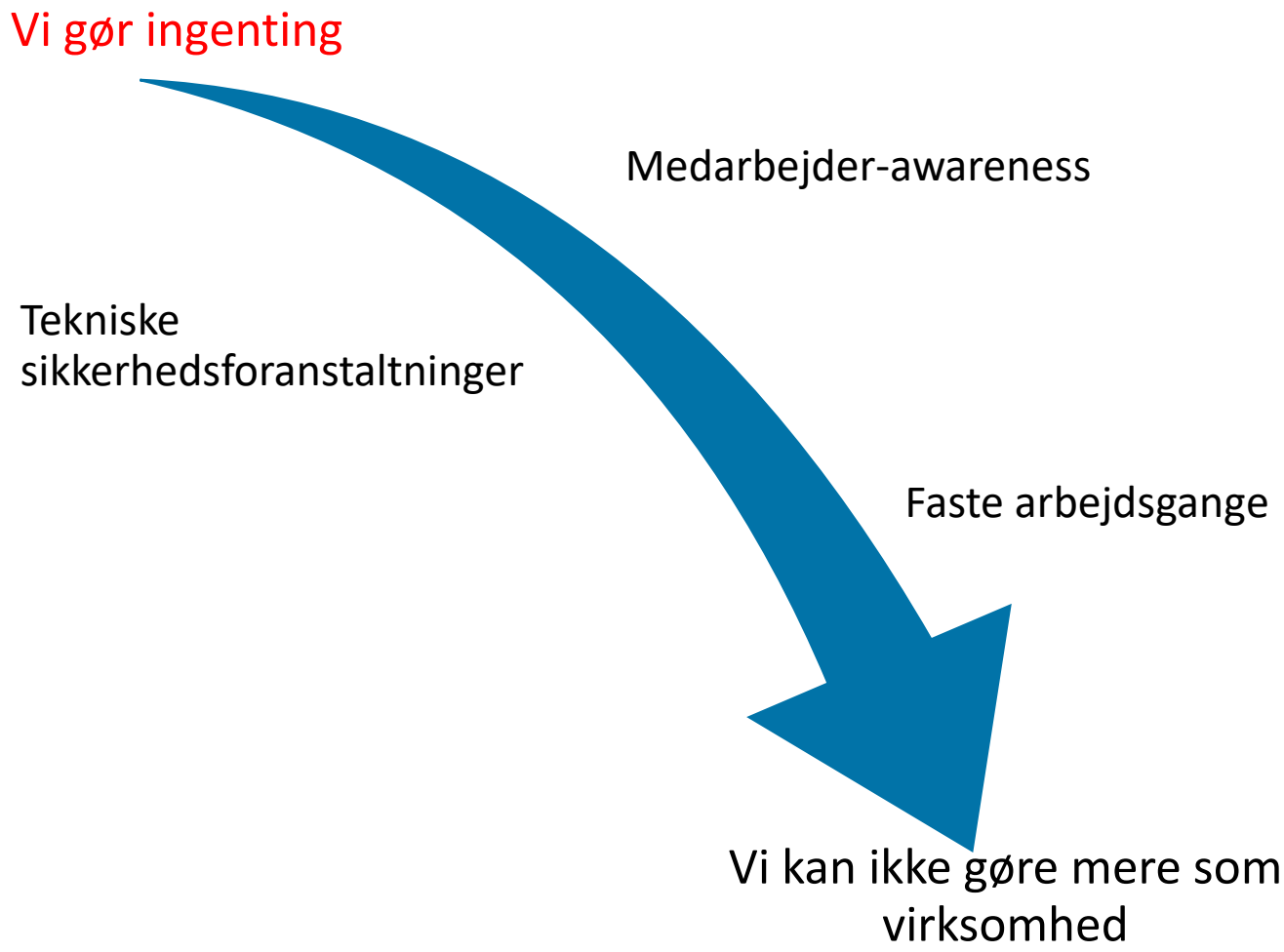
2) Konsekvensen

- Hvad er konsekvensen (potentielt) for **den enkelte registrerede**, hvis en eller flere af de beskrevne risici bliver en realitet?
- Hvilke **typer** af oplysninger behandles i processen eller systemet?
- Hvor **mange oplysninger** behandles om den registrerede?
- **Individuelle** forhold

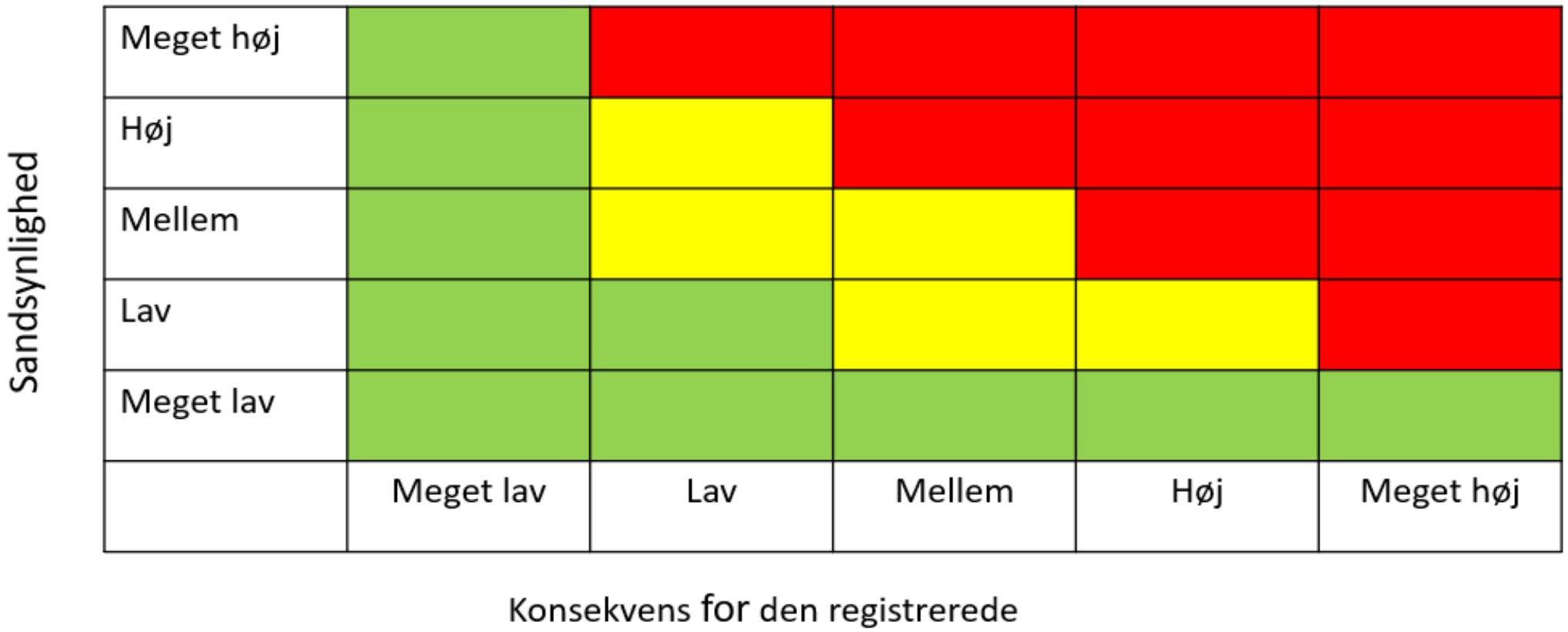
Vejledende vurderingstilgang:

Få almindelige oplysninger:	meget lav
Flere almindelige oplysninger:	lav
Særlige og fortrolige oplysninger:	middel
Følsomme oplysninger:	høj
Følsomme oplysninger + fare:	meget høj

3) Sandsynligheden



Beskrivelse+konsekvens-sandsynlighed = **det samlede risikobillede**



Helt styr på det?

- Eller brug for hjælp?

GDPR-portalen

GapSolutions A/S
Uraniavej 6
8700 Horsens
www.gapsolutions.dk

Work smarter, not harder!

Risikokategorisering!!!

- Muligheden for at samle arbejdsprocesser, it-systemer samt datamodtagere, og lave én risikovurdering
- Sørg for, at dit GDPR-system understøtter arbejdet med risikovurderinger generelt, men særligt ift. kategorisering

Forudsætter:

- Samme kategori af registrerede
- Samme type oplysninger
- Samme type sikkerhedsforanstaltninger

Hvad skal du gøre?

Begrund dine vurderinger!

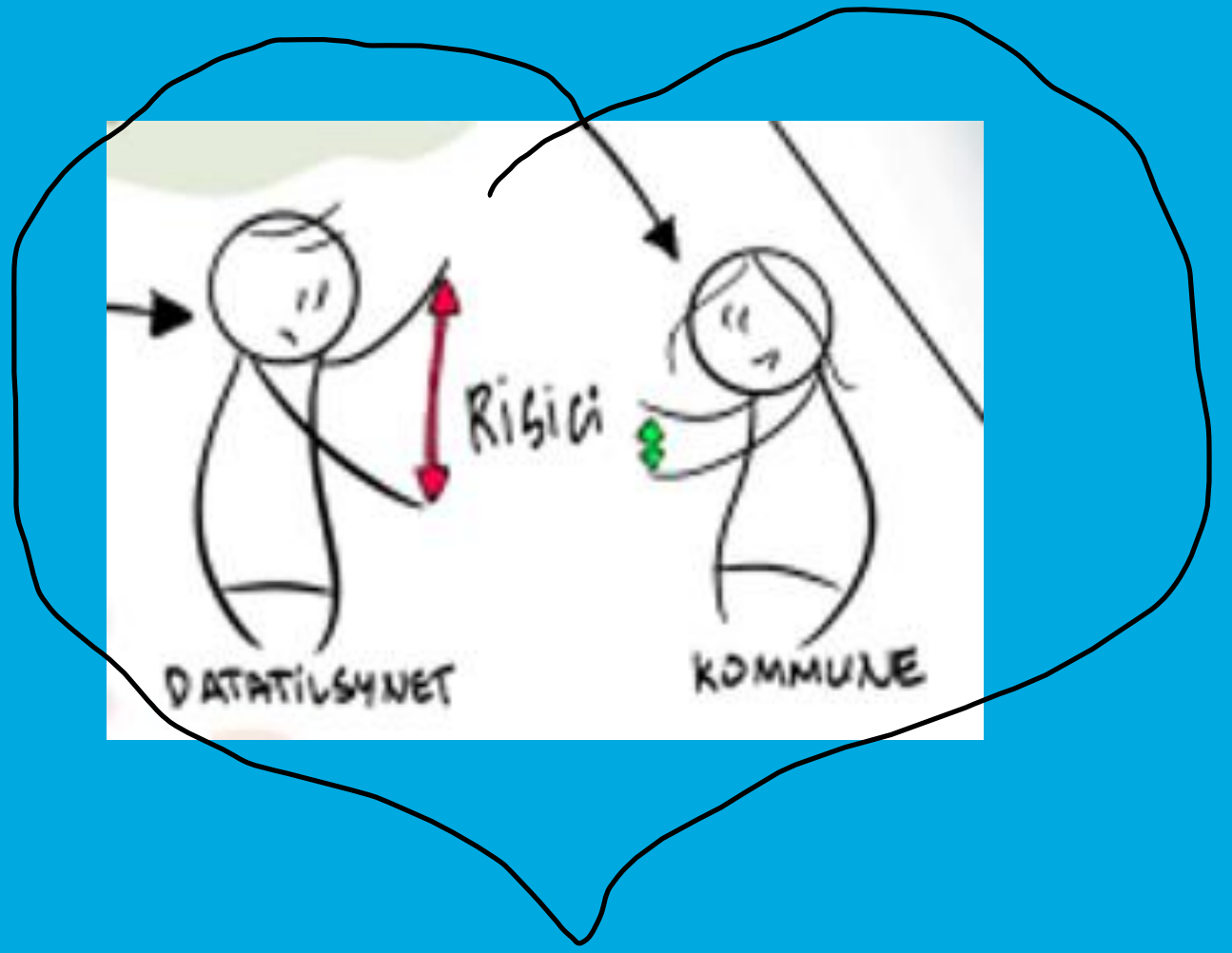
- Lav individuelle begrundelser
- Vær ærlig!
- Udvikling og forbedring er ikke en dårlig ting, men viser ansvarlighed

Resultat

- Munder risikovurderingen ud i gul, skal risikoen som minimum accepteres på ledelsesniveau
- Munder risikovurderingen ud i rød, er det uacceptabelt og bør forbedres

Dagens gode råd

Hvis Datatilsynet først siger,
at en behandling indebærer
en høj risiko,
så er det tid til at lytte!



Så hvordan forebygger man Chromebook-sagen og tilsvarende sanktioner fra Datatilsynet?

- Ved at lave sine *lovpligtige* risikovurderinger
- Og ved at anlægge en anden *holdning* til databeskyttelse og de registreredes rettigheder, end der indledningsvist blev udvist fra kommunens side

Find os på standen

Eller kontakt os på:

kontakt@gapsolutions.dk

Tlf. 8844 0808

www.gapsolutions.dk

Ditte, Christian & Lill-Jana

GapSolutions
WE FIX IT