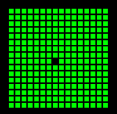
EU-GDPR,

~~Persondataforordningen~~ Databeskyttelsesforordningen

2018-04-03, IT-Samfundsudvalgsmøde @ PROSA



Overblik

- Hvem er jeg (meget kort)
- TL;DR (“*Too lazy; didn’t read*”)
  - En lidt længere opsummering
- DPO-ERFA-GRUPPEN hos Prosa
- Opskrift + Demo

Hvem er jeg (meget kort)

- Ramón Soto Mathiesen (Spanien + Danmark)
- Datalog fra ***DIKU/Pisa*** med bifag i matematik fra ***HCØ***
- ***CompSci*** @ SPISE MISU ApS
  - ***"S**tay **P**ure, **I**solating **S**ide-**E**ffects"*** -- Michael Werk Ravnsmed dixit
  - ***"M**ake **I**llegal **S**tates **U**nrepresentable"*** -- Yaron Minsky dixit
  - Prøver på at løse EU GDPR med en videnskabelig tilgang (datalogi samt matematik)
  - Lidt ***Elm*** (***JavaScript*** på grund af ports) sammen med noget ***Haskell***
- Har været medlem af Free Software Foundation (FSF) siden November 2007
- Medstifter af Meetup for F#unctional Copenhageners (MF#K)
- Frivillig ved Coding Pirates (Kaptajn ved Valby Vigerslev Biblotek afdeling):
- Blog: http://blog.stermon.com/

TL;DR (“Too lazy; didn’t read”)

- ***EU GDPR*** (databeskyttelsesforordningen) træder i kraft den ***2018-05-25***
  - Omhandler benhandliger af ***fysiske personers*** personoplysninger
- ***Personoplsyniger*** er informationer der kan henføres til personer
- Gælder hvis ***dataansvarlig*** er bosat i Danmark og behandlingerne foregår i EU eller hvis der foretages behandlinger af personer der er i Danmark.
  - En ***dataansvarlig***, myndighed eller virksomhed, definere behandlinger og en ***databehandler*** udfører behandlinger på vegne af den dataansvarlige.
- Behandling af data: ***Principper for behandling af personoplysninger (Artikel 5)***
  - Lovlighed, rimelighed og gennemsigtighed; Formålsbegrænsning; Rigtighed; Opbevaringsbegrænsning; og Integritet og fortrolighed.
- Behandlingssikkerhed: ***Databeskyttelse gennem design og standardindstillinger (Artikel 25)***.
  - Passende tekniske og organisatoriske foranstaltninger med henblik at personoplysninger ikke stilles til rådighed for et ubegrænset antal fysiske personer uden det fysiske persons samtykke.

En lidt længere opsummering

- GDPR har virkning fra 25. maj 2018.
- Alle offentlige myndigheder (undtagen domstole), samt private virksomheder hvis kerneaktivitet er behandling af persondata/følsomme oplysninger, skal have en databeskyttelsesrådgiver/Data Protection Officer (DPO), som er:
  - Med til at sikre at den dataansvarlige overholder forordningen
  - De registreredes repræsentant overfor den dataansvarlige
  - I besiddelse af ekspertkendskab til lovgivning, databeskyttelse og teknologi

En lidt længere opsummering

- Oplysningspligten ved indsamling af personoplysninger skærpes:
  - Hvilke oplysninger indhentes?
  - Hvor længe opbevares oplysningerne?
  - Pligt til at informere om muligheden for at klage til tilsynsmyndigheden (Datatilsynet)
  - Informationen skal være kortfattet og udformet i et enkelt og tydeligt sprog

En lidt længere opsummering

- De registreredes vigtigste rettigheder:
  - retten til at modtage oplysning vedr. behandling af sine personoplysninger (oplysningspligt)
  - retten til at få indsigt i sine personoplysninger
  - retten til at få urigtige personoplysninger korrigeret
  - retten til at få personoplysninger slettet

En lidt længere opsummering

- Indhentning af samtykke fra de registrerede.
  - Den registrerede skal indvilge i at oplysninger vedr. personen gøres til genstand for behandling.
  - Et samtykke skal være utvetydigt og ske ved erklæring eller klar bekræftelse.
  - Man skal kunne dokumentere at et samtykke er givet.
- Der skal være procedurer til at opdage, rapportere og undersøge brud på datasikkerheden.

En lidt længere opsummering

- Databeskyttelse skal indtænkes ved udvikling af nye it-systemer eller ændring af eksisterende it-systemer. Dette kaldes “privacy by design”, og dette skal være standard (“privacy by default”).
- Sanktioner:
  - Private virksomheder kan idømmes bøder på op til 4 % af den samlede årlige globale omsætning.
  - Offentlige myndigheder kan idømmes bøder på op til 4% af driftsbevillingen, dog max. 16 mio kr.

DPO-ERFA-GRUPPEN

- Gruppen opstod efter ***Per Mejers*** oplæg: "***EUs Persondataforordning - hvad betyder den for dig?***" afholdt den 2016-11-24 hos PROSA
- Første møde var den ***2017-01-31*** og der fastsatte vi retningslinjerne for gruppen:
  - Fokus på jura, praksis / teknologi, etik, …
  - Læse lovgivningen (***CELEX_32016R0679_DA_TXT.pdf***) samt diskuttere fra flere forskellige synspunkter: Forretning, juridisk, datalogisk, …
  - Desværre blev der valgt at vi skulle være en lukket gruppe: "*Ting der siges i netværket, bliver i netværket*"
  - Målet var at udarbejde et "***skriv***", som ville gavne PROSAs medlemmer

DPO-ERFA-GRUPPEN

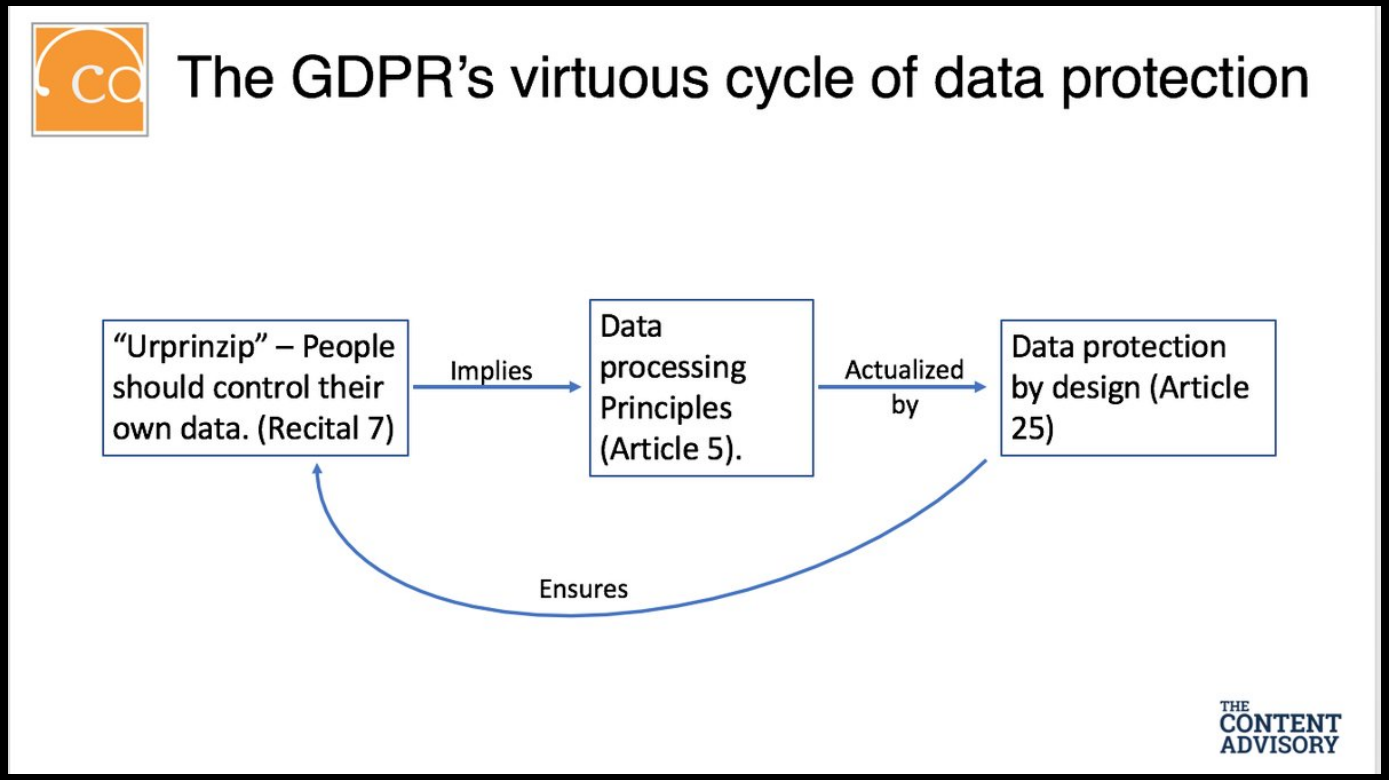
- Da de personer, som ønskede den lukkede gruppe, ikke længere er medlemer, har vi valgt at åbne op for gruppen.
  - Det vil helt sikkert gavne flere af PROSA medlemmer
- Vi forsætter med at læse de nationale vejledninger, udarbejder af Datatilsynet:
  - https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

  Bemærkning: De tidligere slides, ***TL;DR + længere opsummering***, er udarbejdet af gruppen og skulle gerne komme på ***DPO.dk*** efter korrekturlæsning fra ***Ole Tange***. Yderliggere skulle vi gerne linke til PROSA Forum samt andre relevante sider.

DPO-ERFA-GRUPPEN

- Vi holder til:
  - Fysisk, hos PROSA hver anden sidste tirsdag i måneden
  - Elektronisk, ved PROSA Forum:
    - https://prosaforum.dk/c/dpo-erfaringsgruppe

Opskrift + Demo



LinkedIn Post (Tim Walters, Ph.D.)

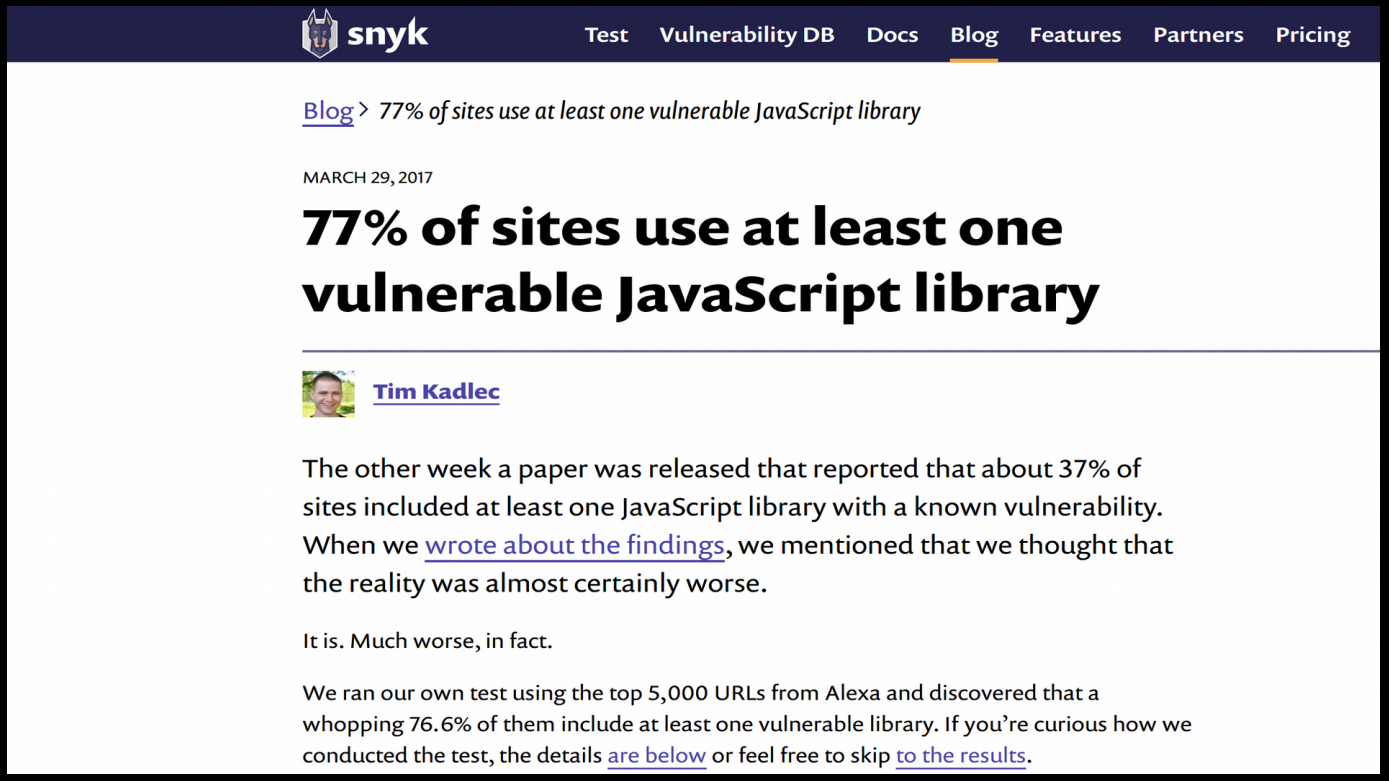
Opskrift + Demo

- Article 5. Principles relating to processing of personal data
  - *"One example: The requirement for **data minimization** (Article 5(1)(c)) means that you must be able to **demonstrate** that every business **process** that **touches personal data** (and **every technology** that contributes to it) is **designed** in such a way that it **uses the smallest possible amount** of data for the **shortest possible period of time** while **exposing** it **to the fewest** possible **eyeballs** and **ensuring** that it is **deleted as quickly as possible** when the processing purpose is completed."* -- **Tim Walters**

Opskrift + Demo

- Article 25. Data protection by design and by default
  - Ensure to "*... implement appropriate **technical** and organizational measures, ..., which are **designed** to implement **data-protection principles**, ..., in an effective manner and to integrate the necessary **safeguards** into the processing in order to **meet the requirements** of this Regulation **and protect** the **rights** of **data subjects***"

Opskrift + Demo



snyk Test Vulnerability DB Docs Blog Features Partners Pricing

Blog > *77% of sites use at least one vulnerable JavaScript library*

MARCH 29, 2017

77% of sites use at least one vulnerable JavaScript library

Tim Kadlec

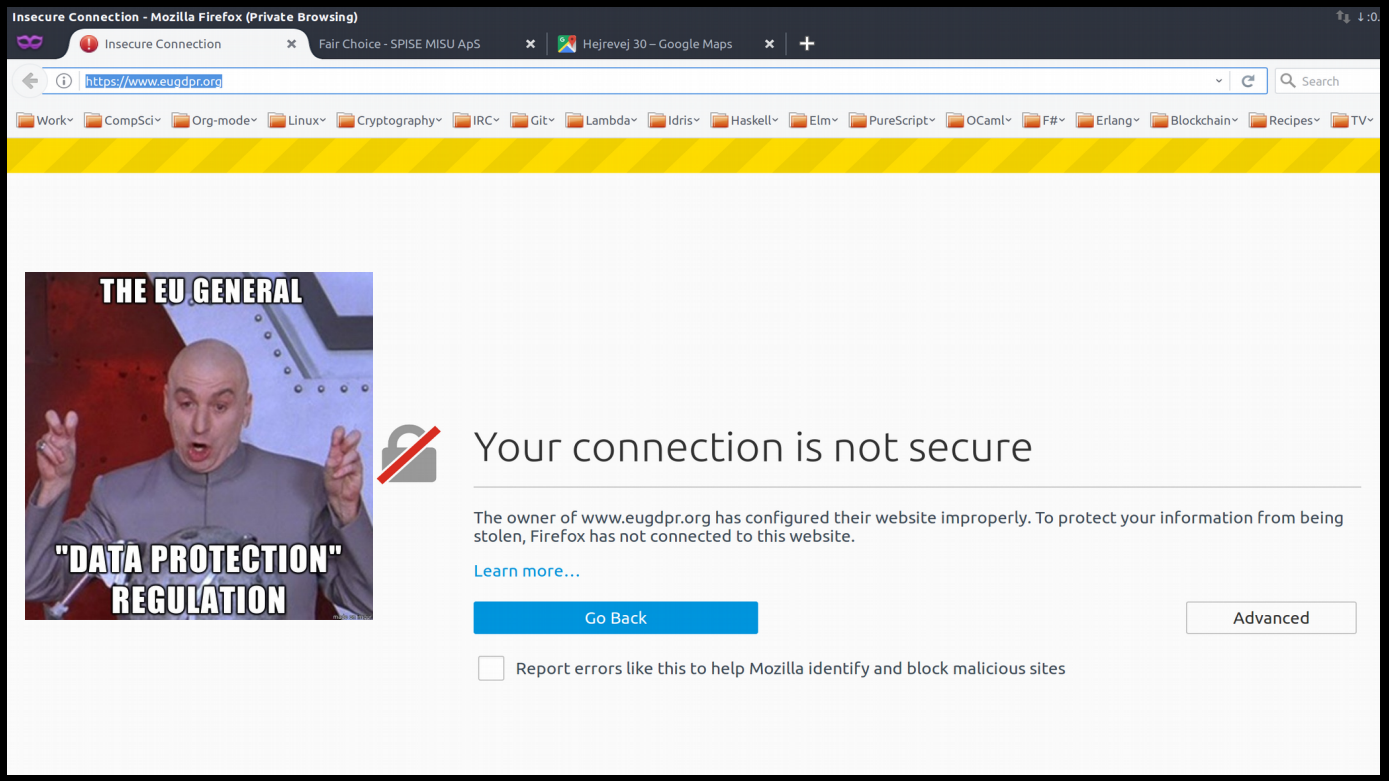
The other week a paper was released that reported that about 37% of sites included at least one JavaScript library with a known vulnerability. When we wrote about the findings, we mentioned that we thought that the reality was almost certainly worse.

It is. Much worse, in fact.

We ran our own test using the top 5,000 URLs from Alexa and discovered that a whopping 76.6% of them include at least one vulnerable library. If you're curious how we conducted the test, the details are below or feel free to skip to the results.

Desværre, den verden vi lever i ... Snyk Blog

Opskrift + Demo



Og HTTPS ved EU GDPR officielle hjemmeside :(

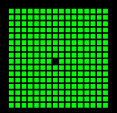
Opskrift + Demo

- Løser problemet med at udpege personer, i en tilfældig rækkefølge, til at prøve “noget”:
  - Fair Choice:
    - http://spisemisu.com/spa/fairchoice/

Opsummering

- Databeskyttelsesforordningen er ikke dårligt, men rigtigt godt for os EU borgere, også selv om det medfører lidt hovedpine i erhvervslivet
- DPO-ERFA-GRUPPEN er fremover en åben gruppe
- Man kan sagtens leve op til loven ved at følge en meget simpel opskrift som nemt kan realiseres teknisk. Vel bemærke hvis man bruger de rette værktøjer:
  - "*I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail*" – Maslow's law of the instrument

  Bemærkning: Stephan Engberg gjorde mig opmærksom på at ordet ***Privacy***, slet ikke findes i databeskyttelsesforordningen. Der kan man bare se …



Q & A

Spørgsmål?