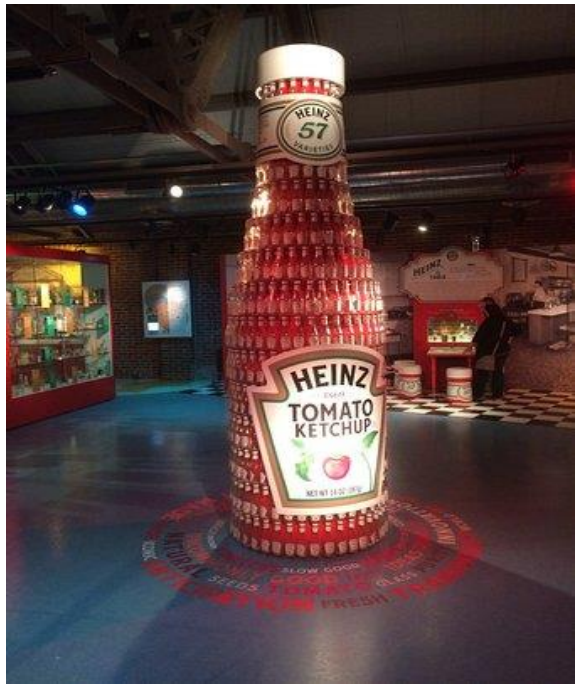
EU General Data Protection Regulation: what you need to know in 15 minutes!

8 April 2018



convergent

IT'S A DRY BUT CRUCIAL SUBJECT!

8 April 2018

So, what is the GDPR and how does it affect us?

- Any company that works with information relating to EU citizens will have to comply with the requirements of the GDPR, making it the **first global data protection law**
- GDPR considers any data that can be used to **identify an individual** as personal data
- Coming into effect **May 25, 2018**!

It will impact on the personal data we process and keep; from production through to subscription based services.

It affects crews and actors, through to marketing and monitoring activities, third party service providers and the entire supply chain.

convergent

KEY CHANGES

- **Harmonisation**
- **Broader Scope**
- **Wider definitions**
- **Increased Obligations**
- **Strengthened Individual Rights**
- **Increased Enforcement & Liabilities**

convergent

Accountability – is this just a formality?

- Companies must be able to **demonstrate** that their processing activities comply with the requirements of the GDPR
- How can you achieve this?
- **GOVERNANCE> PROCESS (end to end) >SECURITY>TRAINING**

- **Data protection officer** appointment
- Appropriate privacy and information security **policies and procedures**
- Internal **records** of data processing activities
- **Data processing agreements** with processors (i.e. third party service providers)
- Data protection by **design** and by **default**
- Data protection **impact assessments**
- Implementation of appropriate **technical and organisational security measures**

convergent

What level of security will I need to implement?

- You must ensure an **appropriate level of security**
- How you achieve this is **not prescribed** – will depend of the nature of the data and what you do with it

- Companies must consider how to protect personal data **before initiating any process** (e.g., signing an agreement which does not follow a company's templates, launching a new promotion, event etc.) which involves the collection of personal data – this cannot happen after the fact, it has to happen **by design**
- Companies must implement measures for ensuring that, **by default**, only personal data which are **necessary** for each specific purpose of the processing are processed
- Data breaches must be reported to Regulator's within **72 hours**

convergent

How should I process the personal data of EU citizens?

- Personal data must be processed **lawfully**, **fairly** and in a **transparent** manner
- **Legal bases** for processing personal data include (but are not limited to!) complying with a legal obligation, performing a contract, legitimate business interests, individual consent
- Under the GDPR, consent becomes **increasingly tricky but important** to implement
- Consent must be **freely given**, **specific**, **informed** AND a **clear unambiguous indication** of the data subject's wishes

- No more pre-ticked boxes - **affirmative action** is required!
- **Transparency** requirements of the GDPR will lead businesses to review their privacy notices and disclosures

convergent

I’m only a service provider, so will the GDPR apply to me?

- Rather than relying on data owners to **contractually flow down** compliance obligations to vendors, the GDPR imposes a number of **direct obligations**

- These **direct obligations** include:
  - implementing appropriate security measures
  - informing the controller in the event of a data breach
  - maintaining records of processing activities
  - cooperating with the relevant regulator
  - complying with the requirements of the GDPR regarding cross-border data transfers
- Vendors will have to sign up to a **written contract**, with **pre-determined additional obligations**

convergent

What happens if we get it wrong?

- The **fines can be potentially huge** - up to a maximum of **EUR 20 million or 4% of total worldwide global turnover** of the preceding financial year (whichever is higher)

- BUT **risk to reputation** could be even higher…. last year alone, we have witnessed:

  - HBO hack - FBI called in after hackers steal data including Game of Thrones spoilers
  - Larson Studios – hackers had stolen the company's data, and demanded ransom payment
  - Equifax - 145 million accounts compromised, highly sensitive financial data (this is happening weekly and we are all a potential target)

- Breach failures can **cost** CEO's and top execs their **jobs**

- U.S. style "**class actions**" - risk of group privacy claims against consumer businesses, costly compensation (including for distress and hurt feelings even where individuals are not able to prove financial loss)

- Regulator's can also issue **warnings, reprimands and corrective orders**

convergent

Key things to takeaway…

Prevention is better than cure and will be **less expensive** in the long run!

- **Determine how it impacts upon your business and its supply chain;** GDPR applies to **all companies** worldwide that process the personal data of EU citizens.
- **Know your Data;** what do you have? Where is it? Where does it go? How is it processed? How is it protected? How long are you keeping it? How do you get rid of it?
- **Roles and Responsibilities;** appoint **a DPO** if you have large scale processing, appoint controllers and formally document processing activity even if you are small
- **Remember liability extends beyond data controllers**
- **Be prepared to respond; to incidents and to data subjects exercising there rights**

convergent

Contact Us

Website: http://convergentrisks.com/

Email: privacy@convergentrisks.com

Chris Johnson
Director, Convergent Risk Privacy
E: chris@convergentrisks.com
T: +44(0)7951 011 080

Stephanie Iyayi
Director, Convergent Risk Privacy
E: stephanie@convergentrisks.com
T: +44(0)7384 617 473

Phil Herbert
Director, Convergent Risk Privacy
E: philh@convergentrisks.com
T: +44(0)7508 521 649

convergent