As seen on: Forbes Bloomberg independent G | M | F The German Marshall Fund of the United States STRENGTHENING TRANSATLANTIC COOPERATION

GDPR: Key concepts & data supply chain management

Emerald de Leeuw LL.B LL.M MSc CIPP/E

E: Info@eurocomply.com

T: +353 87 989 35 12

EUROCOMPLY

Agenda

1. Introduction
2. GDPR update
3. Personal data and actors of the GDPR
4. Vendor obligations
5. Contractual requirements
6. How to make it work
7. Q&A

EUROCOMPLY

Key development since May 25th

- National implementations of the GDPR have been introduced
- First enforcement notice issued in the UK against analytics company
    - Facebook currently under investigation by Irish DPC following recent data breach.
- Pressure on companies to sign data processing agreements sometimes. with unlimited liability – Traditionally capped at 2x, 3x or 4x contract value.
- Class actions filed on May 25th against a number of social media companies by NGO noyb.eu collectively worth €3.9 billion.
- Many consumer rights groups rallying against companies in class action.
- Cannot insure against GDPR fines in the EU except in Norway & Finland.

Choose humanity - ICDPPC

Ethics is the sense we all have, often subconscious, of right and wrong in different circumstances.

We do not yet have consensus in Europe as regards what Digital Ethics is.

Technology used to be driven by humans for humans. But how do we manage ethics when machines start determining what is built, consumed or seen?

And our leisure time also is spent on what machines determine we should see. Autoplay and recommendations – automated, algorithmic decisions – are responsible for 70% of online video viewing.

Europe is developing a standard on digital ethics and AI.

Who is being sued and investigated?

Max Schrems & NOYB.EU

Google

facebook

Coimisiún Cosanta Sonraí
Data Protection Commission

ico.
Information Commissioner's Office


An Coimisinéir
Cosanta Sonraí
Data Protection
Commissioner

Foundations of the claims

- **Privacy à la “take it or leave it”?**
- **GDPR prohibits “Bundling” of consent**
- **Separation of necessary & unnecessary data usage.**
- **Important for SMEs.** Usually cannot force their customers to agree to policies - other than big online monopolies

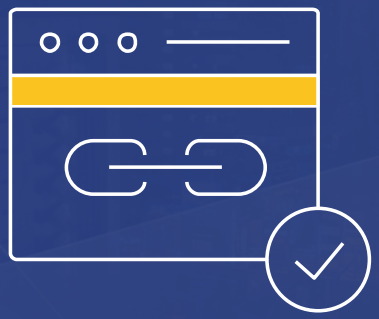
Company	Authority	Maximum Penalty
Google (Android)	CNIL (France)	€ 3.7 Mrd
Instagram	DPA (Belgium)	€ 1.3 Mrd
WhatsApp	HmbBfDI (Hamburg)	€ 1.3 Mrd
Facebook	DSB (Austria)	€ 1.3 Mrd

GDPR & its impact

HUGE FINES

Non-compliance puts companies at risk of being fined 4% of annual global turnover or €20 million whichever is greater

DATA SUPPLY CHAIN



Liable for entire data supply chain

- **Struck off approved vendor list**
- **stifles landing new B2B customers.**

TERRITORIAL SCOPE

GDPR applies when you target EU residents with products or services or monitor their behaviour.

i.e. Global impact

It wasn’t me!


WASN'T ME
exposay.com
imgflip.com
Landmark / PR Photos
quickmeme.com

Understanding “personal data” (not PII)

What is personal data? – Breyer Case

Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier etc..

What is personal data processing?

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring**, storage**, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, **erasure or destruction**;

Understanding Controllers v Processors

Controller: determines the means and purpose of the processing. May only use processors that offer “sufficient guarantees”

Processor: processes data on behalf of the controller (must be governed by a contract in accordance with article 28 GDPR)

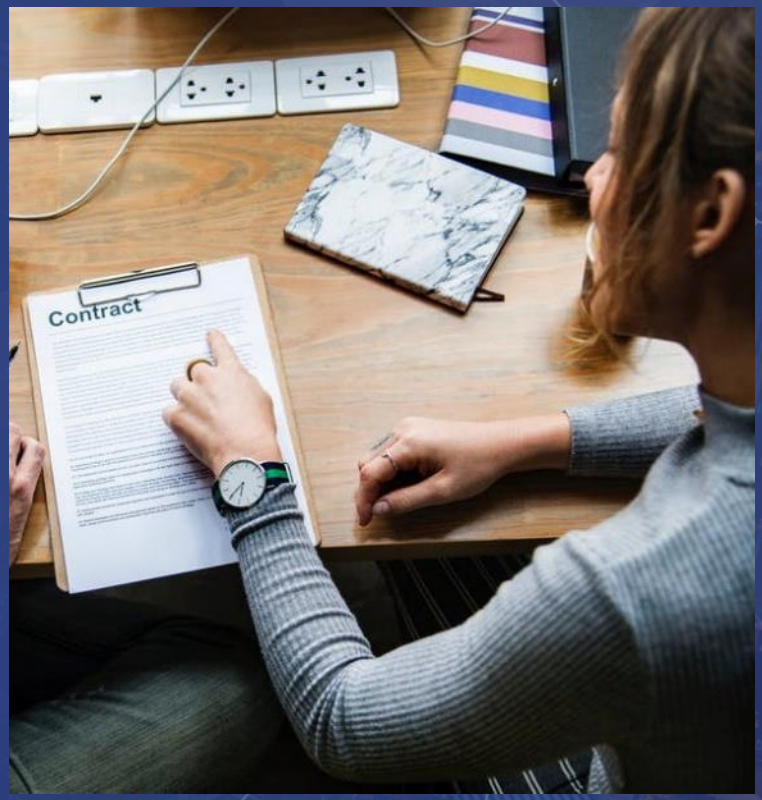
Joint-controller: two controllers who together determine the means and processing of the data. Relevant in practice when a processor acts outside of the written instructions.

Sub-processor: relationship must echo the terms in the contract between the controller and processor. May only be engaged with prior written permission from the controller.

Processor obligations and operational challenges

As a vendor you would usualy be a data processor and will be asked to sign a DPA.

Article 28 (1) GDPR. […] the controller shall **use only processors** providing **sufficient guarantees** to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation **and** ensure the protection of the rights of the data subject.



What goes into the contract?

1. the subject-matter and **duration** of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

2. **Instructions from the controller**

3. Instructions as regards transfers of personal data **outside of the EU**

4. Rules regarding access controls & confidentiality agreements

5. **Ensure adequate levels of security (article 32 GDPR)**

6. Not engage sub-processors unless prior consent from the controller is obtained

What else?

7. Assist the controller with executing data subject rights

8. Assist with data protection impact assessments

9. At the end of the provision of services the processor must delete or return all personal data.

10. Make available any documentation that will aid the controller in demonstrating compliance with the regulation. **(Accountability!!)**

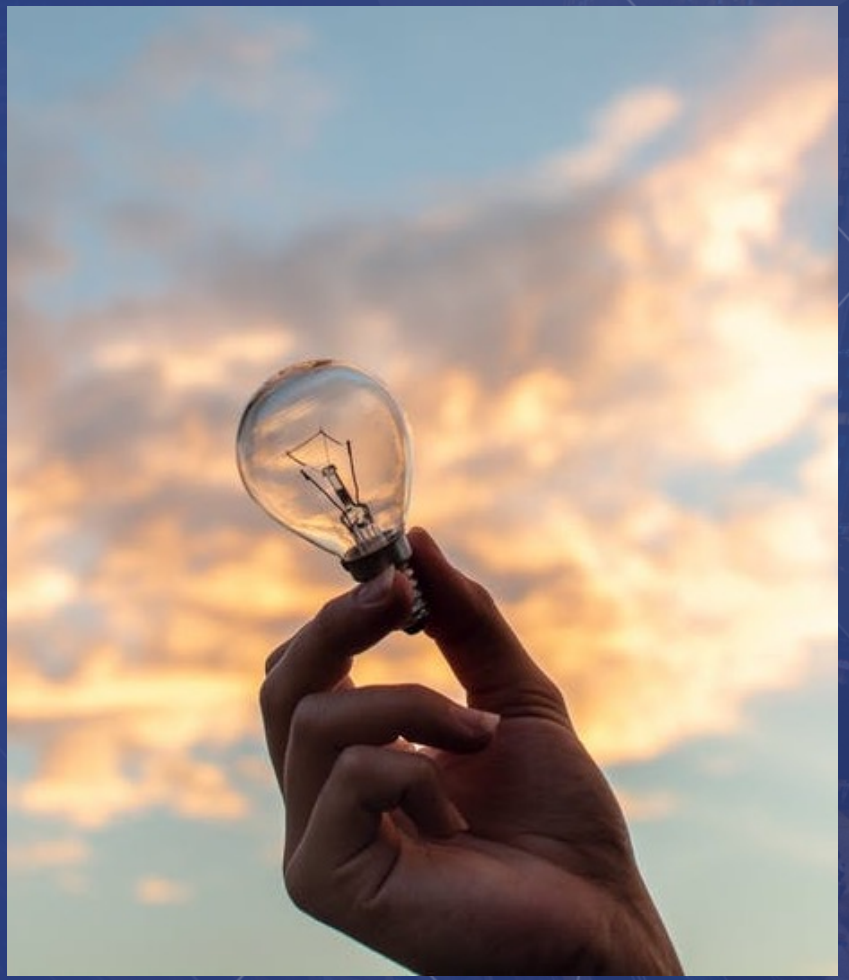
How to manage all of this?

People: who is responsible?

Process: View vendor management as a lifecycle. Think of the ability to audit as well as ensuring procurement and legal are aware of what is required.

Technology: Compile and maintain a complete inventory of vendors and vendor contracts.

KPIs: GDPR is about accountability and demonstrating your compliance journey. This means keeping documentation which demonstrates compliance with GDPR.



TC

Startups

Apps

Google+ to shut down after coverup of data-exposing bug

7,713 views | Sep 20, 2018, 12:21pm

Opinion

Did Facebook Learn Anything From the Cambridge Analytica Debacle?

An even bigger data breach suggests it didn't.

Forbes Billionaires Innovation Leadership

Breach Will Reveal The True Cost Of GDPR

CNBC

MENU MARKETS BUSINESS NEWS INVESTING TECH POLITICS CNBC TV

TECH

CYBERSECURITY | ENTERPRISE | INTERNET | MEDIA | MOBILE | SOCIAL M

Uber will pay $148 million in connection with a 2016 data breach and cover-up

Sign in Search

Sport Culture Lifestyle More

The Guardia

evelopment Football Tech Business Environment Obituaries

acebook fined for data breaches in ambridge Analytica scandal

most viewed

Nikki Hale ambassado

The New York Times

Facebook Security Breach Exposes Accounts of 50 Million Users

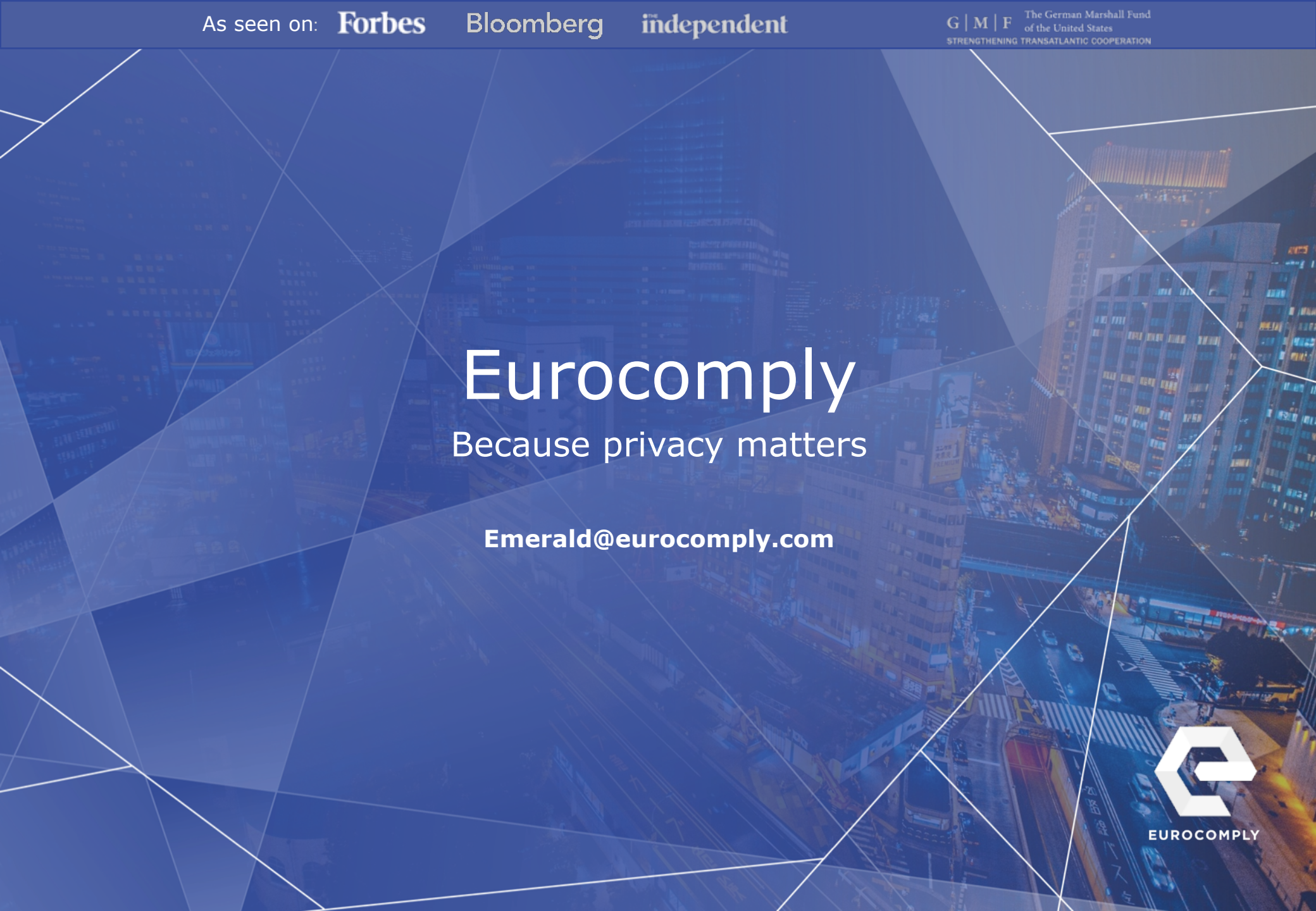
Google Plus Will Be Shut Down After User Information Was Exposed

As seen on: Forbes Bloomberg the independent G | M | F The German Marshall Fund of the United States STRENGTHENING TRANSATLANTIC COOPERATION

Eurocomply

Because privacy matters

Emerald@eurocomply.com



EUROCOMPLY