

ORACLE®

EU-GDPR

The General Data Protection Regulation

Lucas Heymans, Higher Education Applications Product Strategy

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle. Not all technologies identified are available for all cloud services.

Disclaimer

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of any vendor's products or services.

From the Eurobarometer:

81% of Europeans feel that they do not have complete control over their personal data online
31% think they have no control over it at all.

69% would like to give their explicit approval before the collection and processing of their personal data

Only **24%** of Europeans have trust in online businesses such as search engines, social networking sites and e-mail services.

Almost all Europeans say they would want to be informed, should their data be lost or stolen.

A majority of people are uncomfortable about Internet companies using their personal information to tailor advertisements.

71% of Europeans feel that there is no alternative other than to disclose personal information if they want to obtain products or services.

Around **seven out of ten** people are concerned about their information being used for a different purpose from the one it was collected for.

Timeline

- 25.01.2012 European Commission presented the initial proposal
- 12.03.2014 First reading in the European Parliament
- 15.06.2015 „First reading“ in the European Council
- 24.06.2015 Trilogue starts (total of 10 meetings)
- 15.12.2015 Commission, Council and Parliament come to an agreement
- 04.05.2016 Published in the Official Journal of the European Union
- 25.05.2016 Regulation enters into force
- 25.05.2018 Grace Period is over (Application of the regulation starts)



The Guardian
26 Feb 2017

EU referendum and
Brexit
The Observer

Revealed: how US billionaire helped to back Brexit

Robert Mercer, who bankrolled Donald Trump, played key role with 'sinister' advice on using Facebook data

● [In-depth: Mercer, Breitbart, Farage and the data war against mainstream media](#)



This article is 3 months old

30,220

Carole Cadwalladr

@carolecadwalla

Sunday 26 February 2017 00.04 GMT



Leave supporters cheer results at a Leave.eu party after polling stations closed in the EU referendum on 23 June 2016. Photograph: Toby Melville/Reuters

● *This article is the subject of a legal complaint on behalf of Cambridge Analytica LLC and SCL Elections Limited.*

The US billionaire who helped bankroll Donald Trump's campaign for the presidency played a key role in the campaign for Britain to leave the EU, the *Observer* has learned.



Financial Times
18 May 2017

Facebook fined €110m by European Commission over WhatsApp deal

Social media group penalised for misleading EU over data sharing



© Getty



Save

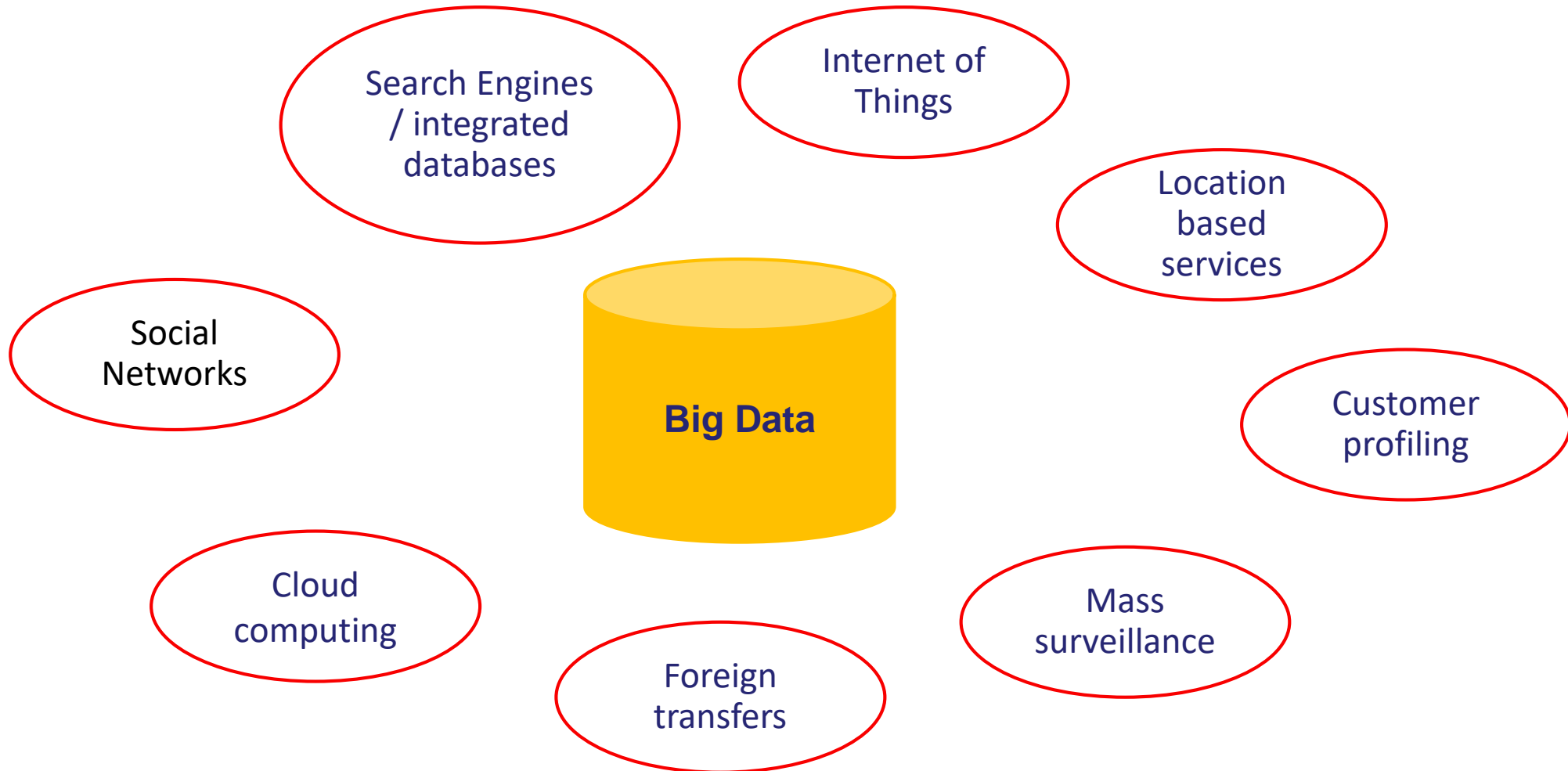
MAY 18, 2017 by **Madhumita Murgia**, European Technology Correspondent

[Facebook](#) has been fined €110m for misleading the European Commission during its 2014 takeover of WhatsApp, handing the social media company one of its biggest regulatory penalties days after data and privacy authorities in Italy and France slapped it with their own charges.

ORACLE®

GDPR: WHY?

TRUST NEEDED



The objective of GDPR

...to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.

IT Security, Data Protection and Privacy

- **IT-Security**
the potential damage for the university (reputation, money, ...)
- **Data Protection**
„the risk of varying likelihood and severity for the rights and freedoms of natural persons”
- **A change of perspective**
from the perspective of the **university** to the perspective of the **data subject**

GDPR simplifies!

The GDPR introduces
the concept of a
one-stop shop

The Concept: Self Regulation

You decide, which technical measures you implement,
but you have to **justify and document** the measures

GDPR Applies to all

Quite exceptional
and unique

Applicable on any organization

- in the EU that processes personal data
- outside of the EU that processes data of EU citizens ('a person residing in the EU')

The GDPR widens the definition of personal data



personal data' means 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The GDPR tightens the rules for obtaining valid consent to using personal information

Explicit consent needed for each purpose, processing type ...

in a concise, transparent, intelligible and easily accessible form, using clear and plain language,

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. (Art7§4)

In General: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be **prohibited**.

Except with explicit consent, specific purposes or organizations etc.

More individual rights

- **The right to be forgotten**

Do you have technology and procedures in place to execute?

- **Data access**, rectification or erasure

- **Data portability**

Individuals can ask a copy of their data in a structured, commonly used and machine-readable format

- **Object to processing for direct marketing purposes and automated individual decision making**

explicit, clear and separate communication on this kind of processing needed

- **Information**

E.g. About the **purposes** of the processing for which the personal data are intended as well as the legal basis for the processing

E.g. about **data transfer** to third parties, access rights, correction rights, period of storage, controller & DPO contact details, ...
















E.g. About the existence of automated decision-making, including **profiling**, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The GDPR requires privacy by design and by default

- **Data protection by design**
... implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as **data minimisation**, 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.
- **Data protection by default**
... implement appropriate technical and organisational measures for ensuring that, by default, only **personal data which are necessary** for each specific purpose of the processing are processed

Find a setting

Privacy

-  General
-  Location
-  Camera
-  Microphone
-  Notifications
-  Speech, inking, & typing
-  Account info
-  Contacts
-  Calendar
-  Call history
-  Email
-  Messaging
-  Radios
-  Other devices
-  Feedback & diagnostics

Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

Off

Send Microsoft info about how I write to help us improve typing and writing in the future

Off

Let websites provide locally relevant content by accessing my language list

On

Let apps on my other devices open apps and continue experiences on this device

On

Let apps on my other devices use Bluetooth to open apps and continue experiences on this device

Off

[Manage my Microsoft advertising and other personalization info](#)

[Privacy Statement](#)

The GDPR introduces mandatory PIAs

Privacy Impact Assessments

The GDPR makes the appointment of a DPO mandatory for certain organisations

A Data Protection Officer needs to be appointed

- An independent, competent and senior person
- Shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices
- Is involved, properly and in a timely manner, in all issues which relate to the protection of personal data

The GDPR expands liability beyond data controllers

The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation

The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures.

Notification of a personal data breach

To the supervisory authority: “without undue delay and, where feasible, not later than 72 hours after having become aware of it “ (art. 33)

To the data subject: When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, (...) without undue delay

Details of the notification content are defined too.

Administrative fines (shall) be effective, proportionate and dissuasive.

Infringements (shall) be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover (...) whichever is higher

Where to start?

- **Appoint a DPO**
- **Update your privacy procedures and information portals**
- **Start documenting**
- **Work together, share,**

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct

- **Use the technology that is available: e.g.masking, security, user access rights**
- **Talk to your security colleagues about reporting breaches**

An example from Finland

ONGOING ACTIONS:

- 1. Analyze the legal framework**
- 2. Analyze the personal data processing activities**
- 3. Identify and document privacy risks, including risks in agreements**
- 4. Create and update necessary Data Protection Rules, Policies and Processes**
- 5. Create the General Data Processing Agreement**
- 6. Provide necessary infrastructure and services for the researchers and other employees**
- 7. Create Communication Plans and Communicate**
- 8. Create Data Protection and Data Security Training for employees**
- 9. Handle Data Security and Data Breach Notification in 72 hours**
- 10. Monitor compliance with the GDPR continuously**
- 11. Report regularly to the University's Management**

An example from The Netherlands

Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs (IBPDO1)							REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT				
Mbo roadmap informatiebeveiligings- en privacy beleid (IBPDO5)											
Model informatiebeveiligings- en privacy beleid voor de mbo sector (IBPDO6)											
Toetsingskader informatiebeveiliging: clusters 1 t/m 6 (IBPDO3)					Toetsingskader privacy: cluster 7 (IBPDO7)						
Toetsingskader examinering pluscluster 8 IBPDO8		Tk digitaal ondertekenen pluscluster 9 IBPDO9		Toetsingskader vmbo-mbo pluscluster 10 IBPDO10		Benchmark mbo sector IBPDO11		Functie-waardering ibp IBPDO12	Positionering ibp IBPDO13	Risico inventarisatie ibp IBPDO29	
Handleiding BIV classificatie IBPDO14		BIV en PIA bekostiging IBPDO15		BIV en PIA indiensttreding IBPDO16		BIV en PIA online leren IBPDO17		Bewerkers-overeenkomst mbo versie IBPDO18		Certificerings-schema ibp ROSA IBPDO19	
Format dataregister IBPDO20		Handleiding Privacy by Design IBPDO22		Autorisatie architectuur IBPDO23		Starterkit BCM (Continuïteit) IBPDO24		Integriteitscode (eigen personeel) IBPDO25		Verantwoord Netwerkgebruik IBPDO26	Responsible disclosure IBPDO27
Implementatievoorbeelden van kleine en grote instellingen						Technische quick scan, APK (IBPDO30)					
Handboek mbo-audits (IBPDO21)											
Hoe? Zo! Informatiebeveiligingsbeleid in het mbo				en	Hoe? Zo! Privacy in het mbo						
ibp mbo		Voorbeelden		Service document							
Mbo ibp architectuur (IBPDO4)	Privacy compliance kader mbo (IBPDO28)	Normenkader informatiebeveiliging mbo (IBPDO2A)									

An example from Germany (Max Planck Institute)

ISO 27002 controls

5. Information security policy
 6. Organization of information security
 7. Human resource security
 8. Asset management
 9. Access control
 10. Cryptography
 11. Physical and environmental security
 12. Operations security
 13. Communications security
 14. System acquisition, development and maintenance
 15. Supplier relationships
 16. Information security incident management
 17. Information security aspects of business continuity management
 18. Compliance
- Use it as a checklist



An example from Germany cont'd

Encryption

- Login on Web-Pages must be encrypted
- E-Mails with personal data must be encrypted
- Hard-Disk encryption on Notebooks, Desktops ...
- Encrypted mobile data (USB-Sticks ...)
- Encryption on Smart-Phones must be activated
- How to back-up personal data?



Probably the trickiest: Herding your PhD Cats



Just my opinion...

Take this serious

But:

- Universities are not THE target

- Proportionality is key : appropriate, sufficient, ...

the controller, taking account of available technology and the cost of implementation, shall take reasonable steps,

- **Very balanced regulation:**

the public interest, common good, fundamental rights, logical and reasonable sense prevail.

“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing (...) the controller (...) shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”

- **It's a journey, not a destination**

Questions and Answers

ORACLE®