GDPR Myths and Legends: Sifting fact from market hype

Duncan Brown
Associate Vice President
European Security
@DuncanWBrown
There is fact
There is uncertainty
There is myth
What do these firms have in common?
Europe is now #cloudfirst

Western Europe Infrastructure Spending By Location ($M)

Source: IDC EMEA Public Cloud Services Forecast; IDC Infra Spending Including Server, Storage, Ethernet Network, 2Q16
It’s all got out of hand…

Data brokers collect more than 50 trillion unique data transactions per year.

82% of Android apps track your other online activities.

If you read all of the terms of service for all of your apps it would take 76 days.

PayPal’s Terms of Service is 36,275 words long: that’s longer than Hamlet.

‘Free’ online services are ‘paid for’ using personal data which have been valued in total at over EUR 300 billion.

LinkedIn would like to WHAT???

"LinkedIn" would like to make data available to nearby Bluetooth devices even when you're not using the app.
We will help you connect with others that are nearby.

Don't Allow  OK

"LinkedIn" would like to make data available to nearby Bluetooth devices even when you're not using the app.
We will help you connect with others that are nearby.

Don't Allow  OK
“The trouble with privacy is the half the world is paranoid and the other half’s password is ‘password’.”

Equity
GDPR is a “good thing”

- Updates law hopelessly out of date
  - 95/46/EC act predates Google, Facebook, Twitter, Uber, AWS, AirBnB, salesforce.com, Dropbox, etc

- Unifies DP law across all 28 states
  - And beyond (where EU goes many follow)
  - With extra-territoriality jurisdiction
The GDPR Timeline

27.4.16
Signed into law

4.5.16
Published in OJEU

25.5.18
Application
GDPR is a game-changer

- Fines up to 4% of global revenues
  - “Effective, proportionate and dissuasive”
- Mandatory Breach Notifications
  - Consequential loss of reputation
- Class-action lawsuits
  - Brought by activists…?
- Ban on personal data processing*
  - In extreme cases

*Article 58
Personal Data

Article 4

Definitions

For the purposes of this Regulation:

(1) ‘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;

Article 9

Processing of special categories of personal data

1. 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.
Handy hint…
What is in GDPR*

- Data transfer rules
- Rights to erasure & rectification
- Joint liability for Controllers & Processors
- Consent
- Right to access
- Data portability
- Continuous compliance

*Not exhaustive!
GDPR Myths
“administrative fines … shall be effective, proportionate and dissuasive”

Articles 83, 84
“Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action.”

Information Commissioner Elizabeth Denham

- 15,656 bank account details
- 101,000 customers lost
- GDPR 4% fine: £73m
There are worse penalties than fines…

FINE JUST TAKE MY MONEY
GDPR is just like…
‘processing’ means 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;”

Article 4(2)
Article 83

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, 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 of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects’ rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
How many breaches do we expect?

Dutch Data Protection Authority report breaches 2016

“If this number is indicative of the number of notifications under the GDPR … larger European countries may be in for a surprise.”

IAPP

*IDC, IAPP estimates
So I’ll just encrypt everything, yes?

“How hard can it be?”
CEO, major European enterprise
Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

Regulation (EU) 2016/679 (aka GDPR)
The hidden costs of encryption

- Key management is the hard part
- Vulnerabilities to advanced decryption technologies
- Reduces business functionality
  - Search, sort, analytics, etc.
- Reduces security functionality
  - Encrypted traffic can’t be read by many detection technologies
What the heck is ‘state of the art’?
Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
Why “state of the art”? 

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
GDPR talks about…

“State of the art”

Cost

Risk

Context
So what does this all mean?

You must have a view on what state of the art means in your organisation that you can defend
Is it all doom & gloom?
“The trouble with privacy is the half the world is paranoid and the other half’s password is ‘password’.”
Lack of awareness of GDPR, or its application to the business

A plan is in place and in the process of execution

Processes are compliant within an acceptable level of risk

Compliance is an outcome of improved business processes

Compliance is a product that is sold to others with less maturity
% Confident that all personal data can be located

% seeing GDPR as an Opportunity

Bubble size shows focus on advanced requirements (Extend data governance into the cloud)

Utilities
Banking
Oil and gas
Telecommunications
Healthcare
Insurance
Other Financial Services
Manufacturing
Transportation
Retail trade
Wholesale trade
Business Services
Education
Media
Government

Maturity of Information Governance

% Confident that all personal data can be located

Opportunist

Obstaclers

Utilities
Banking
Oil and gas
Telecommunications
Healthcare
Insurance
Other Financial Services
Manufacturing
Transportation
Retail trade
Wholesale trade
Business Services
Education
Media
Government

IDC
Analyze the Future
“GDPR comes at the right time. We have big data, a wholesale move to the cloud, and IoT. GDPR tells us how we should handle personal data in this digital world.”

Imdad Hussain, Senior Information Risk Manager, Barclays
Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, 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.
“The Bluebee genomics platform has been designed from the bottom up with confidential patient information and multi-layered data security in mind”

Hans Cobben, CEO at Bluebee
The role of technology in GDPR

Information Governance
What personal data do I have, where is it, how sensitive is it, why do I have it, do I have consent to use it, can I delete it, etc.

Meeting Specific Requirements
RTBF, Consent, Encryption, Data Portability, Record keeping, incident response, etc.

Review State of the Art
“appropriate technical and organisational measures” Encryption, backup & restore, testing, access control, etc.
Thank you