Hewlett Packard Enterprise

GDPR: Make Compliance Good for Your Business

Branislav Makyta
HPE Software

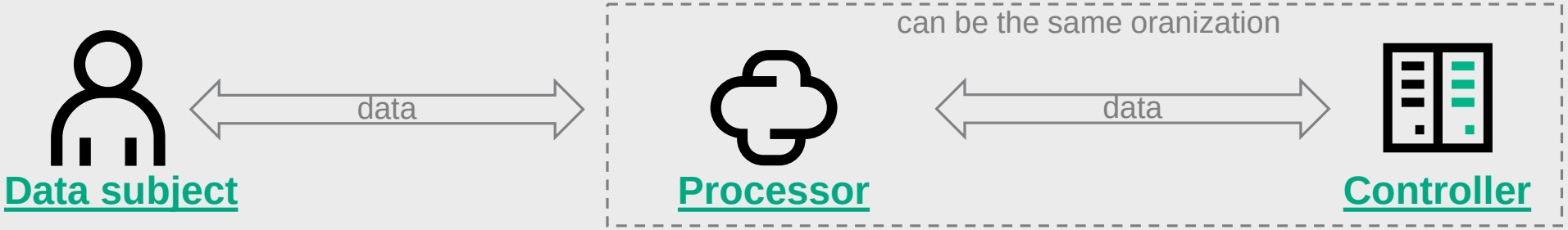
Nov 22, 2016

Agenda

- Why should you care about the General Data Protection Regulation (GDPR)?
- What opportunities does it pose for you?
- How We Do It

Key Terms and Definitions

Personal data: Information relating to an identified or identifiable natural person/data subject
(*e.g. Name, Address, IP Address, biometric data, gene sequence*)



Natural persons who can be directly or indirectly identified by the processor, controller or a third party

Processes personal data on behalf of the controller
(e.g. cloud service, call center)

Determines the purposes and means of the processing of personal data, making decisions
(organization delivering the service)

What is The EU General Data Protection Regulation – (GDPR) ?

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

- GDPR replaces previous Data Protection Directive
- Data Protection Directive created to regulate control of Personally Identifiable Information (PII)
- GDPR will harmonize data protection laws across 27 EU member states
- Clearer rules for data transfer across borders
- Better control over individual's data and its use
- Comes into force on 25th May 2018

Hewlett Packard Enterprise

EU General Data Protection Regulation (GDPR) - Key Changes

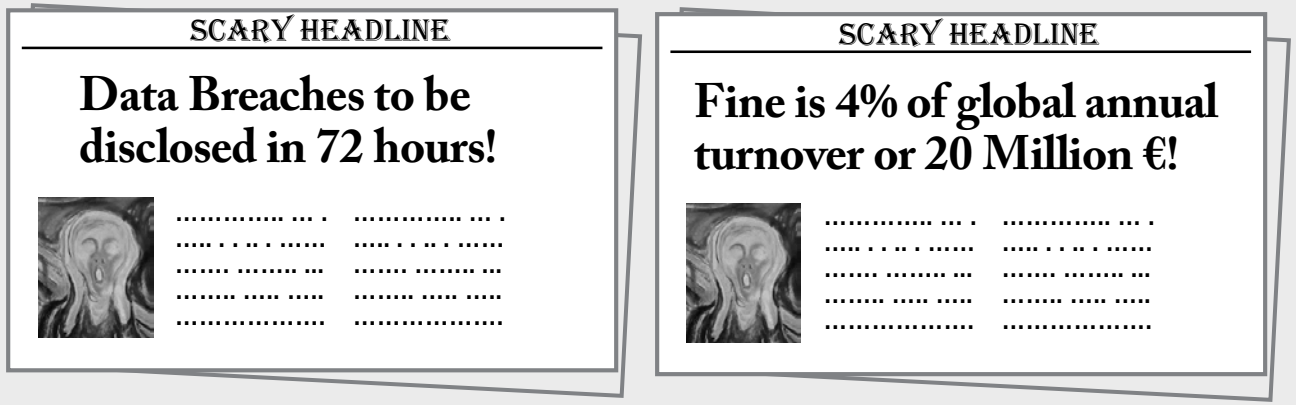
- **Data Protection Officer** (DPO)
- Increased responsibility around security **breach notification**
- Heavy non-compliance sanctions – **4% of Global Sales**
- Privacy **by design** and privacy by default
- **Right to be forgotten** and data portability
- A **single set of rules** and a **single data protection authority**
- EU Regulation will apply **across borders**
- Greater **compliance** requirements

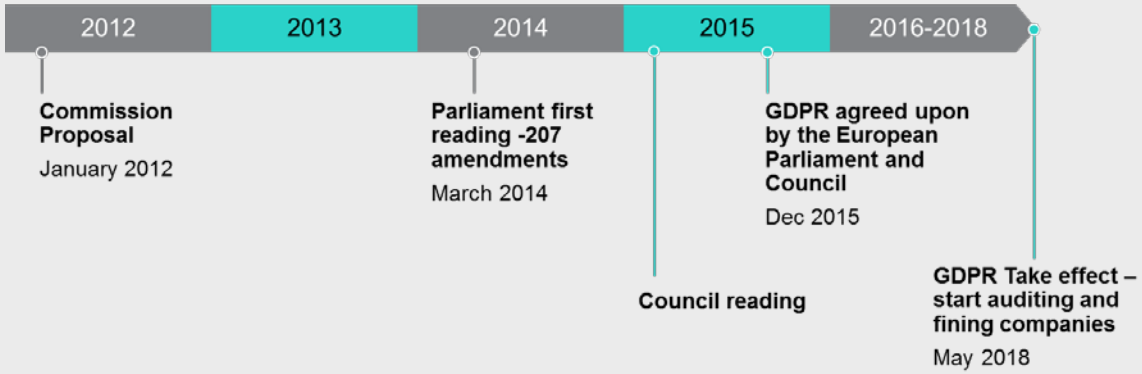
“The **[GDPR]** returns control over citizens’ personal data to citizens. ”

Martin Schulz , President of the European Parliament

“ The **[GDPR]** requires companies handling EU citizens’ data to undertake major operational reform”

Jan Philipp Albrecht, MEP





Hewlett Packard Enterprise

What technical delivery does GDPR compliance require ?

- Corporate Governance monitoring and enforcement
- Social media monitoring - internal & external where permitted
- Ability to freeze data across a complex IT legacy architecture
- Cross-media visibility and comprehension
- De-duplication, clustering and synthesis of mass data
- Necessity to respect national and international data privacy standards
- Fast and effective response to the Business

Hewlett Packard Enterprise

The industry should see this as an opportunity

- better data management and governance
- overall enhancement of companies IT security
- avoid very! costly data breaches
- avoid reputational damage
- competitive advantage thru GDPR compliance
- customers will appreciate strengthened security of their very own data

The Window of Opportunity

In order to prepare for the May 2018 deadline, organizations *must interpret the GDPR requirements, map technology to them, and quickly identify the correct information to be tightly managed and protected.*
Information insight is the key to solving these challenges of large volumes of data and high levels of complexity.
The risks are high - lost customer confidence, security breaches, fines, sanctions, and potential lawsuits.

GDPR – Key Challenges

Report Compliance

Get Customer Consent

•What can be done with what data?

Find All Customer Data

•Within all systems, across boarders

•At Processor and Controller

•Show it on demand to customer – Subject Access Requests (SAR)

•Comply to „Free Movement of data“ – or „Right for Portability“

Protect All Customer Data

•Data Pseudonymization

•Breach Detection & Notification

•Comply to „Right to be Forgotten“

Which “Entities” should be most engaged in GDPR preparation?

B2C corporates

Those acquiring personally identifiable information from private citizens in the normal course of business e.g.

a. Retailers - supermarkets

b. Personal insurance

c. Retail Banks

d. Telcos

B2B corporates

a. Those with a large workforce where the PII is employee data

b. Those which have agents who are B2C

Government agencies

Those who acquire PII due to their engagement with the public e.g.

a. Healthcare

b. Municipal Authorities

Seven Recommendations for immediate action

1. Adopt a **comprehensive framework** and strategy for digital security
2. Focus on the **DATA** - **records management**, **classification**, **encryption** and **retention**
3. Conduct a **full audit** of current and **likely risks initiatives**
4. Bake **security into all processes** (Security by design)
5. Mobilize the larger workforce around **data security** (prod. design, supply chain …)
6. Bring **partners** & **customers** up to rigorous security standards
7. Rethink the role of IT (become a **valued business partner**)

GDPR Risk Assessment Map

Domain	Capablity	sub-capabilities	High Risk	Medium to High Risk	Medium Risk	Medium to Low Risk	Low Risk	Scores		
Governance	Assurance / Respond / Report	Assurance (Personal Data Records Mgmt. and Security)			X			3		
		Respond to Data Subjects	X					5	4.00	
		Respond & Report to Litigation / Regulatory Investigation		X				4		
	Inventory	Data Processing Models					X	1		
		Personal Data Inventory			X			3	2.00	
		Systems & Applications Inventory				X		2		
	Policies	Policy Management				X		2		
		Personal Data Protection					X	1	1.33	2.73
		Records Management					X	1		
	Design / Accountability	Privacy by Design / Privacy by Default	X					5		
		Data Flow Mapping	X					5	4.67	
		Accountability		X				4		
	Assess / Remediation	Data Protection Impact Assessments			X			3	1.67	
		Program GAP Analysis				X		2		
			High Risk	Medium to High Risk	Medium Risk	Medium to Low Risk	Low Risk	Scores		
Data Processing / Lifecycle Management	Consent	Consent Structure and Management	X					5		
		Obtaining Methodology and Coverage	X					5	4.67	
		Registry and Mapping		X				4		
	Capture / Discover	Accuracy				X		2		
		Purpose Limitation		X				4	3.33	
		Data Minimisation		X				4		
	Transform / Transfer	Pseudonymisation / Anonymisation			X			3		
		Storage Limitation		X				4	3.33	
		Transfer Controls			X			3		3.60
	Use / Share	Lawful & Transparent Processing				X		2		
		Legal base for Data Processing	X					5	3.00	
		Contractual Necessity				X		2		
	Archive / Retention	Data Retention Management			X			3	2.50	
		Archival Management				X		2		
	Destroy / Erase	Right to be Forgotten		X				4	4.00	
	Records Management	Records Mgmt. for Personal Data			X		Automated updates	3		
		Data Flow Mapping	X					5	4.33	
		Records Mgmt. for Personal Data processing	X					5		
			High Risk	Medium to High Risk	Medium Risk	Medium to Low Risk	Low Risk	Scores		
Security	Breach Notification	Notification for Authorities			X			3	4.00	
		Notification for Impacted Data Subjects	X					5		
	Data Security (Integrity & Confidentiality)	Data Encryption / Pseudonymisation			X			3		
		Server / Disk / Volume Security				X		2	1.75	
		Encryption Key Management					X	1		2.92
		Encrypted e-mail					X	1		
	IT Security & Operatons	Security Monitoring & Breach detection				X		2		
		Breach Root Cause Analysis & Remediation				X		2	3.00	
		Detection Non-compliant Behavior		X				4		
		Application Security		X				4		

HPE delivers a flexible, modular, intelligent set of solutions to help customers identify & take action on customer data in accordance with GDPR

GDPR Use Cases	How HPE delivers
Personal Data Assessment	HPE ControlPoint HPE Structured Data Manager
Defensible Disposition	HPE ControlPoint HPE Structured Data Manager
Secure Content Management	HPE Secure Content Management Suite
Litigation Readiness and Response	HPE Verity Suite
Adaptive Backup and Recovery	HPE Adaptive Backup and Recovery Suite HPE Enterprise Secure Key Manager (ESKM)
Encryption and Pseudonomysation	HPE Adaptive Backup and Recovery Suite HPE SecureData, HPE Atalla HSM HPE Secure Mail and HPE ESKM
Breach Response and Reporting	HPE ArcSight HPE Secure Data, HPE Atalla HSM HPE SecureMail and HPE ESKM
Breach Prevention and Neutralization	HPE ArcSight HPE Fortify HPE SecureData, HPE Atalla HSM HPE SecureMail and HPE ESKM

Encryption and the GDPR

> "The GDPR is clear that if data is encrypted or otherwise obfuscated, then a data breach will not be deemed to have occurred even if the encrypted data is exposed."*

Data Security capability	HPE product	GDPR article reference
Pseudonymizing data in production applications and databases	HPE SecureData with Format-Preserving Encryption (FPE)	• **Page 51, Article 83:** Calls out encryption as an approach to mitigate risk associated with data protection • **Page 121, Article 6, Section 4:** Calls out encryption and pseudonymization as appropriate safeguards • **Page 161–162, Article 32, Section 2:** FPE satisfies guidelines a, b, & c for pseudonymization and encryption of personal data • **Page 163, Article 34:** If data is encrypted, communication of data breach is not required
Pseudonymizing data in analytics, production warehouse, or non-production systems	HPE SecureData with Format-Preserving Encryption (FPE)	
Encryption and key management for bulk data on server/storage infrastructure	HPE ESKM + KMIP enables storage	
Collaborate to protect and share data over open public networks for legitimate business purposes	HPE SecureMail	

Field level, format-preserving, reversible data de-identification

Customizable to granular requirements addressed by encryption & tokenization

	SST	FPE		
	Credit card **4171 5678 8765 4321**	**SSN/ID** **934-72-2356**	**Email** **bob@voltage.com**	**DOB** **31-07-1966**
Full	8736 5533 4678 9453	347-98-8309	hry@ghohawd.jiw	20-05-1972
Partial	**4171 56**81 5310 **4321**	634-34-**2356**	hry@ghohawd.jiw	20-05-1972
Obvious	**4171 56**AZ UYTZ **4321**	AZS-UD-**2356**	hry@ghohawd.jiw	20-05-1972

NIST SP800-38G – Methods of Format Preserving Encryption

Hewlett Packard Enterprise

GDPR enacted to help protect EU citizen data from risk

New pan European Regulation designed to protect the privacy of EU citizens

Reduces complexity for organizations dealing with Personally Identifiable Information (PII)

Applies also to companies outside the EU that deal with EU citizens' data

Introduces requirements of privacy by design and the 'right to be forgotten'

Enterprises must start preparing for the enforcement data of May 2018

Some exceptions for enterprise with less than 250 employees

The risk of non-compliance

- Fines of up to 4% of parent company annual revenue (max. 20 million Euros)
- Mandatory breach notification within 72 hours unless the PII was encrypted

Hewlett Packard
Enterprise

Thank you

hpe.com/solutions/GDPR

Branislav Makyta

branislav.makyta@hpe.com

"… the opportunity for security software GDPR-related concerns will be $811 million in 2016, rising to $1.8 billion by 2019.

GDPR-related storage software will grow $258 million in 2016 to $1.7 billion in 2019"

IDC, EU Data Protection Reform will Drive Growth in European Software and Storage Market",
By Duncan Brown, Carla Arend and Archana Venkatraman, Nov 2015