A Practical Approach To GDPR
Featuring Duncan Brown, IDC
Agenda

- Logistics
- A Practical Approach to GDPR, Duncan Brown
  - GDPR Readiness
  - The Role of DPO
  - Technology Framework
  - Recommended Timeline
  - Action Plan
- The Atos Approach to GDPR, Zeina Zakhour
- Q&A
Duncan Brown

- Leads IDC’s security research program in Europe
- Broad security expertise including:
  - Incident response
  - Threat intelligence
  - Global privacy
- Established and leads IDC coverage:
  - GDPR
  - RPEC
  - NIS Directive
A Practical Approach to GDPR

Duncan Brown
Associate Vice President, European Security
dbrown@idc.com
GDPR is a game-changer

*Article 58
GDPR is a game-changer

- Fines up to 4% of global revenues
  - “Effective, proportionate and dissuasive”
GDPR is a game-changer

- Fines up to 4% of global revenues
  - “Effective, proportionate and dissuasive”
- Mandatory Breach Notifications
  - Consequential loss of reputation
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…?
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
It is mainly ready now
There is a solid plan in place to ensure readiness by May 2018
We will start addressing it this year (2017)
We are awaiting further guidelines
We really do not know where to start
Not relevant, as GDPR does not affect our organization

Source: IDC EMEA GDPR Survey, March 2017, n=560
GDPR Readiness

Source: IDC EMEA GDPR Survey, March 2017, n=560

© IDC   Visit us at IDC.com and follow us on Twitter: @IDC
GDPR Readiness

57%

43%

- Not relevant, as GDPR does not affect our organization
- We really do not know where to start
- We are awaiting further guidelines
- We will start addressing it this year (2017)
- There is a solid plan in place to ensure readiness by May 2018
- It is mainly ready now

Source: IDC EMEA GDPR Survey, March 2017, n=560
Who leads GDPR?

Source: IDC EMEA GDPR Survey, March 2017, n=560
Who leads GDPR?

Q. In which division or department is the leader based?

- Corporate management: 39%
- IT: 21%
- Finance and accounting: 7%
- Legal: 31%
- Other: 2%

Source: IDC EMEGA GDPR Survey, March 2017, n=560
Who leads GDPR?

Q. In which division or department is the leader based?

- Corporate management: 39%
- IT: 21%
- Finance and accounting: 7%
- Legal: 31%
- Other: 2%

Q. We have established a cross-functional compliance taskforce or governance board?

- Yes: 36%
- No: 64%

Source: IDC EMEA GDPR Survey, March 2017, n=560

© IDC   Visit us at IDC.com and follow us on Twitter: @IDC
The role of the Data Protection Officer

IDC does not provide legal advice
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice

IDC does not provide legal advice
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice
- Applies to controllers & processors
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice
- Applies to controllers & processors
- Requires ‘expert knowledge’ and ‘ability to fulfil the tasks’
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice
- Applies to controllers & processors
- Requires ‘expert knowledge’ and ‘ability to fulfil the tasks’
- In-house or external, full- or part-time

IDC does not provide legal advice
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice
- Applies to controllers & processors
- Requires ‘expert knowledge’ and ‘ability to fulfil the tasks’
- In-house or external, full- or part-time
- No conflict of interest

IDC does not provide legal advice
The role of the Data Protection Officer

- Mandatory for public bodies, and
  - Processing of ‘large scale’ systematic monitoring
- Voluntary DPOs are encouraged as good practice
- Applies to controllers & processors
- Requires ‘expert knowledge’ and ‘ability to fulfil the tasks’
- In-house or external, full- or part-time
- No conflict of interest
- Can’t be fired for ‘performing their duties’

IDC does not provide legal advice
Sourcing a DPO

- Appoint someone from within the organization: 51%
- We already have a DPO in place: 22%
- Appoint a dedicated person from outside the organization: 13%
- Not appoint a DPO: 7%
- Use a contract resource: 7%

Source: IDC EMEA GDPR Survey, March 2017, n=560
GDPR Technology Framework

Information Governance

Meeting Specific Requirements

Review State of the Art
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.
GDPR Technology Framework

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.

- Discovery  Data visibility assessment
GDPR Technology Framework

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.

- Discovery ➔ Data visibility assessment
- Automation is essential
GDPR Technology Framework

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.

- Discovery  ➔ Data visibility assessment
- Automation is essential
- Data loss prevention for real-time classification & protection of data-in-transit
GDPR Technology Framework

Meeting Specific Requirements

RTBF, Consent, Encryption, Data Loss Prevention, Data Portability, Access Control, Record keeping, Incident Response, etc.
GDPR Technology Framework

Meeting Specific Requirements
RTBF, Consent, Encryption, Data Loss Prevention, Data Portability, Access Control, Record keeping, Incident Response, etc.

- Data Discovery, Classification and Control
- Access Control & Identity Management
- Privileged User Management
GDPR Technology Framework

Meeting Specific Requirements
RTBF, Consent, Encryption, Data Loss Prevention, Data Portability, Access Control, Record keeping, Incident Response, etc.

- Data Discovery, Classification and Control
- Access Control & Identity Management
- Privileged User Management
- Encryption and Pseudonymization
- Auditing and Forensics
- Breach Detection and Notification
- Managed Services
Review State of the Art

“appropriate technical and organisational measures”
Encryption, backup & restore, testing, and everything else…
GDPR Technology Framework

Review State of the Art

“appropriate technical and organisational measures”
Encryption, backup & restore, testing, and everything else…

- “Taking into account state of the art…”
- Cost
- Risk
- Context
When to start?

- Normal Business
- Manage

- 2015
- 2016
- 2017
- 2018
- 2019
When to start?
When to start?

Normal Business
- Discover
- Assess

Manage

- MAY 2015
- APR 2016
- JAN 2017
- AUG 2017
- DEC 2017
- APR 2018
- AUG 2018
- DEC 2018
- MAY 2019
When to start?

- Discover
- Assess
- Protect

Normal Business

Manage

- May 2015
- April 2016
- January 2017
- August 2017
- September 2017
- December 2017
- April 2018
- April 2019
When to start?
Manage
Manage

- Select a leader
Manage

- Select a leader
- It’s a program!
Manage

- Select a leader
- It’s a program!
- Stakeholder engagement
- Select a leader

- It’s a program!

- Stakeholder engagement
- Select a leader

- It’s a program!

- Stakeholder engagement

- Visibility
Manage

- Select a leader
- It’s a program!
- Stakeholder engagement

Discover

- Visibility
- Risk exposure
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Impact assessments
Manage

- Select a leader
- It's a program!
- Stakeholder engagement

Discover

- Visibility
- Risk exposure
- Scale of effort

Assess

- Role of Technology
- Impact assessments
- Behaviour changes
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Impact assessments
- Behaviour changes
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Impact assessments
- Behaviour changes

- Access control
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Impact assessments
- Behaviour changes

- Access control
- Data control
- Select a leader
- It’s a program!
- Stakeholder engagement

- Visibility
- Risk exposure
- Scale of effort

- Role of Technology
- Impact assessments
- Behaviour changes

- Access control
- Data control
- Breach response
Executive Brief

GDPR is Coming and There’s Nowhere to Run: A Practical Approach

Sponsored by: Atos and Digital Guardian
Duncan Brown
April 2017

INTRODUCTION

The General Data Protection Regulation (GDPR) represents a substantial increase in business risk to most organizations within the EU and beyond. Companies are faced with a wide variety of decisions, including how to approach the process of becoming compliant with GDPR, the organizational prerequisites, and the introduction of technologies that may enable or hasten compliance.

This IDC Executive Brief provides a short introduction to the main characteristics of GDPR, and proposes a number of technologies that companies should consider in their compliance activities. It concludes with several action points that provide some guidance on essential elements of a compliance program.

GDPR OVERVIEW

The General Data Protection Regulation (GDPR) represents the biggest change to EU data protection and privacy legislation in three decades. The impact on organizations globally is profound, because the risk in dealing with personal data escalates to a level comparable with anti-money-laundering and anti-bribery and corruption legislation. A fine of 4% of global annual revenue is possible, and also introduced are mandatory breach notifications, class-action lawsuits, and the suspension of processing personal data (including employee payroll and customer information), effectively stopping a business from trading.

Why is GDPR so fundamental a change to data processing law? If the substantial penalties for non-compliance are insufficient to demand attention, what about the new requirements? In fact, in principle, there is much commonality between the current legal framework (based on the Data Protection Directive 95/46/EC). But there are some new requirements, such as data portability and the right to erasure (aka the right to be forgotten) that will challenge the information governance processes of any organization however mature. Joint liability between data controllers and their data processors represents a fundamental change in the relationship and responsibilities of companies throughout the supply chain.
Thank you
Zeina Zakhour

- 17 years cybersecurity
- Manages end-to-end spectrum
  - Security advisory
  - Integration
  - Managed security services
  - IoT & big data security
- CISSP
- ISO 27005 certified Risk Manager
Atos approach to GDPR
Journey towards compliance
How to get prepared?
The Journey for GDPR compliance

1. Do you know where the personal data is stored in your organization, Who has access and how data is used/exchanged?

2. Did you identify none-compliance risks related to personal data processing?

3. Did you nominate a DPO (Data Protection Officer) for your organization and does he or she have a clear visibility of all personal data lifecycle?
   - Do your business lines understand the impacts of this regulation? (changes to Data Consent Forms, providing legal forms for access/modification/erasure, running Data Protection Impact Analysis (DPIA) for projects processing personal data?)

4. Are you using cloud service for personal data?

5. Do your suppliers mobilize their efforts to implement compliancy procedures to the regulation? How do they demonstrate compliance?

6. Can you report personal data breaches (stolen personal data) and notify the national authorities within 72 hours?

7. Can you demonstrate the compliance of your organization to the GDPR?
How to get prepared?
A structured and continuous improvement approach

- Incident management
- CERT/CSIRT
- Data breach notification
- People, Process & Information alignment

- Agile architecture
- Security controls (Including data encryption Article 33)
- 24/7 security monitoring
- Audit and penetration testing
- Compliance Reporting

- Consent forms update
- Security by Design & implementation of DPIA
- Provide forms for data access/modification/withdrawal requests

- Personal data mapping
- GDPR Readiness Assessment
- Data classification
- Data Protection Impact Assessment

- Contractual commitment update (New/old)
- Define organisational and technical controls
- Update SLAs for GDPR compliance follow-up
- Auditability and Traceability of access, data flows
Atos & Digital Guardian
GDPR Readiness Assessment

▶ 30-day software guided data security consulting assessment
▶ Data at Rest Assessment
  ▶ Discover personal data across network shares, databases and cloud storage
▶ Data in Motion Assessment
  ▶ Identify sensitive content leaving your network (web and email)
▶ Detailed report on data protection risks & recommendations
▶ Requires no additional customer resources

GDPR Data in Motion by Channel by Policy (Incidents)
Atos & Digital Guardian
Locate Personal Data & Gaps with GDPR
GDPR Governance
Shared responsibility on GDPR compliance

Data Controller
- Monthly discussion, reassessment and adoption of measures (aligned process for change requests and cost impact)
- Monthly Reporting
- Operate Controls and defined services
- Define Metrics / KPI
- Define Data Location / Restrictions / Controls / Contractual agreement
- Risk Assessment

Data processor
- Create Data Catalogue
- Visibility study to identify personal data

Technology Catalog
- IAM / PAM
- Data Encryption
- Data Masking
- SIEM/IM
- CSIRT
- Data Breach Notification Process
- Data Breach Emergency Process

IT Managed Services data processing
# GDPR Data Protection Controls
## Security Service Packages

### GDPR Data Protection
- AHPS (Log Management)
- AHPS (Detection & Monitoring)
- Access Control (Privileged Account Management)
- Access Control (IAM)
- Data Encryption/Masking
- Data Loss Prevention
- Behavior Analytics
- Threat Intelligence

### GDPR Reporting
- GDPR KPI setting & reporting automation
- GDPR Compliance Dashboard

### GDPR Response
- CISO Processes Interface
- CISO Processes Interface
- DB – Notification readiness
- DB – Notification exec
- DB – Forensics
- DB – Insurance
Intelligence Driven Security Management
For GDPR Compliance
You cannot protect what you don’t see

GDPR compliance is a journey towards a secure & efficient data management lifecycle
You cannot protect what you don’t see

GDPR compliance is a journey towards a secure & efficient data management lifecycle

Break the Silos
GDPR compliance is a journey towards a secure & efficient data management lifecycle

You cannot protect what you don’t see

Adopt Purpose Driven Data Collection

Break the Silos
You cannot protect what you don’t see

Think Extended Enterprise

GDPR compliance is a journey towards a secure & efficient data management lifecycle

Break the Silos

Adopt Purpose Driven Data Collection
GDPR compliance is a journey towards a secure & efficient data management lifecycle

You cannot protect what you don’t see

Think Extended Enterprise

Adopt Auditable & Controlled Data Processing

Adopt Purpose Driven Data Collection

Break the Silos
GDPR compliance is a journey towards a secure & efficient data management lifecycle

Think Extended Enterprise

You cannot protect what you don’t see

Adopt Auditable & Controlled Data Processing

Update your Risk Assessment matrix

Adopt Purpose Driven Data Collection

Break the Silos
You cannot protect what you don’t see

Adopt Auditable & Controlled Data Processing

Update your Risk Assessment matrix

Think Extended Enterprise

Adopt Purpose Driven Data Collection

Break the Silos

The challenge is not to be ready on May 25th 2018 but to remain compliant thereafter...
Questions & Answers
Thank You

For more information please contact:
security@atos.net