GET UP TO SPEED ON GDPR FAST

Rashmi Knowles CISSP
Field CTO EMEA
RSA
Sometimes the **FASTEST WAY DOWN** is to jump off a cliff.
What is the EU General Data Protection Regulation (GDPR) & what impact will it have?

**What Is it?**

- Replaces EU’s Data Protection Directive with one EU regulation and is effective 25 May 2018
- **Significantly increases penalties** for violations—potential fines of up to Euro 20M or 4% annual turnover
- **Definition of personal data**—is broader, includes online identifiers for example
- Much of what is included was in former Directive but some new requirements

**Scope**

GDPR applies to controllers & processors established **within** the EU & **outside** the EU where:
- they offer goods & services to individuals in the EU or
- their processing includes the monitoring of individuals’ behavior within the EU, **thus substantially increasing those who are covered**
- Processors will have additional obligations that were previously reserved for controllers
<table>
<thead>
<tr>
<th></th>
<th><strong>Companies Must Also...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tell individuals how their personal data will be used</td>
</tr>
<tr>
<td>2</td>
<td>Grant individuals access to correct or erase their personal data upon request</td>
</tr>
<tr>
<td>3</td>
<td>Comply with requests from individuals to stop using their personal data for marketing</td>
</tr>
<tr>
<td>4</td>
<td>Keep personal data secure</td>
</tr>
<tr>
<td>5</td>
<td>Make sure staff are appropriately trained in the care and handling of personal data</td>
</tr>
<tr>
<td>6</td>
<td>Put data processing agreements in place to ensure third party vendors follow the same protective rules</td>
</tr>
<tr>
<td>7</td>
<td>Notify regulators and/or affected individuals in the event of a serious data breach (usually within 72 hours)</td>
</tr>
<tr>
<td>8</td>
<td>Limit transfers of personal data out of the European Economic Area to only those that comply with EU international data transfer rules</td>
</tr>
<tr>
<td>9</td>
<td>Build privacy compliance into product, software and services design, processing tools and system development</td>
</tr>
</tbody>
</table>
Who’s who in GDPR

- EU Data Protection Board
- Data Protection Authority (member state)
- Data Protection Officer
- Data Controller
- Processor
- Third Parties
- Data Subject

Security of Data

Rights and Duties
Where Are We Today?
Which of the following statements best describes the current state of GDPR compliance operations in your organization?

- **42%** Driven by a small team of managers and directors
- **18%** Advanced security and risk program driven by a DPO
- **13%** Driven by legal counsel; approach GDPR mainly as a legal issue
- **6%** Delegate to individual business units
- **21%** Established security and risk program driven by a CISO or CRO

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017
Polling Question #1

Who is driving your organization towards GDPR?

- CISO
- CIO
- Compliance Team
- Other
How involved are the following teams in driving your organization toward GDPR compliance?

<table>
<thead>
<tr>
<th>Team</th>
<th>Participation Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>53</td>
</tr>
<tr>
<td>PRIVACY</td>
<td>41</td>
</tr>
<tr>
<td>INFRASTRUCTURE &amp; OPERATIONS</td>
<td>39</td>
</tr>
<tr>
<td>MARKETING &amp; OTHER BUSINESS UNITS</td>
<td>36</td>
</tr>
<tr>
<td>LEGAL</td>
<td>34</td>
</tr>
<tr>
<td>PROCUREMENT/THIRD-PARTY VENDOR MANAGEMENT</td>
<td>33</td>
</tr>
<tr>
<td>CUSTOMER EXPERIENCE</td>
<td>29</td>
</tr>
<tr>
<td>HUMAN RESOURCES</td>
<td>15</td>
</tr>
</tbody>
</table>

- Final decision maker, owns the entire process and is highly involved
- Key contributor, has significant involvement in driving the process

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017
What is your organization’s timeline for achieving full GDPR compliance across the following requirements?

- **Breach response**: 50% Yes, we’ve named a data protection officer, 20% We have plans to name a DPO or have no plans to name a DPO
- **Compliance program management**: 48% Yes, we’ve named a data protection officer, 27% We have plans to name a DPO or have no plans to name a DPO
- **Risk management**: 46% Yes, we’ve named a data protection officer, 21% We have plans to name a DPO or have no plans to name a DPO
- **Data governance**: 39% Yes, we’ve named a data protection officer, 29% We have plans to name a DPO or have no plans to name a DPO

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017
Percent of those **very confident** about what the company has in place to comply with GDPR requirements

53% Technologies

43% Processes

39% Policies

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017
A recent PwC pulse survey asked C-suite executives from large American multinationals about the state of their plans for GDPR. The “pulse” revealed:

- Over half of US multinationals say GDPR is their top data-protection priority
- Information security enhancement is a top GDPR initiative
- 77% of survey respondents plan to spend $1M or more on GDPR

Source: “GDPR Preparadness Pulse Survey” published by PwC – January 2017
40% of organizations will be in violation of the GDPR by 2020; this is expected to be near zero by 2023.

Gartner
GDPR is an Opportunity

- Drive real value from your data
- Come to grips with Consent!
- Create new Governance Models
  - Data Management Policies
  - Data processes
- Build trust with customers/consumers
- Revisit security
- Employee skills, access management
Beyond compliance benefits, what do you see as the business advantages of becoming GDPR-compliant?

- **53%** Improved customer experience
- **47%** Improved data strategies
- **45%** Better privacy policy management
- **42%** Efficient practices for data governance and privacy
- **40%** Greater operational efficiency
- **37%** Better KPIs and metrics for data security and privacy
- **36%** Enhanced design of analytics projects
- **35%** Address growing customer expectations for privacy

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017
Biggest Concerns in Achieving Compliance

- Business Process Change
- Detecting, protecting and responding to....
- Implementation costs
- Infrastructure change
- Loss of customer confidence/productivity
- Policy Complexity
- Revealing sensitive data/protecting data
- Possible fines...
GDPR: Fact or Fiction?
Record Keeping & Demonstrating GDPR Compliance – Who cares

Rights of the Data Subject – Does this matter?

To comply with GDPR we should encrypt everything...
GDPR Compliance – Is this optional? **FICTION!**

Data Location is irrelevant **FICTION!**

A DPIA must always be conducted... **FACT!** **FICTION!**
All Personal Data Breaches Results in a Fine  

**FICTION!**

You Must Notify the Supervisory Authority of a Personal Data Breach Within 72 Hours  

**FACT!**
Four Key Areas to get Started
Four Steps to GDPR Planning

Primary objective:
Detect and respond to the threat *before* a breach occurs but if a breach *does* occur, you need to know the details and exact impact.

Primary objective:
Know where data is in the enterprise and who has access and implement controls in data processing activities.

Primary objective:
Establish a risk assessment process to ensure controls are appropriately designed and implemented.

Primary objective:
Establish a compliance program to ensure controls are effective and operational.
Polling Question #2

Considering these four requirements – How is your organization prioritizing each?

- Risk Assessment
- Breach Response
- Data Compliance Management
Working to a Plan

Does your organization process, store or handle personally identifiable information (PII)/Personal Data (OR plan to)?

Are you affected?

Yes

Does any of this PII include EU residents including customers and/or employees?

Have you initiated a project around GDPR?

Have you performed a risk assessment or analysis with regards to GDPR?

Which area(s) concern you the most?

No

Educate on GDPR

What is your strategy for identifying and responding to data breaches?

How do you manage your risk of advanced cyber threats and attacks?

Breach Response

What steps towards automation have you taken to reduce “breach exposure time?”

What is your strategy to ensure access to personal information is proper and controlled?

Data Governance

How do you establish policies around data governance?

Do you have an accurate data processing catalog?

Risk Assessment

Where does data privacy fit into your risk management strategy?

How does your organization handle risk assessments in general?

Compliance Management

How do you catalog data and associated custodians & regulatory requirements?

How do you identify, prioritize and track compliance issues?

How does your organization handle compliance in general?

DON’T FORGET ABOUT THIRD PARTIES...

Build your plan.

Stop (maybe)
Polling Question #3

Do you use Third Parties to process or store EU resident data?

YES  NO
Breach Readiness

Data Governance

Risk Assessment

Compliance Management

KEY INGREDIENTS
The Journey Forward
Take Command of your Journey

Siloed
Streamline compliance, Build business context & reporting

Managed
Expand risk focus, Improve analysis & metrics

Advantaged
Connect risk and the business with cross functional processes

The Maturity Journey

Meet
Compliance requirements

Address
known & unknown Risks

Enable
new business Opportunities

Time
Steps to Take Now

1. Raise Awareness
2. Understand Personal Data
3. Communicating Privacy Info
4. Individual’s Rights
5. Subject Access Requests
6. Legal Basis for Processing Data
Steps to Take Now

7. CONSENT
8. CHILDREN
9. DATA BREACHES
10. PRIVACY BY DESIGN PROCESS
11. DATA PROTECTION OFFICERS
12. INT’L SUPERVISORY AUTHORITY
Sometimes the **FASTEST WAY DOWN** is to jump off a cliff
THANK YOU