GDPR ESSENTIAL ENFORCEMENT: WHEN WILL THE BIG SCARY FINES HAPPEN, AND HOW DO YOU AVOID THEM?

Pierre-Luc REFALO
Global Head of Cybersecurity Consulting & GDPR Services
Capgemini
@plrefalo
GDPR is not a matter of Laws and Techs. It’s more important than that!
Always the same old long story…

« You must be tough
When defining
the laws.
You must be
indulgent
When applying
the laws. »

« The cristal clear
laws are often a
nightmare to
implement. »
Agenda

- WHEN Enforcement can / could happen
- HOW Enforcement will / could start
- WHY Enforcement actions will / should target you
- HOW you should avoid the big fines
What if you don’t understand what to do, when and how … And did not do…

**Timeline**
- Adopted in April 2016
- Comes into force May 25th 2018

**Scope**
- All EU and foreign companies processing data of EU citizens

**Principles**
- Citizen regain control of personal data
- Harmonise national data protection regimes

### Key Concepts
**Personal Data Protection GDPR reinforces concepts**
- ✔ Consent
- ✔ Processing limitation
- ✔ Right to be forgotten
- ✔ Protection of minors
- Genetic
- Mental
- Cultural
- Economic
- Social
- ✔ Right to data portability
- ✔ Complaint management
- ✔ Right to compens. & liability
- ✔ Profiling

### Key Implications
**Principle of Accountability**
- ✔ Data Protection Officer
- ✔ Processing record
- ✔ Controlling and monitoring
- ✔ Processor
- ✔ Extraterritoriality
- ✔ Tech & Org. Measures
- ✔ Privacy by design
- ✔ Privacy Impact Ass.
- ✔ Cross-border processing
- ✔ Data breach notification

**Fines of up to 20 million euros or 4% of world wide annual turnover**

**Authority can issue instruction to cease processing**

**Non-compliance can lead to loss of brand reputation and trust**

privacy for customers, accountability for enterprises, power for regulators
All organizations are not on the same boat...
How enforcement can / could start?

Basic scenarios

All lead to DPAs
WHY Enforcement actions will / should target you?
Art. 83 describes criteria to be analyzed in case of infringement
Infringement of the Regulation should lead to the imposition of “equivalent sanctions”. Like all corrective measures chosen by the supervisory authorities, administrative fines should be “effective, proportionate and dissuasive”.

HOW TO AVOID THE BIG SCARY FINES?

The big scary fines for big organizations handling big volume of data

Not only! Reputation + Operations and small organizations are in the scope too
Apply what the DPAs recommend Guidelines and tools

Guidelines and tools

European Data Protection Board

Art. 29 working party
Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679
Adopted on 3 Oct. 2017

Capgemini
11 assessment criteria of infringements (Art.83) leading to warnings, reprimands or fines

(a) the nature, gravity and duration of the infringement
(b) the intentional or negligent character of the infringement
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of the personal data affected by the infringement
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement
Simplification: 12 basic solutions are needed to demonstrate compliance

<table>
<thead>
<tr>
<th>Consent and Individuals’ Rights Management</th>
<th>Obligations regarding Processing</th>
<th>Organizations’ Accountabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights Mgmt</td>
<td></td>
<td>DPO Organization &amp; Documentation</td>
</tr>
<tr>
<td>Consent Mgmt</td>
<td>Data Discovery</td>
<td>Data Protection Register Mgmt</td>
</tr>
<tr>
<td></td>
<td>Data Protection Impact Assessment</td>
<td>Processor and 3rd Party Mgmt</td>
</tr>
<tr>
<td></td>
<td>Data Lifecycle Mgmt</td>
<td>Breach Mgmt and Reporting</td>
</tr>
<tr>
<td></td>
<td>Data Protection (Encryption, Pseudonomizing, …)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identity and Access Mgmt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data leak Prevention</td>
<td></td>
</tr>
</tbody>
</table>
Build a consistent plan to cover the full GDPR playing field
Digital GOVERNANCE

3 duos and 6 stakeholders to be onboarded

CDO / DRO
CDO / DPO
CIO / CISO
Agile Organization and Acculturation
Platform based to manage digital risks for Data & People

Digital Risk Management

(Cyber) Security

Privacy

Safety

Continuity

(Physical) Security
Build GDPR automated services to ... Demonstrate how you run effective compliance

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **1** | **GDPR Assessment Services**  
Program Scoping, Deep Dive Assessment, Data Protection Impact Assessment |
| **2** | **GDPR Program Services**  
Data Protection Register management, Awareness & Change management, Program coordination and follow-up (incl KPI’s, Risk and reporting), DPO Organization & Tooling, Processor and third party management, GDPR organization, methodology and procedures |
| **3** | **Data Discovery Services**  
Data discovery services |
| **4** | **Data Lifecycle Services**  
Data retention and data disposal |
| **5** | **Consent & Individual’s Rights Mgmt Services**  
Consent management, Individual’s rights management |
| **6** | **Pseudonymizing Services**  
Pseudonymizing Services |
| **7** | **Data Protection Services**  
Identity Access Management & Identity as a Service, Data & Database Security |
| **8** | **Breach Management & Reporting Services**  
Security Operations Center as a Service, Data Leak Prevention as a Service |
| **9** | **GDPR Assurance Services**  
Data Breach Simulation, GDPR compliance tracking, Application security & privacy testing, DPA Visit Simulation |
Be prepared for incident and breach management
CONCLUSION

May 25th is just the beginning!

Build digital trust with automated solutions for GDPR.
Next week you should:
- Control your GDPR compliance journey is running (governance, program, data processing accountability incl. third parties, register, trainings, incident & breach management, security audits & controls)

In the first three months following this presentation you should:
- Have minimized personal data of EU citizens handled in your systems (incl. data processors) in the long term (Data lifecycle management)
- Have controlled implementation of basic security solutions such as vulnerability & patch management, encryption and access control to personal data (privileged users, DB monitoring, transfers, etc.)
- Have tested incident / breach management procedures

If not in place or launched, within six months you should:
- Industrialize a data masking / pseudonymization process
- Develop a “application security & privacy testing” process
- Transform your “infra” based SOC into an “application & data leak” monitoring platform