RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCS-T06

EU General Data Protection Regulation (GDPR): Compliance, Security for Non-EU Firms

Giampiero Nanni

Government Affairs EMEA
Symantec Corporation
@GiampieroNanni

#RSAC

GDPR: A new dawn for personal data protection

Agenda

- GDPR Overview
- Why GDPR matters to this Region
- How to get compliant. Why cyber security.
- Q&A

GDPR Principles

- The General Data Protection Regulation (GDPR) applies to all companies trading in the EU and processing personal data of EU Residents
- GDPR can become the global standard of data governance
- GDPR harmonizes privacy law in all EU Member States
- GDPR comes to effect on 25th May 2018
- Fines up to 4% global annual turnover

GDPR Principles

- Always think user/data subject first
- Understand what personal data you process
- Know where it is and how it flows in the organisation
- Consider privacy at every level
- Review your information risk management
- Ensure you have appropriate mitigations in place
- Don’t forget detection and response planning
- Ensure you can demonstrate compliance

Key Stakeholders

DATA CONTROLLER

DATA PROCESSOR

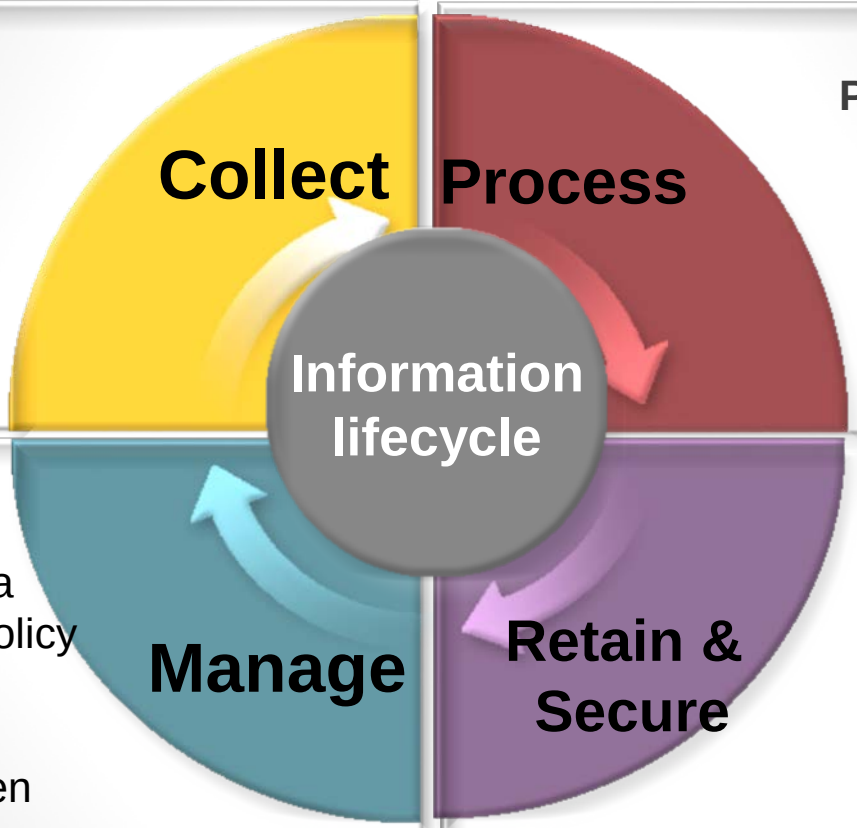
DATA SUBJECT

DATA PROTECTION OFFICER (DPO)

DATA PROTECTION AUTHORITY

GDPR relates to Data Governance

Principles of data collection
- Fairly and lawfully
- Receiving consent
- Relevance
- Proportionality
- Types of data



Permission applies to:
- Specific data
- Specific purpose
- Notify of changes

Management of:
- Access
- Right to rectify data
- Data destruction policy
- Data transfers
- Applicable rules
- Right to be forgotten

Retain
- Duration
- Types of data

Secure
- People
- Process
- Technology
- Data loss

Privacy most important criteria for customers

From the Symantec State of Privacy Report 2015

Symantec State of Privacy Report 2015

https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

Scope of the GDPR

Defines Personal data

Legal basis for processing

Embedding privacy

Data security

PROTECT PERSONAL INFORMATION THROUGH ITS LIFECYCLE

Key drivers

Accountability

Information Security

Cloud and International Data Transfer

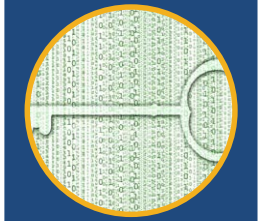
Penalties for Breaking the Law

PROTECT PERSONAL INFORMATION THROUGH ITS LIFECYCLE

Accountability

Information Security

Improved Security Requirements



Encryption and ID management

Information Security a Legitimate Interest

Requirement to Secure Private Data

Effective Detection and Response

PROTECT PERSONAL INFORMATION THROUGH ITS LIFECYCLE

Symantec

Fines and penalties

Up to **€20m** or **4%** of Global Annual Turnover if bigger

Enforcement by National
Data Protection Authorities

GDPR: collateral benefits

Legitimate concerns

- Severe sanctions, large fines
- Stringent compliance requirements
- Corporate image at risk
- Compliance needs frustrate technological choices
- Negatively effects on labor relationships
- Negatively impacts customer/business relationships, marketing, data processing, global outsourcing, cloud computing, etc

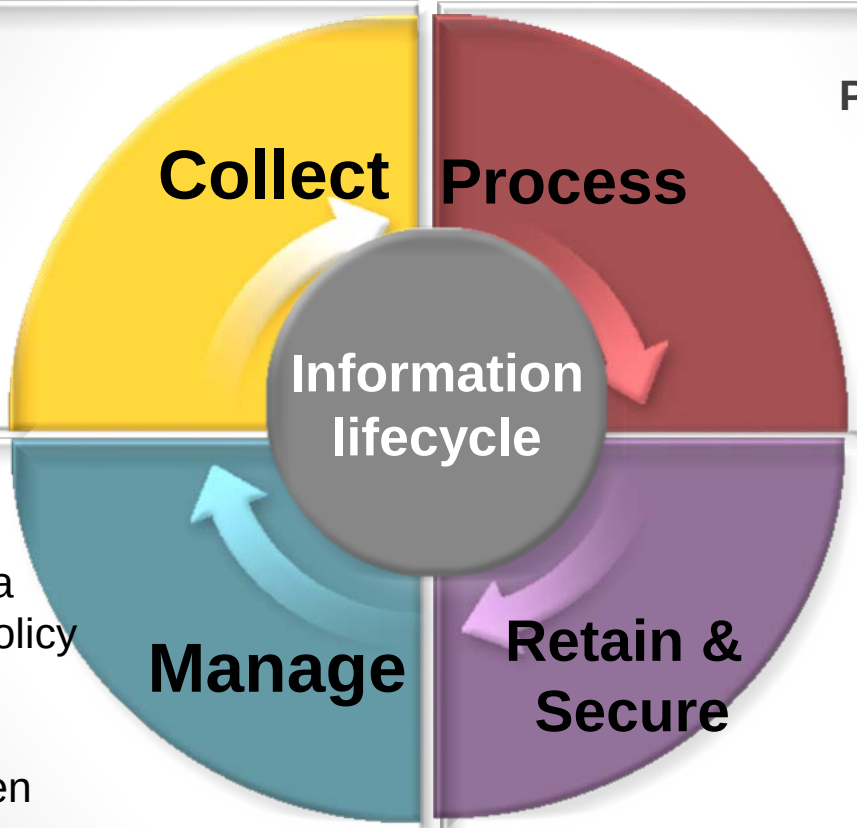
True spirit and benefits of GDPR

- ✓ Positive enhancement of data security (including other areas, like IP)
- ✓ Avoids financial losses (data breaches are costly)
- ✓ Prevents reputational problems
- ✓ Improves brand image
- ✓ Encourages investors/partners' attitude
- ✓ Reduces illegal data trafficking
- ✓ **Customers want more confidentiality and personal data protection**

Symantec

GDPR relates to Data Governance

Principles of data collection
- Fairly and lawfully
- Receiving consent
- Relevance
- Proportionality
- Types of data



Permission applies to:
- Specific data
- Specific purpose
- Notify of changes

Management of:
- Access
- Right to rectify data
- Data destruction policy
- Data transfers
- Applicable rules
- Right to be forgotten

Retain
- Duration
- Types of data

Secure
- People
- Process
- Technology
- Data loss

Protecting Information across the Lifecycle

Collect	Process	Retain-Secure	Manage
Define and locate personal data	Detect and block threats to data in use	Restrict processing of data you have to retain	Risk management throughout lifecycle
Secure devices that collect personal data	Privacy impact assessments	Prevent data loss	Validate data subjects invoking rights
Record consent from data subjects	Validate data processors	Respond to incidents	Enable DPOs to assess cyber risk
Secure transfer and storage of collected data	Document processing activities	Protect data at rest	Train, educate staff who handles personal data

Solution mapping (Sample)

Articles	Provision/ Requirement	What it means for the customer	How to implement (With the help of internal and external resources)	Technology
Article 4(1), recitals 26 and 30	Definition of personal data	You need to know perfectly your information assets, know exactly what data is personal data, what data is not, be able to segregate it and handle it accordingly. Are personal data: all your HR data, your client/customer data, your prospect/direct marketing/targeted advertising data, and also pretty much all the IT activities of your personnel (emails, browsing history, logs, login credentials, etc).	Analyse the complexity of your datasets, the location and the flows of personal data. Select and deploy relevant technology.	Data mapping tools
Articles 5(2), 24, Recitals 74, 77, 78, 82	General principle of accountability of data controllers	Controllers must take every technical and organizational measure appropriate to ensuring and demonstrating compliance.	Analyse the relevant technical and organizational measures especially around information protection, information security and incident response, track and document the implementation and the effectiveness of your policies.	Compliance monitoring and documentation of policy implementation tools
Article 25	Principles of Privacy by Design, Privacy by Default	From the very first moment you process personal data, you should make sure you have taken every step to protect privacy and data. This includes adequate risk-based security around any personal data assets and personal data processing operations you have. This is also covered by the notion of “Accountability” (above).	Assess and define what is your IT risk profile and what would be the appropriate security measures for your data assets and processing, so that you can “do the right thing” at all times, i.e. be an accountable data custodian for your employees, customers, consumers, clients, patients, partners, etc.	N/A

GDPR Compliance Questionnaire (Sample)

Art.	Process question	Level 0	Level 1	Level 2	Level 3	Level 4
4(5), 11, 32(1)(a)Rec 26	Do you apply pseudonymization and anonymization to personal data you hold, so as to minimize exposure to privacy risk?	I don't know how to do that	I know about those concepts but I don't think they are relevant to us	We only implement pseudonymization and anonymization when specifically asked to do so	We integrate pseudonymization and anonymization in most of our processes when convenient	We apply them wherever possible, including technical controls to prevent the reversal of pseudonymization or anonymization
28	Do you follow a clear selection process to choose the suppliers who process personal data for you?	I don't think we use any suppliers to process data on our behalf	We try to aim for cost efficiency and ease of use	We try to use only large reputable vendors	We select specialized vendors with references and certifications specific to our needs	We thoroughly vet eligible candidates and select those which offer all of the guarantees required by the GDPR
46, 47, 48, 49	Do you implement mechanisms to ensure that any export of personal data outside of the European Economic Area is compliant with EU privacy law?	I am not aware that we export any personal data out of Europe	If we do any export at all, we trust our contractors to do what's required	We only export data to countries we have reasons to believe are safe	We make specific approved arrangements for every particular case	We have a structured streamlined and documented process to legally transfer data outside of the EEA
15	Do you enable individuals to get access to personal data you hold about them?	No, the data is ours, I don't see why we should	Maybe we can do that if we get asked to	In general, if it's not unreasonable, we try to be helpful when people ask	Yes, to the extent that we are able to figure out which data belongs to the person who's asking	Yes, we have a contact point and a process to respond swiftly, giving all relevant information as required
21	If an individual withdraws consent or raises an objection to what you are doing with his/her data, are you able to immediately stop processing that data?	No, individuals don't have a means to object in that way	If the individual can justify the request, we could probably try to accommodate	To the extent that the objection looks reasonable to us, we will consider it	Unless it is excessively cumbersome to do, we will normally respect such objections	Yes, we inform people of their right to object, we provide them means to do it, and we are able to stop processing unless we can demonstrate a compelling need for us to carry on

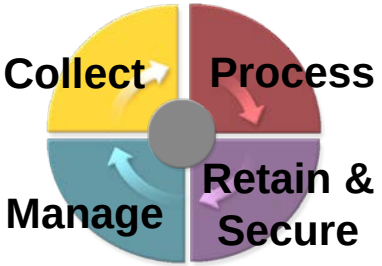
How security technology can help

- The GDPR is a legislation about data protection
- The GDPR is NOT a legislation about cyber security
- However, cyber security technology is required in order to be compliant, and can help to achieve compliance, and this is how:
  - Governance and accountability of policies
  - Implementation of policies, record keeping and reporting
  - Management of identities and authentication
  - Data and infrastructure security (e.g. encryption, data loss prevention)
  - Data breach notification and Incident response
  - Cloud security and cloud management

“Apply” Slide

- **Next week you should:**
  - Assess whether GDPR applies to your organization:

    Do you process personal data of EU Residents?
- **In the first three months following this presentation you should:**
  - If so, identify and select legal, consulting and technological partners
  - Understand what personal data you process, know where it is and how it flows in the organisation (with an eye to the supply chain ecosystem)
  - Understand what business or internal processes are involved in the Governance of Personal Data
  - Identify relevant stakeholders
  - Review your information risk management
- **Within six months you should:**
  - Put in place detection and response planning
  - Select security technology that can map and protect personal data, and drive the compliance journey
  - Ensure you can demonstrate data protection and mitigations features



Thank you

Q&A

Giampiero Nanni
Government Affairs EMEA
giampiero_nanni@symantec.com
+44 780 8248100
@Giampieronanni

Symantec