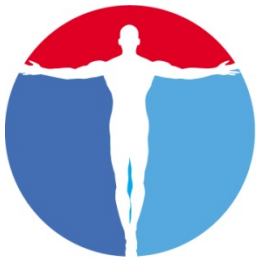


APDL

Association pour la Protection des Données au Luxembourg

GDPR: STEP BY STEP TOWARD COMPLIANCE

VINCENT WELLENS

KEEP CALM AND prepare for GDPR

18 months to comply

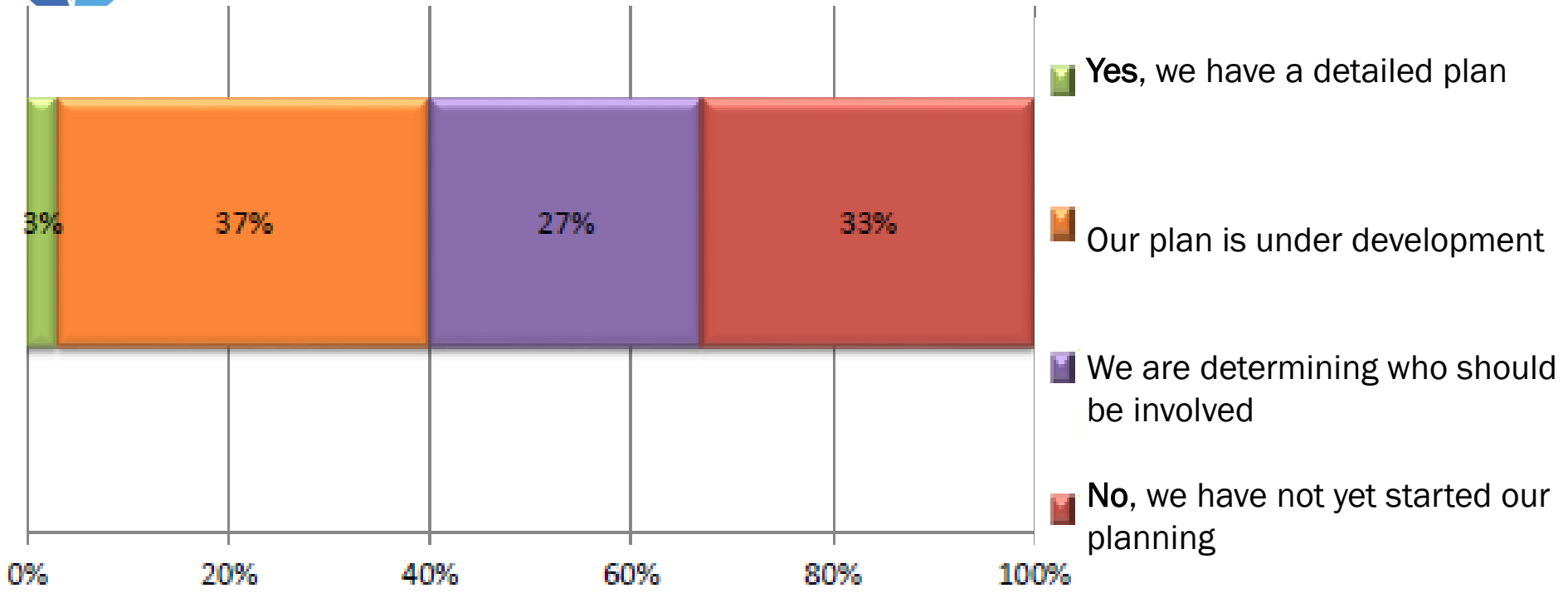
14 April 2016

Adoption

25 May 2018

Entry into force

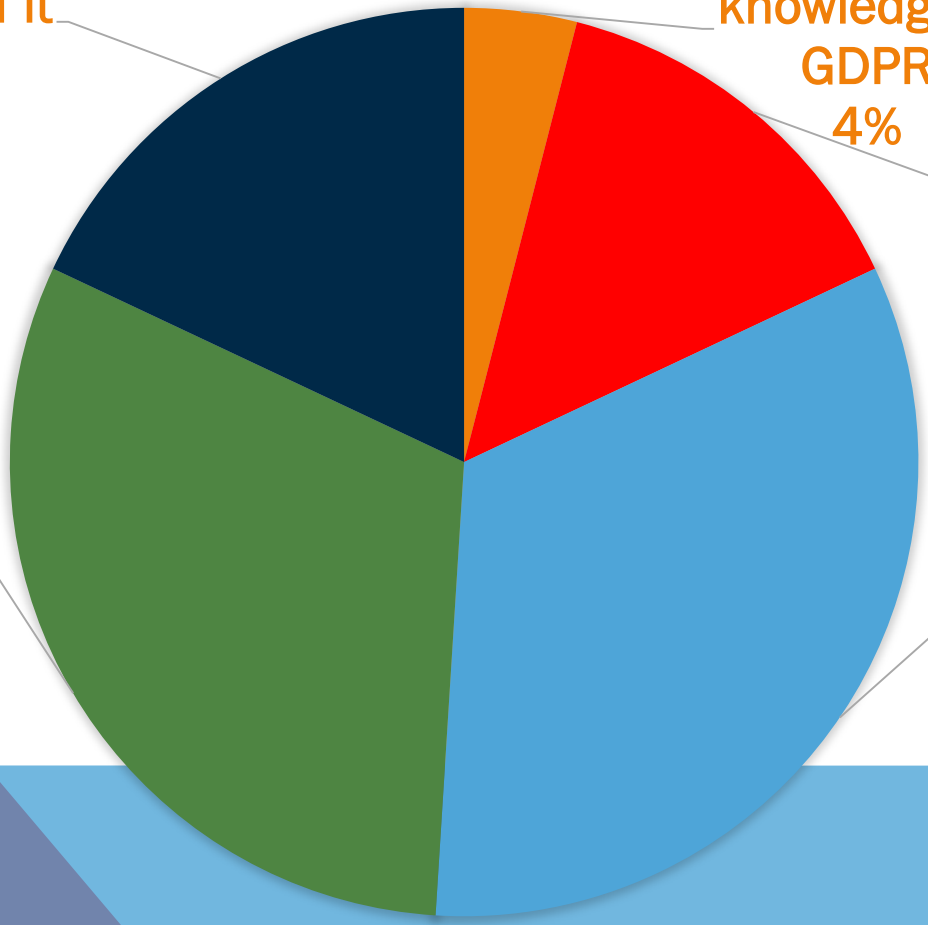
DO YOU HAVE A PLAN TO PREPARE YOURSELF?



Dimensional research – Sponsored by: DELL
Septembre 2016

Only 3% of organisations have a plan. Do you?

HOW WOULD YOU DESCRIBE YOUR KNOWLEDGE OF GDPR?



Dimensional research -- Sponsored by: DELL
Septembre 2016

SYMANTEC / STATE OF PRIVACY REPORT 2015

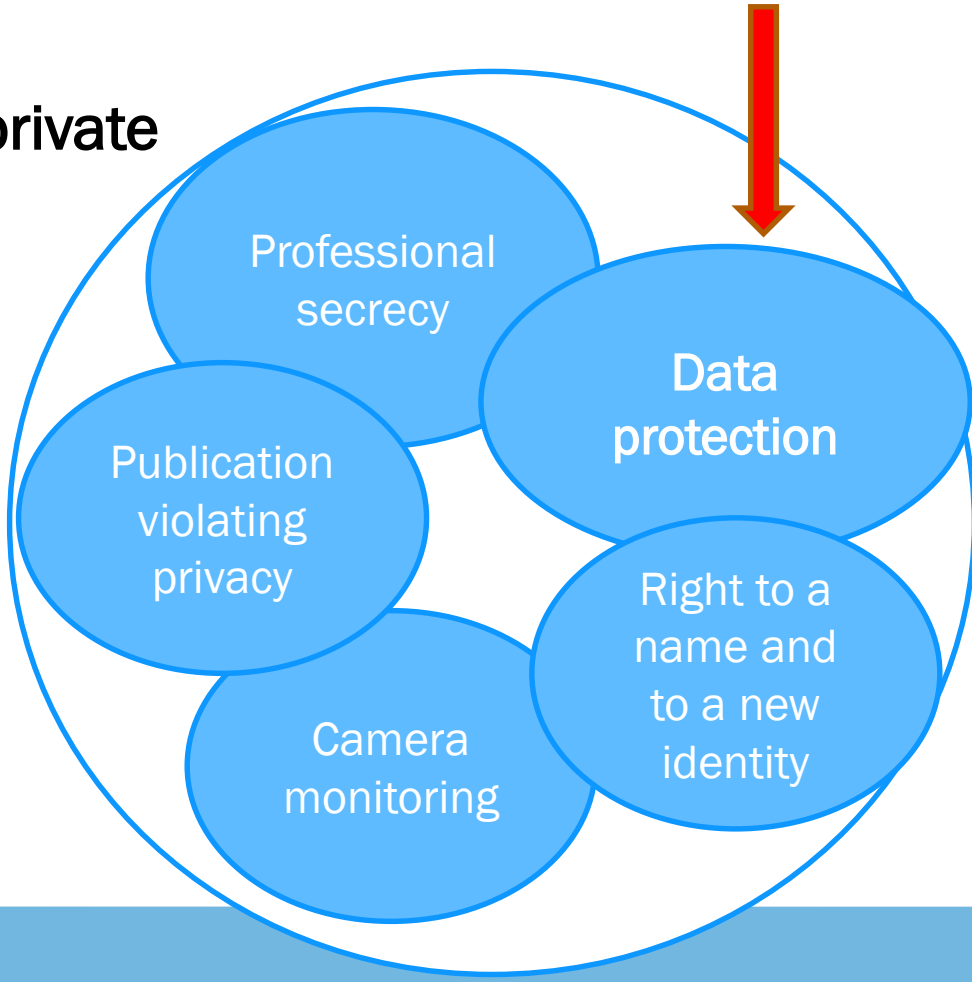
- Definitions
- Get ready in 10 steps
- Conclusion

PRIVACY

Right to respect for his/her private and family life

What:

- You do in your private life
- You do at home
- You write in your letters or emails
- You say over the phone



DATA PROTECTION

What is meant by data « protection »?

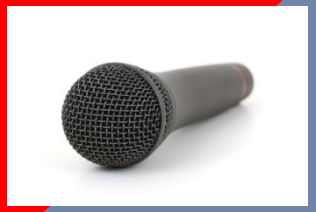
- ✓Protect the rights and freedoms of the individual
- ✓Fundamental right of the individual to know that their personal data is protected

PERSONAL DATA

… Any information relating to an identified or identifiable natural person …

… Directly or indirectly …

Biometric, genetic, health-related data



Ref: Art. 4

SPECIAL CATEGORIES OF PERSONAL DATA

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- genetic data
- data concerning health
- data concerning a natural person's sex life or sexual orientation
- ...

Ref: Art. 4

DONNÉE À CARACTÈRE PERSONNEL

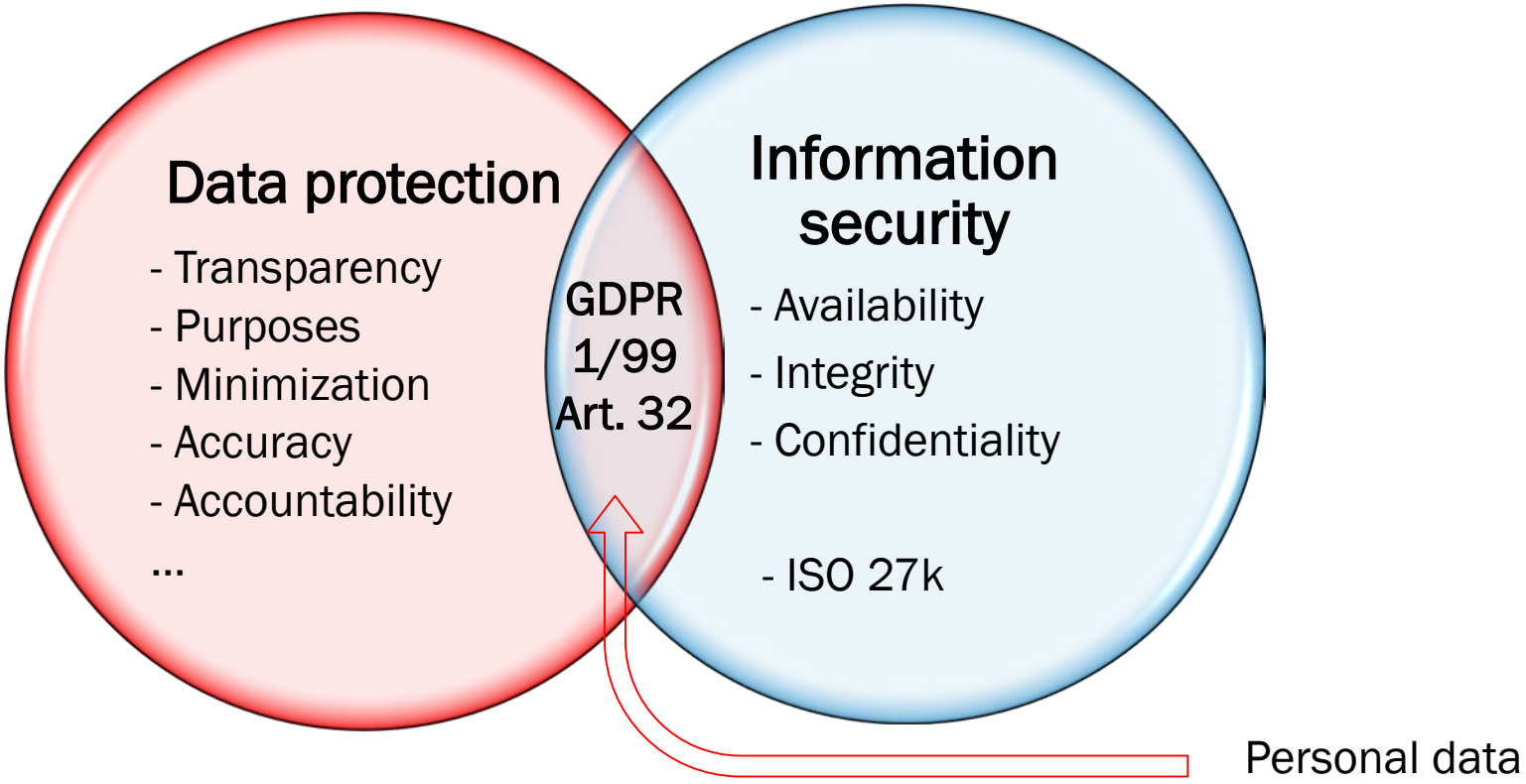
Data collected for the purchase of an airline ticket (online):

- Name, physical address, telephone number, email
- Passport number/ identity card
- Coming and goings (visited countries, length of stay, accompanying person, etc.)
- IP address (dynamic or not)

Special category of collected data (art. 9):

- Allergies
- Illness
- Support needs (wheelchair, handicap, etc.)

DATA PROTECTION *AND* SECURITY



Data protection ≠ security

SECURITY OF PROCESSING

Article 32

Implement appropriate technical and organizational measures in order to ensure a level of security appropriate to the risk, including:

- pseudonymisation and encryption
- constant confidentiality, integrity, availability and resilience of systems and processing services
- restore the availability of personal data and access to it
- processes in order to test, analyse and evaluate regularly the effectiveness of technical and organizational measures to ensure security of processing

Consider:

- Implementation costs
- Nature, scope, context and purposes of the processing
- Risks (degree of probability and seriousness changes)

Ref: Art. 32

DATA PROCESSING

... Any operation or set of operations...

... Performed or not by automated means...

...Performed on personal data or on sets of personal data...

Collection, use, disclosure, storage, destruction, recording, organization, structuring, storage, alteration, retrieval, consultation, use, restriction, ...

Ref: Art. 4

DATA PROCESSOR

Data controller

- Natural or legal person, public authority, agency or other body
- Determines the purposes and means of the processing of personal data

Data processor

- Natural or legal person, public authority, agency or other body
- Processes personal data on behalf of data controller

Mandatory written contract between two parties

Ref: Art. 4

ARE YOU DATA CONTROLLER OR DATA PROCESSOR?

Practical exercise

- Discussion 3 minutes
- Group of 2-3 persons
- Explain, for your core business, if you are data controller or data processor

Definitions

Get ready in 10 steps

Conclusion

STEP 1: AWARENESS

Meet	Key people and decision-makers
Inform	➢Major changes to come ➢Key concepts acquired during this information session
Provide	➢Enough time! ➢Sufficient budget ➢Sufficient resources (internal or external) ➢A multidisciplinary team to build the compliance plan ➢Training of employees who process personal data

It is crucial to get the **management support** to implement a compliance plan!

STEP1: AWARENESS

Major changes

- Strengthened right of data subjects – transparency
- Territorial scope: companies outside the UE when they offer goods or services on the European market or monitor the behaviour of European residents
- Abolition of notifications and authorizations:

➔ Obligation to demonstrate compliance with GDPR and to document the implemented measures

❑ Severe penalties (art. 83)

- 2% to 4% of the company's annual turnover;
- 10 or 20 million EUR for the other organizations

STEP 2: RECORDS OF PROCESSING ACTIVITIES

Identify and review all your data streams (customers, employees, etc.)

What type(s) of data is collected and stored? Special category?

What is the retention period?

Where does that data come from and who are the recipients?

Where is the data stored and who has access to it?

What is the legal basis and the purposes of the processing?

General description of the technical and organizational security measures

Transfer to third parties or non-EU countries?

- Obligation to keep a register of processing activities (controller and processor)
- Exception: undertakings < 250 employees unless the processing:
  - involves a risk to the rights and freedoms of data subjects
  - is not occasional
  - concerns special categories (art. 9 or 10)

Ref: Art. 30

STEP 3: LEGAL BASIS FOR PROCESSING

✓ Document all types of processing and identify the legal basis for each

1. Consent
2. Performance of a contract
3. Legal obligation
4. Protect the vital interests of the data subject
5. Public interest or exercise of official authority
6. Legitimate interests pursued by the data controller or a third party

The legal basis must be communicated:

- In the privacy statement
- In case of access request by the data subject

Ref: Art. 6

STEP 4: CONSENT

- ✓ Active indication: no box checked beforehand or lack of action (opt-in and not opt-out)
- ✓ Explicit consent for certain data processing
  - ➢ Sensitive data (ethnic origin, political opinions, religion, biometric data, health, etc.)
  - ➢ Profiling
- ✓ Specific rules for minors (> 13-16)
- ✓ Data controller has the burden of proof
  - ➔ Provide an audit trail to prove consent

❖ Data subject has the right to withdraw his/her consent at any time!

Consent must be:

- ➢ Free
- ➢ Specific
- ➢ Informed
- ➢ Unambiguous

Ref: Art. 7 et 8

STEP 5: COMMUNICATION

- ✓Evaluate and review your existing privacy statement
- ✓Concise communication, in a clear and understandable language.

- ✓New types of information to communicate to the data subject:
  - Identity and contact of DPO
  - Legal basis of data processing
  - Retention duration
  - Will the data be exchanged outside the EU
  - Possibility for the person to make a complaint

➔ Greater transparency toward the data subject

Ref: Art. 13

STEP 6: DATA SUBJECTS' RIGHTS

Adapt your procedures and provide sufficient resources to enable the data subject to exercise its (new) strengthened rights.

- Right to be forgotten
- Data portability
- Objection to automated decisions making and profiling

➔ Portability: WP29 guide to come in 2017

Ref: Art. 16 à 22

STEP 7: DATA BREACH (1/3)

- Security breach
- Accidental or unlawful
- Intern or extern

- Destruction
- Loss
- Alteration
- Disclosure or unauthorized access

Examples:

1. Asiana Airlines
2. HIV Clinic

A simple mistake can lead to a data breach and have serious consequences for the data subjects

Ref: Art. 4

STEP 7: DATA BREACH (2/3)

Asiana Airlines' customer database leaked

Inquiry launched after HIV clinic reveals hundreds of patients' identities

The 56 Dean Street clinic in London apologises after sending newsletter disclosing names and email addresses of 780 people, many living with HIV

STEP 7: DATA BREACH (3/3)

Notification obligations:

- To the supervisory authority: within 72 hours
- To the data subjects: as soon as possible
- The data processor must notify the data controller

Exceptions: no notification to the data subject if:

- Does not generate a high risk or the risk is attenuated by security measures
  - e.g.: Data encrypted and decryption key is not compromised
- Would involve disproportionate effort

➔public communication

Ref: Art. 33 et 34

STEP 8: DATA PROTECTION BY DESIGN AND BY DEFAULT AND IMPACT ASSESSMENT

Data protection by design and by default

- Appropriate technical and organizational measures in order to:
  - Minimize data
  - Limit the processing to the necessary data

No data collection « just in case »…

Ref: Art. 25

STEP 8: DATA PROTECTION BY DESIGN AND BY DEFAULT AND IMPACT ASSESSMENT

Prior impact assessments if high risk, in particular:

- Systematic and thorough evaluation of personal aspects
- Large-scale processing of special categories of data
- Large-scale systematic surveillance of a public area

Prior consultation of the supervisory authority (CNPD)

➔ When the processing presents a high risk if the data controller does not take measures to reduce the risk

Analysis of security information risk = **impacts on the organization's data**

Impact assessment on data protection = **impacts on the data subjects**

Ref: Art. 35 et 36

STEP 9: DATA PROTECTION OFFICER (DPO)

DESIGNATION

Mandatory when:

- public sector
- regular and systematic monitoring of people on a « *large-scale* »
- processing « sensitive » data or relating to criminal convictions, also on a « *large-scale* ».

Internal or external and independent

MISSION

- ✓Inform and advise
- ✓Monitor compliance with GDPR and legislative framework
- ✓Awareness, training course and audits
- ✓Advise on impact assessments and check their execution
- ✓Contact point + Cooperation with the supervisory authority

Why would you wait 25 May 2018 to appoint a DPO?

Ref: Art. 37, 38 et 39

STEP 10: EXISTING CONTRACTS

Processing operation by a data processor is governed by a contract or another legal act, which:

- Binds the subcontractor with regard to the processing
- Defines the object and duration of the processing
- The nature and purpose of the processing
- The type of personal data
- The categories of data subjects
- Obligations and rights of the data controller

Ref: Art. 28

Definitions

Get ready in 10 steps

Conclusion

THANK YOU FOR YOUR ATTENTION

Vincent Wellens
vincent.wellens@nautadutilh.com