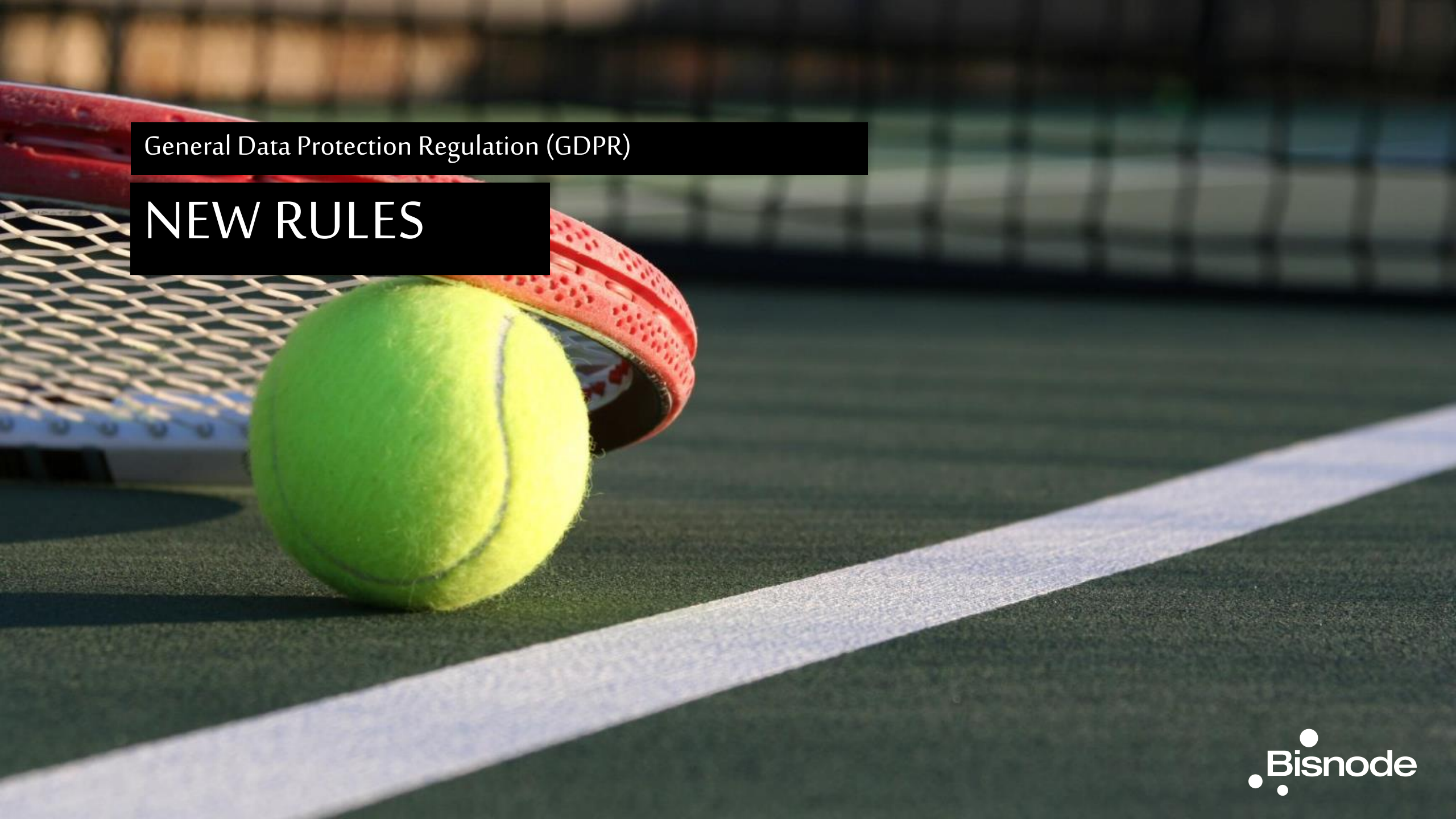


General Data Protection Regulation (GDPR)

NEW RULES

Bisnode

AGENDA

A. GDPR : general overview

B. Sectorial topics and concerns

GDPR

GENERAL OVERVIEW

Bisnode

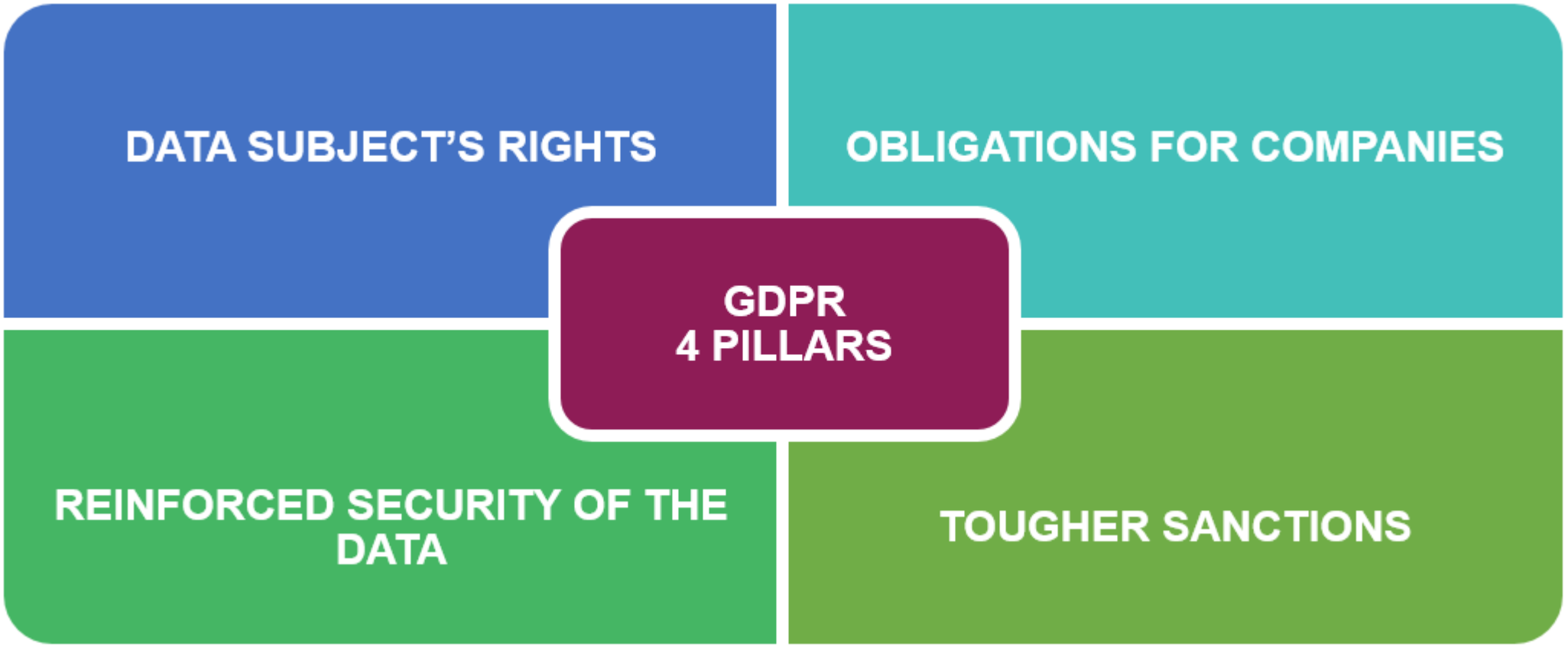
1. GDPR : WHAT IS IT AND WHY CARE ?

27 April 2016 : Approval of the General Data Protection Regulation (« GDPR »)

➔ *replacing the Data Protection Directive 95/46/EC and existing national privacy laws in EU*

- ➔ Entry into force: May 25th 2018
- ➔ Affecting every business that holds or uses European personal data both inside and outside Europe
- ➔ The obligations in the GDPR apply not only to the “controllers” but also to the “processors”
- ➔ Introducing substantial and ambitious changes
- ➔ Backed by heavy financial penalities

2. THE GDPR 4 PILLARS



3. RIGHTS OF THE DATA SUBJECT (1/2)

- **Right to be informed**

  - Via the privacy notice

- **Right to access**

  - What are you going to do with my data?
  - How did you find my name ?

- **Right of rectification**

  - I receive your communication in FR but I speak Dutch. Thank you for correcting my language code in your file
  - I have moved

- **Right to object**

  - I don’t longer want to receive your advertisements,
  - I don’t want you to transfer my data to third parties,
  - I don’t want you to use my data for creating marketing profiles

3. RIGHTS OF THE DATA SUBJECT (2/2)

- **Right to be forgotten**
  - *Delete all my data from your database*
- **Right of the restriction of the processing**
  - *As long as we are in conflict, I don't want you to use my data*
- **Data portability**
  - *Please transfer all information that I have communicated to Company XX (eg : competitor)*

4. OBLIGATIONS OF COMPANIES THAT PROCESS DATA (1/2)

- Respect data subject rights and implement them in the database

- Prove that the company complies with all the GDPR principles (documentation, traceability, data source, date of the data,…)

= Accountability principle

- Collect only what is needed for the processing

= data minimisation principle

4. OBLIGATIONS OF COMPANIES THAT PROCESS DATA (2/2)

- Establish limited data retention period

- Specific rules for the transmission of data inside and outside European Union
  (information of the data subject, right to object to the transfer for direct marketing purposes,…)

- Specific rules when appealing to a processor : the processor must warrant that he respects the GDPR, the processor must sign a contract, containing clauses imposed by the GDPR,…

5. WHAT IS AT STAKE ?

- **Major financial impact**

  Huge fines & financial compensation in case of liability:

  fines up **€ 20,000,000** or **4% of the total worldwide annual turnover**

  easier for individuals to bring private claims against data controllers and processors & possibility to **use "class actions**"

- **Additional consequences**

  Image & brand impact, competitive impact, liability of the decision makers

6. IMPACTS ?

Legal

New privacy notice, new contracts, new rights for data subjects, new formulation of ‘opt in’ and ‘opt out’, privacy by design,….

Operational

Bisnode

7. OPERATIONAL IMPACT

- GDPR requires companies to undertake operational reforms :

8. IMPACTED DEPARTEMENTS

9. STEPS TO BECOME COMPLIANT WITH THE GDPR

1. Preparation of a **road plan** containing the different steps and deadlines to be compliant in 2018

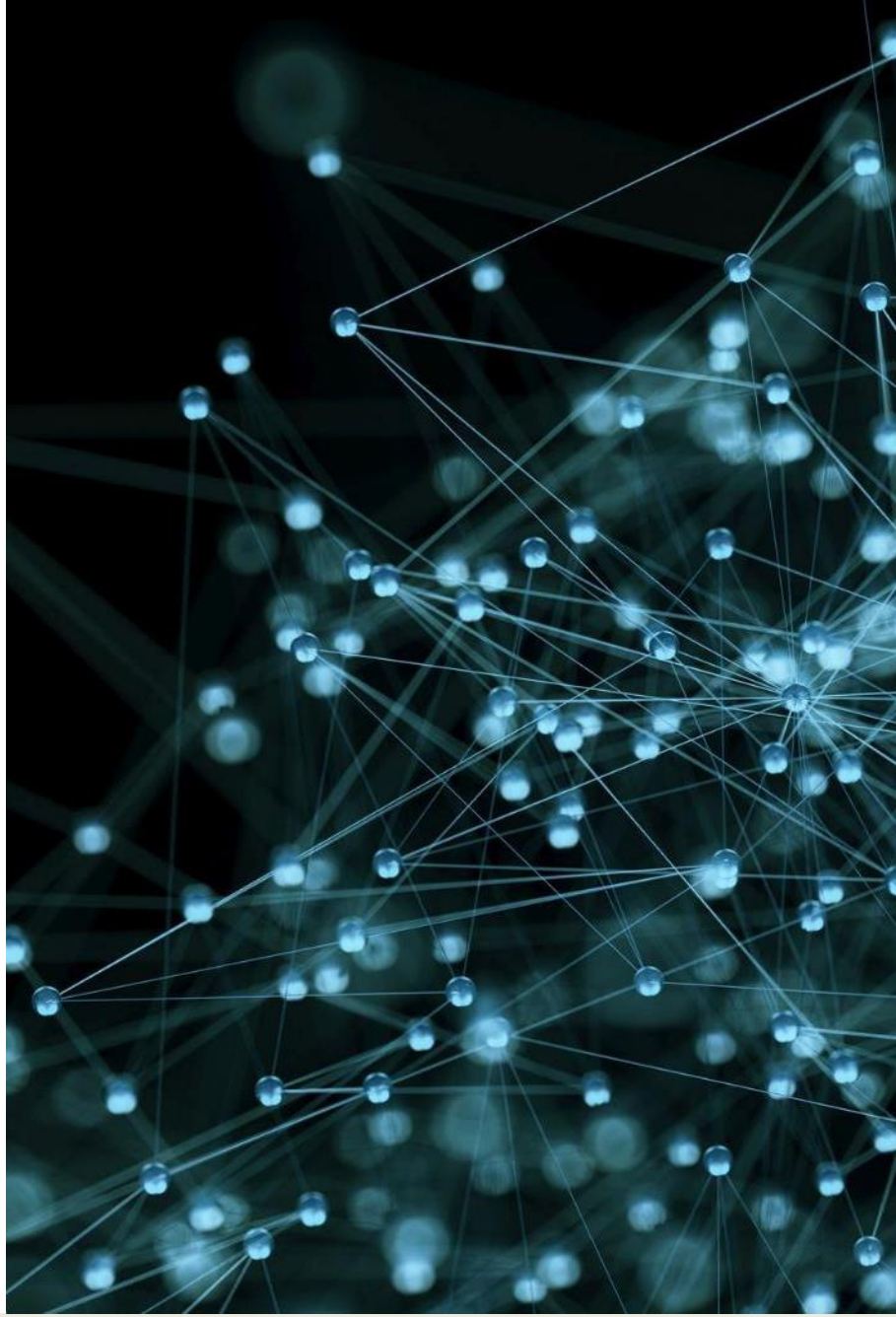
2. Internal **task force managed by a project manager**

3. All the competences must be represented in the task force : legal, IT, Security, Marketing, …

ROAD PLAN IN 6 STEPS

First step : data mapping

- Categories of data
- Source and date for all data/source for every modification
- Date for all data/every modification
- Source and date for each opt in/opt out
- Recipients of each record



ROAD PLAN IN 6 STEPS

Second step : more transparence towards the data subject

- Define all your purposes (as broad as possible)
- Define your legal bases (must be explained in the privacy notice)
- Inform clearly if you want to transfer data to third parties (if not foreseen, you will have to ask for consent afterwards !!!)
- Inform clearly if you want to enhance your data with external data

Bisnode

ROAD PLAN IN 6 STEPS

Third step : Data subjects's rights

- Data retention policy
- New rights to implement in the database
- Registration of each request and management
- Right to be forgotten : how ?
- Notification to the recipients in case of erasure, restriction, correction
- New standard letters
- website

Bisnode

ROAD PLAN IN 6 STEPS

Fourth step : Formalize new concepts

- Privacy by design : standard assessment to use in case of new project

- PIA : Standard assessment to use in case of new project, with risk for the data subjects rights

ROAD PLAN IN 6 STEPS

Fifth step : Security measures

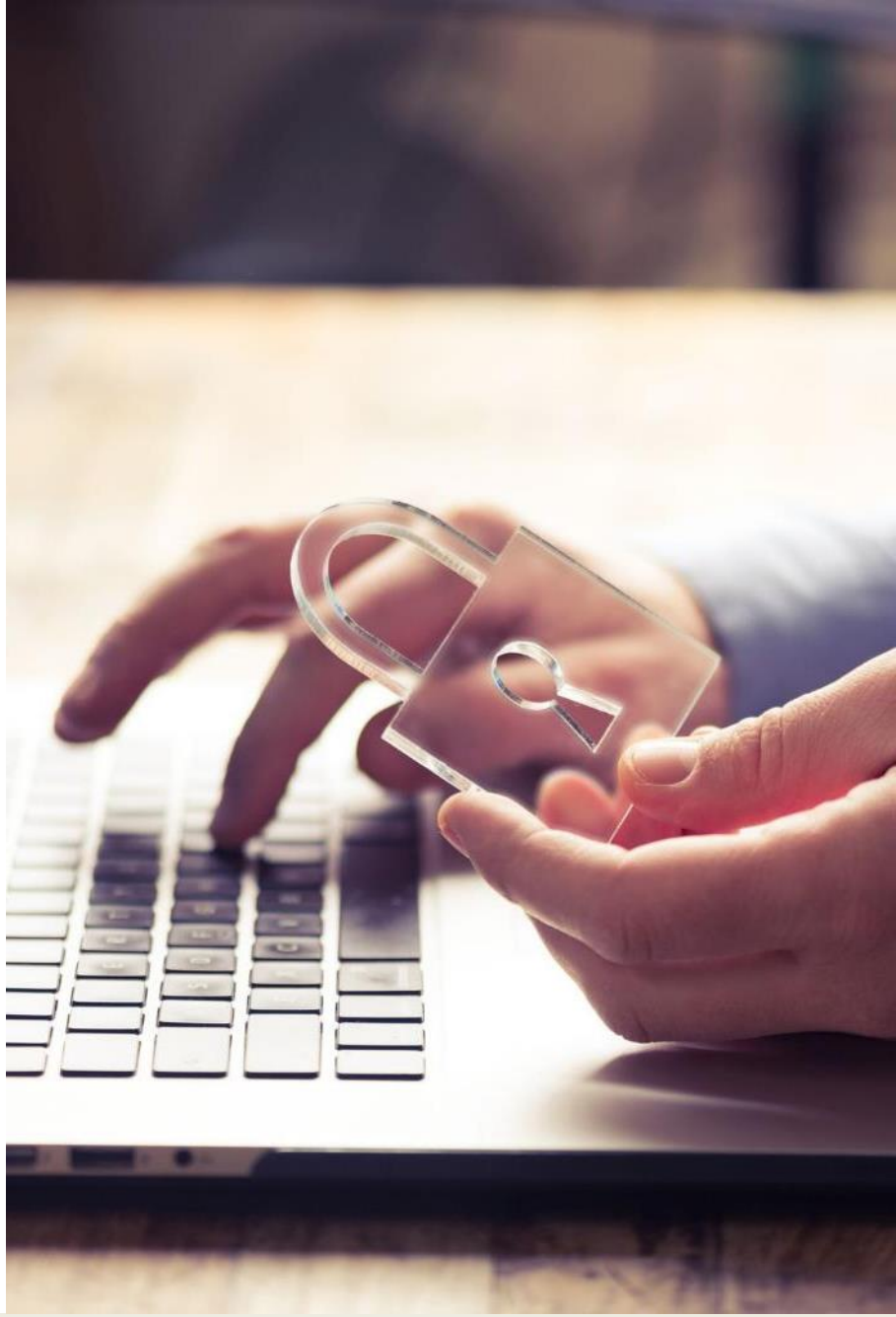
- Record of processing activities
- Technical and organisational measures to ensure a level of security appropriate to the risk
- Documentation
- Traceability of the processing (who, what, when)
- Audits (internal and external)
- Data breach procedures

Bisnode

ROAD PLAN IN 6 STEPS

Sixth step : Designation of a Data Protection Officer

- Verify if mandatory
- If not : appoint a responsible anyway



GDPR

SECTORIAL TOPICS AND CONCERNS

Bisnode

B. Sectorial topics and concerns

- Legitimate interest/Consent
- Status existing clients

1/2. CONSENT / LEGITIMATE INTEREST TODAY

a) GENERAL RULE :

Free choice between the different legal bases :

- Prior consent
- Legitimate interest
- Contract
- Public interest (law)
- Vital interest

b) APPLICATION OF THE RULE TO DIRECT MARKETING :

- Prior consent
- Legitimate interest

c) EXCEPTION :

Law about electronic communications (email, SMS, MMS, WhatsApp,…)

- Prior consent to send an electronic communication for DM purpose

= legal obligation (no free choice between the legal bases)

1/2. CONSENT / LEGITIMATE INTEREST TOMORROW

a) GENERAL RULE :

Free choice between the different legal bases :

- Prior consent
- Legitimate interest
- Contract
- Public interest (law)
- Vital interest

b) APPLICATION OF THE RULE TO DIRECT MARKETING :

- Prior consent
- Legitimate interest

c) EXCEPTION :

E-Privacy Regulation (= DRAFT !!)

- Prior consent to send an electronic communication for DM purpose

= legal obligation (no free choice between the legal bases)

2/2. STATUS EXISTING CLIENTS

- Right to be informed
- New information to be provided
- New consents ?

CONCLUSION

Some concepts need more interpretation and clarification.

Best practices to develop taking into account the spirit of the GDPR : transparency and proactive protection of the data subject is key !

Becoming compliant is a journey: not a one off project but an ***ongoing process, iterative approach and continuous improvement…***

dominique.pissoort@bisnode.be

Bisnode