

GDPR applied to the non-profit sector: How to be compliant by May 2018?



Jan Decorte
Antoine Druetz
28 September 2017




TABLE OF CONTENTS

- I. THE ROAD TO GDPR – FACTS AND FIGURES
- II. PRIVACY – ESSENTIALS
- III. THE GDPR
- IV. HOW TO GET READY FOR THE GDPR?
- V. SPECIFIC POA FOR NON-PROFIT ORGANISATIONS
- VI. Q&A – FAQ NON-PROFIT SECTOR

PRIVACY IN THE VIRTUAL WORLD

“Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that **wants to find out everything about you**. And once it has found out everything about you and two hundred million others, that is a very valuable asset and **people will be tempted to trade and do commerce with it**”

(quote from Andrew “Andy” Grove in “What I’ve Learned” by Mike Sager in Esquire, 1 May, 2000 - see www.esquire.com)

3

KOAN
Law Firm

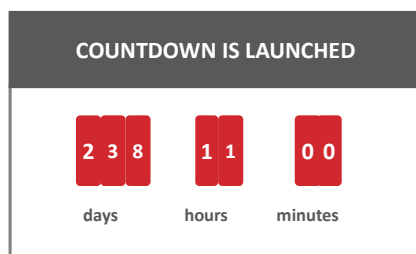
I. THE ROAD TO THE GDPR Facts & Figures



4

KOAN
Law Firm

GDPR COUNTDOWN

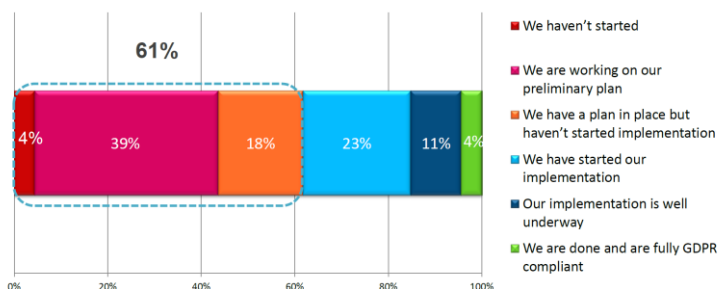


5

KOAN
Law Firm

HAVE YOU STARTED PREPARATIONS?

Wide Range of GDPR Readiness (May 25, 2018 Deadline)
61% have not begun implementation yet



Question: "Which of the following best describes the state of your GDPR compliance?"

- 43% do not have a full plan yet

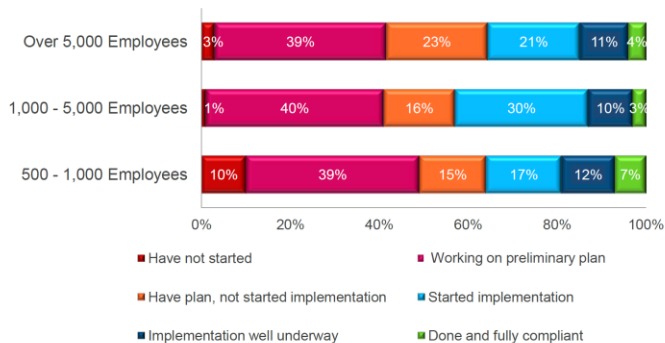
6

© 2017 TrustArc Inc

KOAN
Law Firm

ARE YOU FULLY READY AND PREPARED?

GDPR Preparedness by Company Size



Question: "Which of the following best describes the state of your GDPR compliance?"

7

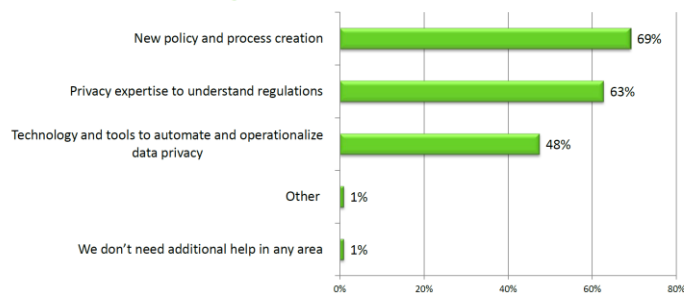
© 2017 TrustArc Inc

KOAN
Law Firm

WHAT HELP DO YOU NEED?

Companies Need a Wide Range of Help With GDPR

99% report needing additional help



Question: Which of the following areas will you need additional help to meet GDPR compliance in 2017 and 2018?

- Need for technology help rises to 59% for larger enterprises (5,000+ employees) vs 36% small (500 – 1,000 employees) and 46% medium (1,000 – 5,000 employees)
- Need for technology help rises to 59% for respondents IT function vs 37% for Legal function

8

© 2017 TrustArc Inc

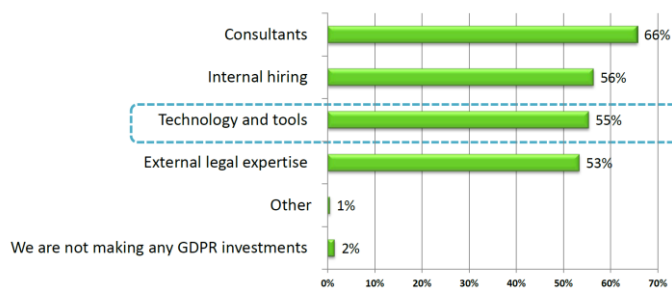
KOAN
Law Firm

IN WHAT DO/MUST YOU INVEST ?

GDPR Investments For Wide Range of Areas

99% will invest in additional capabilities

55% will invest in technology and tools



Question: "What areas will you be investing in to prepare for GDPR?"

- Investments in technology and tools increases to 67% for privacy professionals in IT department vs 47% in Legal department

9

© 2017 TrustArc Inc

NOJAN
Law Firm

II. PRIVACY Essentials



10

KOAN
Law Firm

ESSENTIAL CONCEPTS AND PRINCIPLES

1. Current **Belgian** regulatory framework (until 25 May, 2018)
2. Scope: who to **comply**?
3. Different **types** of data
4. General **concepts**
5. General **principles**



KOAN
Law Firm

1. CURRENT **BELGIAN** REGULATORY FRAMEWORK

➤ **Belgian Privacy Act:**

Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data

➤ **Data Protection Directive:**

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data



KOAN
Law Firm

2. MATERIAL SCOPE

WHO HAS TO COMPLY WITH CURRENT PRIVACY LAWS?

WHAT: (article 3 current Belgian Privacy Act)

“This [Act] applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”

CRITERIA:

≠ statutory purpose of the entity (commercial, not-for-profit, club, etc.)

≠ promotional or non promotional, informational or non informational

BUT:

= Is there **processing** of personal data?

→ in a *systematic* manner

13

KOAN
Law Firm

2. TERRITORIAL SCOPE

WHO HAS TO COMPLY WITH CURRENT PRIVACY LAWS?

The [Act] **applies** (article 3bis Belgian Privacy Act):

- (a) To data controllers who have a **fixed establishment on Belgian soil**;
- (b) To data controllers who have their **(permanent) establishment outside the EU but use means** (whether or not automated) **situated on Belgian soil**.

→ **Obligation:** designation of a **representative** established in Belgium

→ **Exception:** Act not applicable if it concerns a pure **transit** of data

14

KOAN
Law Firm

3. DIFFERENT TYPES OF PERSONAL DATA

Personal data (general)

Any information relating to an **identified or identifiable natural person** who can be identified, **directly or indirectly, in particular by reference to an identifier** such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person

Sensitive data (specific categories)

Personal data relating to **race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, genetic or biometric data, health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions, or related security measures.**

15

KOAN
Law Firm

3, DIFFERENT TYPES OF PERSONAL DATA

Pseudonymes

Personal data that **cannot be attributed to a specific data subject without the use of additional information**, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution.

Anonymous data

Data which are **neither personal data, nor pseudonymous data.**

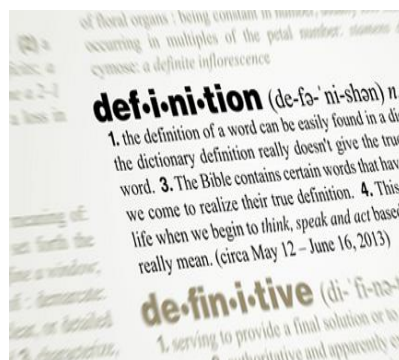
16

KOAN
Law Firm

4. GENERAL CONCEPTS

- **Processing**

any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;



KOAN
Law Firm

4. GENERAL CONCEPTS

- **Controller**

the natural or legal person, public authority, agency or any other body which alone or jointly with others **determines the purposes and means of the processing of personal data**; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his/its nomination may be designated by national or Community law;

- **Processor**

a natural or legal person, public authority, agency or any other body which **processes personal data on behalf of the controller**;

- **Recipient**

a natural or legal person, public authority, agency or any other body **to whom data are disclosed**, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients

KOAN
Law Firm

5. GENERAL PRINCIPLES

- **Principle of legality**
 - There must be a legal ground for the processing (6 grounds – see next slide)
- **Principle of finality**
 - The objective must be specific, adequate and legitimate
- **Principle of proportionality**
 - Processing must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- **Security and confidentiality**
 - Adequate safeguards for access to the data (secured servers, password, etc.)
 - Confidentiality engagements
- **Notification to the privacy commission** (until 25 May 2018)
 - Some exceptions (Royal Decree 13 February 2001)

19

KOAN
Law Firm

5. GENERAL PRINCIPLES

PRINCIPLE OF LEGALITY: processing of personal data must be based on 1 of 6 legal grounds to be permitted

	Consent		Necessary for execution of a contract
	Legal obligation		Protection of vital interests
	Missions of public interest or exercise of public authority		Legitimate interests of the controller (or recipients)

20

KOAN
Law Firm

5. GENERAL PRINCIPLES

ALL TIMES RIGHTS OF THE DATA SUBJECT

1. Right of **ACCESS** to personal data
2. Right to request **RECTIFICATION** of personal data
3. Right to request **ERASURE** of personal data
4. Right to request **RESTRICTION** of processing personal data
5. Right to **OBJECT** to processing of personal data
6. Right to have clear and full **INFORMATION**



21

KOAN
Law Firm

5. GENERAL PRINCIPLES

WHAT WITH TRANSFER OF DATA ACROSS THE BORDERS?

- TRANSFER OF DATA **WITHIN THE EUROPEAN ECONOMIC AREA**
- TRANSFER OF DATA **OUTSIDE THE EUROPEAN ECONOMIC AREA**
→ TO THE US
- TRANSFER OF DATA **OUTSIDE THE EUROPEAN ECONOMIC AREA**
→ TO OTHER COUNTRIES



22

KOAN
Law Firm

III. THE GDPR

General Data Protection Regulation



23

KOAN
Law Firm

CURRENT EU DATA PROTECTION DIRECTIVE VERSUS THE GDPR

Data Protection Directive

- ✓ Old directive (1995) vs new technology
- ✓ Fragmentation and inconsistency due to 28 local flavours
- ✓ Forum Shopping
- ✓ Scope limited to EU vested establishments
- ✓ Low punitive sanctions



General Data Protection Regulation (GDPR)

- ✓ Adapt legal framework to the globalised digital society
- ✓ "One ring to rule them all"
- ✓ One stop shop
- ✓ Global scope (but IPR conflicts?)
- ✓ Increased rights for individuals
- ✓ Increased obligations for Controllers AND Processors
- ✓ High punitive sanctions

24

KOAN
Law Firm

TOP GDPR KEY ISSUES

1. **Scope**
2. **Consent requirements**
3. **Adequate and effective data protection system**
4. **The Data Protection Officer (DPO)**
5. **Punitive sanctions**



25

KOAN
Law Firm

1. MATERIAL SCOPE

WHO HAS TO COMPLY WITH THE GDPR?

THE SAME:

This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

NEW:

- Processor now also directly responsible – specific obligations
- Extended definition of "Personal Data" (all "online identifiers")
- Pseudonymisation as a process
- Privacy by default /privacy by design
- Data retention /data portability
- Confirmation of the principle of the "right to be forgotten"

26

KOAN
Law Firm

1. SCOPE

WHO HAS TO COMPLY WITH THE GDPR?

➤ **THE SAME:**

*Processing of personal data of data subjects by a controller or a processor with an **establishment in the Union**, regardless of whether the processing takes place in the Union or not*

NEW:

- *Processing of personal data of data subjects who are in the Union by a controller or processor **not established in the Union**, where the processing activities are related to:

 - (a) the **offering of goods or services** (free or against payment) **to data subjects in the Union**; or
 - (b) the **monitoring of their behavior** (within the Union)*
- *Processing of personal data by a controller not established in the Union, but in **a place where Member State law applies by virtue of public international law***

27

KOAN
Law Firm

2. CONSENT REQUIREMENTS

- Consent for **ordinary categories of personal data**
 - Free, specific, informed and unambiguous
- Consent for **sensitive personal data**
 - Ex: personal data revealing race, political opinions, religious affiliation, trade union membership, health or sex life details
 - Consent must be explicit (not defined but stronger than 'ordinary' consent)
- Parental consent for **children** up to the age of minimum 13 and maximum 16 (each Member State to determine)

28

KOAN
Law Firm

3. ADEQUATE AND EFFECTIVE DATA PROTECTION SYSTEM

1. A relevant **filing system**
> exception: entities < 250 employees under certain conditions
2. Adequate data protection **measures**
3. A specific breach **notification procedure** (“72 hours deadline”)

RIGHTS OF DATA SUBJECTS
><
REPUTATIONAL DAMAGES ?

29

KOAN
Law Firm

4. DATA PROTECTION OFFICER (DPO)

Obligatory DPO for certain organisations

- ✓ The processing is carried out by a **public authority or body**
- ✓ The **core activities** consist of processing **on a large scale** of personal data which require **regular and systematic monitoring**
- ✓ The **core activities** consist of any processing **on a large scale of special categories of data**

30

KOAN
Law Firm

4. DATA PROTECTION OFFICER (DPO)

Requirements

- ✓ Expert level
- ✓ Questions related to personal data (appropriate way and in due time)
- ✓ Necessary resources (personal, time, financial means...)
- ✓ Full autonomy (internal or external DPO)
- ✓ No conflict of interests (cannot be CEO, COO, CFO, CMO...)

Tasks

- ✓ Ensure conformity with the GDPR and an effective protection of data
- ✓ Develop, review and update data protection systems (IT ,policies, etc);
- ✓ Inform, educate and advise the officers and personnel/subcontractors
- ✓ Point of contact and cooperation with the Privacy authorities
- ✓ + ...

31

KOAN
Law Firm

5. PUNITIVE SANCTIONS

- Fines up to **€10 million or 2% of worldwide annual turnover** for issues related to:
 - Security failures related to processing
 - Infractions re DP by design/by default
- Fines up to **€20 million or 4% of worldwide annual turnover** for issues related to:
 - Sensitive data
 - Transfers of personal data
 - Non-compliance with a supervisory authorities' order
 - Issues re-data subjects consent



32

KOAN
Law Firm

IV. HOW TO GET READY

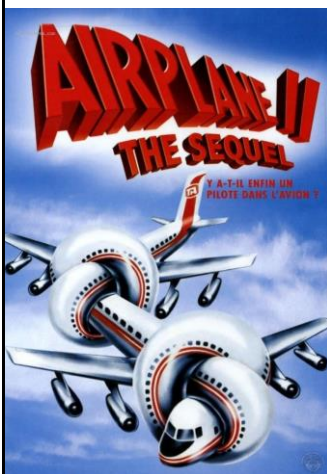
In 4 steps



33

KOAN
Law Firm

A STRUCTURED AND EFFICIENT APPROACH IN FOUR STEPS

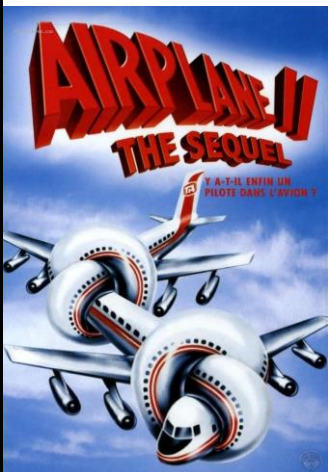


34

1. Appoint the right **pilot** and the necessary **crew**
 - members of management; operational departments, IT/legal department + possible external assistance.
2. Carry out a **Privacy Risk Assessment**
 - map inbound-outbound flows of personal data;
 - Carry out an audit;
 - Identify risks and shortcomings.

KOAN
Law Firm

A STRUCTURED AND EFFICIENT APPROACH IN FOUR STEPS



35

3. Carry out a **Privacy Impact Assessment**

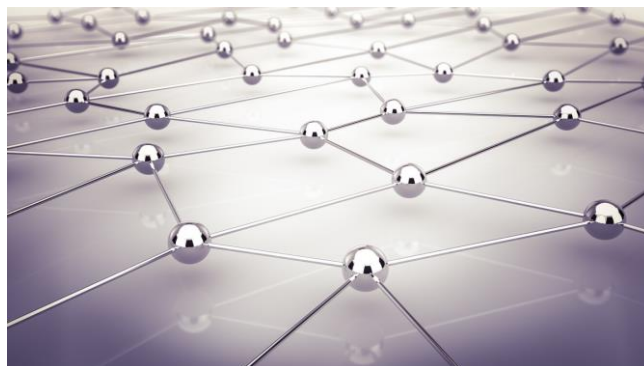
- ➔ Determine actions and steps that need to be taken to be compliant;
- ➔ Assess level of impact on the activities, internal organisation, external partners, cost, etc.

4. Set up an accurate **Data Management Process**

- ➔ Standardized legal compliance measures BUT tailor made solutions in view of the specific organisation
- ➔ Immediate effective and pragmatic remedies BUT also a long term vision and strategy

KOAN
Law Firm

V. SPECIFIC POA NON-PROFIT ORGANISATIONS Tips & Reminders



36

KOAN
Law Firm

SPECIFIC POINTS OF ATTENTION FOR NON-PROFIT ORGANISATIONS

Tips & Reminders

- Decision powers vs representation powers
- Liability of the directors
- Specific insurance
- Governance and management opportunity
- Reputation

VI. Q&A

FAQ NON-PROFIT SECTOR



Q&A

FAQ NON-PROFIT SECTOR

Capita selecta:

- Can a non-profit association record data of its donors and supporters?
- Can a non-profit association use these data to contact these donors and supporters to request additional donations (e.g. before the end of the tax year, explaining that if the donor donates more he/she can reach the tax deductible amount)?
- Can a non-profit association use these data to send newsletters and flash news to these donors and supporters or to invite them to an event it organizes?

Q&A

FAQ NON-PROFIT SECTOR

Capita selecta:

- Someone within a non-profit association receives a business card. Can the contact details of this person be included in the database of the association in order to send him/her newsletters, updates and information?
- The non-profit association is contacted by email. Can this email address be automatically included in the database of the association in order to send newsletters, updates and information?
- There is an online contact form on the non-profit association's website with a pre-ticked box regarding the sending of newsletters. Is it sufficient?

Q&A

FAQ NON-PROFIT SECTOR

Capita selecta:

- Lobby/representation activities: the association creates a database of contact stakeholders, influencers, policy makers, etc. with their contact details as well as their political opinion and/or religion or philosophical beliefs. Can the association do that? What are the measures which shall be undertaken in order to be GDPR compliant?
- What about databases the association bought or obtained from third parties?
- Etc.



Your team



Jan DECORTE

Partner

jdc@koan.law

+32 2 566 93 89



Antoine DRUETZ

Partner

adr@koan.law

+32 2 566 90 08



Alix DEGREZ

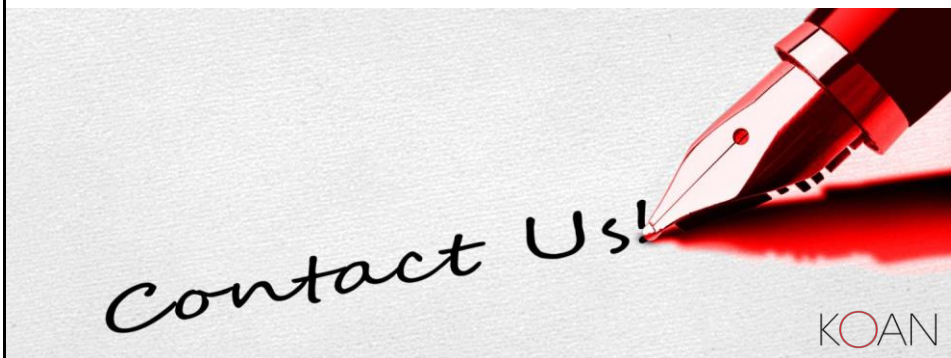
Associate

adg@koan.law

+32 2 566 90 37






Thank you



Ch. de la Hulpe 166 Terhulpesteenweg
B-1170 Brussels
Belgium
+32 2 566 90 00

47 rue de Monceau
F-75008 Paris
France
+33 1 56 69 71 20

 www.koan.law
 [@KoanLaw](https://twitter.com/KoanLaw)
 [www.linkedin.com/
company/koan](https://www.linkedin.com/company/koan)