

# The General Data Protection Regulation

Compliance with the New Regulation:  
How to prepare?

19th October 2017

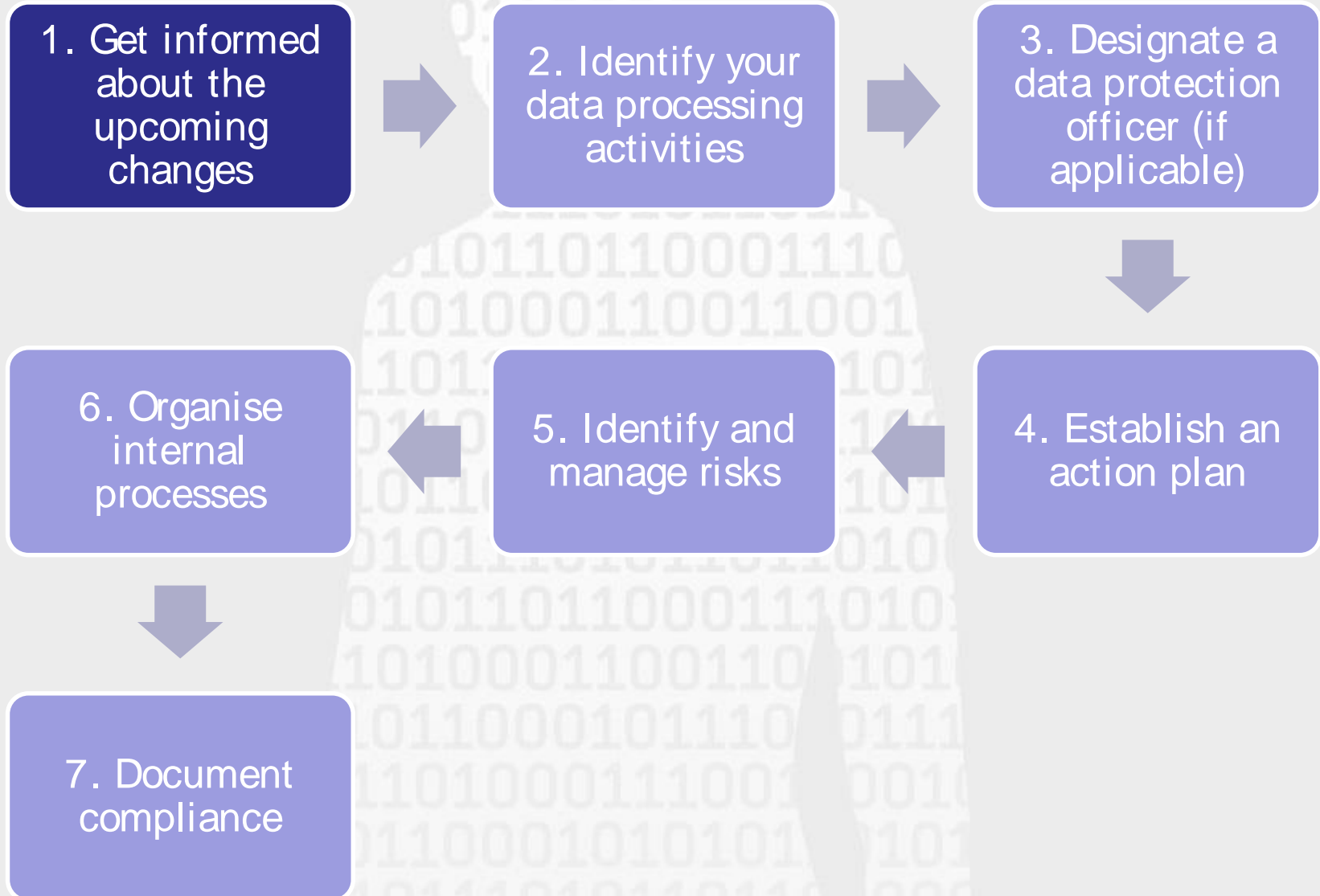
Esch-sur-Alzette (Belval)



Christophe Buschmann

Claudia Pfister

# 7 steps to prepare for GDPR compliance



# 1. Get informed about the upcoming changes 1/11

4.5.2016

EN

Official Journal of the European Union

L 119/1

I

(Legislative acts)

## REGULATIONS

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 27 April 2016**

**on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

**GDPR – THE KEY CHANGES**

# 1. Get informed about the upcoming changes <sup>2/11</sup>

## ■ a) Strengthening individuals' rights:

- Restricted definition of consent (+ consent of a parent for a child under the age of 16);
- Right to data portability;
- Right to erasure (RTBF);
- Right to get informed in case of a data breach;
- Introduction of a class action option;
- Other already existing rights have been strengthened:
  - Right to information;
  - Right to object to processing.



# 1. Get informed about the upcoming changes 3/11

## ■ b) Controller & processor:

- **Accountability:** the GDPR introduces a legal accountability obligation; the controller & the processor will be responsible for its implementation (prior formalities like notifications and authorisations will be strongly limited);

**Risk based approach!**



- **More obligations for processors:** new obligations as regards security, confidentiality, accountability, advice to the controller in order for the controller to be compliant with certain obligations + new conditions for the engagement of a sub-processor.

# 1. Get informed about the upcoming changes 4/11

## ■ c) New concepts:

- Data Protection Officer (DPO)
- Notification of a data breach to the national authority
- Data Protection Impact Assessment (DPIA)
- Codes of conduct, Certification
- Record of processing activities
- Privacy by design ↔ Privacy by default
- Enhanced security measures

## 1. Get informed about the upcoming changes 5/11

- **d) Extended territorial scope:**
  - The GDPR applies not only to EU based controllers and processors, but also to controllers and processors offering goods and/or services to EU residents or if the behaviour of individuals within the EU is monitored;



## 1. Get informed about the upcoming changes 6/11

- e) The “one stop shop” and a stronger European cooperation:
  - One single point of contact for companies → the place of the main establishment of the company will determine which national authority will be the “**lead authority**”. The main establishment will be either the place of the central administration in the EU, or the place where decisions on the purposes and means of the data processing are made.
  - Stronger cooperation between European authorities, so that companies receive **one binding decision** based on a consensus between all the concerned authorities.



# 1. Get informed about the upcoming changes 7/11

## ■ f) Complaints and administrative fines:

- **Complaints:** can be lodged with the supervisory authority of the habitual residence or place of work of the data subject, or of the place of the alleged infringement
- **Administrative fines:** imposed by the competent supervisory authority in addition to or instead of other corrective powers



Fines can reach a maximum of **20,000,000 EUR** or, for companies, of up to 4% of the total worldwide turnover.

# 1. Get informed about the upcoming changes 8/11

Inform key persons and decision makers

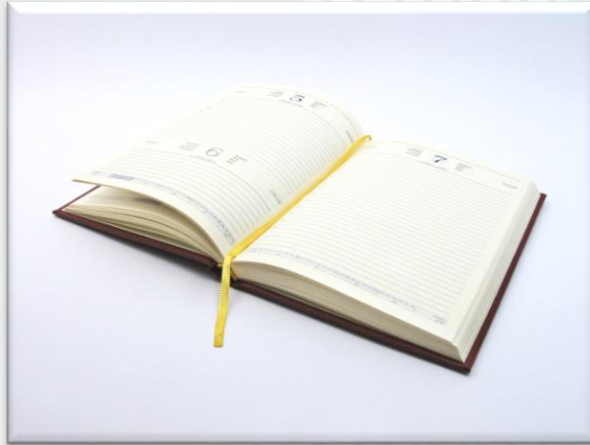
+

Raise awareness among employees



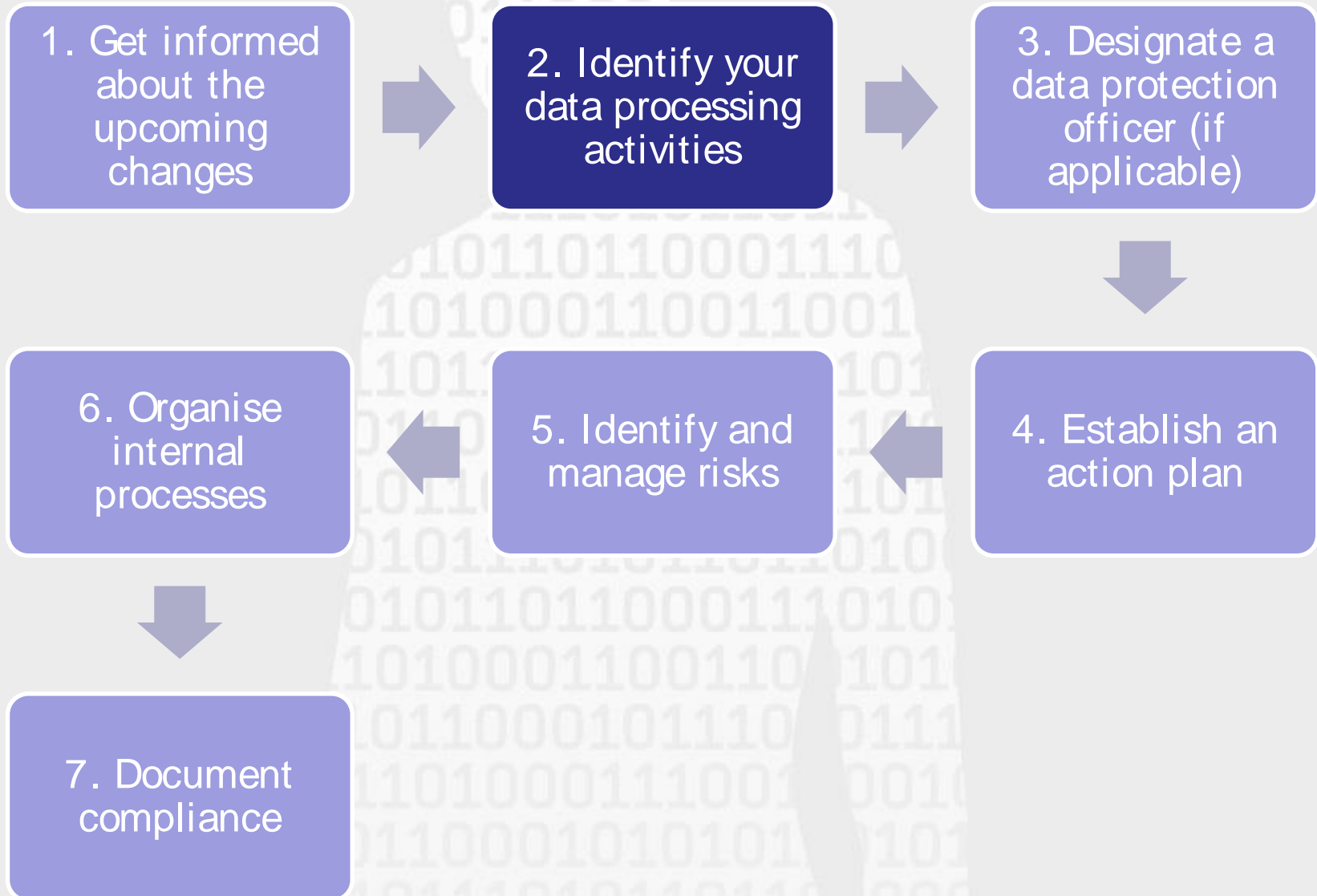
Evaluate possible consequences

# 1. Get informed about the upcoming changes <sup>9/11</sup>



**Deadline:  
25 May 2018**

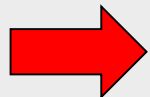
# 7 steps to prepare for compliance



## 2. Identify your data processing activities <sup>1/3</sup>

Impossible to comply without knowing:

- the collected data
- the data flows
- the processing activities

 Solution: create an inventory of all the data processing operations as of now.



**Obligation** to keep a **record of processing activities** from May 2018 (with some exceptions).

Fiche de registre		ref-000
Description du traitement		
Nom / sigle		
N° / REF ref-000		
Date de création		
Mise à jour		
Acteurs		
Nom	Adresse	CP Ville
Responsable du traitement		
Délégué à la protection des données		
Représentant		
Responsable(s) conjoint(s)		
Finalité(s) du traitement effectué		
Finalité principale		
Sous-finalité 1		
Sous-finalité 2		
Sous-finalité 3		
Sous-finalité 4		
Sous-finalité 5		
Mesures de sécurité		
Mesures de sécurité techniques		
Mesures de sécurité organisationnelles		
Catégories de données personnelles concernées		
Description	Délai d'effacement	
Etat civil, identité, données d'identification, images		
Vie personnelle (habitudes de vie, situation familiale, etc)		
Informations d'ordre économique et financier (revenus, situation financière)		
Données de connexion (adress IP, logs, etc)		
Données de localisation (déplacement, données GPS, GSM, etc)		

**Illustrative**

@ CNIL

Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.

Ces listes sont indicatives, tant en ce qui concerne le niveau de détail que l'exhaustivité. Il incombe au responsable du traitement d'indiquer au besoin des informations plus détaillées au sujet du traitement.

Cliquez sur le '+' à côté du nom d'une liste pour l'ouvrir.

- Liste indicative de types de finalités
- Fondement du traitement
- Liste indicative des catégories de données fonctionnelles
- type de traitement
- catégorie de données RGPD
- liste indicative de catégorie(s) de destinataires
- nature de la transmission vers un pays tiers/une organisation internationale

@ CPVP

**Illustrative**

GDPR-CST

Project Mgr. Visualization

Registre des activités de traitement

<p>Partie 2: Traitements</p> <p>Title: <b>Contract management</b></p> <p>Creat. on: 18 July 2017 Updat. on: 05 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>	<p>Partie 2: Traitements</p> <p>Title: <b>Analyse</b></p> <p>Creat. on: 18 July 2017 Updat. on: 05 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>	<p>Partie 2: Traitements</p> <p>Title: <b>Invoicing</b></p> <p>Creat. on: 08 August 2017 Updat. on: 05 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>
<p>Partie 2: Traitements</p> <p>Title: <b>Payroll</b></p> <p>Creat. on: 05 October 2017 Updat. on: 05 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>	<p>Partie 2: Traitements</p> <p>Title: <b>Marketing</b></p> <p>Creat. on: 06 October 2017 Updat. on: 06 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>	<p>Partie 2: Traitements</p> <p>Title: <b>Infrastructure</b></p> <p>Creat. on: 06 October 2017 Updat. on: 06 October 2017 Creat. by: Paul Richard Updat. by: Paul Richard</p> <p>Draft</p>

**Illustrative**

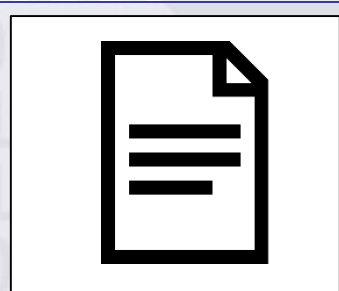
@ CNPD & LIST

## 2. Identify your data processing activities <sup>3/3</sup>

### Key questions:



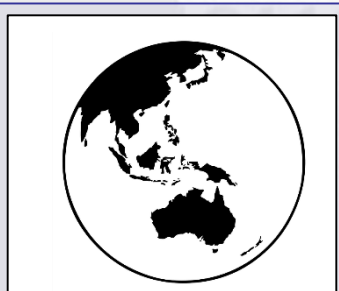
**WHO**  
is responsible for the  
processing activity ?



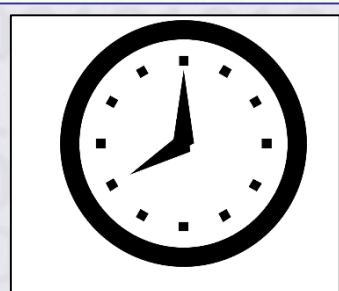
**WHAT**  
is processed?



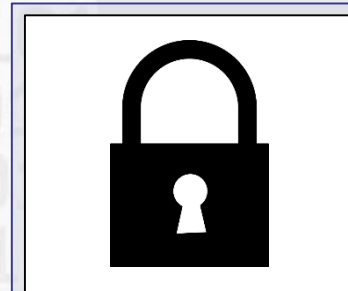
**WHY**  
is it processed?



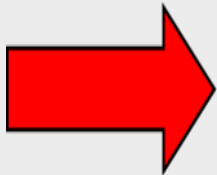
**WHERE**  
is it processed?



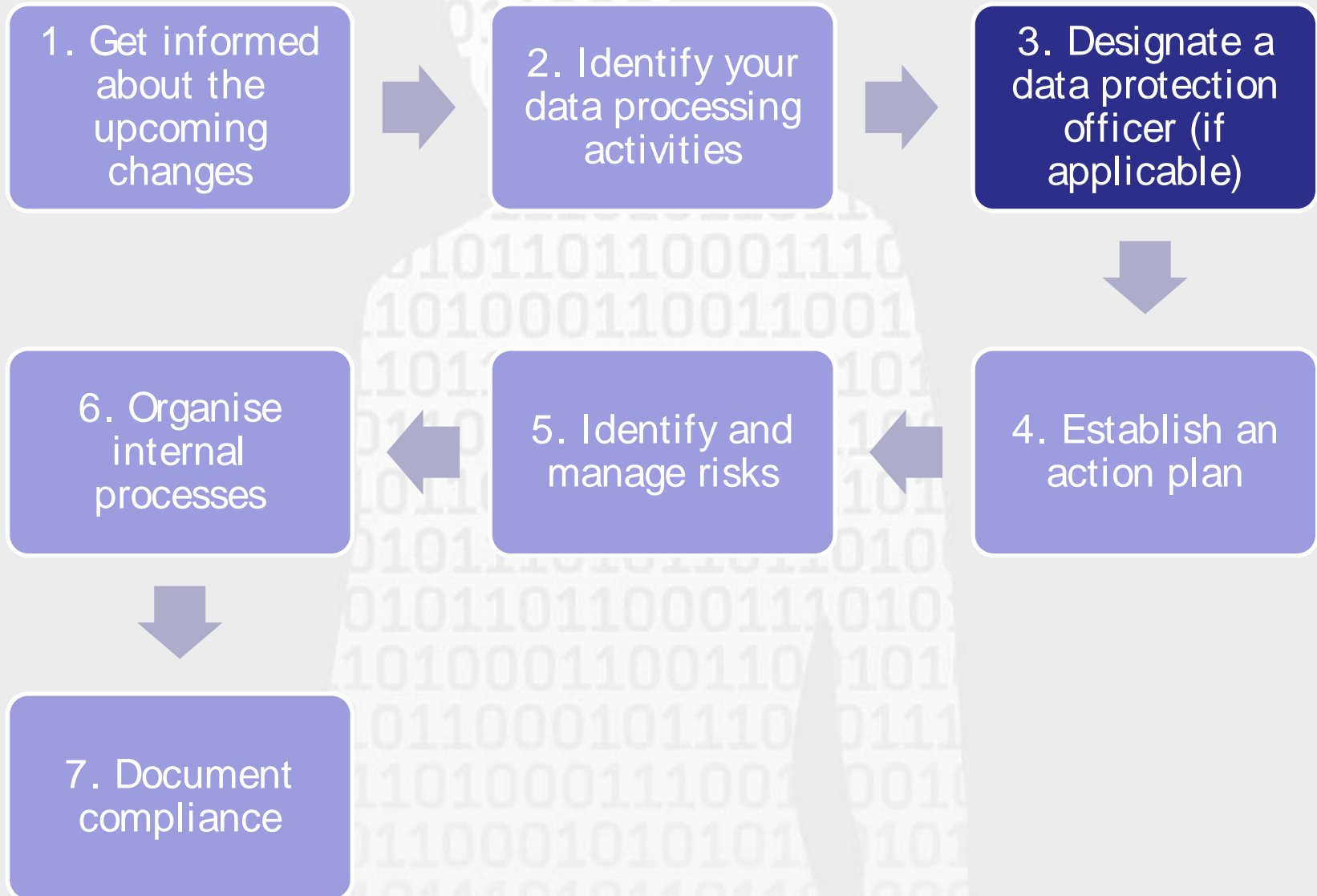
**UNTIL WHEN**  
will it be processed?



**HOW**  
will it be protected?



# 7 steps to prepare for compliance





### 3. Designate a data protection officer (if applicable) <sup>1/3</sup>

A data protection officer will be **mandatory after 25 May 2018** if :



- Public authority or body
- Undertaking fulfilling certain criteria (e.g. large scale processing of sensitive data)

### 3. Designate a data protection officer (if applicable) <sup>2/3</sup>

#### **Role?**

Inform, advise, control and monitor internally and contact point for the supervisory authority.

Major advantage for:

- compliance with the GDPR obligations,
- communication with supervisory authorities,
- reducing the risk of litigation and liability.

### 3. Designate a data protection officer (if applicable) <sup>3/3</sup>

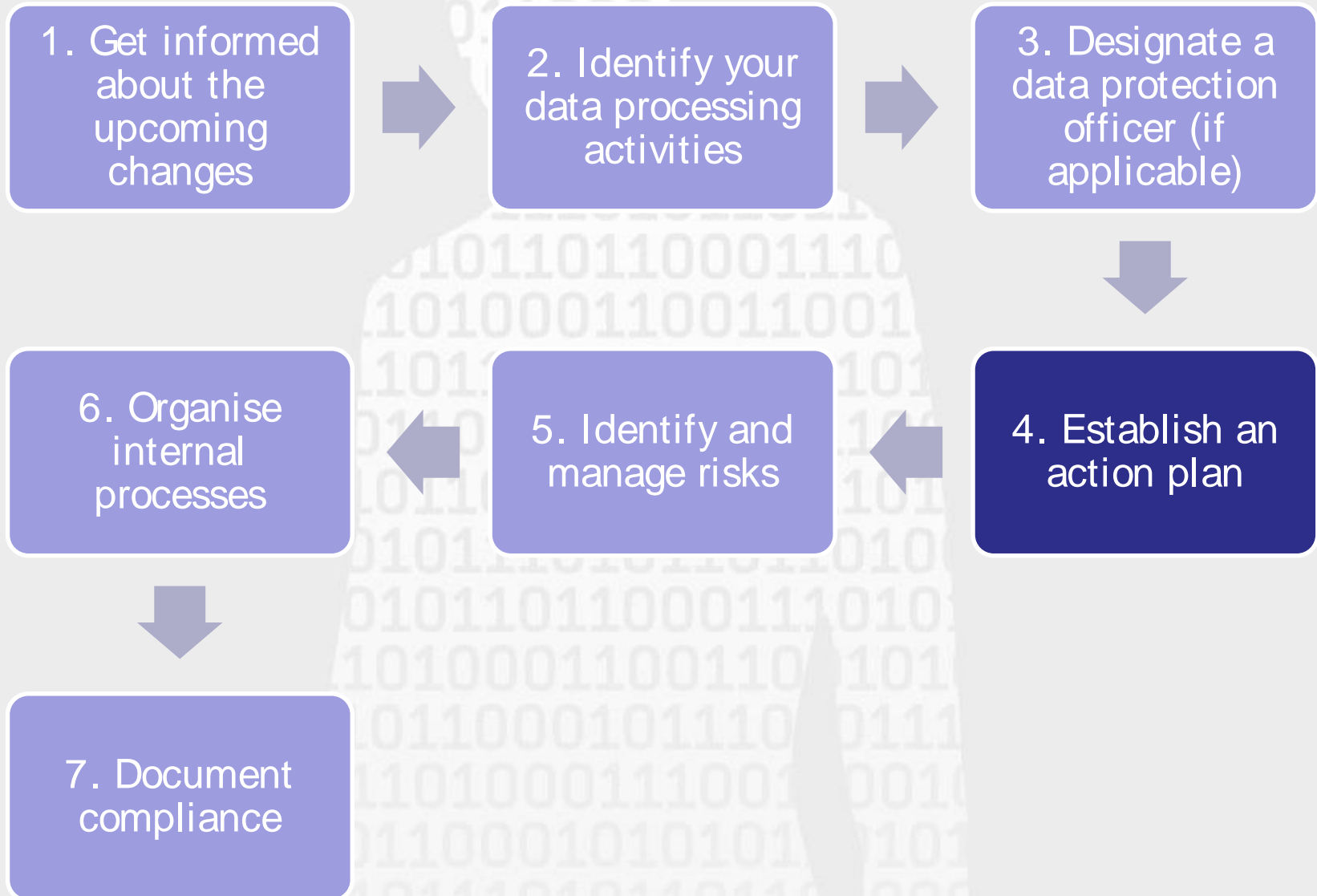
Is there a pilot on board?



Prevention is better:

Designate as of now an internal or external person responsible for data protection.

# 7 steps to prepare for compliance



## 4. Establish an action plan <sup>1/3</sup>

### Key issues:

- Use **only data that is strictly necessary**;
- Identify **the legal basis** on which the data is processed:
  - Consent of the data subject;
  - Necessary for the performance of a contract;
  - Legal obligation;
  - Necessary to protect vital interests;
  - Task of public interest/ Exercise of official authority;
  - Legitimate interest;



## 4. Establish an action plan <sup>2/3</sup>

### Key issues:

- Review your **information notices**;
- Remember your **processors**: review all the contracts with your processors;
- Lay down the procedures for the exercise of the **rights of data subjects** (e.g. internal procedure on how to deal with a data subject's request for rectification or access);
- Check your **security measures**.

## 4. Establish an action plan <sup>3/3</sup>

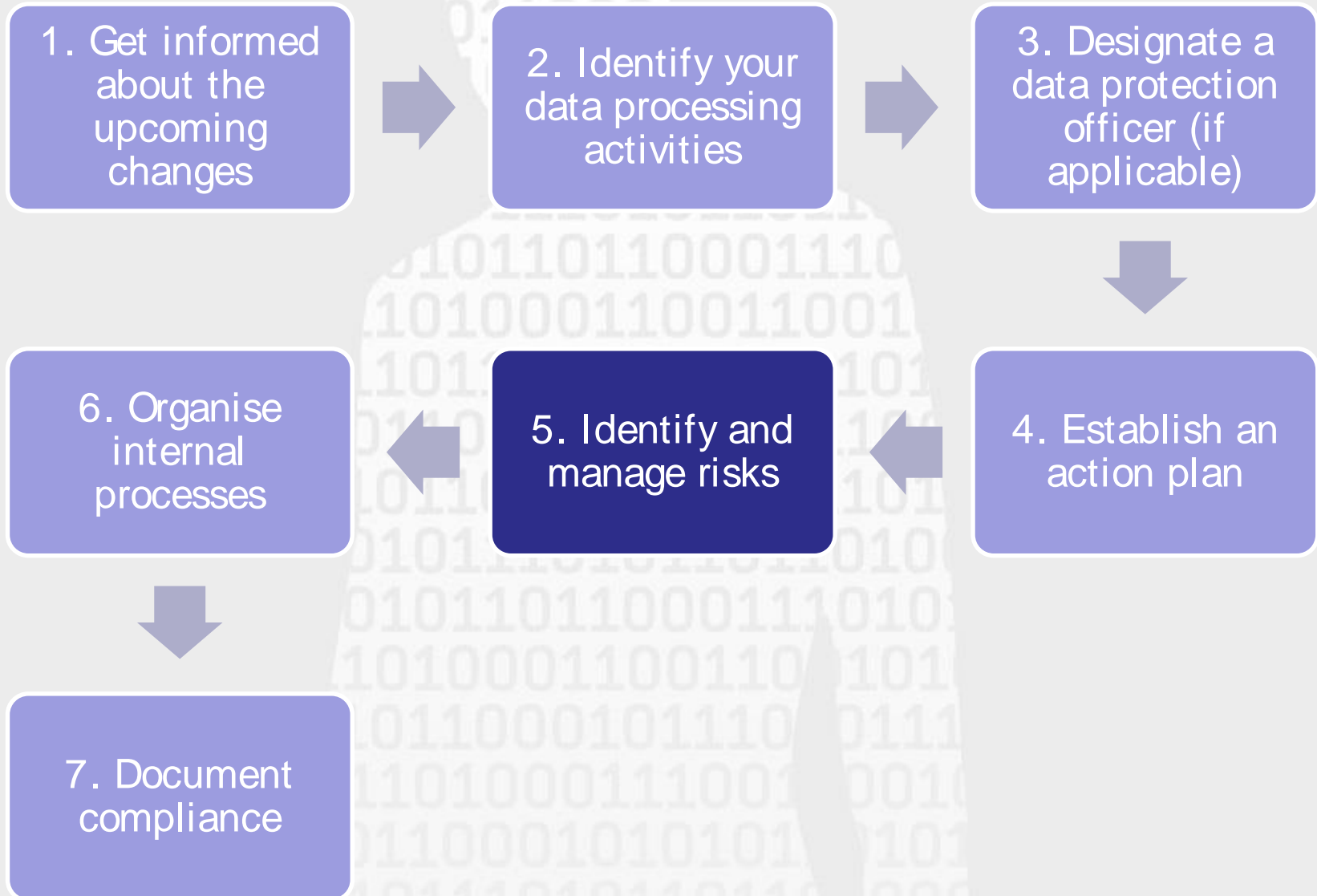
### Particular focus on:

- **Sensitive data** (health, political opinion, union membership, criminal offence...);



- **Specific data processing** (large-scale surveillance, profiling ...);
- Data transfers **outside the EU.**

# 7 steps to prepare for compliance





## 5. Identify and manage risks

If data processing activities are likely to result in a high risk to the rights and freedoms of data subjects

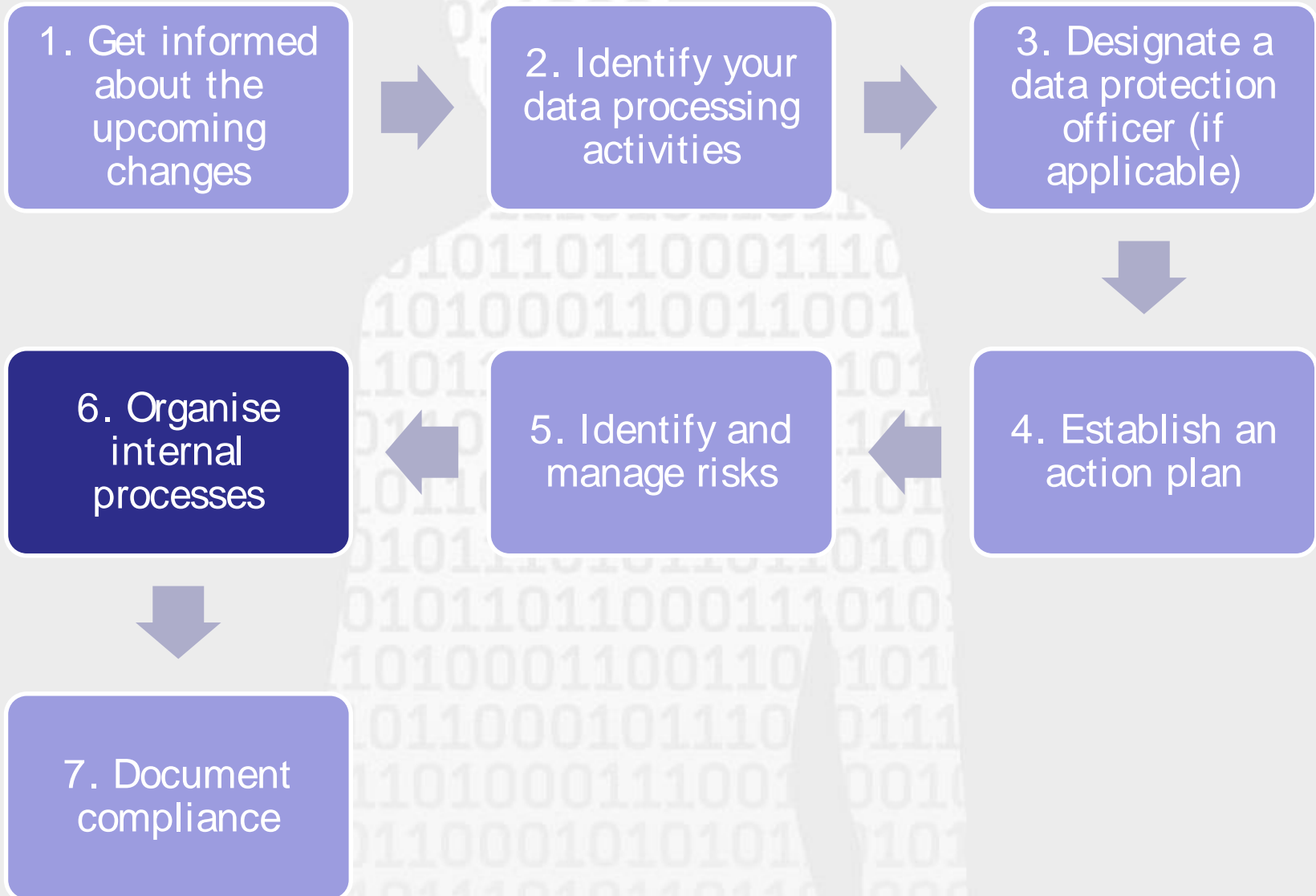


The controller needs to carry out an  
**assessment of the impact**

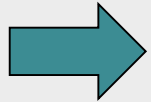
of the envisaged processing operations on the protection of personal data, to evaluate the risks

**(Data Protection Impact Assessment - DPIA)**

# 7 steps to prepare for compliance



## 6. Organise internal processes <sup>1/5</sup>



Set up internal processes to anticipate requests and problems in relation to data processing



### **Example:**

A data subject makes a request for rectification of personal data

- If you have a website, create an online form that can be used for such requests;
- Designate the persons responsible internally who will deal with such requests;
- Who will make the decisions? Rectification and/or reply to the data subject?

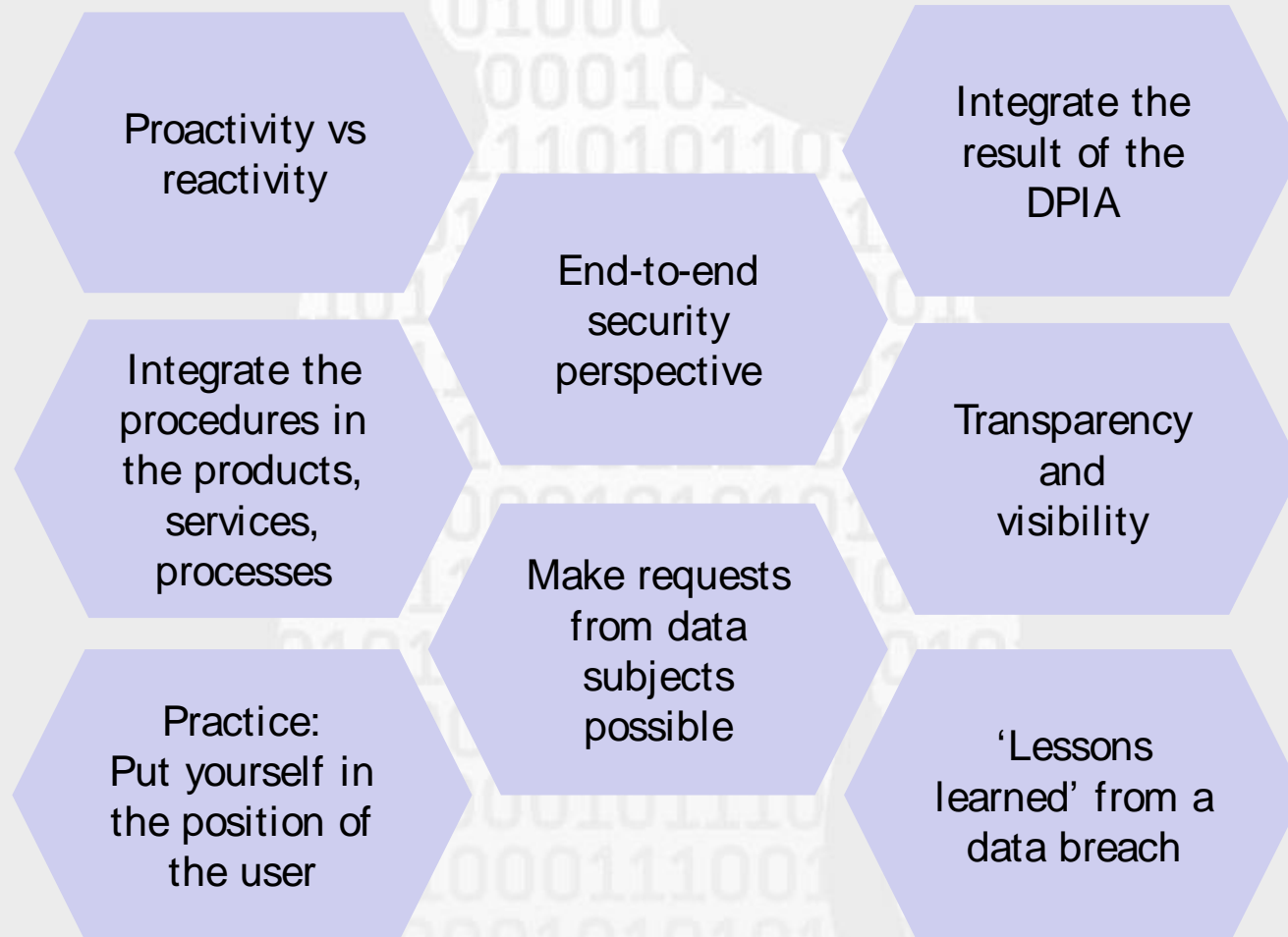
## 6. Organise internal processes <sup>2/5</sup>

Organising internal processes requires :

- Taking into account the principle of **data protection by design and by default**;
- **Raising awareness** among employees and organising **internal reporting**;
- Dealing with **complaints and requests** from data subjects in relation to their rights;
- Anticipating potential data breaches.

## 6. Organise internal processes <sup>3/5</sup>

### Data protection by design: the “what”



## 6. Organise internal processes 4/5

# Data protection by design

**General**

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

On

Let websites provide locally relevant content by accessing my language list

On

Let Windows track app launches to improve Start and search results

On

VS

**General**

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

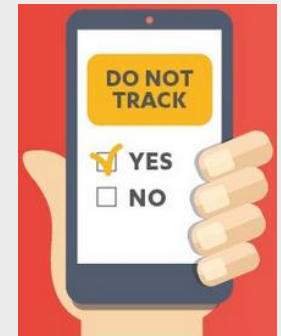
Off

Let websites provide locally relevant content by accessing my language list

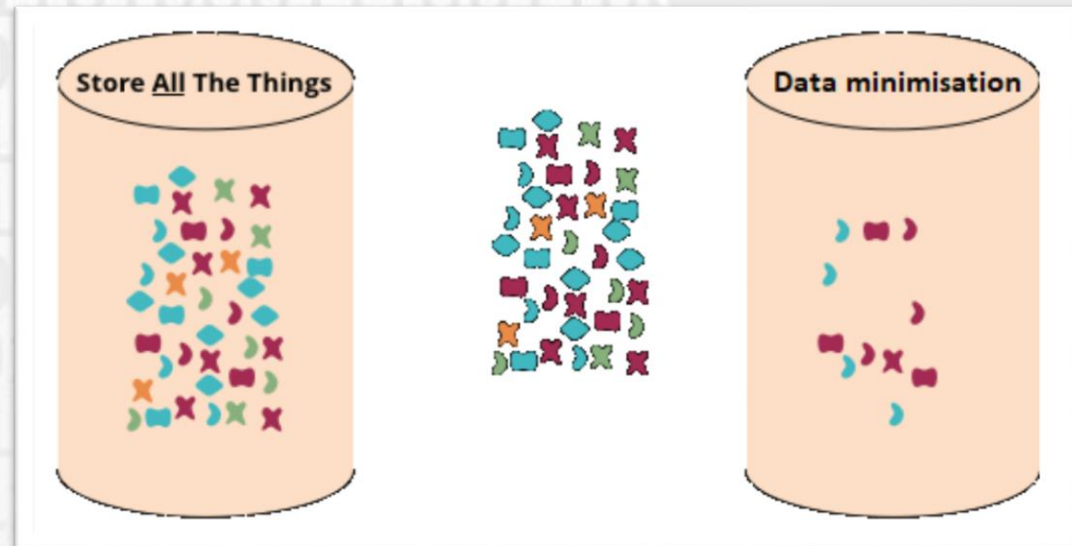
Off

Let Windows track app launches to improve Start and search results

Off



**Data protection by default**

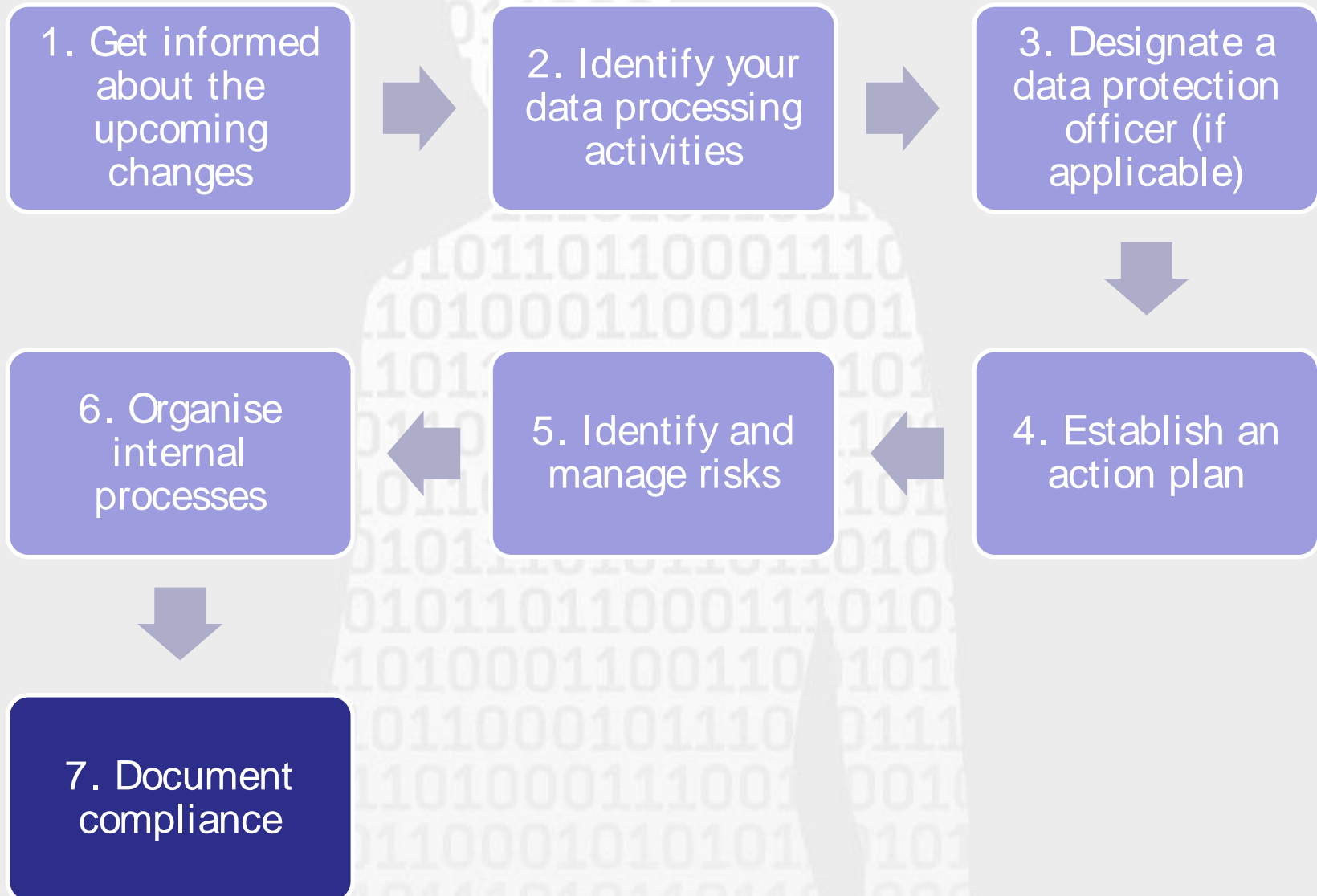


## 6. Organise internal processes <sup>5/5</sup>

Main objectives:

- Develop a **data protection friendly culture**;
- **Anticipate** the risks and possible issues;
- Develop **secure data management** throughout the **entire life cycle of the data**;
- **Be transparent and inform the public** about their rights.

# 7 steps to prepare for compliance





## 7. Document compliance <sup>1/3</sup>

**Obligation** to prove your compliance



Through documents  
and internal procedures  
that need to be  
re-examined and updated regularly.



## 7. Document compliance <sup>2/3</sup>

### **Documentation relating to your processing activities:**

- The record of processing activities (for controllers) or categories of processing activities (for processors);
- The data protection impact assessments carried out for the processing activities which are likely to result in high risks for the rights + freedoms of data subjects;
- The framework for transfers of personal data outside the EU (in particular standard data protection clauses, BCR and certification mechanisms);
- The record of all personal data breaches, which must set out the consequences of the breach as well as the remedial action taken.

### **Interaction with data subjects:**

- The information to the data subjects;
- The manner in which the consent of the data subject is obtained;
- The procedures in place to enable data subjects to exercise their rights.

### **Contracts and other documentation:**

- The contracts with processors;
- The internal procedures in the event of a data breach;
- The evidence that data subjects have given their consent, if consent is the lawful condition for processing.

## 7. Document compliance <sup>3/3</sup>

**Do not forget to document the data flows:**

- Contracts with processors;
- Contracts with third parties for the re-use of data;
- Documents that prove the compliance of external users of your data.

## Info

In order to be of assistance with the implementation of your compliance process, the CNPD will offer:

- a compliance support tool (in cooperation with LIST);
- information brochures;
- an update of its website.

# Commission nationale pour la protection des données



1, avenue du Rock'n'Roll  
L-4361 Esch-sur-Alzette (Belval)  
261060-1  
[www.cnpd.lu](http://www.cnpd.lu)  
[info@cnpd.lu](mailto:info@cnpd.lu)