FUTURA

LAW & TECH

RISK, CYBERSECURITY & DATA PROTECTION

Deep Learning Sessions Lisboa

Legal Concerns for Researching in Machine Learning: A Framework

RODRIGO ADÃO DA FONSECA

CEO, FUTURA – Law & Tech

DPO, NOVA University

9th June, 2021

FUTURA

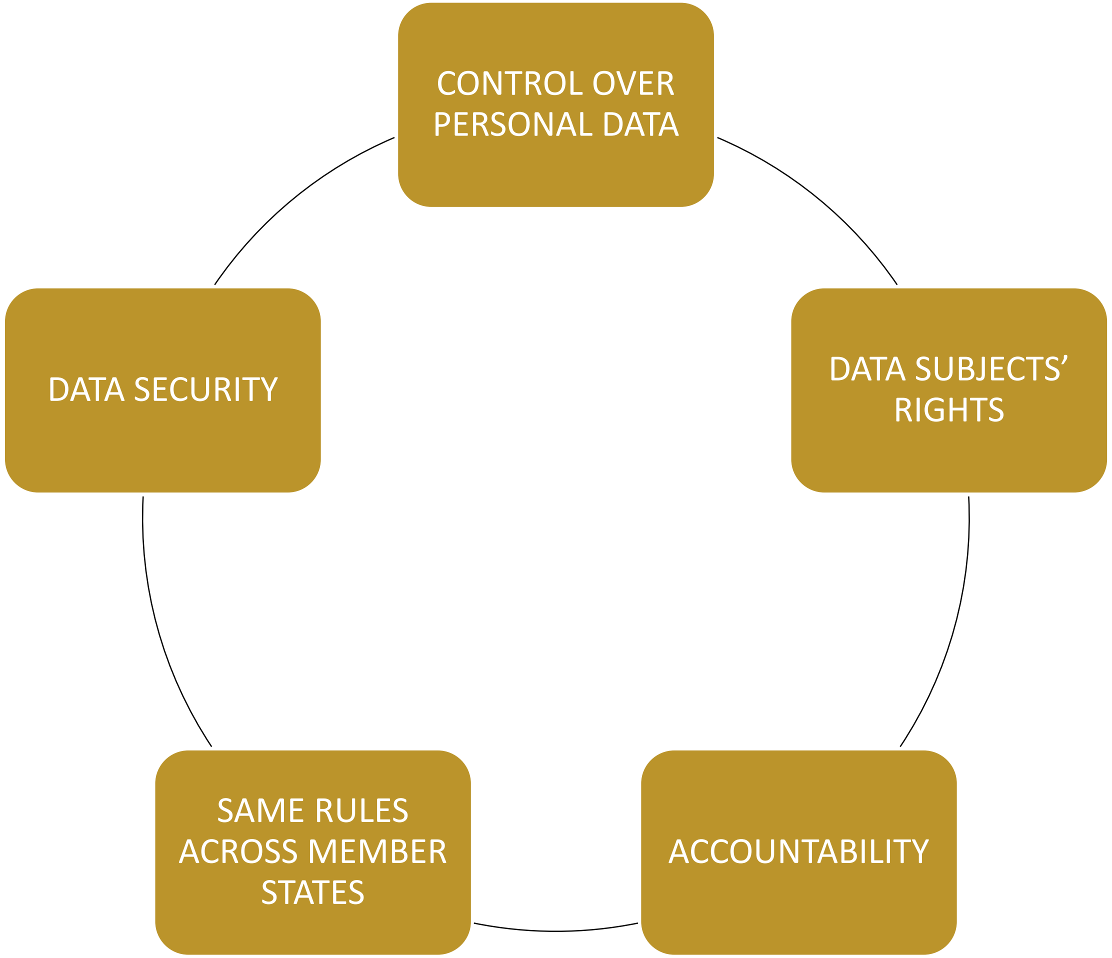
THE WORD IS CHACHING WITH THE DIGITAL REVOLUTION

Reassess the legal framework from 1995 which was inadequate for new technological challenges (cloud computing, social networks, etc.)

GDPR AND OTHER LEGISLATION

Support the "Digital Single Market" and the "Digital Agenda For Europe" – implementing this policies cannot jeopardize fundamental rights

THE GDPR IN A NUTSHELL - GOALS



CONTROL OVER PERSONAL DATA

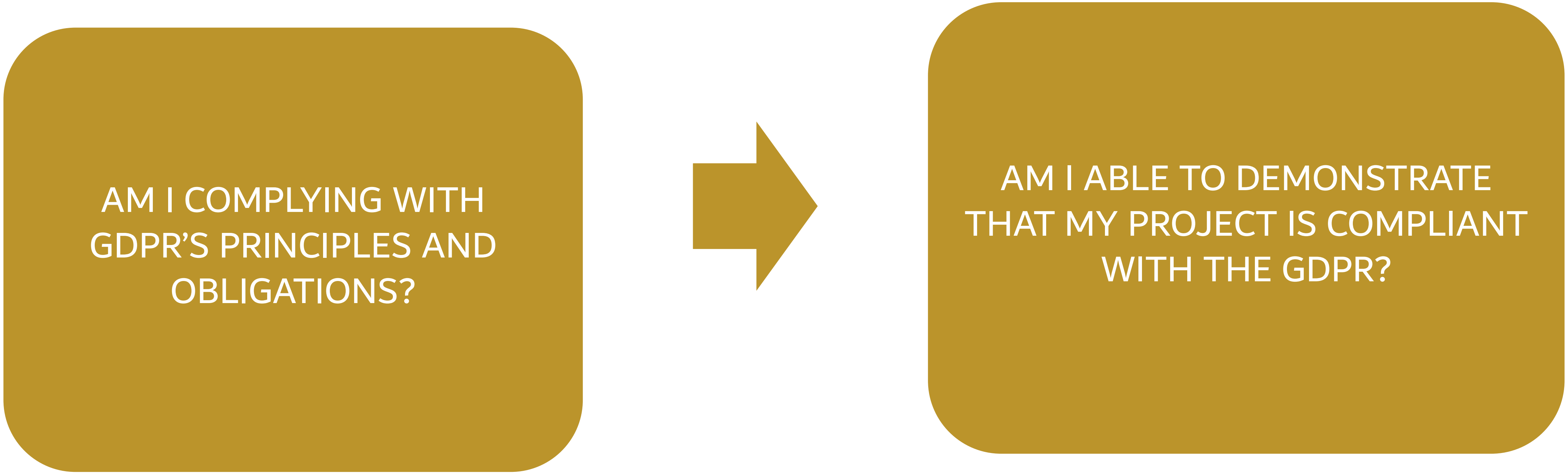
DATA SUBJECTS' RIGHTS

ACCOUNTABILITY

SAME RULES ACROSS MEMBER STATES

DATA SECURITY

ACCOUNTABILITY IN SCIENTIFIC RESEARCH



AM I COMPLYING WITH GDPR’S PRINCIPLES AND OBLIGATIONS?

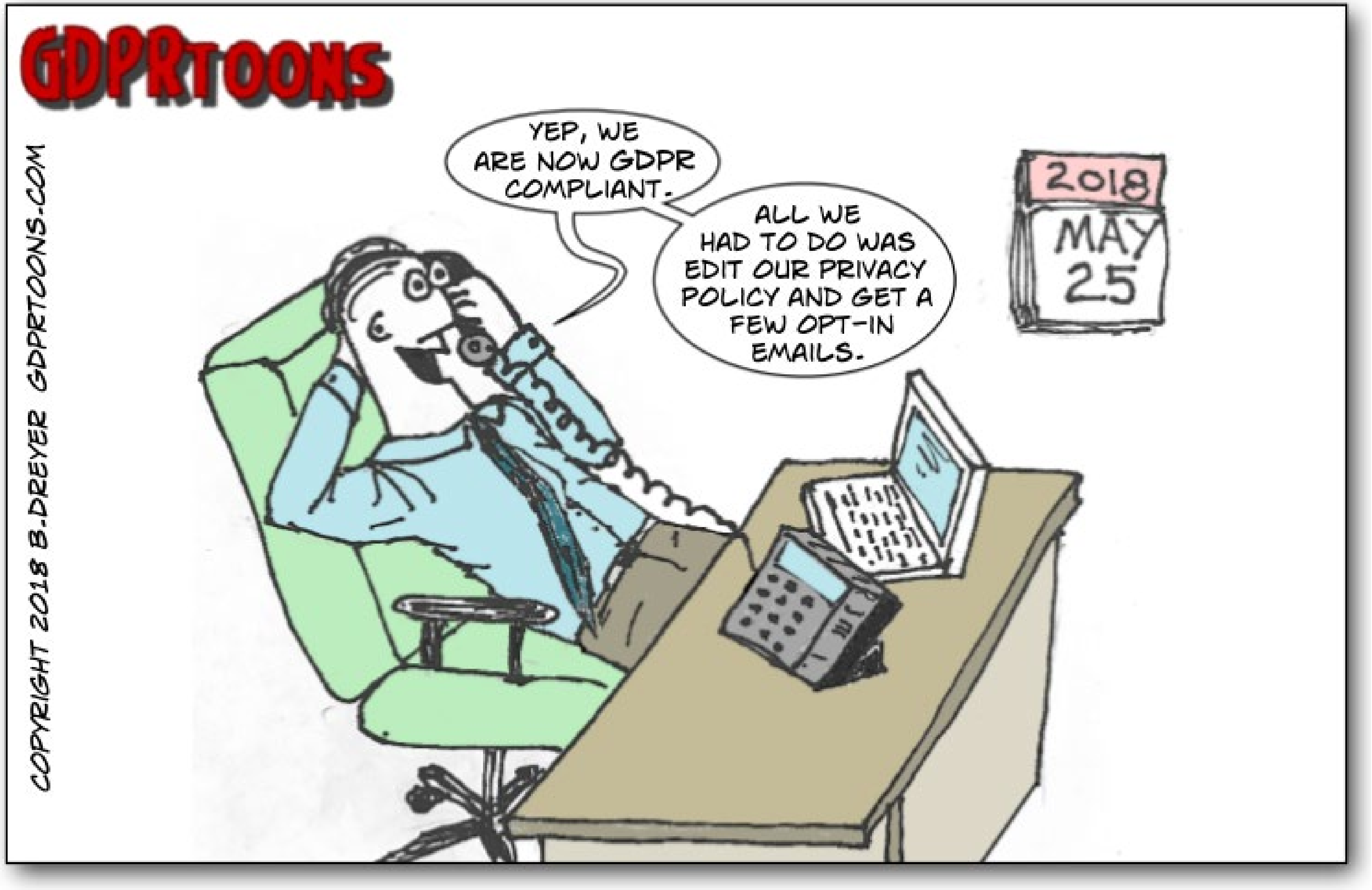
AM I ABLE TO DEMONSTRATE THAT MY PROJECT IS COMPLIANT WITH THE GDPR?

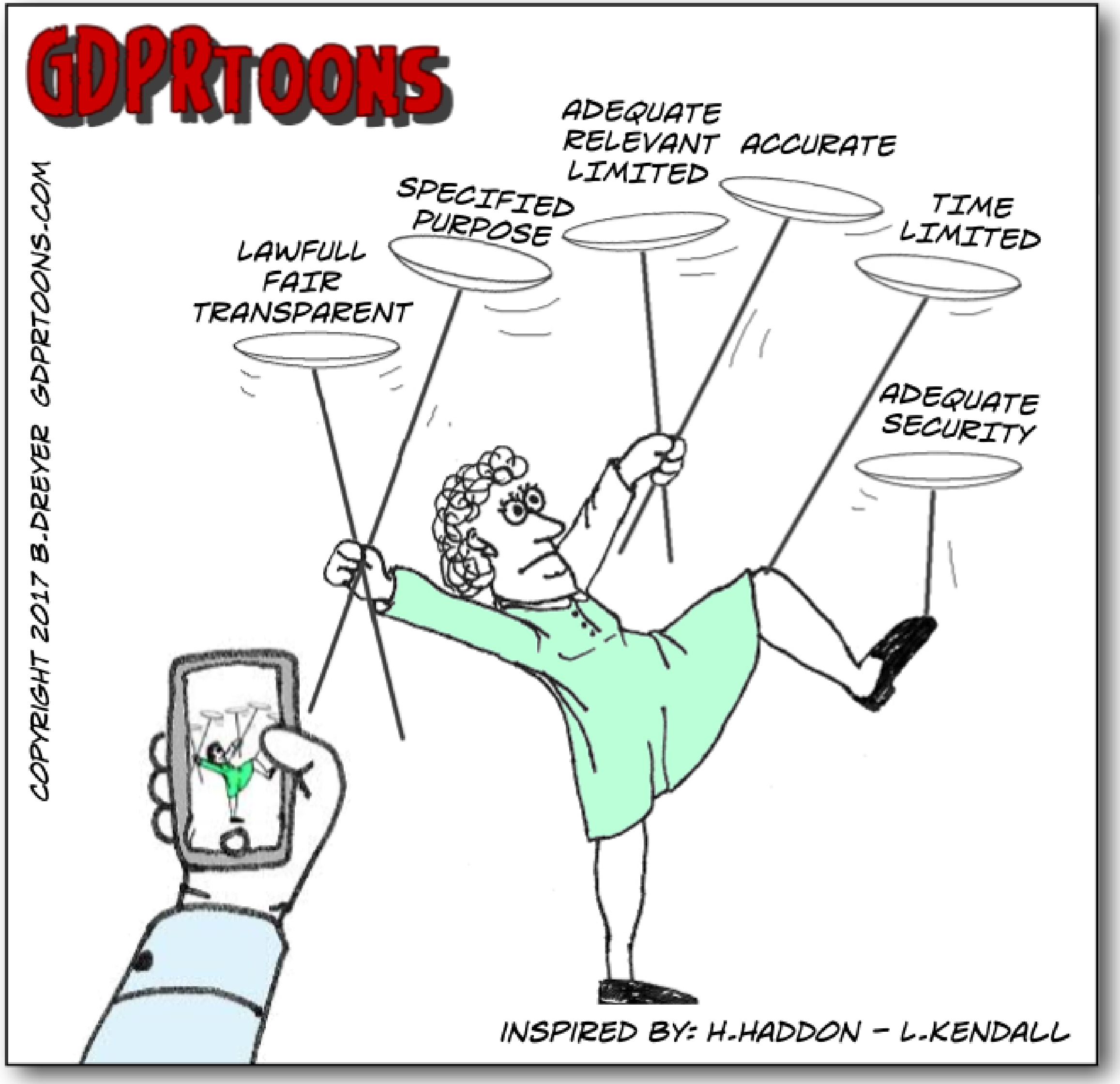
GDPR AND RISK

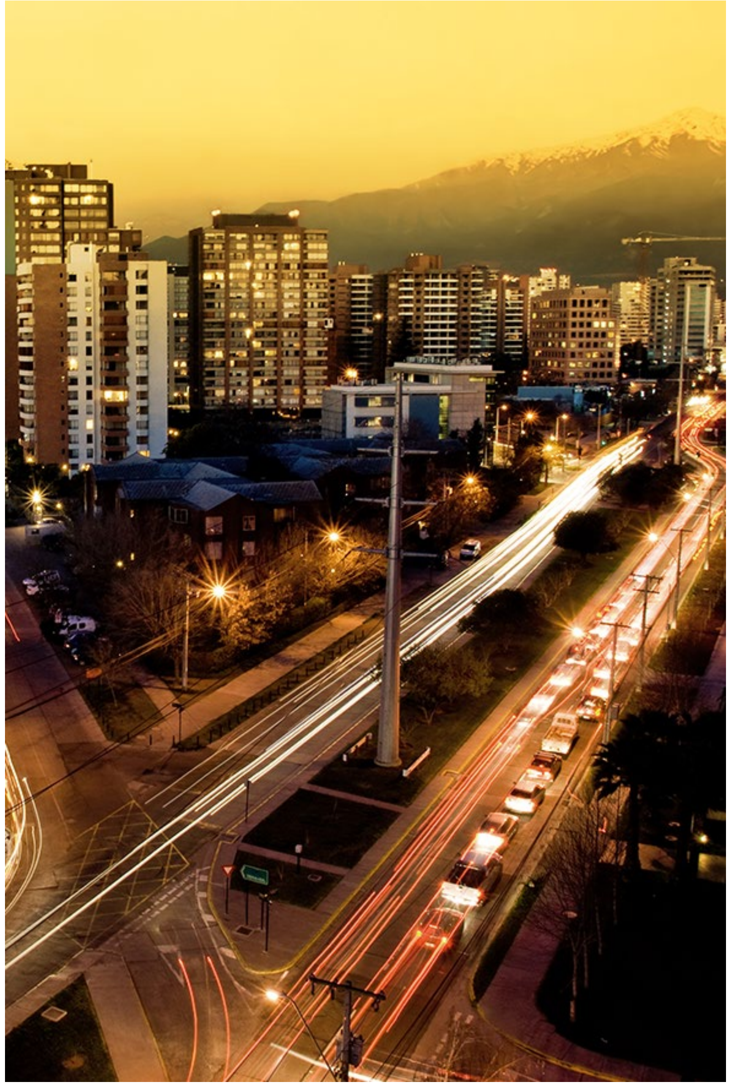
RIGHTS AND FREEDOMS OF THE DATA SUBJECT

TECHNICAL AND ORGANISATIONAL MEASURES

ACCOUNTABILITY


GDPRtoons
YEP, WE ARE NOW GDPR COMPLIANT.
ALL WE HAD TO DO WAS EDIT OUR PRIVACY POLICY AND GET A FEW OPT-IN EMAILS.
2018
MAY 25
COPYRIGHT 2018 B.DREYER GDPRTOONS.COM

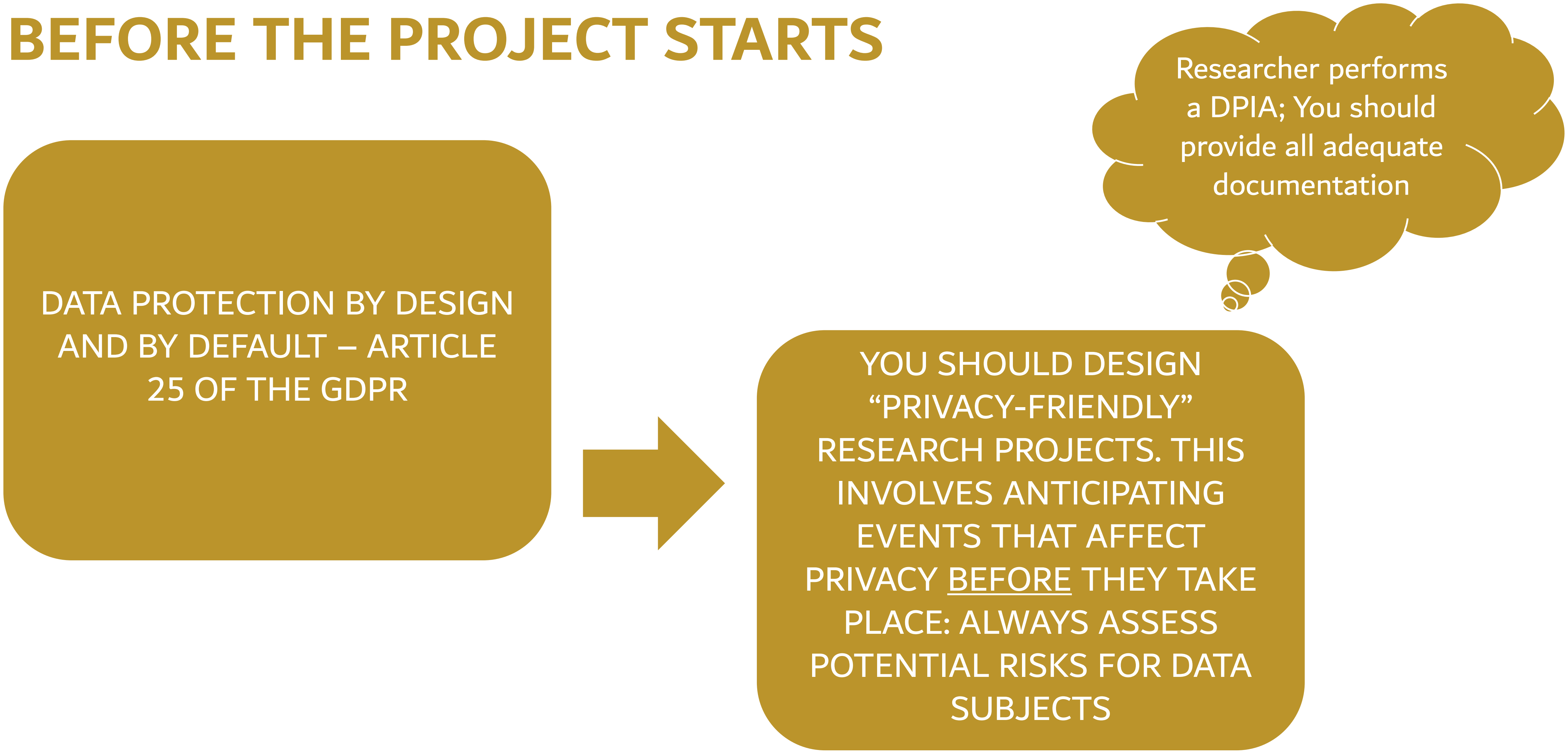

GDPRtoons
COPYRIGHT 2017 B.DREYER GDPRTOONS.COM
LAWFULL FAIR TRANSPARENT
SPECIFIED PURPOSE
ADEQUATE RELEVANT LIMITED
ACCURATE
TIME LIMITED
ADEQUATE SECURITY
INSPIRED BY: H.HADDON – L.KENDALL



HOW TO COMPLY?

- **BEFORE** THE PROJECT STARTS;
- **DURING** THE PROJECT;
- **AT THE END** OF THE PROJECT.

BEFORE THE PROJECT STARTS



DATA PROTECTION BY DESIGN AND BY DEFAULT – ARTICLE 25 OF THE GDPR

YOU SHOULD DESIGN "PRIVACY-FRIENDLY" RESEARCH PROJECTS. THIS INVOLVES ANTICIPATING EVENTS THAT AFFECT PRIVACY BEFORE THEY TAKE PLACE: ALWAYS ASSESS POTENTIAL RISKS FOR DATA SUBJECTS

Researcher performs a DPIA; You should provide all adequate documentation

BEFORE THE PROJECT STARTS

Measuring the Risk: assess the risk of your project for data subjects (performing a “Data Protection Impact Assessment”):

1. Identify all personal data and, in particular, special categories of personal data (article 9 of the GDPR: health data included);
2. Will you use new technologies? If so, consider performing a specific Data Protection Impact Assessment for the use of technology.
3. Are the tools you will use invasive for data subjects?
4. What will be the impact of your project for data subjects?
5. Can the processing give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?
6. Can data subjects be deprived of their rights and freedoms?
7. Will I process personal data of vulnerable natural persons, in particular of children?
8. Does the processing involve a large amount of personal data and affect a large number of data subjects?

BEFORE THE PROJECT STARTS

Lawfulness: you need to have a valid legal ground to process personal data.

1. Understand the reason and the legal ground why you can process data (contract, legal obligation, public interest, vital interests, legitimate interest); and
2. Collect consent, when necessary.

BEFORE THE PROJECT STARTS

Minimise: minimisation of personal data can be achieved by collecting data of less people, or collecting less data of people:

1. Determine beforehand what personal data (name, age, date of birth, sexual preferences, genetic information, bank account details?) you need for your project;
2. Select only relevant data subjects and relevant attributes;
3. Exclude people or attributes in advance.

BEFORE THE PROJECT STARTS

Purpose and storage limitation: the data you collect must be necessary for the purposes of your project. When the purposes end you should erase the data:

1. Understand why you need the personal data you collect;
2. You will have to explain to data subjects why you are collecting his/her data;
3. The purpose of processing determines the retention period (general practice: 2 years after the project is over?)
4. Identify whether any legal requirements apply for the retention of any particular data;
5. Where will personal data be stored (this may include own servers, third party servers, email accounts, desktops, researchers owned devices, paper files)?

BEFORE THE PROJECT STARTS

You may have to disclose privacy notices to provide to data subjects

Transparency and accuracy: what you will do with the data collected must be explained in a very clear and concise way to data subjects. Also, you must only process accurate personal data.

1. If possible, directly collect the data from data subjects himself (interview, inquiry, other);
2. Inform data subjects according to articles 13 and 14 of the GDPR;
3. Verify the accuracy of the data you process and ensure that you process only updated personal data.

BEFORE THE PROJECT STARTS

You may need to sign third party contracts

Third parties: who are the third parties of your project? Suppliers or institutional partners?

1. Verify if third parties are GDPR compliant;
2. Assess the contracts with third parties and eventually conclude new contracts or add contractual clauses to previous contracts.

DURING THE PROJECT

You may need a procedure to respond to data subjects requests

Data subjects' rights: data subjects have several rights according to the GDPR.

1. Ensure you have a procedure to reply to data subjects' requests;
2. Ensure that all researchers can identify a request of data subjects;
3. Access if the request is valid or not.

DURING THE PROJECT

You should at least follow best practices on what to do online and offline to ensure security

Security: ensure the security of processing.

- Actions:

1. Prepare backups;
2. Restrict access to personal data upon request and only the collaborators who actually need it for a task;
3. Ensure that all staff uses strong passwords and/or multi-factor authentication;
4. Ensure that all staff uses the latest versions of software and other apps;
5. Ensure the traceability of personal data;
6. Anonymise (re-identification of data subjects is not possible) or pseudonymize the data;
7. Ensure that all staff is capable of identifying a data breach and is aware of the procedures related to this kind of incident.

DURING THE PROJECT

Transfer of personal data: is there anyone involved in the project who is in a country outside the EU or in an international organization?

- Actions:

1. Identify the third country or international organization;
2. Is there any adequacy decision?
3. If not, adopt adequate safeguards (example: contract).

When in doubt, ask your DPO!

AT THE END OF THE PROJECT

Erasure: safely ensure the erasure of personal data and document it.

1. Erase personal data no longer necessary;

2. Be sure to document this since the national supervisory authority, (in Portugal, the CNPD or Comissão Nacional de Proteção de Dados Pessoais), can ask to verify;

3. You can anonymise the data. This may, for example, be achieved by:

- Erasing unique identifiers which allow the allocation of a data set to a unique person;
- Erasing single pieces of information that identify data subjects (whether alone or in combination with other pieces of information);
- Separating personal data from non-identifying information (e.g. an order number from the customer’s name and address); or
- Aggregating personal data in a way that no allocation to any individual is possible.

DATA PROTECTION AND AI
THE ARTIFICIAL INTELLIGENCE ACT

The European Commission has been working on several guidelines on the challenges associated with artificial intelligence.

The goal is to balance the many opportunities offered by AI and potential high risks it poses to safety and fundamental rights equally.

The Comission issued recently a Proposal for a regulation laying down harmonised rules on artificial intelligence (The Artificial Intelligence Act) and amending certain union legislative acts.

The Artificial Intelligence Act is without prejudice and will complement the GDPR.

Assess Risk

IT'S ALL ABOUT MANAGING RISK

Mitigate Risk

FUTURA

Sobre a FUTURA

A FUTURA é uma empresa de consultoria de Law & Tech, que presta serviços especializados de gestão do risco, cibersegurança e proteção de dados.

A FUTURA foi criada para ajudar as empresas a compreender a Revolução Digital 4.0. e as novas ameaças cibernéticas, os riscos que lhes estão associados, e as novas exigências legais e regulamentares aplicáveis. A FUTURA nasceu para apoiar as empresas, em particular, os seus quadros diretivos, a definir estratégias para identificar, integrar, gerir e mitigar o ciberisco, num contexto de gestão da mudança.

Falamos uma linguagem de gestão. Traduzimos o conhecimento técnico e jurídico para uma linguagem tangível, reduzindo a opacidade que rodeia os riscos de cibersegurança.

Para mais informação:
https://futuranet.eu

Rodrigo Adão da Fonseca
Founder & CEO
afonseca@futuranet.eu

EMPRESA
FUTURA – Law & Tech

ESCRITÓRIO
EDIFÍCIO SPACES
Praça Marquês de Pombal 14
1250-162 Lisboa