GDPR

- RESEARCH AND DATA MANAGEMENT –

Prepared by:
dr. Irisz Szel
In-house legal counsel
Central European University, Budapest

CEU CENTRAL EUROPEAN UNIVERSITY

CONTENT

I. GDPR – General impacts

II. GDPR and Research – Conducting a DPIA

III. Open Access & Data Management

I. CEU's Best Practice

Part I.

GDPR
- General Impacts -

A new data protection landscape

May 25, 2018 the new GDPR becomes applicable in all Member States (national laws will need to be amended in order to regulate certain aspects of data protection).

Compared to the Directive, the Regulation:

- ✓ strengthens **data protection principles**,
- ✓ requires organisations to implement internal measures to **demonstrate compliance** and
- ✓ provides **greater enforcement powers** for regulators.

The main aim of the Regulation is to strengthen the right of individuals:

- ✓ the right to be forgotten
- ✓ rights in relation to profiling.

Accountability approach: organisations must be able to demonstrate that they have **procedures and policies** in place for dealing with their obligations to data subjects and their data processing practices are **transparent**.

THE SIX GDPR PRINCIPLES – Principles of data processing

1. **Lawfulness, fairness and transparency**
   - ✓ Transparency: Tell the subject what data processing will be done.
   - ✓ Fair: What is processed must match up with how it has been described
   - ✓ Lawful: Processing must meet the tests described in GDPR

2. **Purpose limitations**
   Personal data can only be obtained for "specified, explicit and legitimate purposes". Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

3. **Data minimization**
   Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". No more than the minimum amount of data should be kept for specific processing.

4. **Accuracy**
   Data must be "accurate and where necessary kept up to date".

5. **Storage limitations**
   Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary". Data no longer required should be removed (anonymized, destroyed, etc.).

6. **Integrity and confidentiality**
   Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".

Part II.

GDPR and Research
- Conducting a DPIA -

What's new under the GDPR?

- The GDPR introduces a **new obligation** to do a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk that you cannot mitigate, you must consult the National Data Protection Authority

- New focus on **accountability** and **data protection by design**

- Some organizations already carry out privacy impact assessments (PIAs) as a matter of good practice

- DPIAs are **mandatory** in some cases, and there are specific legal requirements for content and process

Treating Personal Data in Research

1. Privacy by design and by default

- In your research design, address the six security and privacy principles
- Conduct a data protection impact assessment to identify risks and formulate countermeasures
- Communicate the security and privacy measures for your research with all participants and data subjects.

2. Before research

- Make sure your data subjects are well informed about the purpose of the research and their risks before they sign the informed consent form (Privacy Notice).
- Only generate and use data that are relevant for the purpose of your research.
- Use a computer with an encrypted hard drive, encrypt your sensitive data, use safe and secure file storage and sharing.

3. During research

- Anonymize and/or pseudonymize the data and work with the de-identified data.
- Work safe: do not leave printouts on the printer desk, do not use public wifi, do not work where others can easily watch your screen or can hear you talk.
- During research feel free to consult the DPO in case of practical issues or just reflect on aspects.

What is a DPIA?

A DPIA is a way to

- systematically and comprehensively analyze personal data processing
- help **identify** and **minimize** data protection risks
- assess whether or not remaining risks are **justified**.

DPIAs should consider

- compliance risks,
- broader risks to the rights and freedoms of individuals,
- the potential for any significant social or economic disadvantage.

The focus is on the **potential for harm** - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the **likelihood** and the **severity** of any impact on individuals.

DPIA - a legal requirement

- Part of the **accountability** obligation
- Requirement for **data protection by design and default**
- Legal requirement for any type of processing, including certain specified types of processing, that are likely to result in a high risk to the rights and freedoms of individuals.
- Failing to carry out a DPIA may result in a fine of up to €10 million, or 2% global annual turnover if higher.

Article 25 of the GDPR:

"*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures… and … integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*."

DPIA – a compliance tool

- Consistent use of DPIAs increases the **awareness** of privacy and data protection issues within the organization
- Effective way to assess and **demonstrate compliance**
- Helps to to **identify and fix problems** at an early stage
- Security of individuals ⟹ (consultation)
- Improved **transparency**, reputation and trust
- **Financial benefits**
  - a simpler and less costly solution
  - avoiding potential reputational damage
  - minimizing the amount of information and reduce the ongoing costs

How are DPIA-s used?

"*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*."(Recital 84)

- DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to **integrate the outcomes** of the DPIA back into your project plan.
- DPIA is not a one-off exercise to file away. A DPIA is a '**living' process** to help manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and reassess if anything changes.

What kind of ‘risk’ do they assess?

“*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.*” (Rec. 85)

- Focus: any **potential** harm to individuals
- Not just actual damage - the possibility for more intangible harm, incl. any “significant economic or social disadvantage”
- The impact on society as a whole may also be a relevant risk factor (loss of public trust)
- A DPIA must assess the **level** of risk, and in particular whether it is ‘high risk’.
- Assessing the level of risk involves looking at both the **likelihood** and the **severity** of the potential harm.

When do we need to do a DPIA?

"*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is* ***likely to result in a high risk*** *to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks*." (Art 35 (1))

High risk

- potential for any significant physical, material or non-material harm to individuals
- consider both the likelihood and severity of any potential harm to individuals

Likely to result in a high risk

- Are there features which point to the potential for high risk? Screen red flags which indicate that you need to do a DPIA to look at the risk

What types of processing automatically require a DPIA?

In particular, the GDPR (Art. 35 (3)) says you **must do a DPIA** if you plan to:

- use systematic and extensive **profiling** with significant effects
- process **special category of data** or **criminal** offence data on a large scale or
- **systematically monitor** publicly accessible places on a large scale.

Further processing that <u>may</u> require a DPIA – UK example

- **New technologies:** processing involving the use of new technologies, or the novel application of existing technologies
- **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
- **Large-scale profiling:** any profiling of individuals on a large scale
- **Biometrics:** any processing of biometric data
- **Genetic data:** any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject
- **Data matching:** combining, comparing or matching personal data obtained from multiple sources
- **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort
- **Tracking:** processing which involves tracking an individual's geolocation or behavior, including but not limited to the online environment
- **Targeting of children or other vulnerable individuals:** The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children
- **Risk of physical harm:** Where the processing is of such a nature that a personal data breach could jeopardize the [physical] health or safety of individuals

Also **consider** a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is **good practice** to do a DPIA for any major new project involving the use of personal data.

Other factors indicating a high risk – EU Art 29 WP's recommendations

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organizational solutions
- Preventing data subjects from exercising a right or using a service or contract

In most cases, a combination of two of these factors indicates the need for a DPIA. You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high risk, but you should **document** your reasons.

On the other hand, in some cases you may need to do a DPIA if only one factor is present – and it is good practice to do so

Exceptions

You **may not** have to carry out a DPIA if:

You are processing on the basis of legal obligation or public task

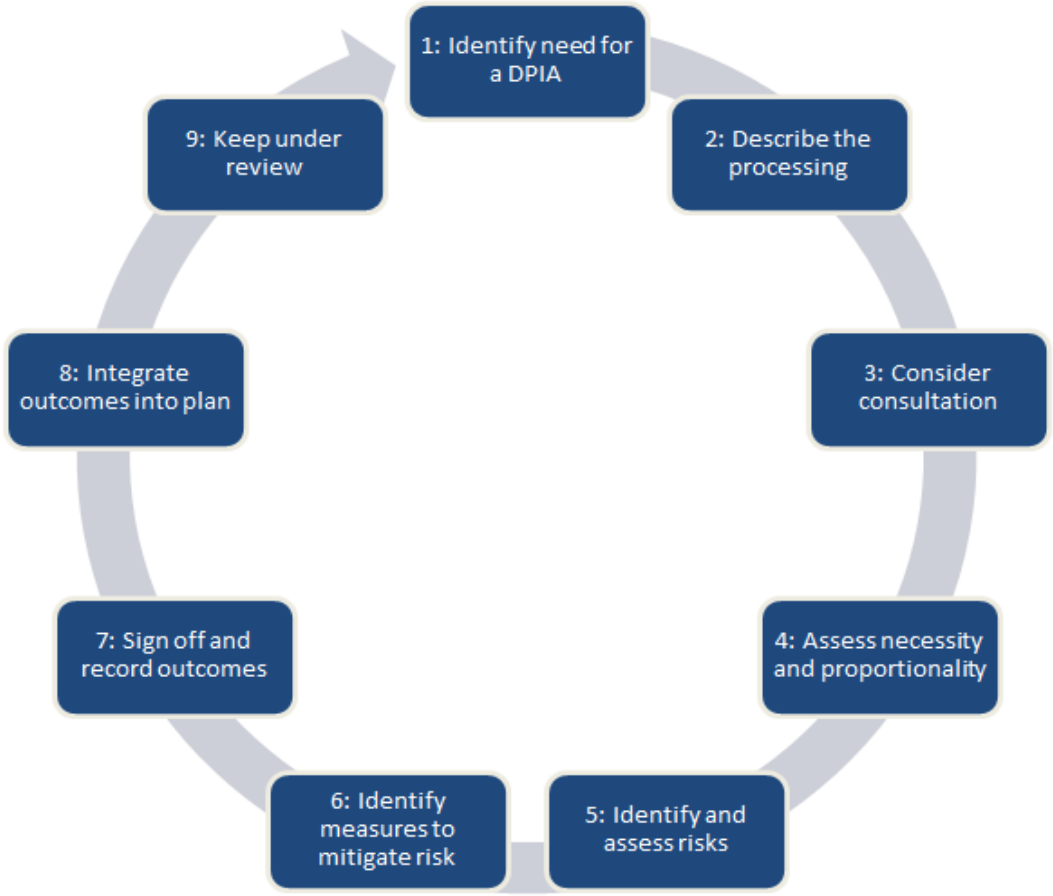
This exception only applies if:

- you have a clear statutory basis for the processing;
- the legal provision or a statutory code specifically provides for and regulates the processing operation in question;
- you are not subject to other obligations to complete DPIAs, or
- a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted.

- **You have already done a substantially similar DPIA**

- **National authorities may issue a list of processing operations which do not require a DPIA**

How do we carry out a DPIA?



Step 1: How do we decide whether to do a DPIA?

- Ask your DPO for advice. If you have any major project which involves the use of personal data it is good practice to carry out a DPIA.

- Check whether your processing is on the list of types of processing which automatically require a DPIA. If not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.

- If you carry out this screening exercise and decide that you do not need to do a DPIA, you should document your decision and the reasons for it, including your DPO's advice.

- **If you are in any doubt, do a DPIA.**

Step 2: How do we describe the processing?

Describe how and why you plan to use the personal data. Your description must include **"the nature, scope, context and purposes** of the processing".

I. **The nature of the processing** is what you plan to do with the personal data. This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

II. **The scope of the processing** is what the processing covers. This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

Step 2: How do we describe the processing? (cont.)

III. The context of the processing includes internal and external factors which might affect expectations or impact

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern;
- whether you comply with any GDPR codes of conduct;
- whether you have considered and complied with relevant codes of practice.

IV. The purpose of the processing is the reason why you want to process the personal data

- your legitimate interests, where relevant;
- the intended outcome for individuals;
- the expected benefits for you or for society as a whole.

Step 3: Do we need to consult individuals?

- You should **seek the views of individuals** unless there is a good reason not to.
- If you decide that it is not appropriate to consult individuals then you should **record this decision** as part of your DPIA, with a clear explanation. For example, consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.
- If your DPIA decision is at odds with the views of individuals, you need to document your **reasons for disregarding** their views.

Step 4: Do we need to consult anyone else?

- If you use a **data processor**, you may need to ask them for information and assistance. Your contracts with processors should require them to assist.

- You should consult all relevant **internal stakeholders**, in particular anyone with responsibility for information security.

- Consider seeking legal advice or advice from other independent experts such as **IT experts, sociologists or ethicists** where appropriate. However, there are no specific requirements to do so.

- In some circumstances you might also need to consult the **National Data Protection Authority** once you have completed your DPIA.

Step 5: How do we assess necessity and proportionality?

- ✓ Do your plans **help to achieve** your purpose?
- ✓ Is there any **other reasonable way** to achieve the same result?
- ✓ The Article 29 guidelines also say you should include **how you ensure** data protection compliance, which are a good measure of necessity and proportionality.
- ✓ In particular, you should include relevant details of:
  - your lawful basis for the processing;
  - how you will prevent function creep;
  - how you intend to ensure data quality;
  - how you intend to ensure data minimization;
  - how you intend to provide privacy information to individuals;
  - how you implement and support individuals rights;
  - measures to ensure your processors comply; and
  - safeguards for international transfers.

Step 6: How do we identify and assess risks?

Consider the **potential impact on individuals and any harm or damage** that might be caused by your processing – whether physical, emotional or material.

In particular look at whether the processing could possibly contribute to:

- ✓ inability to exercise rights (including but not limited to privacy rights);
- ✓ inability to access services or opportunities;
- ✓ Loss of control over the use of personal data;
- ✓ discrimination;
- ✓ identity theft or fraud;
- ✓ financial loss;
- ✓ reputational damage;
- ✓ physical harm;
- ✓ loss of confidentiality;
- ✓ reidentification of pseudonymised data; or
- ✓ any other significant economic or social disadvantage.

Likelihood and severity of risks

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

Step 7: How do we identify mitigating measures?

Options for reducing that risk

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

Step 8: How do we conclude our DPIA?

Record

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of ‘residual risk’ after taking additional measures; and
- whether you need to consult the authorities.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

What happens next?

- **Integrate** the outcomes of your DPIA back into your project plans.
- **Monitor** the ongoing performance of the DPIA.
- If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to **consult the authorities** before you can go ahead with the processing.
- It is good practice to **publish** your DPIA to aid transparency and accountability.
- You need to keep your DPIA under **review**, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

Part III

- Open Access & Data Management -

Open Access

Horizon 2020 requirements

- **open access to scientific publications**, which is an *obligation*, and
- **open access to research data**, where opt-outs are possible, and
- **research data management**

What is Open Access (OA)?

- Open access can be defined as the practice of **providing on-line access to scientific information that is free of charge to the reader**. In the context of R&D, open access typically focuses on access to '*scientific information*' or '*research results*', which refers to two main categories:

Peer-reviewed scientific research articles (primarily published in academic journals)

Research data

Open Access to Research Data

- **Research data is information** (particularly facts or numbers) collected to be examined and considered, and to serve as a basis for reasoning, discussion or calculation.
- **Open access to research data** - the right to access and reuse digital research data under the terms and conditions set out in the Grant Agreement.

Horizon 2020 Open Research Data Pilot and Data Management Plan

In Horizon 2020 the Commission has launched a **flexible pilot for open access to research data (ORD pilot)**. The pilot **aims to improve and maximise access to and re-use of research data generated by Horizon 2020 projects**, taking into account

- the need to balance openness and protection of scientific information
- commercialisation and IPR
- privacy concerns
- security
- data management and preservation questions

Scope of the pilot

- In previous Work Programmes the ORD Pilot was limited to some areas of Horizon 2020.
- As of the Work Programme 2017 the Open Research Data pilot is extended to cover all thematic areas of Horizon 2020 per default. However, the Commission recognizes that some research data cannot be made open and applies the principle of '**as open as possible, as closed as necessary**'. It is therefore possible to **opt out of research data sharing at any stage** - before or after the signature of the grant agreement - but reasons have to be given e.g. for intellectual property rights (IPR) concerns, privacy/data protection concerns, national security concern, if it would run against the main objective of the project or for other legitimate reasons (see General Annex 1 of the 2017 Work Programme adopted at 25 July 2016).

Data set

The Open Research Data Pilot applies primarily to the **data needed to validate the results** presented in scientific publications. Other data can also be provided by the beneficiaries on a voluntary basis.

Data Management Plan – general definition

- Data Management Plans (DMPs) are a **key element** of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a Horizon 2020 project.

- As part of making research data findable, accessible, interoperable and re-usable (FAIR), a **DMP should include information** on:

✓ the handling of research data during & after the end of the project
✓ what data will be collected, processed and/or generated
✓ which methodology & standards will be applied
✓ whether data will be shared/made open access and
✓ how data will be curated & preserved (including after the end of the project).

- A DMP is **required for all projects participating in the extended ORD pilot**, unless they opt out of the ORD pilot. However, projects that opt out are still encouraged to submit a DMP on a voluntary basis.

- Participating projects will be required to develop a Data Management Plan (DMP), in which they will **specify what data will be open**: detailing what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved.

- **Costs** associated with open access to research data, including the creation of the data management plan, can be claimed as eligible costs of any Horizon 2020 grant.

Proposal submission & evaluation

- Whether a proposed project participates in the ORD pilot or chooses to opt out does not affect the evaluation of that project. In other words, proposals will not be penalized for opting out of the extended ORD pilot.

- Since participation in the ORD pilot is not an evaluation criterion, **the proposal is not expected to contain a fully developed DMP**. However, good research data management as such should be addressed under the impact criterion, as relevant to the project.

- **Your application** should address the following issues:

✓ What standards will be applied?
✓ How will data be exploited &/or shared/made accessible for verification & reuse?
✓ If data cannot be made available, why not?
✓ How will data be curated & preserved?

- **Your policy** should

✓ reflect the current state of consortium agreements on data management
✓ be consistent with exploitation and Intellectual Property Rights (IPR) requirements

- You should also ensure **resource and budgetary planning** for data management and include a deliverable for an initial DMP at month 6 at the latest into your proposal.

Research data management plans during the project life cycle

First version

- Once a project has had its funding approved and has started, you **must submit a first version of your DMP (as a deliverable) within the first 6 months of the project**. The Commission provides a DMP template in annex, the use of which is recommended but voluntary.

Updates

- The DMP needs to be updated over the course of the project whenever **significant changes** arise, such as (but not limited to):

✓ new data

✓ changes in consortium policies (e.g. new innovation potential, decision to file for a patent)

✓ changes in consortium composition and external factors (e.g. new consortium members joining or old members leaving).

- The DMP should be updated as a minimum in time with the periodic evaluation/assessment of the project.
- If there are no other periodic reviews foreseen within the grant agreement, then such an update needs to be made in time for the final review at the latest.
- Furthermore, the consortium can define a timetable for review in the DMP itself.

Periodic reporting

- For general information on periodic reporting please check the relevant sections of the **online manual** (How to fill in reporting tables for publications, deliverables and process for continuous reporting in the grant management system of the Participant portal).

Support

Reimbursement of costs

- Costs related to open access to research data in Horizon 2020 are eligible for reimbursement during the duration of the project under the conditions defined in the **H2020 Grant Agreement**, in particular Article 6 and Article 6.2.D.3, but also other articles relevant for the cost category chosen.

Data Management Plan

- A **H2020 DMP template** is provided in Annex 1 of the **Guidelines**. While the Commission does not currently offer its own online tool for data management plans, beneficiaries can generate DMPs online, using tools that are compatible with the requirements set out in Annex 1 (see also section 7 of Annex I).
- **ERC Data Management Plan Template**

Horizon 2020 DMP Template

In general

The Horizon 2020 FAIR DMP template has been designed to be applicable to any Horizon 2020 project that **produces, collects or processes** research data.

You should **develop a single DMP for your project** to cover its overall approach. However, where there are specific issues for individual datasets (e.g. regarding openness), you should clearly spell this out.

The template is not intended as a strict technical implementation of the FAIR principles, it is rather inspired by FAIR as a **general concept**.

FAIR data management

Research data should be 'FAIR', that is **findable, accessible, interoperable and re-usable**. These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution.

Horizon 2020 DMP Template (cont.)

Structure of the template

- The template is a **set of questions** that you should answer with a level of detail appropriate to the project.

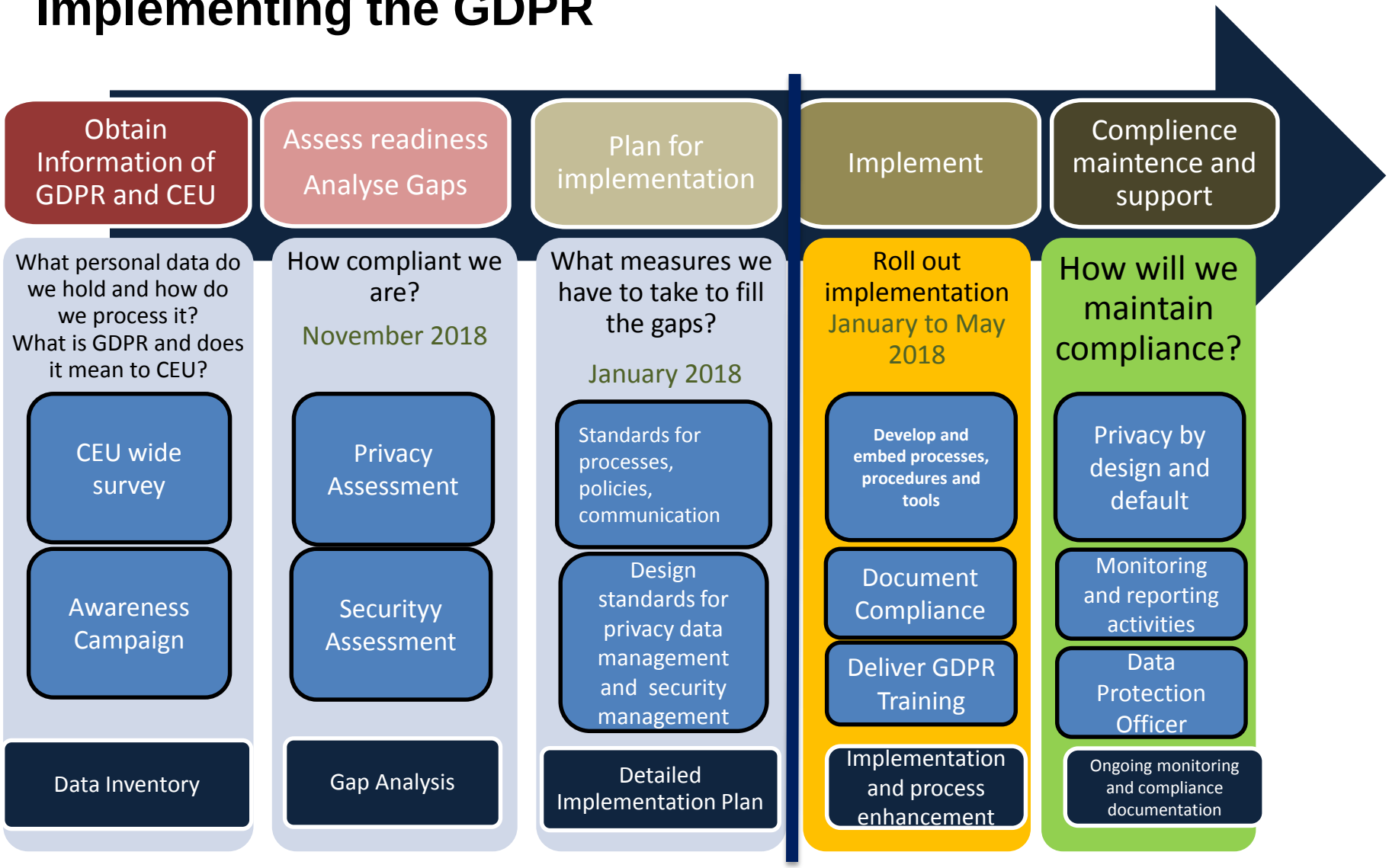
- It is not required to provide detailed answers to all the questions in the first version of the DMP that needs to be submitted by month 6 of the project. Rather, the DMP is intended to be a **living document** in which information can be made available through updates as the implementation of the project progresses and when significant changes occur. Therefore, DMPs should have a *clear version* number and include a *timetable for updates*. As a minimum, the DMP should be updated in the context of the periodic evaluation/assessment of the project. If there are no other periodic reviews envisaged within the grant agreement, an update needs to be made in time for the final review at the latest.

- You can find a **Template Summary Table** ready to use to prepare your Data Management plan at the end of the **Guidelines on Data Management** in Horizon 2020 document.

Part IV.

CEU’S Best Practice

Implementing the GDPR



THANK YOU FOR YOUR ATTENTION

Source:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020