GDPR: action steps to ensure your organization is in compliance

Dr Adrian Ioannou
PECB Certified Data Processing Officer
High Q Consulting Ltd

CyAQ

I The EU General Data Protection Regulation

To quote the homepage of eugdpr.org:

"The EU General Data Protection Regulation (GDPR) … was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy."

This regulation is about individuals' rights over information about themselves; when it may be obtained, how it must be protected, and what may or may not be done with it.

1.0 EU General Data Protection Regulation

- "It is perfectly clear that the General Data Protection Regulation will be a complex and demanding legal requirement which would involve all functions within the organisation.
- I would therefore encourage all organisations to prioritise preparation for this significant change now and not risk the hefty fines and reputational damage."

1.1 Personal data…

…. data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

II Data Protection Principles

GDPR states *six principles* that are related to personal data:

1. *Lawfulness, fairness* and *transparency (Article 5, 1a)*
2. Purpose *limitations (Article 5, 1b)*
3. Data *minimisation (Article 5, 1c)*
4. *Accuracy (Article 5, 1d)*
5. *Storage* limitations *(Article 5, 1e)*
6. *Integrity* and *confidentiality (Article 5, 1f)*

What can one do to prepare

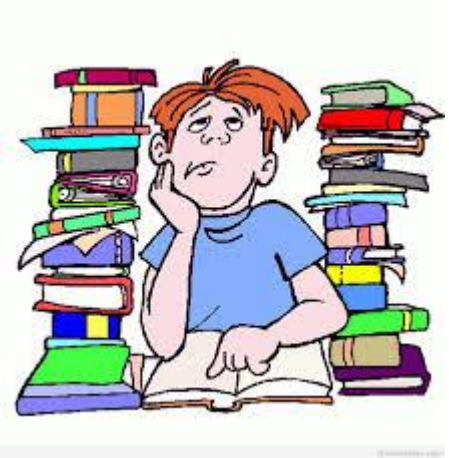
3.1 Steps in preparing for GDPR

While every organization needs proper consultation and legal advice on the matter, there are a number of actions to take and reflect on as a framework for GDPR compliance which will give you a head start on your own efforts, or to compare to the work you've already undertaken.

Step 1 Raise awareness/create alignment

Many individuals and teams have access to the organization's data. It's important to ensure that decision-makers and key members are aware that the law is changing and that they correctly foresee the impact and potential risks of GDPR. There are webinars, events, conferences devoted to this subject, *so there's no excuse for not getting educated.*

Ultimately, the organisation would require external expertise and in dew course legal teams will need to be involved each step of the way.



Step 2 (i) Information mapping and data audit

Document and understand at a micro level ***WHAT*** personal data is being held, ***WHERE*** it came from, ***HOW*** it was collected, with ***WHOM*** and ***HOW*** it is shared. Identify all sources of data and all types of data relationships.

This can be a big task, so you may want to consider undertaking a formal information audit were the following question would be asked:

Who are our data subjects? *Who* has access to sensitive data?

Where do we keep their personal data? *Where* do we transfer personal data to?

Step 2 (ii) Information mapping and data audit

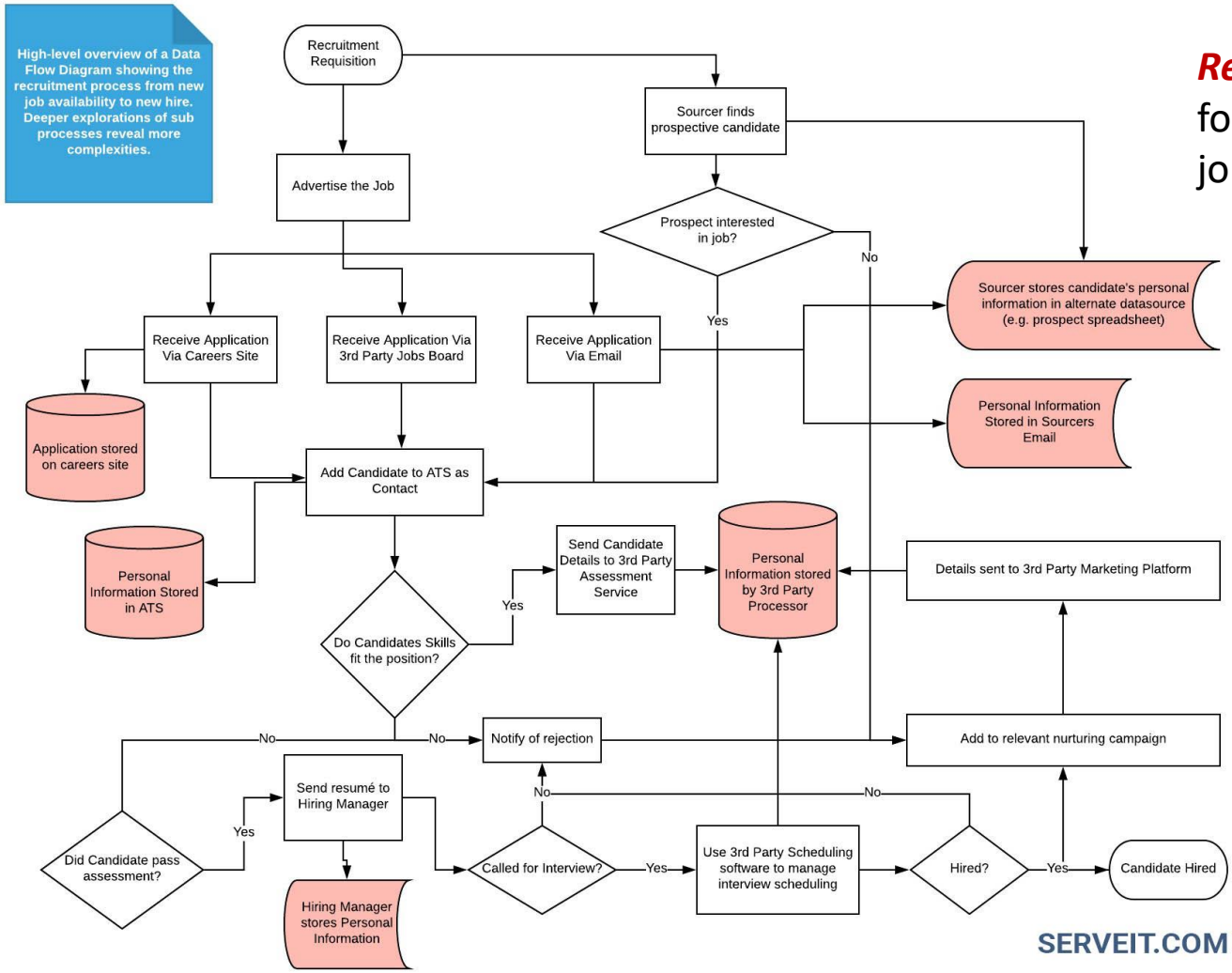
Why is personal data under our control (for what legitimate purpose)? *Why* do we share it with third parties? Do third parties share it with other entities? If so, who, how many and to what purpose?

When are we keeping personal data until? *When* do we share personal data with others?

What mechanisms do we have in place to safeguard personal data?

How is data being processed? *How* long should it be kept?

Information Mapping Diagram



Recruitment Process for a new employee job application.

LEVEL 2
The ***Data Mapping Diagram*** will be generated following a ***Level 1*** data flow analysis showing the organisation's data journey and storage.

Step 3 (i) Notices & privacy communications

Do a full review of current privacy notices and ensure that these will align with requirements under GDPR.

Notices must:

- *indicate* the processing activities occurring at the time personal data is being collected
- *inform* what processing activities are occurring if personal data has not been obtained directly
- *be present* at all points where personal data is being collected.

Step 3 (ii) Notices & privacy communications

- The following must be publically available as a minimum:
  - Identity of the *Controller* and *Data Protection Officer*
  - Data *storing period* (how long data will be kept)
  - The *right* of access, rectification, restriction and objection
  - Right to lodge a *complaint*
  - *Recipients* and *transfers* of data
  - State the *right to withdraw* consent at any time
  - Explain the *legitimate interest* of the controller or of a third party (if relevant) in the collection of the data.

Step 4 (i) Individual Rights

Under GDPR, the rights of data subjects are greatly expanded and persistent. Organizations must be able to demonstrate that they can respond to a data subject's personal data request, and generally, this must be done *within 30 days.*

Compliance will require that organizations are able to demonstrate that they can:

- *validate* the identity of the requesting data subject
- enable the data subject to request *access to their personal data*
- *respond* to requests for personal data access
- *trace and search* for a data subject's personal data and deliver this within 30 days
- request *rectification* and rectify personal data

Step 4 (ii) Individual Rights

- request the *erasure* of a data subject's personal data
- know which *additional controllers* personal data has been transferred to
- in the event of *data breach,* contact those entities for data erasure
- request the *restriction* of data processing and demonstrate when this is done
- request copies and transmit personal data *(portability requests)*
- locate personal data and *export* such in a structured, machine-readable format
- if processing for *direct marketing*, provide a mechanism to object
- if Consent withdrawn *discontinue* data processing and demonstrate compliance.

Step 5 (i) Legal basis for processing

Organizations are required to review their data processing activities and identify and document the legal basis for each type. They must ensure that:

- ✓ ***NO*** personal data is collected beyond the *minimum* necessary for each specific purpose of the processing
- ✓ ***NO*** personal data is retained beyond the *minimum* necessary for each specific purpose of the processing
- ✓ ***NO*** personal data is processed for *purposes* other than those for which they were collected
- ✓ ***NO*** personal data is *disseminated* to non-public third parties for purposes other than those for which they were collected
- ✓ ***NO*** personal data is *sold.*

Step 5 (ii) Legal basis for processing

- ✓ When data processing is likely to result in a high risk to the rights and freedom of individuals, the organization must perform a *Privacy Impact Assessment (PIA).*
- ✓ This would include:
  - ❑ a description of the processing
  - ❑ an assessment of the necessity and proportionality of the processing operations in relation to the purposes
  - ❑ involvement of the data protection officer where one is designated.

Step 6 Managing Consent

A data subject never surrenders their rights, so managing their *Consent* becomes extremely important. Make sure that consent is sought, obtained and recorded according to the new regulation, and that you are able to respond to enquiries regarding consent. At a minimum, you will need to:

- ✓ *make available* notifications to data subjects, in clear and plain language
- ✓ *request and obtain* the data subject's affirmative and detailed consent
- ✓ *discontinue processing* activities if the data subject denies consent
- ✓ *provide a mechanism* for data subjects to withdraw consent
- ✓ *obtain affirmative* consent from a child's (under age of 16) parent or guardian.

Step 7 (i) Data Security and Breaches

Data breaches create reputational, legal, financial and other types of risk for organizations. So, in GDPR data security procedures are put in place to detect, report and investigate data breaches, and include:

- *providing mechanism(s)* to pseudonymize, encrypt or otherwise secure personal data
- *implementing security* measures
- *confirming* ongoing confidentiality, integrity and availability of personal data
- *providing mechanisms* to restore the availability and access to personal data
- facilitating regular *testing of security measures*
- notifying the data protection authority *within 72 hours* in the event of a data breach incident
- notifying *affected data subjects* of a high-risk data breach incident.

Step 7 (ii) Data Security and Breaches

Step 8 Privacy by Design

Privacy by design requires that all consumer interactions and touch points have privacy designed right into them and that their default mode is one of compliance.

This would require:

- processing activities have to *be planned, designed and performed* with data security and, more generally, compliance with the GDPR in mind
- *by default,* only personal data which is necessary for each specific purpose of the processing should be processed
- *by default,* personal data is not made accessible without the individual's intervention to an indefinite number of individuals.

Step 9 Data Protection Officer (DPO)

Any organization that manages data as a ***"core activity"*** or does so on a large scale or uses data collected via tracking and monitoring tools will need to appoint a data protection officer.

The DPO will need to ensure that they:

- maintain *audit trails* to demonstrate accountability and compliance
- maintain *an inventory of data* detailing categories of data subjects
- maintain *auditable trails* of processing activities
- carry out *data protection impact assessments* of processing operations
- monitor *compliance* with data protection laws
- *liaise and assist* supervisory authorities.

Step 10 Data Transfers

Ensure that the personal data you're collecting can be easily transferred or returned back to the consumer. Bear in mind that, they can ask you to return their personal data at any one time. This means having the ability to make available data:

- ✓ in a structured and commonly used, machine-readable format
- ✓ in a way that can easily be transferred to another *data controller (also known as "data portability")*
- ✓ fundamentally, organizations need to be able to support this data transfer and give customers the ability to receive their personal data in a legible, common format.

4 To Conclude - GDPR compliance actions

Step 1	Raise awareness/create alignment
Step 2	Information mapping and data audit
Step 3	Notices & privacy communications
Step 4	Individual Rights
Step 5	Legal basis for processing
Step 6	Managing Consent
Step 7	Data Security and Breaches
Step 8	Privacy by Design
Step 9	Data Protection Officer (DPO)
Step 10	Data Transfers

4.1 Where to Start?

The process for GDPR compliance is critically important, but if you want to ***"kickstart"*** your efforts, a good place to start is with *information mapping* and *data audit (Step 2 above).* Not only will this help with your compliance efforts, but will also enable you to better understand your organizational data flows, your customers personal data type and operational procedures.

Technology is extremely important and has a role to play as well. With the right guidance on data management and information mapping, organizations can find themselves not just compliant with GDPR but also better positioned to personalize their marketing activities and customer communication for a better return on investment.

Dr Adrian Ioannou

Director

High Q Consulting Ltd

Tel: +357 99551555

E-mail: adrian.ioannou@gmail.com