GDPR Primer

What GDPR IS and IS NOT

IS (Does)

- Global
- But Applies only to Europeans
- Mandates Results
- Bestow Rights
- Mandates Standards
- Mandates Contractual Responsibilities

IS NOT (Does Not)

- European Only
- Enforceable IRT non-Europeans
- Mandate Encryption
- Bestow Personal recoveries
- Define Standards
- Mandate how Responsibilities are fulfilled

Implementation Basics

The next steps are generally taken from website of a company called “IT Governance”, it appears to be a British company that specializes in ...

“IT Governance is a leading global provider of IT governance, risk management and compliance solutions, with a special focus on cyber resilience, data protection, PCI DSS, ISO 27001 and cyber security.”

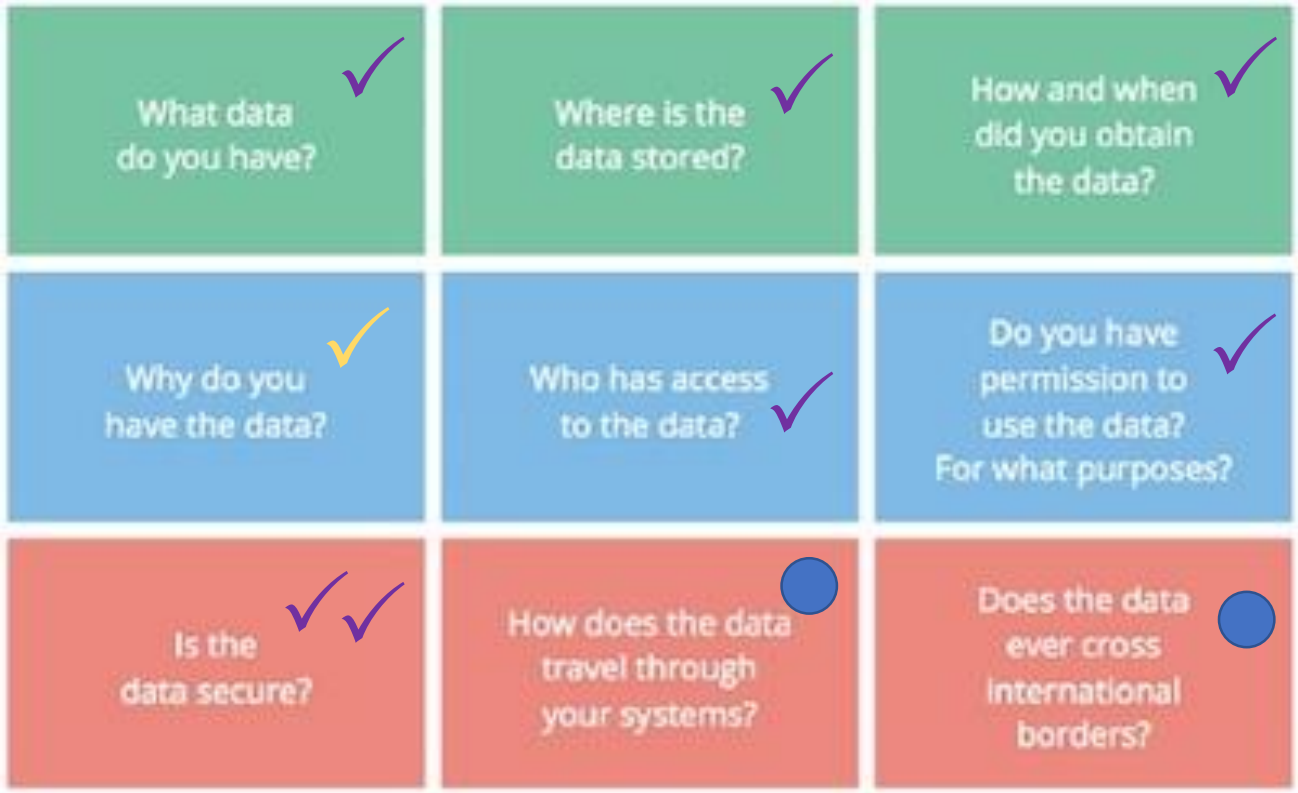
The next few slides are based on their suggested GDPR implementation suggestions. It seems to basically follow Maslow’s hierarchy of needs concept... While these are specific (they are also the most detailed I found), they are also representative of others as well..

https://www.itgovernance.co.uk/gdpr-compliance-checklist

GDPR Steps – Analysis Policies

While reacting to obvious security risks above will take priority, most of the hard work will come via harder analysis of the data and data flow assessment to determine where the personal identity is, how and if it is protected and then move into the deeper aspects of protecting the newly minted rights that GDPR bestows on individual human beings and how the various companies will comply to uphold those rights

The Basics



https://neo4j.com/blog/gdpr-compliance-challenges-personal-data/

Details.... Geeky Stuff

Excerpts from the actual law and how we fit into it... In a more detailed manner....

1. The right to be informed

The right to be informed states how the information you supply about the processing of personal data must be, typically in a privacy notice:

1.concise, transparent, intelligible and easily accessible;
2.written in clear and plain language, particularly if addressed to a child; and
3.free of charge.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. For more detail and what information you must supply to individuals at what stage

2. The right of access

Under the right of access, you must be able to provide processing confirmation and access to an individual's data free of charge and provide it in a commonly used format - an electronic format if the request is made electronically. Ensure careful planning of this if dealing with multiple systems so you can achieve high efficiency to counter the fact that the information must now be accessed free of charge.

3. The right to rectification

Individuals are entitled to have their personal data rectified if inaccurate or incomplete and you must respond to a rectification request within one month if not deemed complex. You must inform related third parties where possible if the personal data is disclosed to them also.

4. The right to erasure

‘The right to be forgotten’, or right to erasure means you must have procedures in place for removing or deleting personal data easily and securely where there is no compelling reason for possession and continued processing. Specific circumstances stated by the ICOinclude:

•Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
•When the individual withdraws consent.
•When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
•The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
•The personal data has to be erased in order to comply with a legal obligation.
•The personal data is processed in relation to the offer of information society services to a child.

Especially for marketing, this right is a main reason why having the appropriate tools and record keeping in place is so important to know why someone’s data is being processed and what it relates to, and if someone has removed their consent to receiving marketing materials and having their data processed. Many investigations will likely arise through people being disgruntled when they have withdrawn their consent from marketing materials, or not given their consent initially for marketing materials, but are still being processed and receiving electronic marketing such as emails for example.

5. The right to restrict processing

Individuals have the right to ‘block’ or restrict processing of personal data, in the following circumstances outlined by the ICO:

- “Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.”
- “Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organization's legitimate grounds override those of the individual.”
- “When processing is unlawful and the individual opposes erasure and requests restriction instead.”
- “If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.”

You must inform any third parties that are also involved with the data about the restriction, and inform individuals when you remove a restriction on processing.

6. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data across different services for their own purposes. The right only applies:

1.to personal data an individual has provided to a controller;

2.where the processing is based on the individual's consent or for the performance of a contract; and

3.when processing is automated.

The right allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting usability. Therefore if a client on your site cannot quickly download their account transactions for example, this will need to be amended.

Personal data must be provided in a structured, commonly used and machine readable format (like CSV files) so other organizations can use it, and must be provided free of charge.

7. The right to object

The right to object means individuals have the right to object to **direct marketing** (including profiling), processing based on legitimate interest, and purposes of scientific/historical research and statistics, in which case you must stop processing personal data immediately and at any time, with no exemptions or grounds to refuse, free of charge.

Ensure you are informing individuals of their right to object in your privacy notice and “at the point of first communication”. If you process personal data for research purposes, or for the performance of a legal task or your organization's legitimate interests. If your processing activity is one of the above and carried out online you must offer the option to object online, e.g. through your website.

8. Rights related to automated decision making and profiling

If any of your processing operations constitute automated decision making including profiling (such as insurance firms), individuals have the right not to be subject to a decision and must be able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it. The right does not apply if the automated decision is a contractual necessity between you and the person, if it’s authorized by law, or if based on explicit consent.

Article 5 of the GDPR sets out 6 main principles. The same principles apply to companies from all sectors that deal with personal identifiable information of EU citizens and need to comply. Article 5 of the GDPR requires that personal data shall be:

Any business that holds data will need to document what personal data they hold, when and where it came from, and who it has been shared with.

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
>
> Article 5(2) requires that
>
> "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

General (familiar) principles

- "Personal data" + special categories of "sensitive data"
- Six principles:

1. lawfulness, fairness and transparency
2. purpose limitation
3. data minimisation
4. data accuracy
5. storage limitation
6. integrity and confidentiality

- Data controllers + data processors

Cookies
IP Address

Processor and Controller

Consent is an affirmative act, record it (audit trail), each type of processing needs specific consent, withdraw as easy as giving

Key Concepts

Controllers and Processors – GDRP puts significant mutual responsibility on both parties to be responsible to and responsible for other organizations who are part of the process