BLUE WAVE SOURCING

GDPR – A new regulation and a new opportunity

Business Possibilities

Summary

Current regulatory landscape

Data Protection Act (UK) – 1988 and 2003

- Data processing principles
- Special conditions for sensitive personal data
- Organizations shall have data protection policies

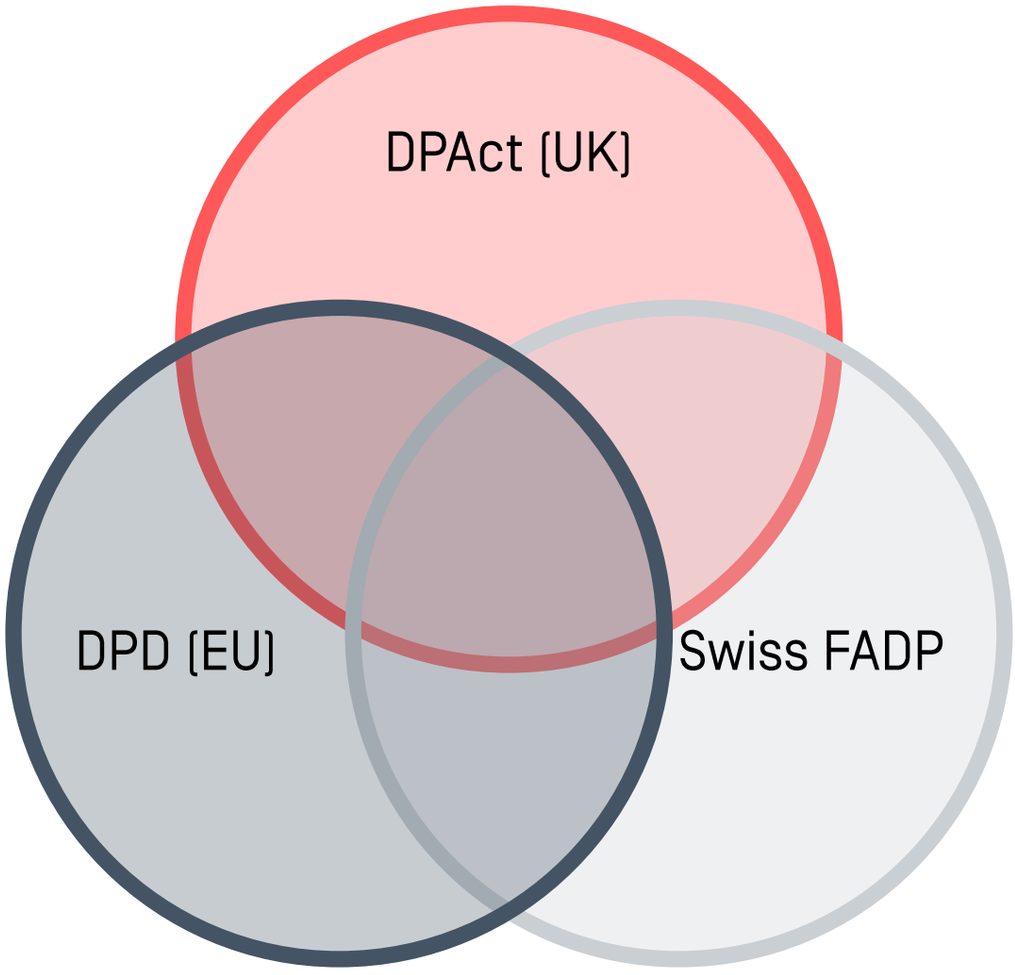
Swiss Federal Act on Data Protection– 1992

- Introduction of “personality profile”, defined to include the collection of data that permits an assessment of essential characteristics of the personality of a natural person
- The processing of personal data must be carried out in good faith and must be proportionate in the circumstances
- Personal data must be protected against unauthorized processing through implementing proper technical and organizational measures

Data Protection Directive (EU) 1995

Personal data should be processed only if the following the conditions are met:

- The data subject has the right to be informed when his personal data is being processed
- Personal data can only be processed for specified explicit and legitimate purposes
- Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected



Regulations issued in different periods have generated different approaches, that need now to be realigned in a global, digitalized world

GDPR: a common approach

Application :

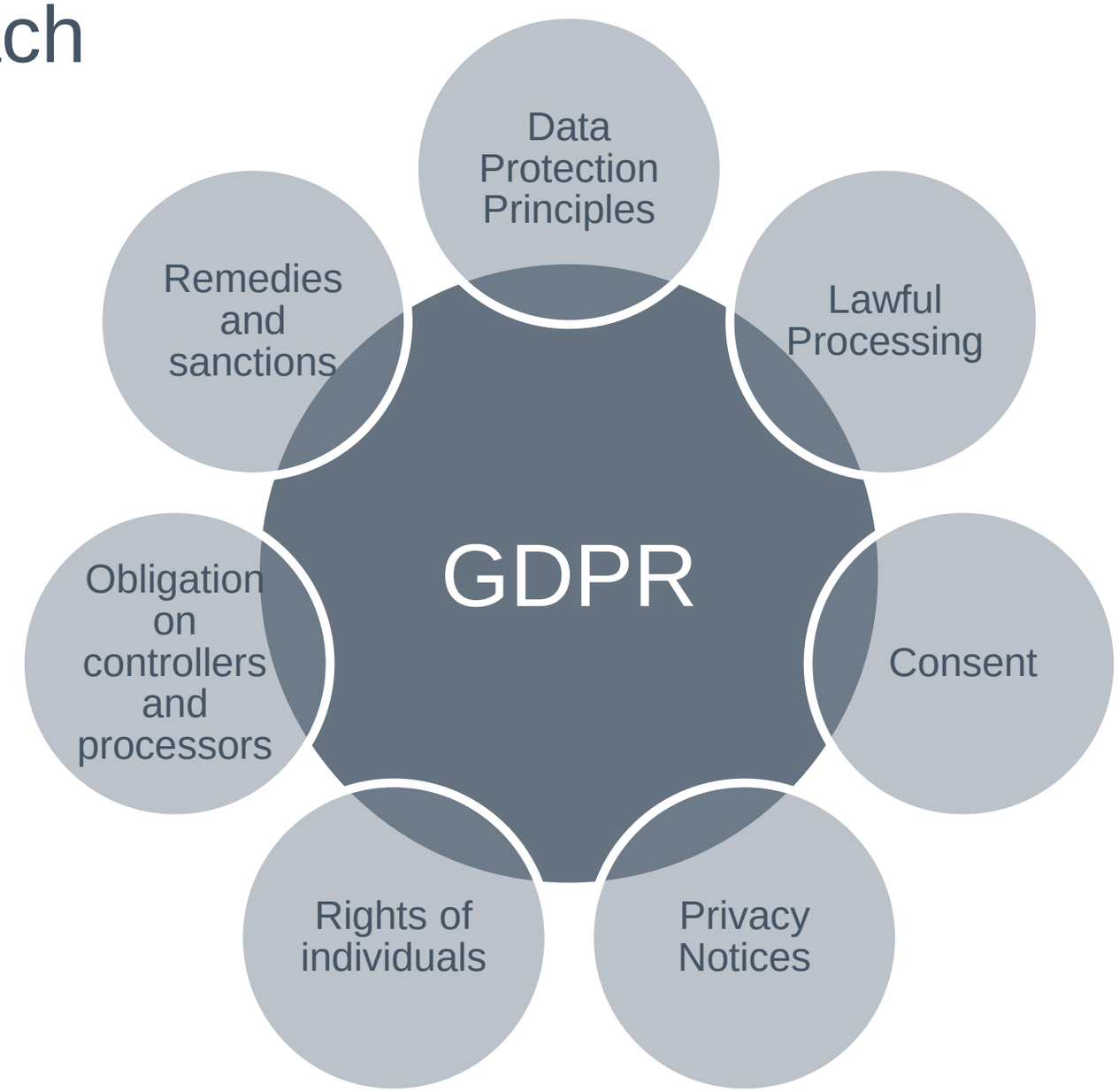
GDPR applies to the processing of personal data by a data controller or a data processor, where:

- Processing: collecting, recording, organizing, storing, retrieving, using, erasing, cancelling data
- Personal Data: any information which allows to identify , directly or indirectly, a person
- Data Controller: decides how and why personal data are processed
- Data Processor: processes personal data on behalf of a data controller

Improvements:

GDPR builds on existing data protection rules and principles, with the following improvements:

- Increased compliance obligations for business and organizations
- Enhanced rights for individuals
- Increased regulatory powers and sanctions



Data protection Principles (art. 5)

- Data must be processed in a way to ensure sufficient security, including prevention of unauthorized or unlawful processing, loss, destruction or accidental modification, using technical or organizational measures

- Data must be kept no longer than necessary for the purposes for which the data have been collected

- Data must not be transferred to third countries unless those countries have an adequate level of data protection

Lawful Processing (art. 6)

Processing of Personal Data must have a legal basis, which shall be identified and recorded:

- the data subject has given consent to the processing of his or her personal data
- processing is necessary for the performance of a contract with the data subject
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest

Processing of Personal Data must comply with the 6 Data Protection principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Security, integrity and confidentiality

Consent (art. 7)

Consent in GDPR should be:

- A freely given, specific, informed indication of the subject's agreement to the processing of personal data
- Verifiable - keep record of when and how is given
- Stated in clear and unambiguous language
- Consent should cover all processing activities carried out for the same purpose. When the processing has multiple purposes, consent should be given for all of them.
- The individual has the right to withdraw consent at any time and should be informed about this right
- Must be as easy to withdraw as to give consent

Privacy notices (art. 13)

Once personal data are collected, the controller must provide to the data subject the following information:

- Identity and contact detail of the controller
- Contact detail of Data Protection Officer (if applicable)
- Purposes of the processing as well as the legal base
- Recipient (s) of the personal data
- When applicable, the transfer of data to third countries or international organizations
- Period for which the personal data will be stored
- Rights to request access, rectification or erasure of the data, rights to restrict the processing, right to data portability
- Right to withdraw the consent
- Whether to availability of the data is a contractual requirement and the possible consequences of failure to provide the data

Rights of individuals

- Right to be informed - transparency (Art. 13-14)
- Right of access – subject to request from data subject (Art.15)
- Right to rectification – if data are inaccurate or incomplete (Art.16)
- Right to erasure – 'right to be forgotten' (Art.17)
- Right to restrict processing – only storage possible without consent (Art.18)
- Right to data portability – right to receive the data in a commonly used format (Art. 20)
- Right to object– especially related to processing for direct marketing purposes (Art.21)

Right of access – details (Art.15)

The data owner has the right to ask to the controller if and how his personal data have been processed and to obtain (free of charge) the following information:

- Purpose of processing
- List of personal data involved
- Recipients to whom the data have been disclosed
- Where the data have been transferred (including third countries or international organization)
- A copy of the personal data under processing

The requests should be handled within 1 month, ad information should be provided in a commonly used electronic format.

Right to erasure- details (Art.17)

The data subjects have the right to have their data ‘erased’ where the processing fails to satisfy the requirements of the GDPR. The data controllers must respond by default no later than within after the request.
The right to erasure applies:

- when personal data are no longer necessary for the purpose for which they were collected;
- if the data subject withdraws their consent to processing;
- when the personal data are processed in breach of the GDPR

If the data controller has made personal data available to third parties, he must also inform other data controllers that the data subject has requested the erasure of those data.

The obligation to comply with data erasure request does not apply if:

- for the exercise of the right of freedom of expression and information;
- for compliance with a EU obligation;
- if required for the exercise or defense of legal claims
- for public health reasons

Third party data processors (Art.28)

- Controller must only use processors providing sufficient guarantees that processing will meet GDPR requirements
- Processing by a data processor must be governed by a contract with the data controller
- Both controllers and processor must maintain a record of the processing activity carried out
- The processor, at controller's request, deletes or returns all the personal data to the controller after the end of the agreed services and deletes existing copies (unless EU law prevents it)

Security of processing (Art.32)

Controllers and processors must implement appropriate technical and organizational measures to ensure a sufficient level of data security, including (as appropriate):

- Encryption of personal data
- Assurance of confidentiality, integrity, availability and resilience of processing systems and services
- Ability to restore the data in a timely manner in the event of a physical or technical incident;
- Existence of a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data.
- Procedures to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or processed

Breach notification (Art.33)

The controller should notify personal data breaches to the supervisor authority within 72 hours, only if the breach can result in a risk to the rights and freedoms of natural persons. The notification should include:

- the nature of the personal data breach including approximate number of data records and subjects concerned
- describe the likely consequences of the data breach
- describe the measures taken to mitigate the possible risks

When the personal data breach can result in a high risk to the rights and freedoms of the persons, the controller shall communicate data breach to the data subject without delay. The communication is not required if:

- the controller has implemented appropriate technical and organisational protection measures (e.g. encryption)
- the controller has taken subsequent effective measures to minimize the risk

What are personal data?

Any information relating to an identified or identifiable living person (data subject), where “identifiable” means that the person can be identified, directly or indirectly .

Personal data include (but are not limited to):

- Names, Date and country of Birth, nationality, Gender, language, marital status, profession, phone number, email, partner or child names, interest or hobbies

Sensitive personal data include:

- Racial/ethnic origin, political opinions, religion, genetic or biometric data, data concerning health or sexual orientation

Practical steps to achieve GPRS compliance

Document your data handling process	Document your lawful base for processing	Document your personal data register
Revise and develop your data protection policies	Appoint a Data Protection Officer	Embed Privacy by Design
Implement your consent strategy	Collect and revise agreements with data processors	Implement the processes to respond to data owner's requests
Raise awareness on Data Protection with training	Undertake a review of processes and systems	Develop a plan for ongoing compliance

Conclusion

Complying with GDPR is not an option: if your company, independently of where it is domiciled with its offices, stores or processes personal data related to natural persons resident in the European Community, GDPR almost certainly applies to you.

The deadline for being compliant with GDPR is rapidly approaching, and the transitionary period is now ending. Organizations are expected to comply immediately once the Regulation goes into force, that is on May 25th, 2018.

Being non-compliant with GDPR will be risky and likely very expensive. In addition to other financial consequences, there are two types of fine foreseen in the regulation, the more expensive of which is a fine of up to €20 million or four percent of the annual worldwide turnover for the organization, whichever is higher.

Even when compliant at day 1, there is the need for continual compliance with the GDPR, since a failed audit can have the same severe financial consequences.

Contact us for more information about our methodology to approach GDPR

About us

Filippo Bernasconi

Most of my 30 years professional career has been devoted to Change Management, contributing to continuous improvements of the effectiveness and quality of company services and products, and to increase the efficiency of processes and organisations.

My working philosophy is inspired by pragmatism and flexibility without renouncing to apply and maintain high quality standard methodologies.

I am a strategic thinker with a solution-based approach, and a proven ability in leading and managing large programs and projects within the banking and financial services domain.

As a “Banking Engineer”, the application of a strict methodology together with rigorous priorities, planning and budget management are the base of my working approach.

My goal is always to support management and stakeholders in their decision with business, economical and scenario analysis, and to put the resulting strategies into actions.

Paolo Ferrari Trecate

Contacts

Contact Us

Blue Wave Sourcing Sagl
Via Cassarinetta 7,
CH-6900 Lugano

Visit us

www.bluewavesourcing.com
info@bluewavesourcing.com
p +41 79 45 94 804
p +41 79 79 69 067

Follow us

Linkedin