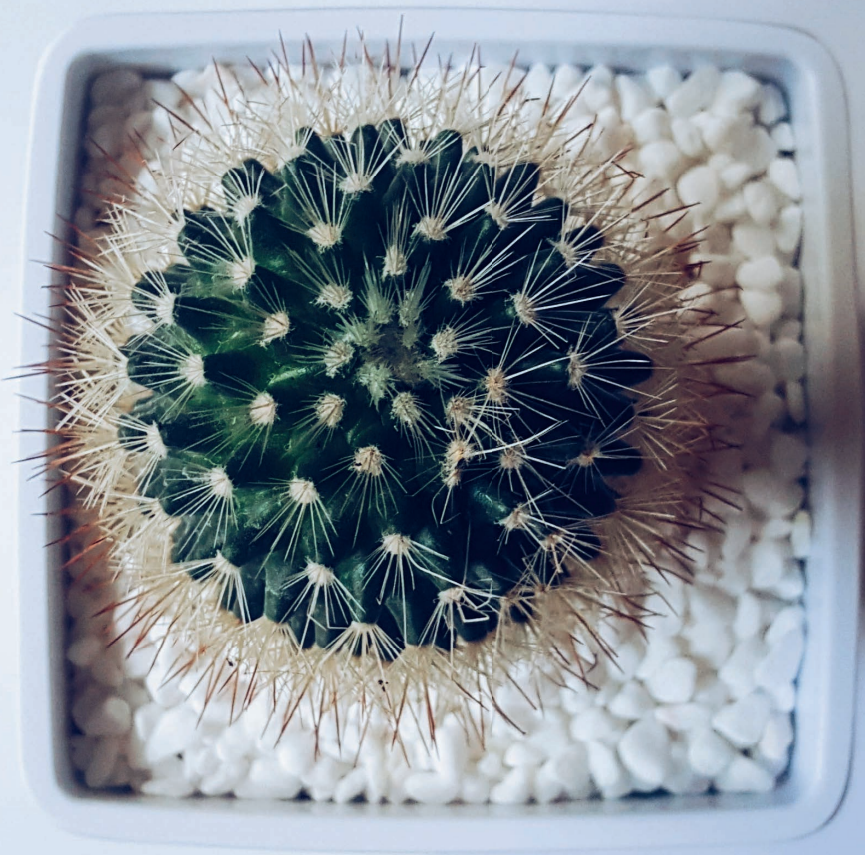
Novagraaf
A NovumIP Company

VADE-MECUM
GDPR



Executive Summary

This brief introduction to the General Data Protection Regulation (GDPR) addresses this new Regulation from a managerial point of view. It is not meant to provide a comprehensive account of the subject, but rather to orient the development and execution of a data management strategy that would be compliant with the Regulation.

We suggest three steps to the process:

1. **Data Mapping: what data types do you have and how are they stored?**
2. **GDPR Principles: what are they and do your data management practices conform to them?**
3. **Gap Analysis and Strategy Development: what measures must be taken to ensure maximum compliance with the GDPR?**

GDPR: key changes

To address them successfully, one should first be aware of the key changes brought about by the GDPR. Put briefly, the GDPR reinforces the obligations of the controller while at the same time increasing the rights of the data subject. These are two sides of the same coin.

The controller is the natural or legal person which, alone or jointly with others, determines the purposes and means of the data processing. The controller may be the company (legal entity), but it may also be one or more individuals within the company. It is important that the controller be clearly identified because the responsibility for compliance with the legal obligations of the GDPR falls on the shoulder of the controller.

Some of the key changes of which the controller should be aware are:

- reinforced information and transparency obligations in relation to the data collected and stored;
- the need to be extremely careful about obtaining consent and to communicate clearly the scope and limits of that consent to all data subjects concerned;
- the requirement to be ready to respond to increased data subject's rights: right to information, access, rectification, erasure, data portability, etc.;
- the necessity of reviewing contractual scaffolding to address international transfers (within or outside Group) and relations with data processors (sub-contractors);
- the need to set up privacy by design and privacy by default;
- the readiness to address a data breach in a fast and efficient manner.

In particular, the GDPR requires that data breaches be reported to the data protection authorities within 72 hours (from the moment of detection) and, in certain circumstances, to communicate them to the data subjects affected. This may have crucial repercussions on the reputation of a company, and should not be dealt with lightly.

STEP I

Data Mapping

The first step is to map your data. To do this, you should identify and classify the data you have collected and stored in your systems, as well as where and how these data are kept, how they are accessed and used, and who in your organisation has access to the data repositories which have been identified. It is important to note the following. Not all information is data, and moreover, not all data is personal data. In carrying out the mapping, it is thus essential to know which of your data fall under the GDPR, and under which of the following three categories.

Personal data are any data relating to an identified or identifiable natural person, a "data subject", that is, a natural person whose data are being collected, stored, or processed. The "identification" criterion is key here, that the natural person be identified, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Art. 4.1 GDPR)

The following data fall outside the scope of the GDPR:

- anonymous data (i.e. which do not relate to an identified or identifiable natural person) or personal data which have been rendered anonymous (for statistics purposes, etc.);
- legal persons as opposed to natural persons

Examples of personal data:

- name, surname, photo, address of natural persons
- IP (Internet protocol) address, email address, login, password
- social security number, passport number
- employment records (copies of diploma, position/title, marital status, etc.)
- billing information (e.g. bank account details, purchase history, credit status, etc.)

The GDPR reinforces the obligations of the controller while at the same time increasing the rights of the data subject. These are two sides of the same coin.

Sensitive data are data which, if compromised, could pose a significant threat to the data subject. As such, they impose additional obligations on the controller, such as obtaining the explicit consent from the data subject. These data include data concerning health (i.e. related to the physical or mental health of a natural person including the provision of healthcare services), but also information on racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. (Art. 9 GDPR)

Profiling relates to the automated processing of personal data for various goals, among which the analysis and prediction of aspects of that person's performance at work, or of that person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements. (Art. 4.4 GDPR)

The first step involves the mapping (identifying and compiling an inventory) of the data processed by your firm, keeping in mind that the concept of processing involves various activities (e.g. collection, recording, organisation, storage, alteration, retrieval, consultation, disclosure by transmission, making available, combination, destruction).

TO DO

- **Map all personal data (+ sensitive / profiling) which you have in your systems;**
- **Locate them all (where are they stored: Japan, Korea, EU, Ukraine?);**
- **Identify additional elements in relation to the data inventoried: who can access it, how is it used, is it subject to international data transfer, etc.**

STEP II

Respect GDPR Principles

The GDPR lays out several guiding principles to be respected in relation to data processing, among which three sets of them are of particular interest to you now:

Lawfulness and fairness: Processing can be carried out on a variety of lawful bases. Of these, a few stand out for special mention: your firm either relies on a legal or contractual obligation (e.g. labor law, to respond to a request for an offer, to act as representative for the client, etc.), or on a legitimate interest (e.g. client relationship), or has obtained the consent of the data subject (e.g. for receiving a e-newsletter). (Art. 6 GDPR)

Transparency and purpose: When data are being collected and processed on a consent basis, the request for consent must be presented to the data subject in an intelligible and easily accessible form, using clear and plain language. Moreover, these data must be collected and processed for a specified, explicit, and legitimate purpose; the consent is given in relation to this purpose only. The consent of these data subjects will have to be obtained in compliance with the GDPR. (Art. 7 GDPR)

Proportionality: The data collected and processed should be adequate, relevant, and limited to what is necessary for the purpose for which they were collected or are processed. This implies in particular that data should not be kept longer than necessary to reach the purpose identified (meaning that one should consider destroying or anonymising data as the need arises) and that no more data than necessary to reach the identified purpose should be collected (i.e. data minimisation). Keeping data "just in case" is now forbidden. (Art. 5 GDPR)

Other obligations of the controller under the GDPR include data accuracy, storage limitation, and that reasonable steps are taken in order to ensure appropriate security and confidentiality of personal data.

Step 2 consists in analysing whether all data mapped out under Step 1 comply with these principles.

TO DO

- **Identify and document lawful basis for data processing:**
  - legal obligation (labour law, tax law, etc.);
  - contractual obligation (respond to an offer, act as representative, etc.);
  - legitimate interest (client relationship);
  - consent;
- **Assess consent: was it freely given, specific, informed, and unambiguous (purpose incl.); document consent;**
- **Assess whether data collected are still processed in line with the initial, stated purpose; otherwise, reobtain consent or consider destroying them;**
- **Always keep in mind proportionality principle (i.e. if purpose can be reached with less data, minimise their volume or length of storage);**
- **Additionally: correct data when possible, to ensure adequacy of data stored.**

STEP III

Bridge the Gap and Establish Long-term Compliance

Once Step 1 and 2 have been completed, four sets of actions must be scheduled:

Gap analysis: List and plan how to address the gaps which have been identified between Step 1 and 2. A deadline should be set and a project manager identified to carry out the compliance plan (familiarity with the GDPR recommended).

Internal privacy policy: Draft a document which will basically respond to the "What", "Why", "Where", "Who", "How Long", "How Secure" in relation to the data processed by your firm. This document is key in ensuring long-term compliance and will address many aspects of data protection. What should be included in the internal privacy policy will be clearer once the data mapping and the gap analysis have been performed.

Document, document, document: If challenged, you will only be able to prove your efforts to be compliant by providing evidence (e.g. of consent obtained, lawful basis for processing, respect of proportionality, technical and organisational security measures).

Appoint a project manager: To ensure that compliance is not only a short-term goal, but an ongoing process. Don't give this person the title of DPO (Data Protection Officer), because this would trigger the unnecessary legal obligations attached to the title.

TO DO

- **Draw gap analysis table: include actions, persons responsible, deadlines; set concrete and clearly-identified goals;**
- **Draft internal privacy policy: insert lessons learned from gap analysis; include data storage and conservation table and policy; address data subjects' rights; plan a specific section on employees' data;**
- **Appoint a designated point of contact for privacy issues (i.e. a person in your team who will wear the "data privacy" hat);**
- **Consider crafting Binding Corporate Rules (BCR) when needed.**

Conclusion

The GDPR provides a new conceptual framework for approaching the management and processing of data. This very short introduction is meant to help your firm approach data in the age of the GDPR. This Regulation provides a vision of how data ought to be collected, processed, stored and disposed of. As firms manage GDPR compliance, a question that needs to be resolved is the following: how do their data practices measure up to the requirements of the GDPR? Answering this question will allow to identify the gaps between what is and what ought to be: once this has been made explicit, you are optimally positioned to get on with compliance. This provides a strong foundation for establishing and maintaining long-term compliance with the GDPR. ■

About the author of this white paper

Anca Dragnescu-Pinawin is IP Counsel at Novagraaf in Switzerland, where she manages the IP needs of clients across a wide range of businesses, from SMEs to multinational companies. Anca also works in the increasingly important field of data protection, helping clients meet the compliance requirements of the GDPR. She can be contacted at: **a.draganescu@novagraaf.com.**

Get in touch

For more information or guidance on developing a GDPR strategy for your business, speak to your Novagraaf attorney or email us at **customerservice@novagraaf.com**.