

HOW YOU SHOULD PREPARE YOUR ORGANISATION FOR GDPR

Action-step guide for meeting GDPR compliance



On May 25, 2018, the new **General Data Protection Regulation – GDPR** will take effect on protecting the privacy rights of all European individuals. GDPR applies to any organisation exchanging offer with EU individuals, and not just those located in the European Union.

This whitepaper seeks to summarise the key changes that you might consider adopting into your organisation, due to the new data regulation, by highlighting the most critical actions in preparing to comply with it.

At Noesis, we believe in ethics and shared responsibilities, providing our clients and partners with the right tools to prepare them to deliver sustainable ideas.

The document is written for decision makers and all members of society who intend on learning more on how they can be prepared for GDPR, by using Noesis methodology.

Technology vs. Information

Over the past 50 years, the Information Technology (IT) sector has evolved primarily on the technological aspect, concentrating more on technology than the information component. This means the focus has been on process evolution, transmission and data store capacity, then on the management and use of information in a strategic way.

By looking at the information component, we see that it is essential for decision making, data segmentation, content targeting, etc. The information within this component needs to be accurate, concise (ease to use), simple (easy to understand) and timely (accessible at the right time) so that it can be truly useful from a management standpoint.

Only now are organisations underlining the importance of information, leading up to the creation of such trends as **Big Data**, **IT Analytics** and **Machine Learning**. However, they are not prepared to use all of the information they possess in a useful and truly optimised way for operational, business or strategic purposes, as a result of the new business models' growth. These business models are based on hybrid multi-cloud distributed services ecosystems and as-a-Service platforms. In addition, they are based on the proliferation of data that is generated by systems, robotic assets and IoTs, due the greater ability to collect, transmit, process and store data.

The key challenge of GDPR is the ability to locate, categorise, relate and search useful, real-time structured and unstructured data, in order to quickly deliver information. It is important to record and track all accesses to ensure the possibility of forensic analysis on existing flows and information movements, in case of audit or for evidence purposes.

There is often no knowledge regarding a number of points:

- > Data lifecycles;
- > Cataloguing information;
- > Authorisation flows;
- > Predicted information flows;
- > Accesses and tracking.

Due to these challenges, IT management models need to be restructured with a higher focus on information components, balancing the focus on both information and technology.

What will change?

Nowadays, organisations gather a lot of information about all stakeholders (for instance clients, partners, employees, suppliers) but this is going to change due to the new regulation regarding data protection, namely the new General Data Protection Regulation (GDPR). Aiming to bring European citizens in control of their personal data and to simplify the rules for international businesses, GDPR was adopted on April 2016 by the European Parliament, to unify all data regulation.

GDPR will formally enter into force on May 25th, 2018. The Parliament requests all organisations to create and adapt procedures to meet the new data protection standards and to create more effective control mechanisms to ensure compliance with the standards. GDPR will impact all organisations in the European Union but also outside, in case of related activities or services with European markets or using data from EU-located holders.

Attached to the new regulation, sanctions from the government will be imposed on non-compliance activities. The sanctions can be of up to **20 million euros, or 4% of the total worldwide annual turnover** for the previous financial year, whichever is higher.

GDPR **should be seen as an opportunity** to close the gap between all maturity levels and information processing processes that exists in most of the companies.

By directing attention to the components of information lifecycles (access management, discovery organisation, categorisation and cataloguing of data) and the security that results from data encryption/tokenisation, anonymisation and masking of corporate data, GDPR allows companies to have more control of their data, as well as how it is generated and consumed inside and outside of the organisation.

Overall, GDPR allows for an **efficient use of operational and corporate information**, leveraging to **better strategic decisions**.

Becoming compliant

As a result of the new regulation and to help everyone be ready for a new data protection era, Noesis has developed a framework on Data Privacy Management. By publishing this step-by-step framework, Noesis aims to support promotion of a privacy protection environment, aligned with the GDPR requirements.

The most efficient way of facing GDPR is by using **automated data discovery** and data mapping technologies, basing identification and categorisation on algorithms & regular expressions and the dynamic control of data in a way that is compliant with company norms and policies.

The generic approach for GDPR is based on a pragmatic attitude towards the goals that need to be achieved, which depends on the levels of risk that are identified in the organisation regarding legal, governance, data management and security dimensions.

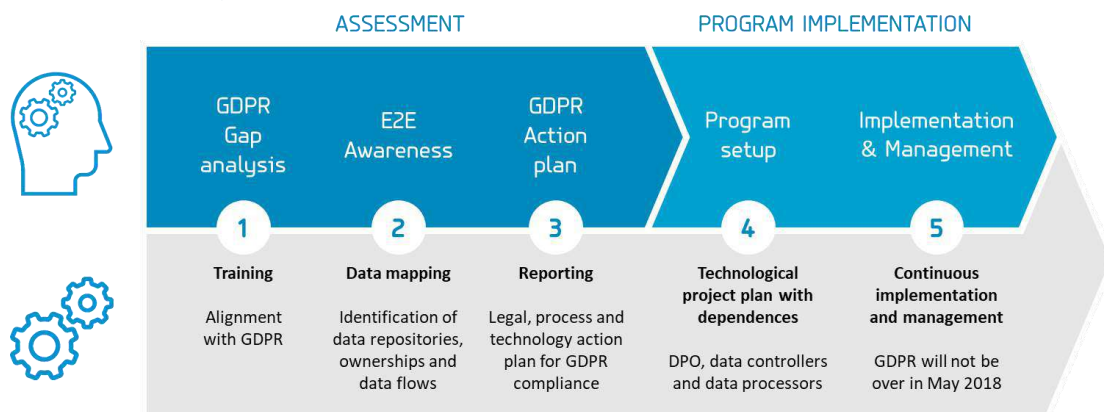
After setting up the approach, concrete actions will follow, resulting in the following activities:

- > Legal gap analysis assessments;
- > Process and data management mapping;
- > Design of the new governance and operational processes
- > Technology mapping plans prioritised by level of the risk.

The actions mentioned above have demonstrated to be an added value for planning analysis, which is necessary for an appropriate GDPR compliance process. We can highlight the following steps:

Step 1. One of the most important steps is to create a team dedicated to GDPR implementation and monitoring, in order to guarantee an efficient and compliant process integration. Next, training is needed to align the teams and to define what GDPR represents for the organisation. During the training period, the team will learn to identify examples and data types that are relevant, to eliminate contamination effects through doubt, and to interpret, classify and analyse all possible data and situations through all GDPR process steps.

5 strategic steps for GDPR action:



After the training period, a report should be created with all legal issues that need to be resolved for meeting GDPR requirements. This step includes a gap analysis on articles that are not fulfilled yet by the organisation and actions that are necessary to comply.

Step 2. The second step includes drawing a report with all the points provided by the gap analysis, containing higher priority activities and indicating the ones that should be considered as high-risk situations (for example, an informal database created by a specific team inside the organisation). All these concerns that you will be exposing can come from structured and unstructured data repositories, ownerships and flows.

Step 3. The final step of the assessment period is to create a roadmap with technological recommendations for the adoption and implementation of Governance, Data Management and Security coverage solutions. Your roadmap should be based on the risk levels that are identified for each compliance-oriented action. The implementation of GDPR compliant solutions is mainly based on tools and technologies that allow the automated discovery and classification of structured and unstructured data, but also the ability to manage centralised access through record repositories, data protection and security tools.

By following the previously mentioned steps, it is possible to design a roadmap with concrete actions as a guideline for a continuous GDPR compliance process. The roadmap meets the first approximation requirements: **operational continuity** and **evolutionary maintenance**.

Steps 4 & 5. With your data mapping and plan created, your implementation period should be focused on data discovery, location, identification and categorisation,

allowing you to have a complete overview of your company's data.

In general, organisations have been using a GDPR approach oriented by a GDPR compliant adaption processes rather than creating good management practices and data categorisation.

By not creating a sustainable base, your organisation will be consuming a lot of time and resources that will be manifested as inefficient treatment of information over time.

Factors to consider

In order to continuously meet GDPR requirements, your organisation must be aware of all of the points below.

With GDPR, organisations can be confronted with new data processing needs that can trigger approaches outside of the procedures that are implemented. These approaches will create risks of regulatory non-compliance.

To continuously manage and monitor all phases and processes, you should be equipped with technologies like data-lifecycle management tools and security tools that identify possible patterns of attack and implement counter-response mechanisms to ensure that all sensitive information is properly encrypted to minimise the effect of improper access to personal data in case of an attack.

By optimising and updating data processing and management mechanisms to be GDPR compliant, we are attentive to changes, in internal and external data flows, being able to identify behavioural and procedural correction needs.

Taking action

GDPR compliance is a continuous process that Noesis wants to support you on, reducing efforts and administrative bottlenecks.

By continuously delivering and treating data that is both accurate, concise and simple, and respecting your stakeholders' data privacy you will be prepared to identify information relevant to GDPR requirements in an automated way, to systematically apply risk management policies security, protection and data lifecycle management, and ensure protection against security breaches through proactive analysis of data most vulnerable to attack.

More information – Walk the Talk

The new data protection regulation will enter into force on May 25 and we have all the answers for you.

What will it entail?

Who will be affected? How should public and private companies proceed?

Can data be saved and which data has to be erased?

Who can be a DPO or in charge of compliance with the Data Protection Regulation within companies?

More information about GDPR is available in [GDPR – Walk the Talk](#), a webinar hosted by Noesis.



Noesis is a multinational consultancy company offering flexible services and solutions to improve competitiveness and optimize our clients' processes.

Creating **sustainable value** across several sectors, Noesis is driven by **technology** and **innovation** and delivers solutions focused on our clients' **infrastructures**, **software**, **quality** and **people**.

With a strong focus in technology, Noesis is the right partner for companies looking to transform and improve their business.

NOESIS Lisbon (HQ)

Centro Empresarial Torres de Lisboa
Rua Tomás da Fonseca
Torre E, 14.º Piso
1600-209 Lisbon, Portugal
+351 21 604 85 40

NOESIS Oporto

Aviz Trade Center
Rua Eng.º Ferreira Dias, 924
Piso 0, E9
4100-246 Oporto, Portugal
+351 22 400 47 13

NOESIS Coimbra

Instituto Pedro Nunes
Edifício D, Sala 2.08
Rua Pedro Nunes
3030-190 Coimbra, Portugal
+351 23 909 08 72

NOESIS Rotterdam

Weena Zuild 130
3012 NC Rotterdam
The Netherlands
+31 010 799 7315

NOESIS Brussels

City Centre
Stephanie Square Centre
Avenue Louise 65, Box 11
1050 Belgium
+32 472 839 721

NOESIS São Paulo

Edifício ETower
Rua Funchal, 418 - 35.º piso
Vila Olímpia 04551-060
São Paulo, Brazil
+55 11 97124 7781

NOESIS Dublin

28-32 Upper Pembroke St
Dublin 2
Ireland
+353 (1) 608 7763

NOESIS Boston

One Marina Park Drive,
Suite 1410, Boston
Massachusetts, 02210
United States of America
+1 617 807 7000

Visit us:

