Privacy by Design

The Impact of the new European Regulation on Data protection

ALTRAN

Introduction

On April 2016 the European Parliament approved the General Data Protection Regulation (GDPR). This new regulation, with mandatory implementation by Member States (MS) and businesses that have activities or provide services in the EU, aims at standardizing concepts and policies, establishing a single law throughout the EU regarding data protection.

Being a European regulation the GDPR becomes immediately enforceable as law in all Member States simultaneously, entering into force after 20 days of its approval and leaving to the various public and private organizations a period of 2 years to comply with its different articles. This means that the new GDPR will take effect on May 25th, 2018.

1 Who's who

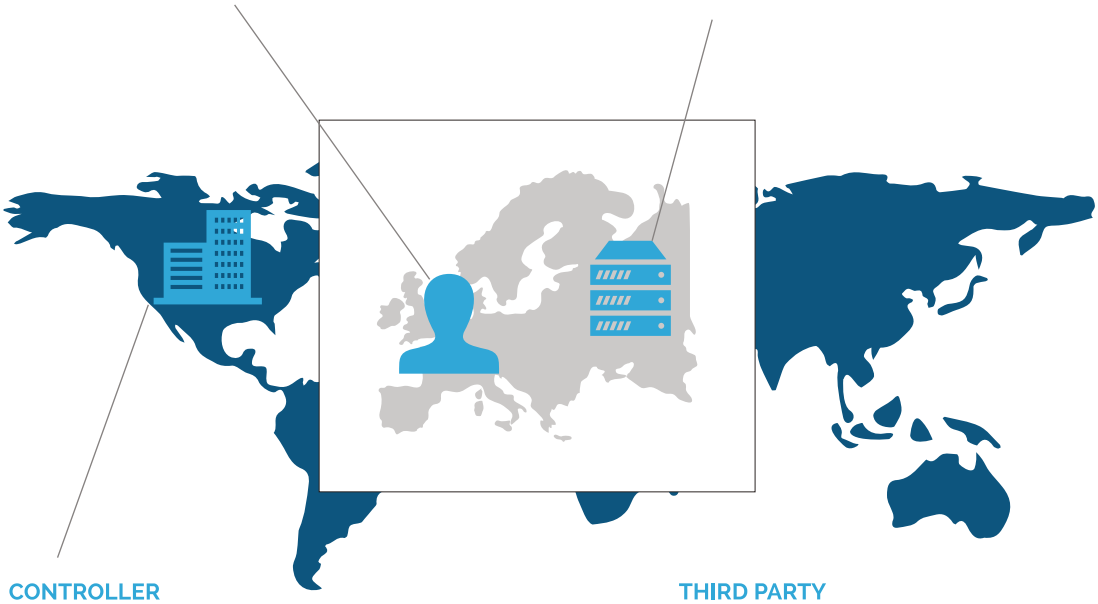
The GDPR applies to the processing of personal data collected in the EU or processed in the EU. It applies both to the controller of data, and its partners, processors of data or third parties.

PERSONAL DATA

Any information relating to an identified or identifiable natural person 'data subject' who is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, etc. i.e. the user.

PROCESSOR

Legal person, public authority, agency or other body which porcesses personal data on behalf of the controller; being processing any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means.
e.g. Cloud Service Providers, ISP



CONTROLLER

Le gal person, public authority, agency or other body which, alone or joinly with others, determines the purposes and means of the processing or personal data, i.e. the business that collects the data.
e.g. Any company making use of any data

THIRD PARTY

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

2 A new set of rules

The GDPR installs a new set of principles and rules as part of the European law:

→ EXPLICIT CONSENT – The data subject should be explicitly informed that his personal data will be collected and/or treated and for what specific purpose. If the data is used for multiple purposes aside the specific treatment the data subject should be informed of every type of treatment that his data will undergo - Explicit Consent.

→ CONTROLLER AND PROCESSOR IDENTIFICATION - The data subject should have explicit knowledge of who treats and processes his personal data as well as his rights, risks, rules and guarantees regarding the treatment of his data.

→ DATA MINIMISATION : Controller's Obligations - "[...] personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed".

→ DATA SECURITY - When a controller (i.e. a company) uses a processor (e.g. a cloud service provider) for processing data, this processor must also meet all the GDPR requirements for the security of data processing.

→ HARMONIZATION - the GDPR is a cross-regulation in all EU MS which means that companies will have greater ease in harmonizing within the EU on its legal obligations regarding data protection concerns.

→ GEOGRAPHICAL CONTEXT - GDPR applies to all companies, including non-European ones, as long as they offer goods or services to EU citizens; or monitor behaviors of EU citizens.

→ NOTIFICATION OF A PERSONAL DATA BREACH - In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority.

→ PORTABILITY AND RIGHT TO BE FORGOTTEN - A data subject will have the right to data portability and to be forgotten as well as the right to have access to personal data, to its rectification or deletion, to the limitation of its treatment, or the right to object to its processing. Data portability principle gives the data subject the right to obtain a copy of his personal data in a format that allows the transfer to another controller.

→ PENALTIES UP TO 20 MILLION EUROS - In order to enhance the implementation of the GDPR, penalties may be applicable, including fines for violation of the rules being imposed by the competent supervisory authority. The fines may reach up to 20 million EUR or up to 4% of a company total worldwide annual turnover of the preceding financial year, whichever is higher.

3 Are you ready for the may 2018 ?

If you handle and monitor data that can be used to identify individuals, GDPR and the perspectives of being significantly fined by the EU authorities should put the management of personal data back into your focus for the next months. Below is a list of key questions that can no longer be left without a clear answer from your organization.

→ Do you have a clear shared vision of how and where personal data is handled in your company?

Is your data collection and processing proportionate with the need of your activity? Do you have policies to help your workers and customers understand how, where and why their data are being handled?

A business now needs to have knowledge and control of all processes involving personal data and its legal framework. The data subject shall have agreed not only to share his data but also to the treatment activities to be performed on it. A review of all processes, documents and forms already used ought to be performed to ensure compliance with GDPR so as to allow the detection of gaps or omissions.
Businesses must indeed be prepared to allow the data subject to require his right to data portability and the right to be forgotten. With few exceptions, the data subject will have the right to have his personal data erased and its treatment being stopped if it is no longer necessary for the purpose for which it was collected, stored or processed.

→ Is personal data being stored securely and its transmission encrypted?

Do you have the technology and procedures in place to identify, handle, respond and communicate to the proper authorities' data breaches within 72 hours? Do you have incident response and risk mitigation plans in place to minimize any data breach and public exposure?

The obligation to notify the supervisory authority of any personal data breach means that companies need to have in place clear policies and procedures to detect and communicate occurrences. In this context, although not mandatory, the company should develop incident mitigation and remediation policies and procedures.

→ Does your business have a data protection officer (DPO) ensuring that personal data processes, activities and systems conform to the regulation?

Do your workers or partners have access to data related to individuals, such as excel sheets, stored on laptops, flash drives, cloud drivers or on their e-mail accounts? Do you have share guides and policies to help them manage the data in compliance with GDPR?

Companies that have the role of controllers or processors, should be able to prove their accountability concerning the processing of personal data they are in charge of. The evidence should include, among others, internal policies, present a corporate culture of monitoring, reviewing and evaluating. As a consequence, any data controller or processor shall appoint a data protection officer that should be involved in all matters related to the protection of personal data. His/Her responsibility will be among others to monitor compliance with the GDPR and to be a point of contact of the supervisory authority on issues related to the access and processing of personal data.

→ Do you exchange personal data from your employees' and clients with third parties? Are they within the EU?

The GDPR acknowledges that whenever personal data crosses the borders of the EU, the risk for data subjects to be prevented from using their right to data protection increases. Consequently, the GDPR specifies that businesses should only transfer and process personal data outside the EU, with legitimate reasons -even if the data remains within the same company- and show evidence that the data subject was conveniently informed of the transfer and the risk associated with it.

→ Do you conduct privacy impact assessments (PIA) in projects where privacy breach risks are high?

The regulation anticipates the following: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". (n. º 1, Article 35)

4 A new perspective needed: privacy by design

The protection of privacy and personal data should be incorporated through the development cycle and life of the underlying technologies and services, from the initial design phase to their deployment, use and disposal. There's no out-of-the-box solution for data protection as each particular business reality has its own features and requirements. There's also no single or even mixed technological approach since its own evolution creates continuous needs and changes. As such only a well-defined strategy with a life cycle of continual improvement can address the challenges and potential benefits that the GDPR brings to businesses. This strategy needs to be comprehensive and integrate Privacy in the design of the company's processes, technologies and people management.

→ The human factor is still the main pillar in data protection

As a consequence, organization and people should be the forefront of your Privacy strategy.
A global risk based approach should be adopted by controllers and the processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk". Having in mind the magnitude of potential fines and lawsuits by data subjects if a data breach takes place, the risk owner should be given sufficient empowerment to implement and enforce a GDPR compliance plan.
Article 30 of the regulation stipulates that "the **Data Protection Officer** shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing".
As such the DPO should have an informed and active role on all issues related to processing operations being an essential part of what should be a well-established data privacy accountability framework.
A risk assessment and analysis need to be accomplished in order to identify critical processes and activities that process, store or transfer personal data. ISO/IEC 27001 - Information security management systems – implements a risk based approach regarding information security and against which a business can be certified.

→ Awareness and training is seen by the GDPR as an important requirement and it may even make a difference when audited by a supervisor authority in the case of a certification process, a data breach or when a fine takes place. Once again the DPO is responsible for the "awareness-raising and training of staff involved in processing operations" as stated in article 39 and as such appropriate data protection training to personnel having permanent or regular access to personal data is a key requirement.

→ **Then a set of Privacy-preserving techniques such as encryption, anonymization, pseudonymisation and data-minimization, among others, are explicitly recommended the GDPR as way to mitigate risks identified during due assessments.**

Article 30 of the GDPR requires controllers to "ensure a level of security appropriate to the risk." These techniques mitigate the risk of data breaches and the exposure of personal data. For instance, if all activities regarding the collection, processing, storage and transfer of personal data use encryption techniques, the likelihood of personal data being exposed is considerable less than if no encryption is used even in only one activity.
Similarly, if there is no need/purpose to collect certain type of data (i.e. data-minimization) and the collected data could be processed, analyzed and stored as a group data set instead of individual data (i.e. pseudonymisation) techniques such as differential privacy should be used in order to decrease the likelihood of an individual personal data being inferred in the event of a data breach.
A certification process regarding the GDPR is indeed likely to exist at some point - as stated in article 42- but for now there is no specific path to follow. ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors - is certainly a good way to start, providing implementation guidance on ISO 27002 controls applicable to public cloud PII as well as an additional set of controls and associated guidance.

→ **Accountability and transparency of processing** are two principles that are recurrently mentioned by the GDPR given their importance to the processing of personal data and that take part on the previously mentioned data privacy accountability framework. As mentioned in article 5 "the controller shall be responsible for, and be able to demonstrate compliance […] ('accountability')" and personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject".
As such a full revision or completion of processes should be performed in accordance with the GDPR. For instance, how a data breach is going to be handled should be clearly orchestrated not only because the GDPR demands that you keep customers informed as well as competent authorities but also because there will be a reputational risk with potential damage that needs to be promptly addressed and mitigated.
The information that needs to be provided to the data subject must also be in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (article 12) and all the processing and parties related to the processing must be clearly stated and explicitly acknowledged and consented by the data subject.
The right to data-portability, to object and to be "forgotten" are also principles that will have to be addressed as well as to have in place mechanisms to make proof of their implementation in order to comply with the GDPR.

Conclusion

The new EU General Data Protection Regulation (GDPR) is the first and long awaited legislative package from the European Union which defines a baseline and shared rules for all its Member States regarding the protection of personal data.

The GDPR will become directly applicable to all Member States and businesses operating in the European Union and/or processing data of European citizens as of 25 May 2018, which is often considered as the D-Day for Data privacy & security. It implicates substantial operational and procedural changes in relevant businesses which needs to start being tackled now.
Having in place a data protection strategy will not only help complying to the GDPR: it will help businesses address new challenges and take advantage of market opportunities based on new consumers' expectations on trust and privacy. Embracing Privacy by Design should not be considered because of fear of GDPR fines, but because it is an opportunity to differentiate on markets by developing superior customer intimacy and trusting relationship.

About Altran

As a global leader in innovation and high-tech engineering consulting, Altran offers its clients a new way to innovate, by developing the products and services of tomorrow. Altran works alongside its clients on every link in the value chain of their project, from conception to industrialization. For over thirty years, the Group has provided its expertise to key players in the Aerospace, Automotive, Defense, Energy, Finance, Life Sciences, Railway, and Telecoms sectors, among others. In 2015, the Altran group generated revenues of €1.945bn. With a headcount of nearly 26,000 employees, Altran has a presence in more than 20 countries.

Privacy by Design

The Impact of the new European Regulation on Data protection