How to understand the European General Data Protection Regulation (GDPR)

The true spirit of the new legislation, (…) is to stop abusing people's data and work on building long-term trusted client relationships"…
Carolyn Harrison, Director at Assured Clarity Ltd

From human being to data subject

Think of yourself as a data subject. Think of your children as data subjects. Think of society as a conglomerate of data subjects. Think of the amount of data that you generate in your daily live. Think that you are either identified or identifiable through data. Think that data grows exponentially and consider the existence of metadata (data about data) and finally ask yourself the question: are you in control of your personal data? Would you like to be in control? Are you entitled to rights in the digital world? Who owns and control the information that you generate in your daily live? Who is making money using your data? Did they ask for your consent? Would you like to have the right to privacy enshrined by law? These are the questions addressed by the new European General Data Protection Regulation (GDPR).

Regulation is not a dirty word

The digital economy has flourished with little or no regulation. For the adherents of the idea that Internet is successful because it is a cool, borderless space, the news that a major regulation is now in place is not necessarily welcome, though there seems to be a growing consensus that there are serious flaws that need to be modified. After a long political process, the European Union approved the GDPR: a binding law, applicable as from 25 May 2018, with jurisdiction upon the data of residents in the European Union, indistinctly of where the data is stored.

This new piece of legislation has universal importance since it will likely be used as a model in other jurisdictions. The GDPR applies not only to companies and organisations located within the EU but also to those located outside of the EU if they offer goods or services to, or monitor the behaviour of individuals residing in the EU. In practical terms, all the large Internet conglomerates are concerned.

From our perspective, the GDPR is, above all, a privacy protection standard; its purpose being to balance the fundamental right to privacy with economic priorities concerning the free flow of personal data considered as a "resource". It introduces the means to make technological progress accountable to the individual user, since the success of the digital economy has been largely built at the expense of fundamental personal rights.

Civil identity vs digital identity

An identity check on the street is a shocking event. It may be racially or politically motivated. It is an ominous occasion, leading, probably, to unwanted consequences. But in the digital world, identity checks are beyond our sensorial perception. We, the community of end users, the data subjects, are associated with online identifiers provided by the devices we use, applications we open and tools we employ. We bathe on protocol identifiers, cookie identifiers, radio frequency identification tags, face recognition devices, intelligent video surveillance and civil identity documents that contain our biometric data. The digital traces that we leave may be used to create profiles of who we are in a manner that makes us all vulnerable.

The risks are real and they are considerable. They are underscored in article 75: *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and aspects concerning performance at work, economic situation, health personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects*".

The focus on "personal data", defined as information leading to or related to an identified or identifiable person, means that the law deals with "digital identity" in its broad meaning. For the first time, from a legal point of view, the individual user has been "empowered" with the means to control his/her digital identity.

See for instance the rights that are bestowed on the individual user by the GDPR. Article 63 states: *"A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing… Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing."*

This creates the ground for the protection and the exercise of personal rights in a technology-driven society.

Data protection by design and data protection by default

Following from the above, technological innovation has to incorporate principles that protect the rights and freedoms of natural persons with regard to the processing of personal data by adopting internal policies and implementing measures which meet in particular the principles of data protection by design and data protection by default (article 78).

The technological dimension – encryption keeps Big Brother away

All this brings us to the role of encryption: the GDPR states that personal data controllers and processors have the legal obligation to mitigate risks regarding confidentiality, preventing accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data which may lead to physical, material or non-material damage by using encryption technologies, such as those proposed by the OISTE root of trust.

The law further states that a GDPR compliant ecosystem must include digital certification mechanisms and data protection seals and marks, allowing data subjects to quickly assess the level of data protection of relevant products and services (article 100), which again enhances the role of digital certification vendors, such as WISeKey, that operate the OISTE root of trust.

The right to be informed of your personal data vulnerability

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "*result in a risk for the rights and freedoms of individuals*". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "*without undue delay*" after first becoming aware of a data breach.

Personal consent: it all depends on it

Personal behaviour remains an unpredictable variable: empirical evidence seems to prove that the individual Internet user is not very concerned by the way his or her personal data is stored and employed. The short-term rewards work largely in favour of the big Internet corporations offering services online. Catering for that structural fact, the GDPR proposes a strongly worded definition of "personal consent":

(1) Consent about the use of personal data has to be given in an informed way. This means that the individual user (or data subject) has to be aware "*at least of the identity of the controller and the purposes of the processing for which the personal data are intended*";

(2) The data subject has to have a "*genuine or free choice (…) to refuse or withdraw consent without detriment*" (article 42)…. "*Consent is presumed not be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*"…. (article 43).

Right to be forgotten and right to object

(65*) "A data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten"… In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where their processing of his or her personal data does not otherwise comply with this Regulation".*

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject's withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "*the public interest in the availability of the data*" when considering such requests.

Why should data concerning you remain in the "public domain" without a time-limit? The law also contemplates that the duration of personal data storage is limited to a strict minimum… "*time limits should be established by the controller for erasure or for a periodic review*… (article 39).

There are a series of derogations to the previous principle, for instant when processing personal data for archiving purposes, scientific or historical research, statistical or public-health related purposes.

Article 59 states that the individual user has the right to "*request and, if applicable, obtain, free of charge (…) access to and rectification or erasure of personal date and the exercise of the right to object"*. So, if you consider that you have sound reasons to ask that data pertaining to you remains available or is additionally processed, you have the right to object.

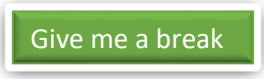
Additionally, article 66 states that: "*To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data*".

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

Terms and Conditions

Terms and Conditions are long and boring documents that nobody reads and most people accept without questions asked. But the truth is that they are "contracts" that the individual user subscribes by clicking on "agree".

Click here: 

In the GDPR:

(1) Online services will no longer be allowed to hide behind legalese about the use of personal data
(2) Consent must be given through a clear, positive action for every use and every user attribute
(3) The user must be able to revoke consent as easily as it was to grant it.

Transparency

Linked to this more protective definition of personal content, the concept of transparency is also underlined by the law: *"it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed…"* (article 39).

Article 58 further states: "*This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom or for what purpose personal data relation to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.*"

Two central legal actors: controllers and processors

Two actors bear the main responsibility in dealing with personal data: (1) the data controller and (2) the data processor. The distinction is not always easy to make. Roles change. For some instances, the same juridical person acts sometimes as a controller, sometimes as a processor. The law defines them as follows:

Controllers

Natural or legal persons, public authorities, agencies or bodies which alone or jointly with others determine the purposes and means of the processing of personal data. Controllers are the principal party for collecting consent, managing consent-revoking, enabling right to access, etc. Controllers are the point of reference for the data subject who wishes to revoke consent for his or her personal data.

Apple, Google, Facebook, Amazon, Microsoft and the "data brokers" that gather information from publically available sources and track Internet use, they are all data controllers. Furthermore, governments, public sector agencies, banks, health care providers and all employers are also data controllers. Retailers, restaurants, hotels, venues and any business with customer records, are also controllers of personal data.

Processor

Any entity that processes personal data under the controller's instructions (e.g., many service providers).

A new job: Data Protection Officers (DPO)

The GDPR introduces the mandatory appointment of a DPO for any organization that processes or stores large amounts of personal data. DPOs must be appointed where the core activities of the controller or the processor involve regular and systematic monitoring of data subjects on a large scale or where the entity conducts large-scale processing of special categories of personal data, like that which details race or ethnicity or religious beliefs.

The DPO has the responsibility of maintaining records of processing activities on behalf of the controller or the processor and is accountable to supervisory authorities.

Public authorities and institutions are directly concerned here, though there are a series of exemptions defined by the law, for instance, courts acting in their judicial capacity. On top of that, the law caters for the needs of small and medium-sized enterprises and derogates this obligation if they have fewer than 250 employees.

Law enforcement and the public interest

The legislators took care not to weaken law enforcement in the European Union through the GDPR… "*the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act*"(article 19 and ss).

The GDPR also contemplates a series of provisions that uphold what is defined as "public interest". For instance scientific or historical research, public-health issues, statistical analysis and a number of social-sciences tools that "*provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services*" (article 157). The preservation and use of personal data for those purposes is allowed, though it should be "*subject to appropriate conditions and safeguards set out in Union or Member State Law*" (ibid).

If you don't fear God – fear the penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

Conclusion

As mentioned before, personal behaviour is an unpredictable variable. What the GDPR does is to provide a legal framework that empowers the individual user to hold accountable – in multiple ways - the companies that deal with his or her personal data. But will individuals change their behaviour and use the legal tools that the GDPR provides in a responsible manner, or will the digital economy be

submerged by pointless individual demands that lead nowhere but an increase of red tape? To me, that is the big question that remains open.

The other question is: how will small and medium size companies cope with the law? Will compliance increase their operational cost to a point where they won't be viable anymore?

Be what it may, the main contribution of the GDPR lies on setting the legal conditions for the next step in the evolution of the digital society: the rights of the individual person have to be preserved at all costs.

Jorge A. Restrepo
Liaison officer, OISTE Foundation
June 2018