How to make your creative business compliant with the General Data Protection Regulation (GDPR)

The General Data Protection Regulation ("GDPR") is upon us: what is it? How is it going to impact you and your business? What do you need to do in order to become GDPR compliant? There is not a moment to waste, as the stakes are very high, and since becoming GDPR compliant will definitely bring competitive advantages to your business.

On 27 April 2016, after more than 4 years of discussion and negotiation, the European parliament and council adopted the

General Data Protection Regulation ("**GDPR**").

1. Why the GDPR?

The GDPR repeals Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data (the "**Directive**").

The Directive, which entered into force more than 20 years' ago, was no longer fit for purpose, as the amount of digital information businesses create, capture and store has vastly increased.

Data, the bigger the better, is here to stay. Today's data more and more greases our digital world. Control of data is ultimately about power and data ownership does seriously impact competition on any given market. By collecting more data, a firm has more scope to improve its products, which attracts more users, generating even more data, and so on. Data assets are, today, at least as important as other intangible assets such as trademarks, copyright, patents and designs, to companies[1]. The stakes are way higher, today, as far as data ownership, control and processing are concerned,

and GDPR addresses that data flow in the 21st century, as we all engage with technology, more and more.

Moreover, many legal cases, brought up in various member-states of the European Union ("**EU**"), pinpointed the severe weaknesses and gaps in providing satisfactory, strong and homogeneous protection of personal data, relating to EU citizens, and controlled by companies and businesses operating in the EU. For example, the Costeja v Google judgment, from the Court of Justice of the European Union ("**CJEU**"), commonly referred to as the "right to the forgotten" ruling, was handed down on 26 November 2014. This ground-breaking judgment recognised that search engine operators, such as Google, process personal data and qualify as data controllers within the meaning of Article 2 of the Directive. As such, the CJEU

ruling recognised that a data subject may "*request (from a search engine) that the information (relating to him/her personally) no longer be made available to the general public on account of its inclusion in (…) a list of results*". Through this decision, the CJEU forced search engines such as Google to remove, when requested, URL links that are "*inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed*". It was a huge step forward for personal data protection in the EU.

In addition, data breaches at, and cyber-attacks of, thousands of international businesses (Sony Pictures, Yahoo, Linkedin, Equifax, etc.) as well as EU national companies (Talktalk, etc.) make the news, consistently and on a very regular basis, dramatically affecting the financial and moral well being of millions of consumers whose personal data was hacked because of these data breaches. These attacks and breaches raise very serious concerns as to whether businesses managing personal data of EU consumers are actually "up to scratch", in terms of proactively fighting against cyber-crime and protecting personal data.

Finally, the GDPR, which will be immediately enforceable in the 28 member-states of the EU without any transposition from 25 May 2018, unlike the Directive which had to be transposed in each EU member-state by way of national rules, standardises all national laws applicable in these member-states and therefore provides more uniformity across them. The GDPR levels the playing field.

2. When will the GDPR enter into force?

The GDPR, adopted in April 2016, enters into force on 25 May 2018, ideally giving a 2-year preparation period to businesses and public bodies to adapt to the changes.

While many EU business owners take the view that the changes

brought by the GDPR onto their businesses, will be of little or no importance or just as important as other compliance issues, there is not a minute to spare to prepare for compliance with the new set of complex and lengthy rules set out in the GDPR.

3. What is at stake? Which organisations are impacted by the GDPR?

A lot is at stake. All businesses, organisations or entities which operate in the EU or which are headquartered outside of the EU but collect, hold or process personal data of EU citizens must be GDPR compliant by 25 May 2018. Potentially, the GDPR may apply to every website and application on a global basis.

As most if not all multinationals have customers, employees and/or business partners in the EU, they must become GDPR compliant. Even start-ups and SMEs must be GDPR compliant, if their business model infer that they will collect, hold or process personal data of EU citizens (i.e. customers, prospects, employees, contractors, suppliers, etc).

The stakes are very high for most businesses and, for many companies, it is becoming a board-level conversation and issue.

To ensure compliance with the new legal framework for data protection, and the implementation of the new provisions, the GDPR introduced an enforcement regime of very heavy financial sanctions to be imposed on businesses that do not comply with it. If an organisation does not process EU individuals' data in the correct way, it can be fined, up to 4 percent of its annual worldwide turnover, or Euros 20 million – whichever is greater[2].

These future fines are way larger than the GBP500,000 capped penalty the UK Data Protection Authority ("**DPA**"), the

Information Commissioner Office ("**ICO**"), or the maximum 300,000 Euros capped penalty that the French DPA, the "*Commission Nationale Informatique et Libertés*" ("**CNIL**"), can currently inflict on businesses.

4. What are the GDPR provisions about?

The GDPR provides 99 articles setting out the rights of individuals and obligations placed on organisations within the scope of the GDPR.

Compared to the Directive, here are the new key concepts brought by the GDPR.

4.1. Privacy by design

The principle of "privacy by design" means that businesses must take a proactive and preventive approach in relation to the protection of privacy and personal data. For example, a business that limits the quantity of data collected, or anonymises such data, does comply with the "privacy by design" principle.

This obligation of "privacy by design" implies that businesses must integrate – by all appropriate technical means – the security of personal data at the inception of their applications or business procedures.

4.2. Accountability

Accountability means that the data controller, as well as the data processor, must take appropriate legal, organisational and technical measures allowing them to comply with the GDPR. Moreover, data controllers and data processors must be able to demonstrate the execution of such measures, in all transparency and at any given point in time, both to their respective DPAs and to the natural persons whose data has been treated by them.

These measures must be proportionate to the risk, i.e. the

prejudice that would be caused to EU citizens, in case of inappropriate use of their data.

In order to know whether a business is compliant, it is therefore necessary to execute an audit of the data processes made by such company. We, at Crefovi, often execute some audits certified by the CNIL or the ICO.

4.3. Privacy impact Assessment

The business in charge of treating and processing personal data, as well as its subcontractors, must execute an analysis, a Privacy Impact Assessment (“**PIA**”) relating to the protection of personal data.

Businesses must do a PIA, a privacy risk assessment, on their data assets, in order to track and map risks inherent to each data process and treatment put in place, according to their plausibility and seriousness. Next to those risks, the PIA sets out the list of organisational, IT, physical and legal measures implemented to address and minimise these risks. The PIA aims at checking the adequacy of such measures and, if these measures fail that test, at determining proportionate measures to address those uncovered risks and to ensure the business becomes GDPR compliant.

Crefovi supports companies in performing PIAs and in checking the efficiency of the security and protection measures, thanks to the execution of intrusion tests.

4.4. Data Protection Officer

The GDPR requires that a Data Protection Officer (“**DPO**”) be appointed, in order to ensure the compliance of treatment of personal data by public administrations and businesses which data treatments present a strong risk of breach of privacy. The DPO is the spokesperson of the organisation in relation to personal data: he or she is the “go to” point of contact, for the DPA, in relation to data processing compliance, but also

for individuals whose data has been collected, so that they can exercise their rights.

In addition to holding the prerogatives of the "*correspondant informatique et liberté*" ("**CIL**") in France, or chief privacy officer in the UK, the DPO must inform his/her interlocutors of any data breaches which may arise in the organisation, and analyse their impact.

4.5. Profiling

Profiling is an automated processing of personal data allowing the construction of complex information about a particular person, such as her preferences, productivity at work or her whereabouts.

This type of data processing can generate automated decision-making, which may trigger legal consequences, without any human intervention. In this way, profiling constitutes a risk to civil liberties. This is why those businesses doing profiling must limit its risks and guarantee the rights of individuals subjected to such profiling, in particular by allowing them to request human intervention and/or contest the automated decision.

4.6. Right to be forgotten

As explained above, the right to be forgotten allows an individual to avoid that information about his/her past interferes with his/her actual life. In the digital world, that right encompasses the right to erasure as well as the right to dereferencing. On the one hand, the person can have potentially harmful content erased from a digital network, and, on the other hand, the person can dissociate a keyword (such as her first name and family name) from certain web pages on a search engine.

Crefovi can support and advise a business facing a request of execution of the right to be forgotten.

4.7. Other individuals' rights

The GDPR supplements the right to be forgotten by firmly putting EU citizens back in control of their personal data, substantially reinforcing the consent obligation to data processing, as well as citizens' rights (right to access data, right to rectify data, right to limit data processing, right to data portability and right to oppose data processing), and information obligations by businesses about citizens' rights.

5. Is there a silver lining to the GDPR?

5.1. An opportunity to manage those precious data assets

Compliance with GDPR should be viewed by businesses as an opportunity, as much as an obligation: with data being ever more important in an organisation today, this is a great opportunity to take stock of what data your company has, and how you can get most advantage of it.

The key tenet of GDPR is that it will give you the ability to find data in your organisation that is highly sensitive and high value, and ensure that it is protected adequately from risks and data breaches.

5.2. Lower formalities and one-stop DPA

Moreover, the GDPR withdraws the obligation of prior declaration to one's DPA, before any data processing, and replaces these formalities with mandatory creation and management of a data processing register.

In addition, the GDPR sets up a one-stop DPA: in case of absence of a specific national legislation, a DPA located in the EU member-state in which the organisation has its main or unique establishment will be in charge of controlling compliance with the GDPR.

Businesses will determine their respective DPA with respect to the place of establishment of their management functions as far as supervision of data processing is concerned, which will allow to identify the main establishment, including when a sole company manages the operations of a whole group.

This unique one-stop DPA will allow companies to substantially save time and money by simplifying their processes.

5.3. Unified regulation, easier data transfers

In order to favour the European data market and the digital economy, and therefore create a favourable economic environment, the GDPR reinforces the protection of personal data and civil liberties.

This unified regulation will allow businesses to substantially reduce the costs of processing data currently incurred in the 28 EU member-states: organisations will no longer have to comply with multiple national regulations for the collection, harvesting, transfer and storing of data that they use.

Moreover, since data will comply with legislations applicable in all EU countries, it will become possible to exchange it and it will have the same value in different countries, while currently data has different prices depending on the legislation it complies with, as well as different costs for the companies that collect it.

5.4. A geographical scope extended by fair competition

The scope of the GDPR extends to companies which are headquartered outside the EU, but intend to market goods and services in the EU market, as long as they put in place processes and treatments of personal data relating to EU citizens. Following these residents on internet, in order to create some profiles, is also covered by the GDPR scope.

Therefore, European companies, subjected to strict, and potentially expensive, rules, will not be penalised by international competition on the EU single market. In addition, they may buy from non-EU companies some data which is compliant with GDPR provisions, therefore making the data market wider.

5.5. Opening digital services to competition

The right to portability of data will allow EU citizens subjected to data treatment and processing to gather this data in an exploitable format or to transfer such data to another data controller if this is technically possible.

This way, the client will be able to change digital services provider (email, pictures, etc.) without having to manually retrieve all the data, during a fastidious and time-consuming process. By lifting such technical barriers, the GDPR makes the market more fluid, and offers to users enhanced digital mobility. Digital services providers will therefore evolve in a more competitive market, inciting them in providing better priced and higher quality services, as their clients will no longer be hostages to their initial provider.

5.6. Labels and certifications

The European committee on data protection, as well as EU institutions, will propose some certifications and labels in order to certify compliance with the GDPR of data processes performed by businesses.

Cashable recognition and true asset for the brand image of a company, labels and certifications will also become a strong commercial tool in order to gain prospects’ trusts and to win their loyalty.

6. What are the actionable steps to take,

right now, to become GDPR compliant?

There is not a moment to lose to implement the following steps, below:

- decide on the ownership of implementing the GDPR provisions in your organisation; assign ownership to the best suited department or team (Legal? Compliance? Technology?);
- liaise with your one-stop DPA, as several of them have prepared useful explanatory information or guidance to comply with GDPR, such as the ICO in the UK, the CNIL in France and the Data Protection Commissioner in Ireland (the latter being the DPA of many a digital giant, such as Google, Facebook and Twitter);
- draft a map of the data processes in your organisation, and identify the gaps in GDPR compliance in relation to these various processes – we, at Crefovi, have drafted some detailed documents on how to make this mapping of data processes and treatments and to support you on identifying the gaps in GDPR compliance;
- value the various data processes and treatments and assess which ones are high risk and make a list of your high-risk data assets;
- execute a PIA on those high-risk data assets (such as Human resources' data, customers' data) – Crefovi supports companies in performing PIAs and in checking the efficiency of the security and protection measures, thanks to the execution of intrusion tests;
- implement legal, technical, organisational and physical measures to lower risks on those data assets and become GDPR compliant;
- ensure that your contractors and subcontractors have put compliant security measures in place, by sending them a

list of points to check;

- do privacy awareness training for your employees as they must understand that personal data is anything that can be linked directly to an individual and that there will be some consequences if they break the GDPR provisions and steal personal data;
- develop a Bring Your Own Device policy ("**BYOD**") and enforce it within your organisation and among your employees, since you are accountable for all data user information stored in the cloud and accessible from both corporate devices (tablets, smartphones, laptops) and personal devices. Also, when employees leave or are terminated, make sure that you have included BYOD in your off-boarding process, so that leaving staff lose access to company confidential data immediately on their devices;
- check and/or redraft the information notices or confidentiality policies in order that they set out the new information required by the GDPR;
- put in place automated mechanisms in order to obtain explicit consent from EU citizens, especially if your business deals with behavioural data collection, behavioural advertising or any other form of profiling;
- put in place a solid management plan in case personal data breaches happen, which will allow you to comply with the mandatory requirement to notify your DPA within 72 hours – our in-depth experience of alert, risk management, analytical and notification plans, in France and the United Kingdom, put us, at Crefovi, in a great position to support our clients to prepare for the demanding requirements set out in the GDPR.

[1] "*The world's most valuable resource is no longer oil, but data*", The economist, 6 May 2017.

[2] “*Preparing for the general data protection regulation: a roadmap to the key changes introduced by the new European data protection regime*”, Alexandra Varla, 2017.

Crefovi regularly updates its social media channels, such as Linkedin, Twitter, Instagram, YouTube and Facebook. Check our latest news there!

Your name (required)

Your email (required)

Subject

Your message

Send

$M_E \gamma^5$

Δ