ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

European Data Protection: New Rules, a Whole New Game

Compliance and Ethics


GDPR
PII

CHEAT SHEET

- ***A new digital world.*** The General Data Protection Regulation in the European Union will be the first major update of EU data protection rules since 1995, and will dramatically alter international data relations.
- ***Imposing sanctions globally.*** GDPR has a global reach, and can extend to any organization that offers goods or services to EU residents with a maximum fine of €20 million.
- ***Comply and obey.*** The most efficient way to tackle GDPR is by appointing a data protection officer to comply with new regulations through diligent record keeping and data mapping.
- ***Consent to share.*** GDPR will implement new data regulations regarding consent that will require a clear and unambiguous agreement to share data for special circumstances.

The flight wasn't bad, and the CEO and CFO appreciated the dinner at the fancy restaurant last night. All in all, the idea of having the second 2018 quarterly board meeting in this European capital, even though you're a NASDAQ-listed and thoroughly US-owned company, seemed to work well. Which was good, as it was your idea. As a recently recruited GC who had spent a few years in Europe, you wanted the company to "look" more global. External communications had a great day showing the board this side of the pond, and favourable press cuttings seemed to show your first suggestion was a success.

It's the next morning, a lovely 2018 summer day. But you're not enjoying it, not a little bit. Looks like the local DPA (data protection authority) has issues with the way your company handles employee data — an anonymous complaint to the DPA has prompted an investigation, and your CEO and board are having to look into it whilst the whole office is being searched in a dawn raid — in full view of the local press, helpfully tipped off by someone. Apparently your company is in gross violation of the EU General Data Protection Regulation, which just entered into force. Your local counsel advises the board to cut the meeting short and head back home, as they are potentially criminally liable for the non-compliance. The board, conscious of the potential PR and stock price fallout, is seething. How did this happen, you wonder, while you try to avoid the CEO's gaze….

Relax — it is still 2016, and you can plan ahead to avoid scenarios like this.

To start, what has changed about EU data protection, and what should you do about it?

In April 2016, the European Parliament adopted the General Data Protection Regulation (GDPR). This generated much media interest so you may have seen the story — but it may still be unclear to you how that impacts your organisation — especially if it is headquartered outside of the European Union.

This article will provide a simple overview of the main aspects of the GDPR, which is a substantial and complicated document (204 pages, 135 recitals, and 91 articles), and will focus on the practical aspects of compliance with it.

The GDPR is the first major update of EU data protection rules since 1995, and will enter into force on May 25, 2018. As a reminder, EU and national data protection laws set out rules for organisations who use or store personal data, and give rights to those people whose data has been collected. The rules apply to data held on any sort of storage system, including paper records.

One thing to bear in mind is that the definition of "personal data" in the European Union is different from those used in other jurisdictions, and includes phone numbers, emails, cookies, or IP addresses. Personal data under the GDPR is therefore far more extensive than the definition of personal identifiable information (PII) in the United States. For example, in California the definition of "personal information" for the purposes of a data breach notification means:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted;
2. Social security number;
3. Driver's license number or California identification card number;
4. Account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

5. Medical information;
6. Health insurance information; and,
7. Information or data collected through the use or operation of an automated license plate recognition system (Civil Code 1798.29).

In contrast, under the GDPR, “personal data” is “any information relating to an identified or identifiable natural person” (data subject). This is so broad that we will need to wait for case law — and guidance from data protections authorities — to see exactly what the definition encompasses.

Data deemed more sensitive also needs to have additional protection. For example, your organisation will need to encrypt or restrict access to employee data (e.g., date of birth, marital status, salary, bank account details, job history, etc.) to ensure that any accidental disclosure (e.g., a laptop or memory stick left on a train, an email incorrectly addressed, etc.) does not cause particular harm. As the GDPR adopts a risk-based approach, if your organization deals with even more sensitive data, it will have to “implement appropriate technical and organizational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and the severity for the rights and freedoms of natural persons.” So, for instance, the safeguards for addresses and credit cards details will be judged against a lower bar than those related to health data, and DPAs will expect stronger protection of the latter.

Global reach

The first, and fundamental, thing to notice is that the GDPR has a global reach. Even if your company is not based in the European Union, the GDPR still applies.

All organisations that offer goods or services to EU residents or monitor their behaviour will need to comply with the GDPR, regardless of where they are based. The part about “monitoring their behaviour” demonstrates the intention to give this regulation global reach. The provision is clearly designed to catch internet-related activities, and it will mean that the new rules apply to companies like Facebook and Google, but also, potentially, to organisations with a website (accessible to EU residents) that has any sort of tracking mechanism (cookies, beacons, etc.). If your organisation provides an app to EU residents, it is probably also caught by the provision if it sip collects usage data, even in aggregate/anonymous format. So even if those tracking mechanisms are managed by a third party but are active on your organisation’s website, for instance for providing targeted ads, your organisation is bound by the new rules.

The downside of this is the obvious increase of regulatory scrutiny. The potential upside is that if your organisation was already trading or dealing with data of EU citizens, you now have one set of clearer rules to follow, as opposed to 28 separate ones (one for each member state). More information on this is below.

Sanctions and enforcement

Another major reason to take notice of the GDPR is the new level of potential risk in terms of enforcement. The maximum fines under the GDPR will be up to €20 million or four percent of annual global revenues, whichever is greater. The rules are clear: it is indeed global, and not only EU revenues. So a US company with US$1 billion revenue, even if mostly generated outside the

European Union, may be liable to fines of up to US$40 million — per each violation. This is a stark increase on the current maximum fines, and put the GDPR on a par with antitrust sanctions in terms of regulatory risk. It should be noted that during the consultations for the finalisation of the GDPR, data protection authorities were expressly asked if they envisaged making use of these increased fining powers, and the answer was affirmative. It does not look like an abstract risk.

Data protection officer

Most organisations must appoint a data protection officer (DPO) to ensure compliance with all relevant obligations. The description of this role sounds almost like that of a chief compliance officer: The position requires not only expert knowledge of data protection, but also the ability to fulfill his/her tasks. The position must report directly to the top of the organisation (in companies to the board). There is an obligation to involve the DPO in all issues related to data protection, and the DPO must be capable of exercising his/her functions in complete independence.

Lead data protection authority

The GDPR introduces a new mechanism for national data protection authorities to cooperate in order to provide a “one-stop-shop” for businesses. Your organisation will need to decide which regulator to choose as the “lead” regulator to report to. The opportunity is there to select a relatively business-friendly regulator, such as the Information Commissioner’s Office in the United Kingdom, as opposed to others that have historically taken a more conservative approach.

Data breach reporting

One of the most important changes is related to data breach reporting. The current situation in the European Union is that there is no general obligation (exceptions exist for certain sectors, such as healthcare, telecommunications, financial services, etc.) to report data breaches. The GDPR introduces such obligations. The definition of a data breach is “a breach of security leading to the accidental and/or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.” This is unrelated to any notion of adequacy of the security measures used to protect the data. It is in fact any incident that impact the so-called CIA principles (confidentiality, integrity, availability).

There are two types of reporting: (1) to data protection authorities; and, (2) to the affected data subjects. Organisations must report data breaches to their supervisory authority (and to individuals affected) without undue delay and no later than 72 hours after becoming aware of it. The main exemption to the rule that all breaches must be reported is when the breach is “unlikely to result in a risk for the rights and freedoms of individuals.” Examples could be a laptop with employee data going astray, but then found on the company premises, or a sealed envelope containing payslips (or credit cards slips) mistakenly put in an ordinary waste bin instead of a shredder, but then recovered unopened.

The “without undue delay” rule is further clarified by saying that if the report does not occur within the stated limit of 72 hours, the company must provide a justification for the delay. As the report needs to contain not just the details of the data concerned, but also the likely consequences and the measures taken to address and mitigate risks to the individuals concerned, it is clear that a robust data breach process needs to be in place. A good suggestion is that the data breach response policy should align with the existing crisis management procedures. Given the dependency all organisations have on

their IT systems, it is quite evident how the need to analyse the breach, and therefore the potential need to freeze/put offline key IT systems (or even just the email server) whilst the forensic analysis is being performed, needs to be treated as a business continuity issue, and the existing Business Continuity Management processes may need to be invoked.

One thing that may be overlooked, but is vital to remember, is that one of your suppliers may be breached and your organisation has obligations vis-à-vis the data subjects for your entire supply chain. Therefore, it is important to plan for this eventuality, and be able to invoke your data breach management policy when you're notified by one your suppliers of a data breach regarding data you are responsible for. In our increasingly interconnected world, it is highly possible that a data breach on a company providing, say, server space or infrastructure/software as a service to your payroll provider would mean you have an immediate obligation to inform your employees of the breach.

It is therefore essential to analyze where your customers/employees/suppliers data is kept alongside your supply chain. This "data mapping" exercise will allow you to have a holistic view of where the risk lies, and to ensure that adequate measures are in place throughout your chain.

What's the difference between the GDPR and the existing Data Protection Directive? Direct applicability.

What is the difference between directives and regulations?

These are the two main forms of EU legislation.

- Regulations are addressed to all member states and are applied in full. They are directly applicable without the need for national legislation.
- Directives are addressed to all EU member states and require an objective to be achieved by a given date. National authorities must draw up national legislation in order to conform with the directive within a certain time frame.

The GDPR is a regulation, so it will become directly applicable on the whole of the territory of the European Union after 25 May 2018.

Data mapping

The GDPR requires that organisations maintain a record of all processing activities under their responsibility, including:

- The name and contact details of the data controller;
- The purposes of the processing;
- A description of categories of data subjects and of the categories of personal data;
- The recipients or categories of recipients of the personal data;
- Transfers of data to a third country and the documentation of appropriate safeguards;
- A general indication of the time limits for erasure of the different categories of data; and,
- The description of the technical and organisational security measures used to safeguard the data.

These records must be kept and — upon request — be made available to the data protection authorities. From a practical perspective, this will require a project to identify all required information, the cooperation of the whole organisation (and its supply chain), and the production of data flow maps to organise and visualise your organisation's data processing activities. One strategy to "eat the elephant" (i.e., one piece at a time) is to limit the scope of the first attempt. For instance, you could start by trying to map only data related to employee (as opposed to, say, customers or suppliers). Or you could start with all the data handled by a specific function (sales, as opposed to marketing or procurement).

Data protection by design

The GDPR introduces new principles of "data protection by design" and "data protection by default," that encourages techniques to minimise and protect the amount of personal data used in business processes (such as "pseudonymisation" and "dataminimisation" — see sidebar on below). This will require a culture shift in many workplaces, as we will all need to revise our business practices to ensure compliance, and consider the data protection aspect for every new business or IT project. The way we have historically acquired, managed, and stored customer data, for example, may need to be reassessed — buying a list of prospects with email addresses, or allowing all employees (not just the ones who need it) access to such data, are now practices that could lead to claims and fines. Equally important will be to receive the same assurance of compliance from our supply chain.

The idea is that each organisation should be able, at any given time, to identify the "5 Ws" (Who/Where/What/When/Why) of the treatment of personal data under the company's control.

Pseudonymisation and data minimisation

The GDPR introduces a new tongue-twister concept: "pseudonymization."

The GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. As long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

It is therefore a privacy-enhancing technique, not unlike some a cyphered message, where directly identifying data is the "key," held separately, which is need to "read in clear" (i.e., identify) the processed data. As any good spy novel or movie illustrates, the key must therefore be kept not just separate, but also secure.

Cross border data transfer

The rule for international data transfers (e.g., reporting pay level of EU subsidiaries so that the Remuneration Committee back in the HQ in the United States can make decisions) is now more prescriptive and has more requirements. This article does not contain details as the situation is still evolving, but there are specific precautions that will need to be observed. There have been several challenges to the existing legal ways to transfer data from the EU to the United States, and the

situation needs to be clarified, awaiting rules from the EU DPAs, which have promised agreed, harmonised guidelines before the end of 2016.

Consent

The consent of the data subject is still a valid basis for processing data under the GDPR but there are two updates.

1. There is a new definition of consent that requires a “clear affirmative action.” Consent needs to be freely given, specific, informed, and unambiguous. The GDPR is very clear that pre-ticked boxes on web forms, silence, or inactivity do not constitute consent.
2. There are new conditions for the consent to be valid, as well as new circumstances where explicit consent is required (e.g., special categories of data that include genetic data, biometric data, and data concerning sexual orientation).

A further challenge will be that consent to data processing will also need to be “specific” (i.e., it must be separated from other types of consent and actions). For example, this means that consenting to the terms and conditions of a vendor for an item you have bought online should be a separate action from consenting to have your data shared with third parties for marketing purposes. Each of these requests for consent to data processing must be “clearly distinguishable” from any other, and it must be provided “in an intelligible and easily accessible form, using clear and plain language.”

There are other issues, such a data portability (which has an impact on the use of cloud computing, the internet of things, etc.), the right to erasure of personal data, (catchily described as the “right to be forgotten”), and other matters, such as the privacy impact assessments, that organisations will need to take into account. However these are beyond the scope of this article. The situation is also very fluid, and helpful guidance is regularly being issued by the Article 29 Working Party (a grouping of all the EU DPAs) and the European Data Protection Supervisor.

Hopefully this introduction will help readers identify the main issues that they may face when complying with the GDPR.

No doubt the next two years will be challenging, but if you make the changes to your data protection regime, you may still get to have your Q2 18 board meeting in Europe.

Alessandro Galtieri

VP for Corporate Law and the Group Data Protection Officer

Colt Group

He has a keen interest in legal ops and is active in the European leadership of ACC.