General Data Protection Regulation (GDPR): What's in it for Australian organisations?

by Giovanni Butera*

The protection of data, particularly personal data, has become a priority for governments and many other organisations worldwide. In 2016, amid the explosion of data available over the Internet and the increased risk of privacy breaches, the parliament of the European Union (EU) was advised to replace the outdated 1995 Data Protection Directive and adopt the General Data Protection Regulation (GDPR). This Regulation came into effect on the 25th of May 2018 and it outlines a new set of enforceable and uniform requirements for protecting the personal data of citizens across the EU.

*Dr. Giovanni Butera is Managing Director, Head of Data Management, Analytics and Innovation at Nixora Group. M: +61 410 860 036 E: giovanni.butera@nixoragroup.com.au
This paper was submitted to Australia-European Union Free Trade Agreement - Department of Foreign Affairs and Trade – Australian Government.
http://dfat.gov.au/trade/agreements/negotiations/aeufta/submissions/Pages/submissions.aspx

Introduction to GDPR Compliance

The protection of data, particularly personal data, has become a priority for governments and many other organisations worldwide. In 2016, amid the explosion of data available over the Internet and the increased risk of privacy breaches, the parliament of the European Union (EU) was advised to replace the outdated 1995 Data Protection Directive and adopt the General Data Protection Regulation (GDPR). This Regulation came into effect on the 25th of May 2018 and it outlines a new set of enforceable and uniform requirements for protecting the personal data of citizens across the EU.

So what? We're an Australian organisation

Right now, you might be assuming that you need not be concerned about compliance because, well, your organisation is Australian-based and this is an EU regulation. Wrong! Obviously the GDPR applies to Australian organisations with an established presence in the EU, as in, for example, having a branch office in one or more of the EU member states.

But let's look at this situation in another way: it is highly likely your organsation has some form of online presence, usually a website, which means you've gone global.
Think for a moment of the number of people from the EU who might be in the country on a permanent visa, temporary visa or a travel visa. Now think of all of their online activity even before they had set foot in the country (accommodation bookings, car hires, job applications, study applications, insurance applications, money transfers and so on), the trail of personal data recorded (each person's name and address, including email address, phone number, driver's license, passport information, educational records, medical history, bank account information and so on), and that this information may be found across different systems and applications organisation-wide (on traditional databases, big data warehouses, cloud environments, file servers and so on). And let's not forget that your organisation may have approved third party access for processing all of this personal data.

The focus is on personal data, not geography

Do you see the bigger picture? It doesn't matter if your organisation is located in one of the remotest regions of the country, the GDPR applies to any organisation, Australian or otherwise, that:

- Has an established presence (branch office) in the EU but processes personal data in another country;
- Has a website that offers goods and services to EU customers in a European language and enables payment in euros;

- Mentions EU customers or users on their website;
- Monitors the on-line activities of individuals belonging to the EU and processes this data to analyse their personal preferences, behaviours and attitudes.

Moreover, it applies to organisations of any size that processes data about EU data subjects whether they are customers, consumers, business partners, suppliers, employees or other individuals.

It is worthwhile emphasising that the GDPR is focused on enhancing the rights of EU individuals to control what personal data is collected and how it is used no matter where or why it is has been collected and stored. The Regulation gives EU data subjects the right to:

- **Be informed and give consent**: you need to be able to demonstrate that data subjects have been informed about their right to consent, and that consent was freely given, specific and unambiguous.
- **Access their information**: whenever requested you need to be able to provide a copy of the data collected, explain how it is used, list any third-party access, and indicate for how long it will be stored within a month from when the request was made.
- **Anonymity, or pseudonymisation**: where necessary, you must be able to transform identifying data into a manner that prevents any person with unauthorized access to trace it back to an individual.
- **Rectification**: you must comply with any request to have inaccurate data corrected.
- **Object to or restrict data processing**: if an individual objects to the processing of their data, or requests it be restricted, you will be required to provide a legal and compelling reason for continuing to do so, or demonstrate that data is processed in limited circumstances and only with the data subject's consent.
- **Data portability**: you must comply with any request by a data subject to have their personal data transferred to another organisation (e.g., a competitor).
- **Erasure, or the "right" to be forgotten**: data subjects have the right to withdraw consent that was previously given, which means that if requested you must permanently remove their personal data from wherever it is held in your organisation.
- **Notification of breach**: if a data breach is high likely to compromise the rights of an individual you must notify the individual immediately, and inform the relevant supervisory authority within 72 hours of becoming aware of the breach.

Australian organisations likely have privacy policies and security measures already in place aligned with the Australian *Privacy Act 1988*, which actually has equivalent definitions and requirements as those outlined under the GDPR.

For example, the GDPR's definition of personal data is "any information relating to an identified or identifiable person," while the definition of personal information under the *Privacy Act* is "information or an opinion about an identified individual, or an individual who is reasonably identifiable."

The challenges posed by the GDPR

While many of the rights set down in the GDPR are similar to those in the *Privacy Act*, the GDPR still poses challenges to your organisation in having to have your data controllers and processors review governance policies and accountability requirements, as well as technical and operational capabilities, in making the journey towards compliance. An important set of requirements under the GDPR is related to extending the obligations and responsibilities of data controllers and processors.

Appointing a Data Protection Officer

Where necessary, and for certain organisations, data controllers and processors must appoint a data protection officer (DPO) to serve as a point of contact between an organisation and GDPR Supervisory Authorities. The role of the DPO is to audit and advise the organisation on compliance with the GDPR, maintain comprehensive records of all data processing activities, including making records available on request, and ensure data subjects are informed of their rights and what security measures are in place to protect against privacy breaches. Educating the organisation on the compliance requirements of the GDPR and ensuring its data processing employees are adequately trained are also part of the DPO's role. In certain cases, the DPO needs to be based in the EU.

Data controllers

Your data controllers, those who determine the purposes and implement the means for processing personal data, must demonstrate compliance with all of the GDPR's principles. Data controllers are required to:

- Undertake a compulsory data protection impact assessment (DPIA) before commencing data processing of EU individuals;
- Consult with a relevant supervisory authority before processing begins if the DPIA indicates processing operations pose a high risk to the rights and freedoms of EU individuals;
- Implement a 'privacy by design and default' approach to indicate that effective measures to protect personal data are integrated into processing activities from the very beginning;
- Maintain records of processing activities under their responsibility;

- Establish codes of conduct for their specific sector, business or department that ensures appropriate application of GDPR principles.

Data processors

There are some new GDPR requirements that apply directly to data processors, those who process the personal data under the direction of a data controller. The Regulation decrees that certain clauses must be included in a contract that sets out the relationship between the controller and the processor. Under contract, the processor is obligated to:

- Process data only in accordance with the documented instructions from the controller;
- Be bound to a confidentiality agreement, or be under an appropriate statutory obligation of confidentiality;
- Only engage another processor with the authorisation of the data controller;
- Assist the controller to meet his or her responsibilities relating to security obligations, including DPIAs and notifications of data breaches.

Another key obligation, one that also applies to controllers, is for a processor to implement technical and organisational measures appropriate to the level of risk posed to the rights and freedoms of individuals.

The data challenge and consequences

As mentioned earlier, personal data may be spread all over your organisation — on databases, data warehouses, cloud environments, multi-user servers, internal hard drivers, legacy operating systems, and even outside of your organisation. This means compliance with the GDPR involves two types of inventory: (1) identifying all of the diverse technology, systems and applications (whether digital, physical or combined) where personal data is recorded and stored; and (2) identifying all of the relevant and in-scope data that the GDPR principles would apply to.

The latter obviously refers to the personal data belonging to EU citizens which your organisation needs to evaluate under several key questions of compliance:

- Why was the data originally collected?
- How was the data collected?
- Who uses the data and is it shared with third parties?
- For how long will you hold onto the data?
- How well protected is the data from unauthorised access?

Importantly, the two inventories are inextricably tied together to achieve effective compliance. What makes effective compliance relevant is that the GDPR has provisions for financial penalties of up to 4 per cent of group financial revenue or Euro 20 million per breach.

.

Nixora Group on Data Intelligence

Compliance with the GDPR may seem very complicated and burdensome, but it has given us an opportunity to create ways to better manage data, an opportunity to fully automate the matching and merging of data subject records, use technology to centralise data organisation-wide, and offer a 360-degree views of each data subject in real time.

Nixora's suggestions for Australian Organisation is to implement a structured approach to ensure GDPR compliance. The key features of this solution should allow your organisation to:

- Discover personal data of EU subjects in structured and unstructured environments
- View this privacy data across all business units and systems
- Create an onboarding application to secure the personal data of EU subjects
- Apply a tailored glossary of regulations and privacy policies
- Implement automated procedures to discover personal data for and within business intelligence, enterprise resource planning and big data environments
- View privacy assessments in dashboards and reports
- Provide program management dashboards to track compliance progress
- Provide data governance capabilities to ensure prompt resolution of issues.

We acknowledge that no single technology will fulfil all of the regulation's many requirements. However, the use of a central data repository and other workflow tools will ease the challenges of identifying personal data workflow as required for GDPR compliance.

Central to this will be the role of a robust data lineage application because it needs to be able to track data as it moves through multiple systems, it needs to be able to work with large datasets, and with the capability to tag personal data so that a firm is capable of responding to queries on how the data is being used.

All this is an opportunity to not only be able to respond to regulatory requirements quickly and efficiently, it also allows your organisation to think of how to use data more creatively and look for competitive advantage.

* * *

If you would like to know more about our unique GDPR compliance approach, you can contact Nixora Group for a consultation.

If you would like to know more information about Nixora Group, call us today for a consultation or connect with us on LinkedIn, follow us on Facebook and Twitter or visit our web site nixoragroup.com.au.