information and privacy commission new south wales

Fact Sheet **Updated September 2020**

NSW public sector agencies and the GDPR

The *General Data Protection Regulation* (GDPR) came into effect on 25 May 2018. This fact sheet has been designed to provide general information to assist NSW public sector agencies with understanding the GDPR and in particular the effect for those NSW public sector agencies that offer goods or services to EU citizens.

Scope of the General Data Protection Regulation

Although a European privacy law, the GDPR is designed to have extra-territorial reach. The GDPR applies to any organisation offering goods or services to, or monitoring the behaviour of, individuals in the European Union (EU).

This could include some NSW public sector agencies.

Examples of activities that may be affected are:

- Selling tickets to attractions or events online to EU tourists
- Universities offering educational packages to EU students

Having a website that people can access from the EU will not bring an organisation under the scope of the GDPR, but actions such as offering sales in Euros or websites targeting EU citizens with European languages may indicate an intention to offer goods or services to people in the EU.[1] Agencies are encouraged to review the articles to ascertain their application to them. Less obvious activities which could potentially fall within the scope of the GDPR include online behavioural advertising, profiling or tracking users.

What is required of NSW public sector agencies?

NSW public sector agencies should carefully assess whether the GDPR will apply to their activities. If the GDPR is likely to apply, we encourage agencies to review their practices, and seek legal advice as required.

The IPC encourages affected NSW public sector agencies to take the following steps:

- Ensure collection notices meet the requirements of Articles 13-14 of the GDPR, as well as IPP 3 and HPP 4
- For situations in which the use or disclosure of personal information can only occur on the basis of having the consent of the individual, ensure that that consent is specific and has been freely given on an informed basis, such as by a positive opt-in by the individual, separate to compulsory acceptance of standard Terms and Conditions
- Ensure the agency's Access and Correction procedures can meet the requirements of an EU resident:
    - seeking data portability
    - erasure
    - human review of automated decision-making
    - a temporary restriction of processing
    - opting out of direct marketing, research, or other forms of collection, use or disclosure
- Ensure the agency's Privacy Officer is well-resourced, independent from influence, reports directly to the executive leadership, is not in a position of conflict with other roles, and has been designated the agency's Data Protection Officer for the purposes of the GDPR
- Ensure the agency's privacy management program includes the routine use of PIAs and other techniques to ensure the agency follows a Privacy by Design approach
- The Privacy Management Plan is updated to reflect the agency is also regulated by the GDPR; includes the contact details for the agency's DPO; and nominates the lead supervisory authority with whom the agency will liaise
- Ensure the agency's Data Breach Response Plan incorporates the GDPR definition of data breach[2],

[1] Recitals 23-24 of the GDPR.
[2] Article 4 of the GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

includes a procedure to notify the lead EU supervisory authority within 72 hours, and a procedure to notify the affected individuals without undue delay if required.

NSW public sector agencies should carefully check whether the GDPR could apply to their activities. The GDPR applies in addition to the existing NSW privacy laws affecting public sector agencies: the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*.

What the GDPR covers – definitions

The GDPR regulates 'data controllers' and 'data processors', with respect to how they handle 'personal data'.

NSW privacy law does not distinguish between 'controllers' and 'processors', but in effect a public sector agency would be a 'controller', and if the agency out-sourced some activities such as data collection or data hosting to a third party provider to conduct on its behalf, then that third party would be a 'processor'.[3]

The scope of 'personal data' is similar to 'personal information' under NSW privacy law: "any information relating to an identified or identifiable natural person". People are known as 'data subjects'.

> The GDPR clarifies that *"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

Each of the 28 member states of the EU will have a supervisory authority (i.e. regulator) known as a 'Data Protection Authority', (DPA) with a similar role and functions to a Privacy Commissioner.

The intent of the GDPR is to offer a 'one-stop shop', with organisations being able to deal only with the 'lead supervisory authority' of most relevance to that organisation. This will be determined according to a number of factors, including your agency's place of central administration.[4] If for example your agency has a physical or legal presence in the United Kingdom but not elsewhere in the EU, your lead supervisory authority is likely to be the DPA for the UK, which is the Information Commissioner's Office.[5]

Privacy principles under the GDPR

The GDPR sets out six principles relating to the processing of personal data:

- Lawfulness, fairness and transparency in processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality.

While the language used in the GDPR is different, these core requirements under the GDPR are similar to those found in the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) already regulating NSW public sector agencies.

For example, where the GDPR uses the language of 'processing', the IPPs and HPPs talk about collecting, using and disclosing personal information. Where the GDPR allows for personal data to be processed if "necessary for the purposes of the legitimate interests" of the data controller, subject to "the interests or fundamental rights and freedoms of the data subject", the equivalent test under NSW privacy law is expressed using terms such as allowing use or disclosure for a 'directly related secondary purpose' within the reasonable expectations of the individual.

The GDPR also has requirements relating to ensuring the security and quality (accuracy, integrity) of personal data, which are similar to NSW privacy law.

Tighter rules for processing on the basis of 'consent'

Under the GDPR and NSW privacy law, there are various grounds under which personal information/data can be used or disclosed, one of which is 'with consent'. The GDPR makes clear that if an organisation is relying on 'consent' as the basis for collecting, using or disclosing personal data, that consent must have been informed (using clear and plain language), and freely given, with the individual having a genuine choice "to refuse or withdraw consent without detriment".[6] For example this means 'consent' must be freely given by the individual and cannot be a condition of a contract or part of standard Terms and Conditions, it must be a pro-active 'opt-in' by the individual. It must be as easy to withdraw as to give consent.[7] The GDPR also notes that freely given consent is difficult to obtain for public sector agencies in situations where there is a clear imbalance between the organisation and the individual.[8]

While privacy case law in NSW has interpreted the meaning of 'consent' in similar ways, and guidance from the IPC and other privacy regulators in Australia have

[3] Definitions are in Article 4 of the GDPR.
[4] To identify your agency's lead supervisory authority in the EU, see the guidelines at https://iapp.org/media/pdf/resource_center/WP29-2017-04-lead-authority-guidance.pdf
[5] The United Kingdom has indicated its intention to comply with the GDPR even after the UK exits the EU.
[6] Recital 42 of the GDPR.
[7] Article 7 of the GDPR.
[8] Recital 43 of the GDPR.

reiterated the need for consent to be informed, specific and voluntary, the GDPR has spelled out these requirements in statute.

Privacy rights under the GDPR

The individual 'data subject' has various privacy rights under the GDPR. Some of those rights have equivalents under NSW privacy law, such as rights of Access and Correction.[9] Even the 'right to erasure'[10] (also known as 'the right to be forgotten') is not radically different to NSW privacy law, where the Correction principle includes allowing individuals to seek amendment by way of 'deletion'.

However, there are some additional privacy rights under the GDPR which do not have direct equivalents under NSW privacy law:

- Data portability: the Access right is strengthened with the right to request one's personal data be transmitted to another party in a "structured, commonly used machine-readable format" in certain circumstances[11]
- Automated decision-making: there is a right to not be subject to a decision (with legal effect) based solely on automated processing or profiling; i.e. individuals must be able to seek human review of automated decisions[12]
- Right to object:[13]
    - to direct marketing
    - to research/statistics: the individual can object to their data being processed for research or statistical purposes, unless an overriding public interest is proven
    - to other processing: the individual can object to their data being processed for 'public interest' or 'legitimate interest' purposes, unless an overriding public interest, or the legitimate interest of the controller, is proven
- Right to restrict processing: individuals can require organisations to cease (or at least pause) processing data about them in certain circumstances, such as where the accuracy of the data is under review, or the individual has objected to processing and a final decision has not yet been made[14]

Notices provided to data subjects at the time their personal data is collected must explain the above rights.[15]

Note: The application of the above rights can differ between countries. EU nations can create local laws which 'derogate' from the GDPR (i.e. limit the above rights) in certain circumstances.[16]

Privacy risk management under the GDPR

The GDPR requires organisations to implement a comprehensive program of privacy risk management. The Accountability principle is intended to drive systemic change.

Taking primarily a proactive focus, the requirements include:

- In order to implement the GDPR's data protection principles,[17] organisations must use both technical and organisational measures[18]
- Data protection should be 'by design and by default' – similar to 'Privacy by Design'[19]
- Organisations must know the data they hold, and document their data processing activities[20] – similar to conducting an information inventory or privacy audit, and developing data governance protocols
- Data Protection Impact Assessment – similar to a Privacy Impact Assessment – is required for all high risk projects[21]
- A Data Protection Officer (DPO) (known here as a Privacy Officer) with expertise, resources and independence must be appointed[22]

The reactive component includes data breach notification requirements. Data breaches involving any level of risk to the rights and freedoms of individuals must be notified to the relevant EU supervisory authority without undue delay (but with a default expectation of within 72 hours after having become aware of the breach), and if the risk to individuals is high then also to the data subjects without undue delay.[23]

Further information

The full text of the GDPR is available here.

The UK Information Commissioner's Office is regularly updating its guidance on the GDPR. Click here for more information.

[9] See IPPs 7-8 and HPP 7-8 in NSW privacy law; and Articles 5, 15 and 16 in the GDPR.
[10] Article 17 of the GDPR.
[11] Article 20 of the GDPR.
[12] Article 22 of the GDPR.
[13] Article 21 of the GDPR.
[14] Article 18 of the GDPR.
[15] Articles 13-14 of the GDPR.
[16] Article 23 of the GDPR.
[17] Article 5 of the GDPR.
[18] Article 24 of the GDPR.
[19] Article 25 of the GDPR.
[20] Article 30 of the GDPR.
[21] Article 35 of the GDPR.
[22] Articles 37-39 of the GDPR.
[23] Articles 33-34 of the GDPR.

For the official guidance from the EU DPAs, see the guidelines being progressively released by the Article 29 Working Party (and its successor body the European Data Protection Board), as advisors to the European Commission here.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

Office of the Australian Information Commissioner (OAIC):

Freecall: 1300 363 992
Website: https://www.oaic.gov.au/

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.