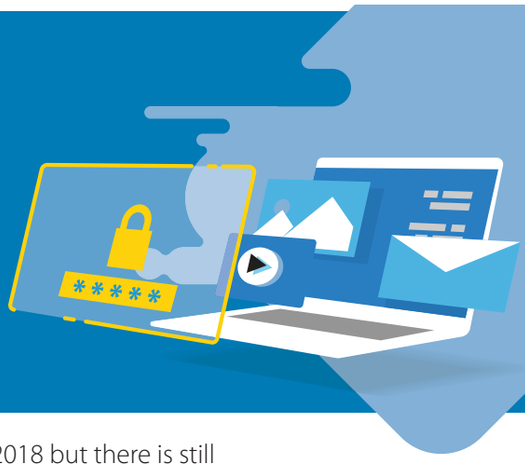
Does the GDPR apply to your organisation?



The EU General Data Protection Regime (GDPR) was introduced on 25 May 2018 but there is still a lot of uncertainty about its application to Australian agencies and organisations. MinterEllison has developed the following tool to help you make an initial assessment. Page 1 will help you to determine whether the GDPR applies to your organisation while Page 2 provides a GDPR compliance requirements checklist for you to consider if it does.

ESTABLISHMENT (ARTICLE 3.1)

Are you processing the personal data of people in the EU in the context of an:

- ☐ EU branch
- ☐ EU subsidiary
- ☐ Do you have a presence in the EU

If 'yes' to any of the above, this is likely to indicate your organisation is covered by Article 3.1

OFFERING GOODS OR SERVICES (ARTICLE 3.2(a))

Does your organisation offer goods or services to people who are located in the EU or target them through:

- ☐ A representative it has in the EU offering goods or services to people

A website that expressly offers goods or services to people in the EU or which has the following features:

- ☐ non-English language of an EU country
- ☐ EU currencies as well as AUD$
- ☐ Website top level domain name of an EU country
- ☐ Physical delivery of goods or services to an EU country
- ☐ Reference to EU people to promote the goods or services
- ☐ Large proportion of customers based in the EU
- ☐ Targeted advertising at individuals in an EU country

The more you answer 'yes' to any of the above, the more likely it is that Article 3.2(a) applies to your organisation.

MONITORING (ARTICLE 3.2(b))

Is your organisation undertaking profiling, for example, through website use by individuals through cookies or other tracking tools:

- ☐ using automated means of processing
- ☐ using personal data of users in the EU
- ☐ for the purpose of evaluating or predicting personal aspects or traits about a natural person

If 'yes' to all of the above, this is likely to indicate that Article 3.2(b) applies to your organisation.

CONTACT US

Veronica Scott National Privacy Leader **T** +61 3 8608 2126 **E** veronica.scott@minterellison.com

MinterEllison

GDPR compliance requirements checklist

- [ ] Identify one or more lawful basis for processing EU personal data (Article 6)
- [ ] Obtain explicit consent to process sensitive categories of personal data unless an exception applies (Article 9)
- [ ] Update and communicate collection notices/privacy policies for EU data subjects (Article 13 and 14)

ESTABLISH PROCESSES TO FACILITATE EU DATA SUBJECTS EXERCISING THEIR RIGHTS WITHIN APPLICABLE TIME LIMITS:

- [ ] right to access personal data (Article 15)
- [ ] right to request correction of personal data (Article 16)
- [ ] right to be forgotten (Article 17)
- [ ] right to restrict processing (Article 18)
- [ ] right to data portability (Article 20)
- [ ] right to object to processing (including automated) and for direct marketing (Article 21)

OBLIGATIONS ON DATA CONTROLLERS AND DATA PROCESSORS:

- [ ] designate a data protection officer, if required, and allocate resources and tasks (Articles 37, 38 and 39)
- [ ] appoint a local EU representative if established outside of the EU (Article 27)
- [ ] maintain records of processing activities (Article 30)
- [ ] cooperate with supervisory authorities (Article 31)
- [ ] enhanced risk based data security obligations, including the pseudonymisation and encryption of personal data, establishing a business continuity plan and regular testing, directions to personnel (Article 32)
- [ ] establish a lawful basis for transferring personal data to a third party outside of the EU (ie onwards from Australia) (Articles 44 – 50)

SPECIFIC OBLIGATIONS ON DATA CONTROLLERS:

- [ ] implement data protection by design and default into data processing activities (Article 25)
- [ ] prior to engaging a data processor, satisfy itself that the processor will implement appropriate technical and organisation measures to meet the requirements of the GDPR and enter into an agreement with the processor that includes specified terms (Article 28)
- [ ] report personal data breaches (data security breaches) to:

  - the relevant EU supervisory authority(ies), within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals (Article 33); and

  - data subjects, without undue delay, if it is likely to result in a high risk to the rights and freedoms of those individuals (Article 34)

- [ ] undertake a data protection impact assessment where the processing (in particular new technologies) is likely to result in a high risk to the rights and freedoms of individuals, and consult with EU Supervisory Authority if required (Articles 35 and 36)