GDPR CHEATSHEET
WHAT YOUR BUSINESS NEEDS TO KNOW ABOUT THE EU’S NEW PRIVACY LAWS

The European Union General Data Protection Regulation (also known as the GDPR) is a new piece of European Union (EU) legislation that comes into effect on 25 May 2018. The main aim of the GDPR is to protect the personal data of individuals based in the EU.

Despite the GDPR being a European regulation, Australian businesses, and in particular, online businesses, may need to comply with it. It is important to note that the size of your business is not a relevant factor in determining whether you need to comply.

Penalties for breaching the GDPR can attract substantial fines – up to 4% of the offending business’ annual global turnover or €20 million (whichever is greater).

1. DOES THE GDPR APPLY TO MY AUSTRALIAN BUSINESS?

The GDPR applies to your business if you collect data and you are:
• established in the EU;
• offering goods or services to EU-based individuals (free or paid); or
• monitoring EU residents’ behaviour.

If you do not have an office or branch in the EU and you do not monitor individuals based in the EU, then working out whether you offer goods or services to EU-based individuals is the most relevant question for you to address.

As most websites are accessible to a global audience, the GDPR is clear that the mere fact that EU-based individuals can access a website does not, in itself, mean that the business is caught by the GDPR. The crucial factor is whether a business envisages to offer goods or services to EU-based individuals.

Factors that indicate this intention to offer goods or services to EU-based individuals can be:
• using a European language on your website;
• using a European currency on your website; or
• mentioning customers or users who are in the EU.

If you tailor your website or your marketing to help you attract and sell to individuals based in the EU, then your business must comply with the GDPR.

2. HOW DOES MY BUSINESS BECOME COMPLIANT?

Becoming GDPR compliant may require you to tweak your IT systems, internal processes and legal documents. Your business may need to engage an IT lawyer to review your documents and processes, but below is a simplified guide of the first steps to becoming GDPR compliant:

1. Make sure that your privacy policy is compliant with the GDPR

Having a privacy policy that is compliant with the Australian Privacy Principles (APPs) is a good start but as the GDPR gives users broader rights (e.g. the APPs do not give individuals the right to ask for their data to be erased) your current privacy policy may need to be updated to cover additional concepts introduced by the GDPR.

Updates should state that:
• individuals over 16 years old can consent to the processing of personal data, but anyone younger needs the consent of their parent or guardian;
• individuals have the following rights and explanations of each: the right to be forgotten, the right of access by an individual, the right to erasure, the right to restriction of processing and the right to data portability; and
• your business processes personal data in accordance with the principles of data processing set out in the GDPR.
2. Update your processes and systems on your website

Ensure that the privacy notices on your website are visible to your users every time that you collect personal data from them.

Under the GDPR, you need explicit and unambiguous consent from a user when you process their data. It is therefore suggested that when you collect personal data, you also include a consent statement next to a "tick to accept" box to record a user's consent to the collection of personal data. The requested consent must be written using clear and plain language.

3. Store personal information in a readily available format

The GDPR introduces new rights for individuals, such as:

- the erasure of personal data
- data portability, and
- the opportunity to object to the processing of your personal data.

You should therefore make sure that, not only are you able to easily erase personal data, but also that you automatically store personal information in a format that is easy for you to extract and provide to your customers upon request. Set up automatic notifications where customers can let you know if they wish to withdraw their consent.

4. Have processes in place for data breach notifications

The GDPR provides a definite time frame for notifying authorities of a data breach. In case a data breach is likely to be a high risk to the rights and freedoms of individuals, your business must notify the affected individual, as well as the relevant supervisory authority in the country of the affected EU resident, within 72 hours of becoming aware of the breach.

Therefore, ensure you have industry-standard, or better, security measures in place to prevent data breaches. Also make sure to prepare a data breach plan, so your business is ready if a breach occurs and you can mitigate its effect.

---

 далеко

**GDPR Checklist**

If your business is required to comply with the GDPR, you must:

- have a privacy policy in place that is compliant with the GDPR
- ensure privacy notices are easily accessible when you collect data from website users
- update your procedures to handle requests from individuals to modify, delete or access their data
- implement security notification procedures to meet reporting obligations
- train relevant staff to ensure they handle data in a compliant manner
- review and audit the data you hold on a regular basis

**How Can LegalVision Help?**

LegalVision is a market disruptor in the commercial legal services industry. Our innovative business model and custom-built technology assist our lawyers to provide a faster, better quality and more cost-effective client experience. The firm was named 2018 Fastest Growing Law Firm in APAC by the Financial Times.

Our experienced IT lawyers can assist you with ensuring your business is compliant with the GDPR. We offer a GDPR compliance package which includes:

- an initial consultation to discuss your business and your privacy risk points;
- a tailored memorandum which includes guidance as to what steps you need to take to become GDPR compliant;
- a privacy policy that it is GDPR compliant; and
- a Data Processing Addendum if required for your business.

If you have any questions about the GDPR, get in touch with our lawyers today by calling us on 1300 544 755.