iab australia

IAB BRIEFING: GDPR COMPLIANCE IN THE AU MARKET

JUNE 2018

Subscribe to our Monthly Newsletter
for regular IAB Resource updates

simplify inspire

KEY POINTS

1. The General Data Protection Regulation (GDPR) is in effect (it commenced on 25 May 2018).
2. It will affect companies located in the European Union but also those that have operations and customers there too.
3. The key principle of GDPR is giving consumers control of their data.
4. There are fines of up to 4 percent of total global turnover if rules in the GDPR are breached.

WHAT IS THE GDPR?

GDPR is a piece of legislation that was approved in April 2016. European authorities have given companies two years to comply and it will come into force this month - on May 25, 2018.

The aim is to give consumers control of their personal data as it is collected by companies. Not only will the GDPR affect organisations located within the EU, but it will also apply to companies outside of the region if they offer goods or services to, or monitor the behaviour of, people in the EU bloc. This is why the GDPR could have a far-reaching impact.

A major focus of GDPR is on conditions of consent received from consumers which have been strengthened. So companies will not be able to use vague, confusing statements when communicating to consumers about what personal data a consumer consents to the company collecting online. Businesses also won't be able to bundle consent for different things together. Under the GDPR, businesses will need "affirmative action" and proactive consent from any consumers who interact with their digital company sites.

How and why is the European GDPR relevant to Australia digital media & publishing companies?

Europe might be on the other side of the world, but in an online world it's only a click away – and so are its data protection laws.

Australian organisations' operations in Australia could fall under the GDPR where they either:

- Supply goods or services to, or monitor, individuals in the EU through digital presence
- Process personal data in connection with the activities of an EU establishment including potentially where this is done via a data centre of a service provider located in the EU.

HOW CAN DIGITAL PUBLISHING COMPANIES KNOW THEY ARE GDPR COMPLIANT?

The answer to this lies in ensuring you, at a minimum, meet the areas of the GDPR which mirror Australian Privacy law. Both legal systems foster transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected.

Both laws require businesses to comply with a set of privacy principles, and both take a privacy by design approach to compliance.

In addition, privacy impact assessments, compulsory in certain circumstances under the GDPR, are expected in similar circumstances in Australia.

Given these similarities, Australian businesses may already have some of the measures in place that will be required under the GDPR. However, IAB Australia recommends the businesses take the following immediate steps in assessing GDPR compliance:

- Map your data practices - begin taking steps to evaluate your information handling practices and governance structures, to understand what changes you need to enact before commencement of the GDPR.
- Immediately revisit your consent requirements. Under the GDPR, consent requirements are stricter than under the Australian Privacy Act and many other national laws. If you rely on consent to process personal data, you will need to ensure already obtained consents will still be valid. You may have to collect new, replacement consents. You must ensure consent is documented. We have extensive guidance & resources on our site about how to respond to the GDPR including a podcast with expert legal advice from Marque Lawyers, on how to handle the GDPR as an Australian business.
- Be aware that strengthened global standards relating to privacy and consent may be in operation via your global partners (e.g. ad servers) Europe might be on the other side of the world, but in an online world it's only a click away – and so are its data protection laws. For this very reason, many participants in your technology stack might be applying a new global standard via the GDPR to all its operations. Speak to any companies you partner with to handle your Demand-Side-Platforms, Supply-Side-Platforms, Ad Servers, Data Management Platforms and other requirements and ask them what changes they will be making to their business operations and how this will impact on your company.

WHERE IS THE GDPR DIFFERENT AND WHERE IS IT THE SAME AS AUSTRALIAN PRIVACY AND DATA LAW?

Familiar Data Protection Concepts for Digital Media Companies in Australia	New Data Protection Concepts for Digital Media Companies in Australia
Concept of personal data is similar to Australia's current legal definition of 'personal data". (In Australia however, the determination of "personal data" is currently under review with report expected Dec 2017)	GDPR contains a right to be forgotten. It means a consumer can demand that your company deletes their data. There is no similar fundamental right under Australian law.
Importance of consent when dealing with personal data remains a core part of both GDPR and Australian Privacy law. Australian Digital Media and Advertising Companies should ensure their methods of obtaining consent from a consumer is in line with Australian Privacy law.	GDPR requires a data controller (Publishers, Advertisers, anyone collecting data directly from a consumer) to provide a consumer's data in a machine-readable format. The point is to make the data "mobile" so the consumer can move it around between data controllers. Australian privacy data law does not demand that Australian digital media and advertising companies provide consumer data in a machine-readable format.
Data breach requirements are mandatory under both the GDPR and Australian law. Authorities must be notified of any breach. Shorter time frames exist in the GDPR - 72 hour limit on notification. Australian data breach require an authority to be notified in 30 days.	Data controllers can only appoint data processors must demonstrate guarantees to implement technical measures to ensure processing meets new GDPR requirements. Australian law does not currently stipulate legal differences between processors or controllers of data for digital media and advertising companies.
Both GDPR and Australian Privacy Law require you to demonstrate compliance with privacy principles. As part of compliance with privacy principles, good governance practices around privacy are included in both data protection law frameworks.	No annual turnover requirement - Digital media and advertising companies with an annual turnover of $3 million or less must comply with Australian Privacy laws. Under new GDPR laws, if you handle EU consumer data, regardless of your annual turnover size, must comply with GDPR.
GDPR and Australian Privacy Principles emphasise transparency and 'privacy by design' approach. This is an area of commonality between both data protection frameworks in EU and the Australian framework.	Digital Media Companies which breach Australian Privacy law can be stung with a fine up to $1.7 million. The penalties under GDPR are much bigger. Your exposure for a breach of the GDPR is €20 million or 4% of your annual worldwide turnover (whichever is higher).

HOW CAN COMPLIANCE BE ACHIEVED AND MAINTAINED WITH COMPLICATED TECHNOLOGY STACKS?

You should conduct a privacy compliance review if you have a complicated technology stack. This allows an Australian business to review existing processes of data value identification and capture, and of protection of the confidentiality of data as handled within multi-party data systems.

Also, as mentioned above, immediately speak to any companies you partner with - Demand-Side-Platforms, Supply-Side-Platforms, Ad Servers, Data Management Platforms etc. - and ask them what changes they will be making in their data processing and how it will impact on business with your company.

FOR BRANDS AND AGENCIES, WHERE DOES THE COMPLIANCE RESPONSIBILITY FALL?

Both Publishers and brands (classed as 'data controllers' under the GDPR) and Agencies ('data processors' under the GDPR) shoulder responsibility for GDPR-compliance and both need to implement adequate technical and organisational measures to ensure data is processed securely and is adequately protected under the GDPR.

For example, a key requirement of the GDPR is that a controller must only use processors that provide sufficient guarantees that they will implement appropriate technical and organisational measures that ensure compliance with the GDPR and protect the rights of the data subject. In the context of digital advertising, a brand seeking to be GDPR-compliant, will now be required by law to partner only with an agency that has provided formal guarantees around data protection and handling processes associated with brand's data.

HOW IS THE GDPR ENFORCED? WHO IN AUSTRALIA COULD/WOULD ACT AS A COMPLIANCE WATCHDOG, WITH ANY AUTHORITY?

One of the most talked about aspects of GDPR is GDPR compliance and non-compliance fines. They can be high 4% of a business' global revenue, or €20M whichever is higher. Supervisory Authorities (SAs) in EU countries will come knocking to enforce the GDPR and they have a number of investigative and corrective powers to bring to bear. In Australia, EU regulators will need to rely on international law to issue fines and it is unclear exactly how they will do this. Written into GDPR itself is a clause stating that any action against a company from outside the EU must be issued in accordance with international law.

Given that the Office of the Australian Information & Privacy Commissioner (OAIC) prepared a business resource for Australian companies on how to prepare for the GDPR, (you can access it here) it is possible that there will be enforcement cooperation between US and AU data protection authorities. (It is very rare for the AU commissioner to provide guidance on overseas laws.)

For further information on the GDPR, data and privacy please contact IAB Australia Director of Regulatory Affairs Kamani Krishnan on kamani@iabaustralia.com.au.

MORE RESOURCES FROM IAB AUSTRALIA

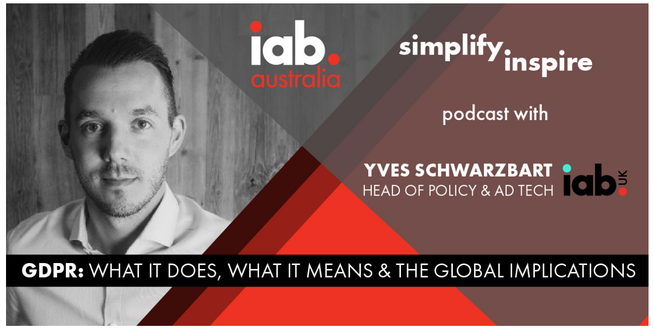
Latest Research & Resources

What do the new laws mean for Australian Digital Companies?

The GDPR means that Australian companies will have to comply with higher privacy standards, even if they have their operations are here in Australia.

Latest Podcast

GDPR: What it Does, What it Means & the Global Implications



Yves Schwarzbart, Head of Policy & Ad Tech at IAB U.K., has lived and breathed the GDPR for the past few years, and he uses his expert knowledge to break down the 200-plus page legislation.

More Podcasts

Mandatory Data Breach Notifications: Cloud-based & 3rd party data breaches

Mandatory Data Breach Notifications are now law. Third parties can often hold details like a mailing lists, credit card data and other personal information. But who owns that data & who is responsible when a network is compromised and who tells the customers?

Stay up-to-date with IAB Australia and the work we do to simplify and inspire the digital advertising industry by following us on LinkedIn, Twitter and Facebook, and subscribing to our monthly newsletter.