13/4/18

alphadigital.com.au

The GDPR and Australian Retailers

On May 25 2018, the new privacy regulations the General Data Protection Regulations (GDPR) will come into force in the European Union. Whilst it's immediately obvious that this will have a massive impact within the EU, Australian businesses are also being put on high alert.

The GDPR aims to give control of personal data back to the individual (the Data Subject). It does this by enacting strict regulations around the collection, retention, and use of the data on the part of the companies collecting the data, and on the companies processing the data.

But why should Australian businesses care about new privacy regulations in the EU? Well these regulations are *very* broad in scope, and aim to apply to businesses based not only within the EU, but across the rest of the world too. It does this by referring to businesses that are either established within the EU, or businesses who offer goods and services or monitor the behaviour of people within the EU.

Basically, if you sell goods or services to customers within the EU - the EU wants you to comply. If you don't, the fines are huge.

This article aims to explain the GDPR as it applies to retailers within Australia, with a slant towards the types of clients we work with. We'll aim to help you determine if the GDPR applies to you, give a range of examples (or use cases), explain how the GDPR could be enforced against someone in breach, and some tips on how to get your business compliant. If you're more of a visual learner, we created an infographic too (coming soon).

Before we get into it, a note. **We are not lawyers. We are a digital marketing agency, enthusiastic about learning and teaching. If you think you may (or may not) be caught by these regulations, speak to a lawyer. This article is merely our opinion based on our readings and is not legal advice.**

Brisbane
20 Agnes Street,
Fortitude Valley, QLD, 4006
(07) 3040 9988

Sydney
Suite 1.06, Level 1,
100 Collins Street, Alexandria, NSW, 2015
(02) 8790 7085

Definitions

Article 3 of the GDPR is key to understand, at it largely drives the rest of the regulations (at least as they apply here).

The key elements (bolded for emphasis and defined below) of Article 3(1) are:

1. The dealing with **personal data**; by a
2. **Controller** or **processor**; who is
3. **Established** in the EU.

Alternately, the key elements (bolded for emphasis and defined below) of Article 3(2) are:

1. Dealing of **personal data**; by a
2. **Controller** or **processor** who is
3. Outside of the EU; where they
4. **Offer goods or services** to people in the EU; or they
5. **Monitor behaviour** of people in the EU.

In essence, where a company is not established in the EU, Article 3(1) does not apply, and you must look to Article 3(2). If you're dealing with personal data of people within the EU, and you're actively selling to and/or monitoring people in the UK, the GDPR may apply to you.

As with anything related to laws, definitions are important. Below are our interpretations of some of the commonly used terms that come up when talking about the GDPR:

- Controller
    - A controller is a business that controls personal data. If you have collected and now possess personal data, and you determine how that data is now dealt with (including giving it to a 3rd party), you are likely considered a controller under the regulations
    - Example controllers: You, CRM systems, Facebook/Google (where they are collecting data directly from profiles, website usage etc)
- Consent
    - Consent under the GDPR has several key elements:
        - Freely given
            - Consent will not be freely given where the subject is unable to refuse or rescind consent easily and without detriment, where the data subject to consent is not necessary to complete the contract, where there is a clear imbalance of power, or where the processing is multi-part and consent cannot be given to each part individually.

        - Specific
            - Must distinctly cover all processing activities - consent to each and every activity must be gained.
        - Informed
            - The subject must be aware of the identity of the business and they must know of their rights to withdraw consent.
        - Unambiguous
            - The consent must be clear and unambiguous that the subject has given their agreement with the intention of actually agreeing to the proposed processing activities. This is really clear where the subject is simply signing up to an email newsletter.
        - Statement or clear affirmative action
            - Silence, a pre-ticked box, or inaction does not equal consent.
    - Other important elements relate to the language used (no legalese!), the ease of removal of consent (must be as easy as giving consent), and that there is a verifiable record of consent.
- Processor
    - A 3rd party company that you might give your data to, who will use or manipulate your data in some way
    - Example processors: Mailchimp, Google Data Studio, Facebook/Google/Programmatic (where you feed customer data into their system in order to help with targeting and segmentation)
- Processing
    - 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- Establishment in the EU
    - Where you have any real and effective activity, no matter if it is minimal or substantial, through a stable arrangement in the EU, you are likely to be 'established' under the regulations.
    - For example, if you have a permanent representative (a single person), that may actually be sufficient. Having a standalone office would almost certainly be sufficient, even if it is minimal in comparison to the rest of your operation.
- Offering of Goods and Services

- Thankfully for Australian businesses, having a website that is merely accessible from within the EU is not likely to be sufficient to fall under this provision. However, If your website is clearly set up with the intent of selling into the EU (for example, you may offer a French version of your website, or include shipping information into an EU member state), you will likely be caught under the provision. Likewise if you are advertising within the EU on AdWords (for example) you clearly intend on offering goods or services within the EU.

Please note that these definitions are a combination of summaries directly from the GDPR itself, and our interpretations of how they would play out in the wild. This is especially true for Establishment and Offering of Goods and Services.

Client Examples

Below we outline scenarios our clients are most likely to find themselves in.

Retailer A

Scenario
Retailer A is a small business. They're not targeting the EU, but they get the occasional sale in the EU. They know that's the case, but they don't really keep track of their customers in any meaningful way.

Outcome
We don't believe Retailer A would be caught by the GDPR. They're not actively targeting people in the EU, even though they've sold a small amount of product into the EU. They're also not controlling any personal information for anyone in the EU, which is an essential element under Article 3(2) (that they be a controller or processor).

Retailer B

Scenario
Similar to Retailer A, Retailer B sells a small amount of stock into the EU. The difference is that Retailer B is a bit more advanced in their marketing. They collect and store customer information and email subscriptions in a CRM, and they use a 3rd party tool (like Mailchimp) to segment and market towards these segments.

Outcome
Because they're collecting and storing personal data for people within the EU, they are likely to be considered a controller under the regulations. They're also deciding how this information should be dealt with and use a 3rd party tool to process the data.

It's unclear at this stage exactly how much a business needs to be selling into the EU, but our best guess is that if they are selling goods into the EU *and* actively marketing to people within the EU (through Retailer B's email marketing), they are showing a clear intention to sell goods to people within the EU. Because of this, it seems likely they would be caught by 2(a).

In addition, because Retailer B uses a CRM to collect and monitor their customers within the EU, it may be that they are caught regardless by 2(b). In either instance, they will need to ensure that all past and future personal data collected has come with the proper consent.

Since Retailer B is selling goods and services into the EU (and actively marketing to people within the EU through their email marketing), and they are likely considered a controller under the regulations, it seems likely that they are required to comply with the GDPR or risk facing a fine.

Retailer C

Scenario
Retailer C explicitly outlines on their website that they do not sell goods outside of Australia. However, due to the popularity of their product, they have had people from the EU sign up to email lists through their website. These email addresses are fed into Facebook to create a lookalike audience and are not properly filtered to remove the emails of people within the EU, though they are only geotargeting within Australia.

Outcome
Retailer C is likely to be a controller under the regulations as they are collecting personal information from people. They are also then passing that data on to Facebook as a processor.

However, they are explicitly not selling products into the EU, so 2(a) will not apply. Retailer C may be caught by 2(b) though, as they are monitoring the behaviour of people within the EU. It therefore seems possible that they are required to comply with the GDPR or risk facing a fine. If they do need to comply, they will need to ensure they have complied with consent provisions.

Retailer D

Scenario
Retailer D used to sell into the EU, however after hearing about the GDPR last year they made the commercial decision to cease trading within the EU.

Due to their previous operations within the EU, Retailer D has collected a large amount of personal data from people within the EU, including email addresses, postal addresses, gender, and purchase history. All of this information has been collected after customers agreed to receive marketing material' during the purchase process. Clicking on the 'What do we use your data for?' link next to the pre-selected check-box took the user to a page with tens of thousands of words of Ts&Cs, written by their lawyer in typical 'legalese'. Without a JD, it's difficult to understand exactly what you're agreeing to.

Despite no longer selling to the EU, Retailer D has decided that they would like to keep their existing customer data as they believe it will be helpful to their future marketing efforts. They don't intend on marketing directly to these people, selling to them, or selling within the UK.

Outcome
Retailer D is clearly a controller under these regulations, as they are controlling how the personal data of people within the EU is being dealt with. Despite the fact that they are no longer selling to the EU, it could be argued that by retaining this data they are monitoring people within the EU. The retrospective 'consent' provision therefore becomes an issue.

Under the GDPR, Consent must be a clear and affirmative action (so the pre-checked box may be an issue), plus any Ts&Cs must be easy to understand (which these were not). Retailer D will now need to decide whether the benefit gained by retaining this historical personal information is greater than the cost they will need to incur in order to get the appropriate consent all data subjects within the EU.

Retailer E

Scenario
Retailer E is a mid-sized retailer based in Australia but selling their goods globally. They're especially popular in France, where about 20% of all sales originate. Retailer E is fairly savvy and runs email marketing campaigns, programmatic, search, and social media campaigns, and has on-site personalisation based on users past behaviour. This retail takes privacy seriously and so has ensured they comply to the letter with all Australian privacy legislation.

Outcome
Retailer E is almost certainly required to comply with the GDPR. They're actively selling a significant amount of product into the EU, and are monitoring data subjects within the EU. An example like Retailer B is quite clear cut - they should aim to comply with the GDPR in its entirety. Much like Retailer D, there is now the commercial decision to make around whether or not the risk of non-compliance whilst not being based in the EU outweighs the cost of implementing GDPR-compliant systems and processes.

Enforceability

It's one thing for the EU to implement the GDPR within its jurisdiction, but it's another entirely to enforce the laws outside of it.

For established businesses within the EU, it's clear that the EU (or the member states) could enforce the penalties in the case of non-compliance. As mentioned, these penalties are serious - up to 20 million Euro or 4% of global turnover.

What's less clear is how this will be done for companies based outside of the EU with no physical presence within the jurisdiction. Currently, there does not seem to be an obvious way for the EU to enforce these rules (read: fine) against companies that are not established within the EU. It may be that countries sign treaties with the EU agreeing to enforce the rules, but at the moment nothing of the sort appears to exist in Australia.

So theoretically then, a small business established only in Australia could breach the GDPR, the EU could make an adverse finding against them and fine them, but at the moment there may not be any way for that fine to be enforced (beyond maybe holding shipments at customs within the EU).

Keep in mind, this could all change with the stroke of a pen, and there's also no precedent here. The only way we'll know for sure what will happen in a case like this is when we see it actually happen.

It's also worth noting that it's very possible (if not likely) that, following the successful roll out of the GDPR, privacy regulations in Australian are strengthened to match. Therefore being proactive and meeting the more laborious GDPR regulations now (or taking steps to work towards meeting them) may be a prudent decision.

13/4/18

alphadigital.com.au

The Small Business 'Exemption'

A lot is being made of Article 30 in the GDPR, around an exemption for businesses with 250 or fewer staff.

This article would only seem to apply to the records of processing activities or types of processing activities - not the actual activities themselves. Regardless, elements like **consent,** and all of the **individual rights** under the GDPR would still seem to apply regardless.

In addition, this exemption only applies in a limited number of circumstances. So limited in fact, that the exemption probably wouldn't apply to most business, and especially not to most retailers, dealing with customer data.

Brisbane
20 Agnes Street,
Fortitude Valley, QLD, 4006
(07) 3040 9988

Sydney
Suite 1.06, Level 1,
100 Collins Street, Alexandria, NSW, 2015
(02) 8790 7085

What do I need to do to get ready?

Okay, so you've weighed up the benefits of selling into the EU or monitoring behaviour within the EU against the cost of complying with the GDPR, and you've decided to get compliant. If you're feeling overwhelmed or unsure of exactly what you need to do, you're not alone. The majority of businesses even within the EU are simply not ready.

The first thing we recommend doing is consulting an expert, or a team of experts. Until then, below are 12 steps from the ICO that businesses should do to prepare from the GDPR.

12 steps from ICO:

1. Awareness
    a. Everyone in your org needs to appreciate how serious this is and how important it is that all new policies and procedures are followed. Board members may be liable if they are found to be negligent.
2. Information you hold
    a. You will have to do a full audit of data held, who it is shared with and how, the provenance, the consent gained, accuracy, etc. You're required to have a record of all of this information, so take note of any missing pieces of data and why that has occured, because it will need to be remedied.
3. Communicating privacy info
    a. Review and update privacy notices. These are usually (or should be!) easily accessible for your website. Among other things, you will need to ensure this clearly communicates who you are and how the data collected will be dealt with.
4. Individual rights
    a. Check you have process and ability to cover all individual rights (delete, provide data etc) and that it is in a commonly used format (an Excel file for example). If someone requests that you send them all of the data you have on them, or request errors be rectified, you will need to fulfil the request in a timely manner, **and for free.**
5. Subject access requests
    a. Ensure process and procedures make it possible to provide data to subjects within time frames (one month).
6. Lawful basis for processing personal data
    a. Determine how you can lawful deal with the data and update policy and privacy notice. You should be ensuring you are not collecting more data than you have specifically outlined will be collected to the data subject.
7. Consent
    a. Review exactly what your consent process looks like at the moment, and update to rectify any deficiencies. Where your business relies upon

consent to process personal data, you will need to ensure that all currently held data has been provided with the same consent that would be required under the GDPR. If it hasn't been, you will need to re-seek consent with new regulations in mind.

8. Children
    a. Put in place systems if you need to seek information from children and therefore obtain parent or guardian consent. The GDPR sets the age of consent at 16 years. Below which you will need to obtain verifiable consent from a person holding 'parental responsibility'.
9. Data breaches
    a. Write procedure to detect report, investigate breach (and inform subjects)
    b. In some cases, where there is a breach, organisations will be required to report that breach to a governing body. In the case where the breach is likely to result in discrimination, reputational damage, financial lose, loss of confidentiality etc it must be reported. Where the breach is likely to result in a high risk to the rights and freedoms of an individual, the individuals themselves will have to be notified of the breach.
10. Data protection by design and data protection impact assessments
    a. Privacy and data protection can not be a bolt-on or afterthought. Systems must be designed with a data protection-first approach. This has always been best practice, but the GDPR makes this legally enforceable, especially if the data processing activities are high risk or there is a significant change to the processing system or infrastructure. Employ someone to help you.
11. Data protection officers
    a. Do you need a DPO? Most AU based clients without an establishment probably won't
12. International
    a. Additional obligations apply if you are a business established in multiple EU Member States.

Conclusion

The intention of the GDPR is to protect individuals and their privacy - an admirable goal. Australian companies who do a significant amount of business within the EU would do well to get their policies and procedures up to scratch, stat (especially where they are also established within the EU). With fines of up to 20m Euro or 4% of global turnover, a serious breach could cause the offending business to topple over.

This does raise the question of whether for a smaller retailer operating within Australia and doing the occasional sale into the EU, total compliance with the GDPR is a reasonable goal. Obviously, if it's achievable it should be done, and total compliance should be the goal. However with the likely cost of compliance and the massive question marks around enforceability within Australia, these businesses will need to make a commercial decision weighing up the risks and costs associated with total or partial compliance with the new GDPR. We recommend consulting with an expert in the area to determine your path forward.

Resources Used

https://gdpr.report/news/2018/01/30/gdpr-numbers-dont-lie-world-isnt-ready/
https://www.eugdpr.org/
https://www.oaic.gov.au/media-and-speeches/news/general-data-protection-regulation-guidance-for-australian-businesses
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
http://www.thedrum.com/opinion/2018/03/05/gdpr-guide-marketers-australia
https://united-kingdom.taylorwessing.com/globaldatahub/article-understanding-consent-under-the-gdpr.html
https://gdpr-info.eu/art-7-gdpr/
http://www.mondaq.com/australia/x/667056/data+protection/GDPR+Change+to+European+privacy+laws+and+its+impact+on+Australian+businesses
https://www.sibenco.com/gdpr-change-to-european-privacy-laws-and-its-impact-on-australian-businesses/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
https://www.cmo.com.au/article/630807/predictions-2018-what-tighter-european-gdpr-will-mean-marketers/
https://www.quantcast.com/blog/gdpr-qa-consumer-consent-and-your-website/
https://www.cmo.com.au/article/630807/predictions-2018-what-tighter-european-gdpr-will-mean-marketers/
https://www.marketingmag.com.au/hubs-c/gdpr-everything-australian-marketers-need-know/
https://www.cmo.com.au/article/632466/cmo-interview-why-gdpr-blueprint-marketers-need-customer-led/
https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/11--guide-to-the-gdpr--material-and-territorial-scope.pdf?la=en
https://community.spiceworks.com/topic/2007530-how-the-eu-can-fine-us-companies-for-violating-gdpr
https://www.adma.com.au/compliance/how-to-prepare-your-non-eu-business-for-the-gdpr
http://www.itpro.co.uk/data-protection/29123/gdpr-for-small-businesses-what-it-means-for-you
https://www.simplybusiness.co.uk/knowledge/articles/2017/11/what-is-gdpr-for-small-business/
FREEMAN, Iain; Ilich, Jessica: (2017). "Additional privacy requirements for Australian organisations under EU privacy laws.". Privacy law bulletin(1449-8227), 14 (8), p. 149.