How marketers can get ready for GDPR

Jo Blazey

Source: WARC Best Practice, October 2017

This article looks at how marketers can prepare for the introduction of the General Data Protection Regulation (GDPR), a European piece of legislation that will come into effect in 2018.

- GDPR only applies to the use of personal data - it is therefore essential to understand what personal data actually is, and what personal data your business is capturing or using.
- GDPR also introduces the principle of accountability, which requires a business to be able to demonstrate it is complying with GDPR.
- If brands don't need consent, they should ensure they don't use language that suggests they are asking for it (e.g."I agree to the Privacy Policy").
- Brands need to be aware of the impact of the forthcoming E-Privacy Regulation and if they are unsure, they should seek legal advice.

Companies and organisations based in the EU, and those with customers in the EU, will need to comply with the General Data Protection Regulation (GDPR) that comes into effect on 25 May 2018. Essentially, GDPR provides greater protection for individuals in relation to how their personal information is collected, stored, shared and utilised by businesses. The potential fines for not complying with GDPR are eye-catching (up to 4 % of global turnover) and add focus to the question of how to be GDPR-compliant.

Definitions

GDPR stands for General Data Protection Regulation, a European piece of legislation that will come into effect on 25 May 2018.

Under GDPR Personal Data is defined as: "Any information relating to an identified or identifiable natural person; an identifiable 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, online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." (**Article 4, EU GDPR "Definitions"**)

Where to start

GDPR replaces the **1995 European Data Protection Directive**. While GDPR imposes new and increased compliance obligations concerning data protection, the level of the step up required of a business to meet these obligations will depend on how well it is complying with existing law.

One of the objectives of GDPR is to minimise inconsistencies in national data protection laws across the EU states. It also attempts to address the new data privacy issues that have arisen due to the rapid advances in digital technology such as those relating to social media, mobile apps, big data and the Internet of Things. GDPR also gives data protection authorities much more firepower for fining businesses that do not comply – a company can be fined up to 4% of global turnover for some data breaches.

Getting ready for GDPR involves good personal data governance across the entire business. To achieve this, it is important for a business to have a clear understanding of what personal data actually is, what personal data it has, where it is stored and why and how it is using it.

In today's marketing environment, brands utilise individuals' personal data to target customers, and prospects, as a way to market to them, and personalise their offers to them. As such, **marketing is a crucial area of business** that needs to pay particular attention to GDPR.

However, GDPR is much more than a compliance exercise. Individuals are now more aware of the value of their personal data, and **consumers are concerned** about the increase in data breaches, thus meeting GDPR requirements gives marketers an opportunity to build customers' trust in the brand. If marketers succeed, customers may be more willing to allow their information to be utilised in return for a value exchange such as more personalised customer experiences, or exclusive offers.

A survey by **SAS**, the analytics firm, found 48% of UK shoppers intend to utilise their rights over their personal data. Specifically, the survey of 2000 UK adults found that 33% would ask retailers to stop using their data for marketing purposes. The most likely demographic to issue a request over their data is the 45-54 year-old age group. Just 13% of 18-24 year-olds said they would do the same. Further, 19% of all those surveyed said they would share their lifestyle and hobby data in exchange for a better service or discounts. However, only 16% said they would share favourite brand information and just 14% would share their media preference.

Essentials

GDPR only applies to the use of personal data - it is therefore essential to understand what personal data actually is, and what personal data your business is capturing or using. The definition of personal data is broad and includes any information relating to an individual from which you can identify a person directly or indirectly.

It also includes **online identifiers**. Examples of personal data include home address, telephone numbers, national insurance number, debit or credit card details, Facebook ID, cookie ID and location data. Some types of personal data are particularly sensitive and have even stricter rules around their use such as health information, race, religion or sexuality.

When a business is using personal data, it also needs to comply with the GDPR privacy principles. These are largely recognisable from existing data protection legislation and include:

- Ensuring that the use of the personal data is lawful and fair.
- Not to capture more personal data than necessary for the purpose.
- Keeping personal data secure, accurate and not for longer than necessary.

Accountability and consent

GDPR also introduces the principle of accountability, which requires a business to be able to demonstrate it is complying with GDPR. Put simply, it is not enough to have policies and processes in place for data protection; organisations will need to be able to evidence that these are operating effectively. As Elizabeth Denham, UK Information Commissioner puts it: businesses need to "be able to understand the privacy risks that they create for others, and to mitigate those risks".

This will, for example, involve:

- Undertaking privacy impact assessments on new products and services.
- Ensuring individuals are clearly informed how their personal information will be used at the point of collecting the data.
- Maintaining records of processing activity.
- Ensuring that suppliers to the company also can demonstrate compliance.

For the use of the personal data to be "fair and lawful", there has to be a legal basis for its use. One basis is that it is necessary in the legitimate interests of the data controller. Another legal basis is that an individual has given his or her consent for their personal data to be used for a particular purpose.

Importantly, GDPR sets the bar high to obtain consent and requires it to be a "**freely given, specific, informed and unambiguous indication of the individual's wishes**" demonstrated by a statement or some form of clear affirmative action to be given. As the **UK's Information Commissioner's Office (ICO) website** puts it: "silence, pre-ticked boxes or inactivity does not constitute consent".

As such, marketing teams need support from legal teams to understand what uses of personal data will require a customer's consent in order to be lawful. For example, in the context of marketing, a business could rely on the grounds of legitimate interest to send out marketing by post but would need consent to send electronic marketing.

The following four steps will help marketing teams prepare for GDPR:

1. Identify the data you are currently capturing

First, identify **what** personal data you are currently capturing about your customers (and using for marketing purposes). This involves understanding both how and when the data is captured.

2. Review how you tell customers how their data is used

Once you have a good understanding of what personal data you are capturing, you need to review **how** you currently inform your customers about how you are using their personal data. Currently, most organisations

inform customers via a privacy notice but, under GDPR, it is important for the organisation to review existing notices and consider the following:

- Is the explanation on how the data is going to be used clear, transparent and comprehensive?
- When is the information provided to the individual? This should happen prior to the collection of the personal data.
- Is it actively brought to their attention or hidden away in the depths of a lengthy and complex privacy policy?
- Are you doing anything else with your customers' personal data that you have not covered in the information you have provided? In other words, are you doing anything else with their data that would surprise them?

You should aim to have privacy notices that are transparent and compelling. An individual should be able to understand how their personal data is being used, and understand the benefits to them of the use of that data. To achieve this, it is advisable to collaborate with your company's legal team to ensure they meet the requirements of GDPR Articles 12-14, which detail a list of information that should be provided.

It can be helpful to set up a privacy portal, or online mechanism, on your company's website. This can help customers understand how their personal data is being used and where customers can easily self-serve and make changes to their privacy settings. One of the requirements on consent is to ensure it is easy for individuals to withdraw their consent.

3. Check whether you need consent to use the data

The third step is to check whether the use of the individual's personal data is a use that requires the customer to give consent for it to be lawful. The law applying to marketing communications and profiling customers is complex and not all uses of personal data will necessarily require consent. For example, as stated above, sending marketing in the post does not require an individual's consent. However, should an individual object to receiving it, this objection must be respected.

If you do not need consent, make sure that you are not inadvertently asking for it by using language such as "I agree", or "I consent" in your data use policy. To add further complexity, even if consent is not needed, an individual does have the right to object about some uses of personal data. A company should therefore inform individuals that they have the right to object. Ultimately, unless you have a strong grasp of the legislation, it is best to seek support and advice from your company's legal team.

4. Check how you are capturing content

When you have established **what** use cases require the customer to give consent, you need to check **how** you are capturing that consent. GDPR has made obtaining consumer consent harder and you need to be satisfied that your consent requests are GDPR-compliant. If challenged, the onus is on the business to show they have obtained an individual's consent.

Consent essentials

- Consent must be freely given. Are you giving the individual a genuine choice?

- Make sure the request for consent is prominent and not bundled together with other terms and conditions. Is it specific and written in a way that is easy to understand?
- The individual needs to give a clear signal they agree – for example, an opt-in box or choosing a certain technical setting when subscribing to an online service. Pre-ticked boxes do not amount to consent.
- Keep a record of the consent. Ensure you have sufficient detail to be able to demonstrate you have obtained consent, if challenged.
- Consent needs to be as easy to withdraw as it is to give.

Hints for privacy notices and consent requests

- Use simple, jargon free language: make it easy for an individual to make an informed choice.
- Tailor the consent request to the demographic of your customer base. This might increase chances of consent being given.
- As an alternative to small print, and consider using animations, video or icons to explain how you use the personal data. **The Guardian**, the UK newspaper, and **Tesco's Privacy Centre** are good examples of best practice.
- Seek legal advice if you are unsure whether your existing consents are GDPR-ready.

Your knowledge of the demographics of your customer base is relevant in the design of privacy notices and consent requests. Different age groups may have different concerns about how you are proposing to use their data. Understanding peoples' concerns and motivations can help you draft the consent request in a way that reassures a customer. This, in turn, can increase the chances of acquiring an individual's consent.

What's more, being more granular in your consent request can help consent levels. Rather than state that you would like to contact (or target) an individual "from time to time", consider specifying how frequent the mailing would be. Providing clarity on this may encourage individuals to consent if they know it is not going to result in daily emails or text messages. The marketing team is best placed to assess what is likely to increase the chances of success for the business, and the channels and interaction required to achieve this.

You also need to review the processes that you have set up to support the customer's choice. For example, what happens when a customer **withdraws consent** or objects to receiving marketing? Are your existing processes working sufficiently well? Are there sufficient controls in place around the use of personal data by marketing teams to ensure that the customer's preferences are respected? Is it clear within your business who is accountable for this?

Assess what training is in place for those who are analysing personal data for profiling and marketing purposes. It's important that customer-facing employees understand the rights individuals have over the use of their personal data and that staff are equipped with the knowledge to respond to customer questions and complaints.

Finally, GDPR is not the only law to be aware of. The existing E-Privacy Directive will be replaced by a **new E-Privacy Regulation**, which will also affect organisations collecting and using information for direct marketing purposes. Like GDPR, the draft regulation includes hefty fines for non-compliance and GDPR-style consent requirements for email, SMS and telephone marketing. The deadline for this to come into force is May 2018 - the same as GDPR. However, this looks to be an ambitious timeframe. While there may be changes to the draft, organisations should start planning for the impact of this now.

Checklist

- Be clear when you need to ask for consent to use personal data (and when you don't).
- Make sure your consent requests comply with GDPR and that you can demonstrate this.
- If you don't need consent, don't use language that suggests you are asking for it (e.g. "I agree to the Privacy Policy"). Remember that consent is only one legal basis for ensuring the processing is lawful. See **Consent is not the 'silver bullet' for GDPR compliance** posted by the UK Information Commissioner on August 16th 2017.
- Be aware of the impact of the forthcoming E-Privacy Regulation.
- If unsure, seek legal advice.

Further reading

WARC Topic: **Data protection & privacy**

WARC Topic: **Regulation & control**

WARC Best Practice: **What we know about data protection and privacy**

WARC Best Practice: **How to manage consumer data responsibly**

How to prepare for GDPR's 'tsunami of change', Event report, DMA Data Protection, February 2017

GDPR: An opportunity to build consumer trust, Event report, DMA Data Protection, February 2017

How new EU laws may transform digital marketing across the globe, Event report, WFA Global Marketer Week, 2017

Data protection reform, Information Commissioner's Officer (ICO)

Consultation: GDPR consent guidance, Information Commissioner's Office, March 2017

Reform of EU data protection rules, European Commission

EU GDPR

About the author

Jo Blazey
Privacy Officer & Counsel, Vodafone

Jo is a qualified solicitor and joined Vodafone in 2010. Since March 2015 she has served as Vodafone UK's Privacy Officer & Counsel and leads its privacy team.

Jo is responsible for Vodafone UK's Privacy Programme and works closely with colleagues across the business on all aspects relating to Data Protection and GDPR readiness. Prior to joining Vodafone, Jo worked in private practice for Taylor Wessing and Thomas Eggar.

WARC Ltd.
Americas: 2233 Wisconsin Ave NW, Suite 535, Washington, DC 20007, United States - Tel: +1 202 778 0680
APAC: 20A Teck Lim Road, 088391, Singapore - Tel: +65 3157 6200
EMEA: 85 Newman Street, London, United Kingdom, W1T 3EU - Tel: +44 (0)20 7467 8100

www.warc.com

WARC