

KINGPIN

What will the GDPR mean for B2B marketing professionals?



Introduction

The purpose of the General Data Protection Regulation (GDPR) is to improve protection for EU citizens and make EU privacy and data laws fit for purpose in the digital age. The regulation has promised to modernise and harmonise the legislative landscape for data protection across the European Union, as that landscape is currently fragmented, causing confusion to individuals and businesses.

The GDPR will replace the EU Data Protection Directive 95/46/ec, which came into force in 1995 – at a time when the internet was still in its dial-up infancy and phones were far from smart. So much has changed about how companies collect and process data, which has become a valuable commercial currency, but the same outdated data protection laws have applied.

The GDPR is a regulation not a directive. This is an important point, as it means that when it comes into full effect in spring 2018 it will be directly applicable in all EU member states as a single law. There will be no need to implement legislation in individual countries. From May 2018, the GDPR will apply, no questions asked.

At its core the GDPR contains a number of principles that will require marketers to think and act very differently. From communicating with customers to managing databases, the GDPR will affect many aspects of a marketer's focus. Some of these require organisations to take action now to be prepared for the advent of the new regulations.

This guide is aimed at explaining to marketers what the new legislation means and what actions can be taken to be ready for the April 2018 deadline. A lot has been written about the ferocious penalties associated with not complying with GDPR and we await the first test legal cases with interest.

However, while compliance with the following criteria and stipulations may seem onerous and, from our current perspective, a little 'over the top', it's important to focus on the endgame. Not simply compliance with GDPR but more effective marketing achieved through improved and better-performing contact lists and databases, better privacy and protection of customer data and more trust in your brand.

What about Brexit?

It is a misconception that the UK's impending exit from the European Union means that British organisations are off the hook as far as GDPR is concerned.

Firstly, the UK will still be a part of the EU when the GDPR is introduced on 28 May 2018 and will remain an EU member state for several months after. After that the position for the UK is less clear and depends on negotiations. It may be that the UK government will review data protection legislation for UK citizens.

Secondly and more importantly, irrespective of the UK's membership of the European Union, if British businesses want to do business in Europe and have to process the personal data of EU citizens they will need to comply with the GDPR. The regulation is universally applicable for any organisation storing or processing EU personal data, wherever the organisation is based.





Key principles that affect marketers

This guidance will cover key areas of the GDPR that will require marketers to review their business practices.

1. **Marketing lists and databases** – customers and prospects need to have given "unambiguous" permission. An opt-out checkbox is no longer acceptable. Customers will need to opt-in to receive communications and be clear what messaging they will receive. Companies will also need to keep "provable" audit trails for personal data that outline when permission was granted and for what.
2. **Right to access** – data subjects now have the right to know what personal data is being processed by an organisation and for what purpose.
3. **Right to be forgotten / Right to erasure** – EU citizens now have the right of erasure, meaning data processors will need to remove their details from their databases on request – while also ensuring no further communications are sent.
4. **Portability of data** – data subjects also have the right to request their data in a readable, electronic format in order to transfer it to a different system.
5. **Privacy by design** – privacy by design is another new concept that marketers and other business divisions need to come to terms with quickly. Put simply, it means that privacy and data protection concerns must be at the forefront of an organisation's plans when it comes to managing data. Privacy can no longer be an afterthought.
6. **Data protection officers** – some organisations may need to appoint data protection officers to oversee the processing of personal data and review organisational best practice in line with the GDPR.
7. **Breach notification** – personal data breaches now need to be reported within 72 hours of being detected. While responsibility for detecting system breaches lies with technology and operations teams, the communications division needs to be prepared to report breaches and deal with potential damage to brand and reputation.



1. Marketing lists and databases

The GDPR has considerably strengthened the conditions for consent. This is one of the areas that will most affect marketing practices, especially for marketing companies processing the data of consumers rather than business individuals.

Marketers need to make sure their email and SMS marketing practice complies with the GDPR. It doesn't matter where your organisation is based, if you communicate electronically with consumers in the EU you will need to be compliant with the GDPR.

One highly significant change the GDPR makes is to require that the message of "consent" must be unambiguous. This means marketers need a clear, affirmative action – you can no longer use a pre-ticked checkbox on a form, long rambling terms and conditions or soft opt-ins at in-store checkouts.

Your prospects/customers have to state clearly that they want to receive your communications. It's essential that marketers opt-in their lists and databases and have a provable record that confirms who has agreed to what communications and when.

Organisations need to show "provable consent" (although there's no black-and-white definition of what this looks like in the GDPR). In practical terms this requirement will call for more database fields to record proof of consent, the consent statement and the shelf life of the data, as well as when and where the consent was obtained.

This data should be consolidated with existing CRM and email marketing data so it can be accessed if a data subject questions when consent was given or makes a request for erasure.

Practical steps:

- With the E-privacy Directive set to come in, be sure to read the 'Marketing to individuals in businesses' section on the next page
- Review your data management requirements and systems
- Run campaigns to opt-in your marketing lists and databases
- Getting provable consent: include the criteria you can use

2. Right to access

The GDPR also introduces the Right to Access, meaning data subjects can request to know whether an organisation is processing data concerning them and for what purpose. The subject can also request a free readable copy of the personal data in a common electronic format.

Practical steps:

- Audit current systems and processes to identify areas where privacy controls need to be strengthened or re-engineered
- Develop new policies for safekeeping customer personal data, using techniques such as pseudonymisation and training staff on best practice

Marketing to individuals in businesses

At the moment, the post-GDPR consent situation looks a little different for B2B marketers. In January 2017 the European Commission published a draft of the new version of the E-privacy Directive, which will sit as a parallel regulation to the GDPR covering privacy rights.

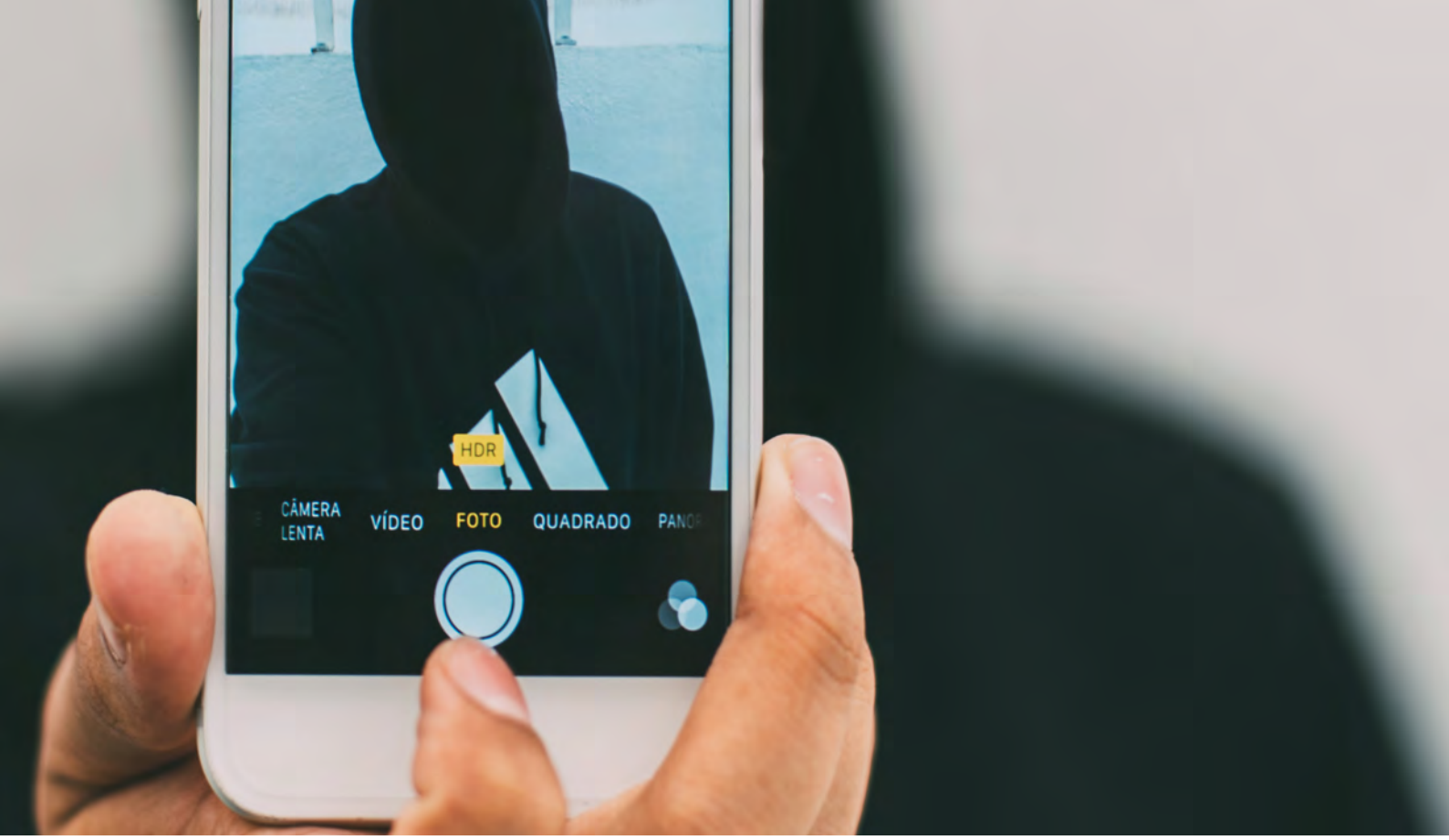
The publication of the draft marks the beginning of the legislative process for the E-privacy Directive. The draft will be reviewed by the EU Parliament as well as by the EU's Council of Ministers. Both will have the chance to make amendments.

However, as it stands in the current draft, the EC has softened its view on the requirements for B2B marketers considerably. The January 2017 draft does not require opt-in consent for B2B email marketing to corporate subscribers, unlike the position with consumers.

The proposed legislation does call for the interests of business individuals to be protected, meaning that corporate subscribers should be able to unsubscribe or opt-out from receiving electronic marketing easily.

However, this is still a draft and could be subject to future amendment to bring it in line with the GDPR. B2B marketers might breathe a sigh of relief but they need to stay abreast of the developing legislation and respond swiftly if need be.





3. Right to be forgotten/erasure

Following a related and well-publicised 2014 European Court of Justice case, the GDPR introduces the right to be forgotten. This means that any individual has the right to request that a data controller delete his or her data from their records. Furthermore, if that data has been shared with third parties, the data controller should take "reasonable steps" to require other controllers to comply with that same request.

The data controller is required to carry out these requests for erasure unless it would require a "disproportionate effort". The "reasonable steps" processors must undertake depend on the technology available and the cost of implementing the erasure process.

The GDPR also enhances the rights of data subjects to know what kind of processing is taking place with their details, to access their data and to be able to change their details to correct any inaccuracies or mistakes.

Practical steps:

- Develop a process for managing requests and train staff to make sure requests can be managed effectively
- Review systems to ensure erasure requests can be processed efficiently



4. Portability of data

In addition to the right to erasure, data subjects also have the right to request their data in a readable format in order to transfer it to a different system. The data controller needs to provide the data in a structured form and in a common electronic format.

Again, this principle underlines the need for organisations to develop systems that can not only consolidate data from multiple sources but can also undertake new functions based on the new requirements of the GDPR. Information systems need to become more agile to deal with customer requests.

Practical steps:

- Develop a process for managing requests and train staff to ensure requests can be managed effectively.
- Review systems to ensure portability requests can be processed efficiently, including the export of user-friendly common electronic formats.



5. Privacy by design

Privacy by design or default is another key tenet of GDPR that will force a shift in how many organisations think about personal data.

Article 25 of the GDPR states that the data controller should "implement appropriate technical and organisational measures… to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". The GDPR cites pseudonymisation as an effective method for protecting customer data. 'Pseudonymisation' is defined as "the processing of personal data in such a way that the data can't be attributed to a specific data subject without the use of additional information".

Put simply, it states that privacy concerns should be a consideration from the offset in any marketing or lead generation campaign and not simply an afterthought. Data protection and processing safeguards must become part of the DNA of all systems and processes. This will be a major shift in thinking for some organisations and a principle that marketers need to be thinking about now, not later.

Article 25 also states that "only personal data which are necessary for each specific purpose of the processing" should be processed.

Privacy by design is another example of how the GDPR has responded to the changing nature of data protection since the inception of the previous guidelines. Directive 95/46/ec didn't even recognise the concept of privacy by design. The UK Information Commissioner's Office has suggested seven "foundational principles for privacy by design"[1].

Practical steps:

- Audit current systems and processes to identify areas where privacy controls need to be strengthened or re-engineered
- Develop new policies for safekeeping customer personal data, using techniques such as pseudonymisation and training staff on best practice

[1] Privacy by design – Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/



6. Data protection officers

The GDPR will clearly create a significant data protection processing overhead on companies. The regulation also recommends that organisations establish a data protection function to manage this.
While not all organisations will need to employ a dedicated Data Protection Officer as initially feared, Article 37 of the GDPR states that organisations that need to employ a DPO are:

- All public authorities
- Organisations where the core activities involve "regular and systematic monitoring of data subjects on a large scale"
- Organisations processing "special categories of personal data, such as personal, biometric or health data"

For the business owner of customer data, it makes sense that this function should reside within the marketing division rather than in IT.

Practical steps:

- Audit current systems and processes to identify areas where privacy controls need to be strengthened or re-engineered
- Develop new policies for safekeeping customer personal data, using techniques such as pseudonymisation and training staff on best practice



7. Breach notification

The GDPR has introduced a stricter regime for reporting data breaches that are "likely to result in a risk for the rights and freedoms of individuals". Organisations will be required to notify data subjects "without undue delay" and report breaches to the national data protection authority within 72 hours of being identified. This means that the IT security functions of organisations need to be able to detect and report breaches. Marketing and communications team also need to be prepared.

Practical steps:

- Audit current systems and processes to identify areas where privacy controls need to be strengthened or re-engineered
- Develop new policies for safekeeping customer personal data, using techniques such as pseudonymisation and training staff on best practice

Bird & Bird

The Legal View: Bird & Bird

Don't the GDPR and the E-Privacy Regulation cover the same ground?

In part they do and it's been a bit of an unhappy crossover in the 14 or so years since the predecessor laws to each came in. But B2B marketers really need to get their heads around both areas so they can understand the specifics of what is restricted. Both new laws are timetabled to take effect in May 2018. Both set maximum fines at four per cent or worldwide turnover. Although the law is well behind what's actually happening on the ground and the way that marketing actually operates, as a marketer you do have to understand the way that the laws are set out.

Is it likely that the UK will stick with GDPR post-Brexit or develop its own?

The GDPR will take effect in May 2018 (so before any Brexit). The government has said it will not do anything to block or unwind this. Potentially the UK could introduce tailored provisions post-Brexit, but going off-piste risks making the UK a more difficult country to transfer data to (from other EU countries).

To explain, the removal of the Safe Harbour agreement was about the US having lower privacy standards than Europe. So fast forward to post-Brexit, the UK will be in the same position as the US if it has a lower standard of legal protection than exists then in the EU. It's hard to imagine the government risking putting UK business at such a disadvantage considering how reliant a lot of our UK businesses are on having access to data which originates outside our borders. Take the financial services sector as prime example. Assuming that the UK wants to keep some of that sector on home territory, the government would be taking a risk if it chose to introduce a 'regulation lite' version of the GDPR.

The second factor to take into account is if you are a UK business with customers or employees located in Europe then you are caught by GDPR in any case. So you will be fined in Germany if you target German customers without regards to the GDPR, for example. There are very few UK businesses that are completely 100 per cent UK-focused. So it will be difficult for businesses if we have a disharmonised approach compared to the rest of Europe.

Penalties and sanctions

The penalties associated with non-compliance with GDPR have garnered headlines in many publications. Organisations breaching the GDPR's guidelines can be fined €20m or four per cent of the organisation's global turnover – whichever is the greater. This is the top level of the GDPR's fine structure and can be imposed for more serious data protection breaches like the failure to have to required consent data in place.

Lesser fines of two per cent of global turnover can be imposed on organisations failing other requirements, such as not reporting breaches properly.

If even one location or individual is not fully compliant, the repercussions could ripple through the whole organisation, as penalties are based on global turnover. Consequently, educating the entire organisation about the importance of data protection and privacy practices will be as important as any project to opt in contacts or adapt databases.

Bird & Bird

The Legal View: Bird & Bird

What's likely to happen after May 2018 if marketing data doesn't meet the requirements of the GDPR? Fined? Or just a slap on the wrist?

We think it will vary from country to country. Enforcement has always been very culturally different and influenced by things such as whether the regulator keeps the fines which are paid or not. That's the case in Spain but is not the case in the UK.

Then there are other countries that again for cultural and historic reasons have a higher regard for data protection than others. Germany is a good example and regulators there have historically been more active than, let's say, in the UK or Ireland.

Although 2018 will bring harmonised – or supposedly harmonised – laws, enforcement on the ground by regulators with different agendas will vary. I would assume though that whichever territory your business operates in that regulators there will be keen to make an example of those making no effort to comply with the new laws. Preparing for the new legislative landscape now is essential.

Summary

The GDPR presents marketers with many challenges and some fearsome penalties for failing to meet them. Marketers, especially those who process the data of consumers rather than businesses, face a significant workload to become GDPR-ready ahead of the May 2018 deadline.

But compliance with the GDPR also offers many benefits to organisations. A leaner more effective customer database of genuine and opted-in contacts, a more transparent process for the management of data. And a commitment toward customer data protection and privacy that can be enshrined in brand values. At a time when customers are putting so much faith in the protection of personal data[2] the value of this last point shouldn't be underestimated.

[2] Businesses and consumers increasingly concerned about data privacy: Deloitte http://www.zdnet.com/article/businesses-and-consumers-increasingly-concerned-about-data-privacy-deloitte/

Contact Kingpin to find out the latest on B2B legislation and what it means for your marketing.

UK +44 (0)20 7803 1000 | US +1 415 793 8370

enquiries@kingpincomms.com com