

WHITEPAPER

A Marketer's Guide to GDPR

GRAVICUSTM

A Marketer's Guide to GDPR

Just in case you didn't already know, GDPR comes into effect on 25 May 2018 and involves maximum fines of up to 4% of global turnover for data breaches.

What Is GDPR?

GDPR will replace the Data Protection Act 1995 and was initially adopted April 2016 by the European Parliament and the European Council, after four years of negotiations. GDPR provides increased control of personal data for EU citizens by making organisations (that collect, process and store such data) much more responsible, especially for data breaches.

A lot of what's covered within GDPR isn't new, it's carried over from the Data Protection Act. What is new is the substantial fines for non-compliance and the enhanced rights for data subjects/individuals. Organisations will also be required to regularly conduct Data Protection Impact Assessments (DPIA) to strengthen the way they seek permission for use of personal data, and must also provide documentation for the ways in which they use this data and report on data breaches.

GDPR is a regulation, not a directive, it's therefore legally binding – meaning there's no opt-out. Failure to comply can result in a **fine of up to €20 million or 4% of your global turnover**, plus an individual/subject affected by a breach can also claim against you.

According to NCC Group, the ICO's total issued fines in 2016 amounted to £880,500 under GDPR this would have been £69 million, 79 times higher.

Talk Talk's recent fine from the ICO of £400,000 would be £59 million under GDPR.¹

Why introduce GDPR now?

The Data Protection Act, 1995 was first adopted in 1980 (later updated in 1995), it therefore doesn't include for social media, smartphones, or advanced web technology (i.e. Artificial Intelligence, Virtual Reality, etc). Plus, the current regulation is only an optional directive, unlike GDPR which is a legal regulation.²

GDPR puts the individual first, to protect and empower them in how their personal data is used, rather than being exploited and ignored. Organisations of all sizes that handle personal data will be held accountable for their actions, transparency and honesty. Personal data will no longer be able to be exploited, an organisation must show when they got the data, where they got it from and how they use it.

In May 2017, [The Economist](#)³ called personal data 'the world's most valuable resource' ahead of oil, because of how much it informs the way companies communicate with their customers and how it positively impacts [customer experience](#).⁴

Now, because personal data is so valuable, it's vulnerable to theft or misuse, hence the need for GDPR.

What does GDPR mean for Marketers?

If you have customers, then everyone inside your organisation will be affected by and responsible for complying with GDPR.

According to a survey by the Direct Marketing Association (DMA) a staggering 54% of businesses expect to be compliant by 25 May 2018 – ready or not, you will be required by law to comply with GDPR or face hefty fines. We all know the Information Commissioners Office (ICO) like to target certain industries/types of organisations and make an example of them, so there's every chance that those who deal with data in a big way will be a target for the ICO once GDPR kicks in.⁵

Get your house in order now! We've known about this new law for over five years, so there are no excuses!

If your organisation takes a responsible stance on data, they'll already have permissions in place and will be making sure these are validated regularly, and can be updated with ease by the individual.

In May 2018, organisations will no longer be allowed to collect or process a European citizen's consumer data without identifying a legal basis for doing so. They will also be unable to use data collected prior to May 2018 if this doesn't have appropriate notice/s and measures for consent in place.

Nina Barakzai, Sky group head of data protection and privacy believes GDPR should require *"just an extra few tweaks,"* if businesses have been operating a transparent and customer-centric data policy.

She sees her main task as documenting evidence of how Sky takes steps to protect consumer privacy. Nina went on to say *"most of our preferred suppliers have been planning for GDPR since 2013. We have contract clauses in place."*

One way to avoid the worry of complying with the law is to *"build an anonymisation strategy"*, she says, treat your personal data as if you don't process it. Data is useful in so many ways and provides meaningful insights that inform your business.

Consistency in data privacy regulations across Europe is good news for all marketers, but will come with its challenges for those that communicate with EU based customers. While some marketers panic, others will embrace the opportunities by way of improved quality of data and peace of mind around the transparency of how we get and manage data, in a way that builds trust and enhances brand strength.

Good quality data means less wastage and cost-effective communications. There's nothing worse than mailing thousands of addresses to get a mass of returns to manage, or even worse, communicating with individuals that are deceased – this type of activity massively impacts the brand, resources/workload and the trust instilled within.

Some 42% of B2B marketers believe that a lack of quality contact data is the single biggest barrier to lead generation; 51% of email marketers believe the same. Focusing on accumulating and processing important, useful, and legally compliant information is a smart move – and if the GDPR provides some incentive for that, then marketers will be better off for it. (Source: [Digital Marketing Magazine](#))

How GDPR affects marketing

There are three key areas of focus for marketers – data permission, data access and data focus:

1. Data permission around opt-ins, opt-outs and consent regarding communications.

Consent must be 'freely given, specific, informed and unambiguous', and articulated by a 'clear affirmative action'. That means you can't assume consent based on 'inactivity' or pre-ticked boxes. Prospects and customers must agree for their data to be used and that they can be contacted.

Also, if you are including third-party consents within your opt-ins you must name the individual company.

There's nothing to be confused about...

Be open, honest, transparent and use plain language – it's simple

Opportunity: the opportunity for marketing lies in the fact that instead of a simple yes or no option you can now provide a range of options to find out what the individual is interested in. Through consent, you gain insights which enable you to provide information they want to receive. This not only helps GDPR compliance, it also helps the segmentation of customers for which you can develop focused communications, rather than a *"one size fits all"* approach.

In practice: this means leads, customers, partners, suppliers etc. need to physically confirm they want to be contacted. Therefore, a pre-ticked box that automatically opts them in won't cut it anymore – opt-ins need to be a deliberate choice.

For example, *Figure 1*, instead of assuming visitors who complete the first form want to receive marketing emails (non-compliant with GDPR), to be GDPR compliant, you would ask visitors to specifically opt-in to newsletters by ticking the sign-up box in the second form in *Figure 1*.

Figure 1.

Your name:

Company name:

Your email:

Your phone:

[Start Free Trial](#)

By signing up to a free trial of SuperOffice CRM, you agree to our [Terms](#) and you have read our [privacy policy](#). You may receive email updates from SuperOffice and you can opt out at any time.

Your name:

Company name:

Your email:

Your phone:

By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.

Yes, please keep me updated on SuperOffice news, events and offers.

[Start Free Trial](#)

[Terms & privacy policy](#)

2. Data access and the right to be forgotten

GDPR allows individuals to have more control over how their data is collected and used – including the ability to access or remove it – in line with their right to be forgotten. As a marketer, it will be your responsibility to make sure that users can easily access their data and update/remove consent for its use.

Google was recently forced to remove pages from its search engine results to comply with this requirement.

Under GDPR, every individual has the "right to be forgotten" and can request an organisation to remove all data held on them. If you keep data in different places for different purposes this can cause issues unless you have a solution in place such as CRM that will help track permissions for compliance.

Opportunity: a CRM provides customers with the opportunity to switch consent on and off for different purposes, so marketers are always up-to-date with what's relevant to the individual customer.

In practice: the unsubscribe link within your emails – link this to the user profile and management to allow users to manage their email preferences (as shown in the example in *Figure 2*. on the following page from Twitter).

Figure 2.

Updates from Twitter

Email me with

- News about Twitter product and feature updates
- Tips on getting more out of Twitter
- Things I missed since I last logged into Twitter
- News about Twitter on partner products and other third party services
- Participation in Twitter research surveys
- Suggestions for recommended accounts
- Suggestions based on my recent follows
- Tips on Twitter business products

[Save changes](#)

3. Data focus - the legal basis for processing personal data

This will necessitate improved data housekeeping on the part of marketers – and less collecting of data for unnecessary, or frivolous reasons.

As marketers, you need to ask yourself, what data do I really need? GDPR requires you to legally justify the processing of personal data collected, meaning you focus on the data you must have, and stop asking for the data that's nice to have. If you can prove why you need specific data, then you can continue asking for it.

Opportunity: Organisations will no longer be able to get away with contacting individuals for marketing purposes unless you have their permission to do so. Be fully transparent and honest, give them a reason to share their personal details with you and its highly likely they will.

People do business with other people (or organisations) that they know, like, and trust. Building brand loyalty and trust comes through projecting transparency about who you are and what you're doing.

In practice: Look at this in a similar way to the Telephone Preference Service – if you've registered and/or blocked certain telephone numbers from your phone you should not be receiving calls and can hold organisations to account on this by reporting them. Likewise, if you not given permission to be contacted, the individual should not be contacted and will question/report organisations due to an increased awareness and the ease with which you can report to the ICO.

The law will always favour the consumer, using personal data for direct marketing will only be classed as legitimate if it's necessary and the consumer would expect to be communicated with i.e. bank account terms and conditions updates/changes, changes to an insurance policy.

It's very clear cut, the communication is either necessary or it's not, and if it's not you need express permissions from the individual.

If you are not sure whether you can contact an individual its highly likely you shouldn't be. If you're not sure don't do it, or get the necessary permissions in place. It's about being responsible, honest and transparent

The big question - who's responsible when there's a problem?

Marketers and publishers are potentially accountable for mistakes made by third parties. Having obtained it, you must make sure nobody in the chain, who might get data, you share will misuse it and expose you.

The whole organisation and everyone within are responsible for data management and the part they play in complying with GDPR

Who's affected the most in Marketing by GDPR?

The three roles within a marketing department that will feel the impact of GDPR the most in their day-to-day role are as follows:

1. Email marketing managers

Email is a key lead generation activity which quite often forms the first stage of the prospect to sales pipeline

A user that willingly gives their email address in exchange for more information, such as signing up to a mailing list or downloading a piece of content, is known as an "opt-in".

This is in stark contrast to firms that buy email lists or scrape (or copy) them from a website. Under the new GDPR regulation, buying lists (or scraping them) will be strictly forbidden.

Ensuring users opt-in and give consent to be contacted will be a requirement of GDPR

2. Marketing Automation/Customer Journey

Make sure automatic emails don't go to those that have opted-out. Every contact must have provided permission to market to them.

3. PR

Communicating with journalists is no different than marketing to an employee of a business. Journalists will have to give you consent to contact them.

This consent could be given through PR platforms, where journalists ask you to contact them, or through requests made on social media platforms – register now.

Obviously if a journalist reaches out to you directly, they've expressed an interest in talking to you.

GDPR is a golden opportunity for marketers to do what they do best and feel comfortable about how they are executing targeted marketing campaigns with people that are engaged with the brand

How marketers can prepare for GDPR

The GDPR will likely cause temporary difficulties in how databases are built, managed and the collection of data. The introduction of this regulation won't be unmanageable. The major change is the degree to which marketers – and all other data processors – are required to take responsibility for the way they collect information.

We are accountable to our prospects and customers as well as our bosses and co-workers

Revisit the three principles of data collection

When it comes to data there are three principles to always work towards - transparency, control and value exchange. Put simply, to ensure transparency we must be able to easily explain what we are doing with individual's data, if we can't we shouldn't be doing it.

Put the individual in control of their data by making sure it's an easy process to opt-out or in to certain things whenever they want.

Lastly, always make sure the individual gets something in return for their data.

According to a new study by W8 data, up to 75% of marketing databases will become obsolete by 25th May 2018 and only 25% of existing customer data meets GDPR requirements⁶

To start preparing for GDPR follow these tips:

- **Audit mailing lists now** by removing anyone where you do not have a record of their opt-in. For new subscribers, make sure the potential subscriber confirms they want to join the mailing list by sending an automated email to confirm the subscription
- **Review the way personal data is currently collected.** Do you buy mailing lists? If so, now might be the time to start a fresh with a new mailing list that will guarantee you a list of engaged and interested readers
- **Create content that's tailored to potential customers?** Invest in a content marketing strategy by creating whitepapers, guides, infographics and eBooks that website visitors can access and download in exchange for them sharing their contact information

- **Invite visitors to add themselves to your mailing list** by launching a pop up on your website for product news, blog posts, general company news etc.
- **Educate your sales team about social selling techniques.** Sales Professionals need to embrace social media and connect with prospects to share relevant content – rather than trying to reach new prospects by email, direct mail etc.
- **Start centralising personal data into a CRM system,** make sure users can access their data, review proposed usage, and make any changes as necessary
- **Understand the data you're collecting in detail.** Do you need all the data that you have? What data can you do without/can't justify? When it comes to sign up forms, just ask for the data that is necessary and let them know what this will be used for. Full name, email address and company name are usually more than enough

- **Check contracts.** Review the supply chain to determine if partner agreements are up-to-date and include GDPR-related clauses, for example, what to do in case of a breach or an enforcement action. This should form part of a Data Protection Impact Assessment (DPIA) as required by GDPR

Conclusions

Failure to comply with GDPR will have extremely high penalties, so align your approach with the regulation for the collection and processing data.

Of course, to comply with this legislation, it's necessary to understand it – and while there is no formal requirement to appoint a dedicated Data Protection Officer, every organisation will need a central contact that is responsible for GDPR to help understand obligations and avoid breaches.

It would help if each function within the organisation has a GDPR representative as well, if in a larger organisation.

Marketers also need to set themselves up to react appropriately to requests to view, amend or destroy prospect or customer data. While they don't yet have to provide online access, they need to be able to facilitate access: it will be a legal right, and though many may choose not to exercise it, it is good practice to make it as easy as possible for those who do.

Remember, GDPR isn't designed to stop businesses from communicating with their customers. GDPR will lead to an increase in data quality, which is why the best and most resourceful marketers are seeing the bigger picture in that it's an opportunity to delve deeper into the needs of their prospects and customers, rather than using the traditional "one-size-fits-all" approach to marketing.

The rules for GDPR compliance are quite simple – don't contact someone unless they specifically ask to be.

Don't assume they want to hear from you. Don't cold contact them, and don't send them irrelevant information that they didn't request.

If you can do all that, then you're taking a huge step towards being GDPR compliant.

Finally, it's going to cost you in terms of time and money. Educating the team, adjusting systems, and reordering your strategy for full compliance will take manpower and financial resources, so getting organised as soon as possible will place you in a strong position.

The months leading up to May 2018 are set to be challenging for businesses across Europe and beyond. GDPR is a big change to the way in which companies operating in EU countries handle personal data, with fines of up to €20 million if you fail to comply. That's why it's important for you to seek advice from a lawyer as to what is or is not a legal requirement for your business.

References and further reading

1. **GDPR fines**
2. **European Union Law**
3. **The Economist**
4. **Customer Experience**
5. **DMA**
6. **GDPR for Marketing**
7. **What does the GDPR mean for marketers?**

About Gravicus

We understand that every business has its own needs, whether you need to find Personally identifiable information (PII), enrich your content, explore dark data or cleanse, Gravicus provide businesses with purpose-built tools to search, analyse and organise their growing data volumes to enable them to achieve compliance without the confusion.

At the core of everything we do is our desire to keep things as simple as possible, enabling our customers to rapidly gain clear insight into their data and help them discover new ways to use it.

Gravicus Osprey is our unstructured data analysis platform in the cloud. It provides a purpose-built solution that's practical and simple to use in analysing data, getting it organised and identifying any necessary actions that are required for compliance.

Using extensive information governance knowledge and a multitude of AI capabilities, Osprey helps make sense of data to understand risk exposure, reduce costs and achieve regulatory compliance. Osprey Cloud, takes the IT complexity out of information and data management, providing key insights into your business data at a glance and instantly.

Data Insights

Osprey gives users real time, and continuous insight into their valuable data assets, whether for managing compliance or regulatory risk; as part of a cyber risk strategy, or to deliver an intelligent migration project.

A Growing Platform

Osprey Cloud provides a range of smart, scalable applications and is a growing platform that tackles a variety of business problems, from a simple data cleanse to managing regulatory risk, up to e-discovery, archiving and M&A Due Diligence.

Scale and upgrade

Whatever your data needs, Osprey gives you the flexibility to choose the solutions you need, allowing you to scale and upgrade as your data needs require.

If you are starting out on your journey to GDPR compliance or you've already started but need to validate your approach, our Data Practice Impact Assessment (DPIA) tool will identify your risks and make key recommendations to help you become compliant.

Contact Gravicus today to protect your data and make it work harder for you.

Sign up to Osprey Free at: **www.gravicus.com**

Call: **0203 858 0636**

Email: **info@gravicus.com**

DISCLAIMER: The information in this whitepaper is for your general guidance only and is not and shall not constitute legal advice. If you need advice on your rights or responsibilities or any legal advice around data protection matters, please obtain specific legal advice and contact an adviser or solicitor.

Web: www.gravicus.com

Call: 0203 858 0636

Email: info@gravicus.com

GRAVICUSTM