

GDPR: A year on

Sponsored by

OneTrust

Responsible Marketing

DM
Data &
Marketing
Association **A**

/ Contents

Foreword.....	02
A word from our sponsor	03
Introduction.....	04
Culture Change.....	07
Teething problems.....	12
Best practice.....	14
Enforcement.....	18
Technology.....	21
Conclusion.....	25
Discover more about GDPR.....	26
Campaign sponsor.....	27
About the DMA.....	28
Copyright and disclaimer.....	29

/ Foreword

One year into the most significant piece of legislation for our community in my lifetime and I have a couple of reflections.

I spent the year prior to enactment meeting as many members as possible to see how you were preparing: and, of course, your preparedness varied. But what was consistent was a dramatic and positive shift in data literacy throughout the organisations I visited, and particularly around the marketing management meeting room table. Everyone was talking about, and more or less taking ownership of data, recognising that it empowered almost every bit of their modern marketing machine.

Data has emerged from the domain of the geeks. I know DMA members recognise this, and transparently treat their customers' data with respect.

As your trade association we did our best to provide guidance across the marketing spectrum in difficult circumstances, always putting the customer first and mindful of our members' sustainable commercial objectives.

We will continue to observe the Regulator's enforcements carefully, share our points of view, and ensure we can all learn from them.

Mark Runacus,
Board Chair, DMA



/ A word from our sponsor

The GDPR started a conversation heard 'round the world, and today, everyone is thinking about privacy.

Privacy has expanded from a compliance checklist item into a boardroom priority. Teams are reaching across the business aisles and working together – marketing, legal, compliance, security, privacy, risk, human resources – to build privacy into the DNA of the organisation. These cross-functional business units are rethinking how to make privacy a market differentiator – not just to avoid being the next headline, but to build trust with consumers and put the control of data back into the hands of the people.

We've come a long way, but still have work to do, together. With the GDPR now fully in place and new regulations on the horizon, it is time for marketers to reshape the idea of privacy as a hinderance into a true competitive differentiator.

OneTrust is proud to sponsor the DMA report on GDPR: A year on, highlighting where we've been and where we are going for a successful future. At **OneTrust**, we work with marketing teams of all sizes to drive opt-in rates and create enhanced customer experiences while staying compliant with the world's global privacy regulations. Teams can collect valid consent and preferences; pinpoint where personal data resides and how it is used; streamline consumer rights to information and deletion; and maintain records in a central location in the event of an audit. Together with partners like the DMA and our base of 2,500 customers, we are enabling business innovation and consumer trust in this new era of privacy.

Ian Evans,
Managing Director, EMEA OneTrust



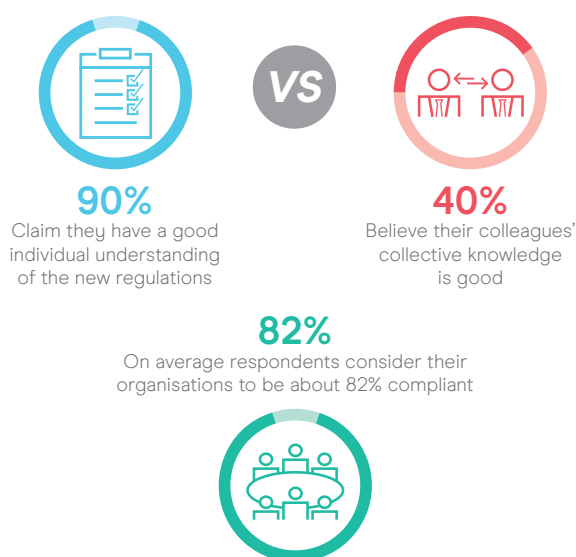
/ Introduction

The introduction of the General Data Protection Regulation (GDPR) in May 2018 marked a watershed moment for the marketing industry and its approach to data protection. In the year since, many organisations have embraced the GDPR's principles and worked hard to ensure that their approach to privacy is a brand asset. On the flip side, other organisations have failed to seize the opportunity and are seemingly being pulled kicking and screaming into this new data protection era.

However, the GDPR is still settling in and there is only sporadic case law from around Europe. As a result, marketers still are not clear on what compliance really means regarding a number of different topics. This has led to confusion, but also a deep sense of frustration that guidance from the regulator has been slow to be published. Even more frustrating was the sheer number of self-professed GDPR 'experts' that have popped up. Many with questionable credentials and who subsequently gave bad advice to businesses. In the worst case scenarios, marketing databases were wiped out on the basis of this bad advice.

It's easy to focus on the negatives and what has been lacking, but a real culture-change has been taking place and it is having a direct impact on consumer trust. ICO research has revealed there is a notable increase in consumer trust and confidence. The research found that one in three people (34%) have trust and confidence in companies and organisations storing and using their personal information. Although this may seem slightly low, this is up from one in five people in 2017 (21%).

The DMA's latest GDPR research 'Data Privacy: An Industry Perspective 2018' revealed that marketers are feeling more confident too with 89% of them having received formal GDPR training in 2018. As a result, 90% claim to have a good understanding of the new regulations and 40% believe that their colleagues' collective knowledge of the law is also good. Some may be surprised to hear that 57% of marketers actually think the GDPR will have a positive or neutral impact on sales.



The DMA created a series of [GDPR guidance for marketers](#) working with the **Information Commissioner's Office (ICO)**. The **ICO** needed assistance to ensure that their message reached as many organisations as possible and so sought to work with the DMA to bolster its presence with marketers. The [DMA's specific guidance](#) for marketers was crucial in helping businesses understand how the GDPR applied to the data and marketing sector.





“I commend the work of the DMA, in particular for putting this timely report together one year on following GDPR implementation. It’s no understatement to say that GDPR has been a big journey and it has meant changes to existing practices, for example, at **Unilever** we felt it important to take on a legal expert in our marketing team.

I think that on the whole, GDPR has been a really positive step as it has made the approach on data better. For example, we have greater transparency and third-party verification. Data has also become much more consumer-centric too. As a result, it means that marketers have a big responsibility to focus on building trust back in, as data and trust are intertwined. And without trust, there won’t be brands.”

Keith Weed

*Chief Marketing Officer, **Unilever***



/ Culture Change

GDPR has made data protection a board room issue where it was not before. Data protection was the concern of IT or legal and something senior leaders did not feel they needed to worry about. However, GDPR has challenged companies to change their corporate culture and ensure that everyone in the organisation understands the importance of data protection policy.

A company cannot hope to comply with the law if their employees do not know what their responsibilities are. After all, it is human error that poses the greatest risk to personal data and is responsible for most data breaches.

GDPR has made organisations that process EU citizens' data more accountable than ever before for their handling of personal information. Changes as a result of GDPR can include having data protection policies, data protection impact assessments, and having relevant documents and evidence for regulators on how data is processed. However, changing a company's culture is by far the hardest task. Ensuring the culture remains respectful of data and uses privacy as a brand asset is even more difficult.

As the Information Commissioner, Elizabeth Denham, pointed out, GDPR is not a box-ticking exercise. An organisation can have the best policies available but they need to be understood and used by employees.

A key challenge for privacy teams was how to get staff to care about data protection. One of the best ways was to appoint privacy champions. **eBay** spoke about their privacy champion policy at our Data Protection 2017 Conference. They appointed privacy champions in teams that used data and therefore had hands-on experience. The champions met regularly at social occasions organised by the privacy team and were able to report any concerns they had. This proactive approach created evangelicals for privacy within the company across different departments helping to influence the culture at **eBay**.

Advertising Association (AA) research showed that trust in advertising is in decline, a worrying trend for any marketer. In the 1990s around 50% of the general public had a favourable opinion about the advertising industry. It has dropped to just 25% today.

The DMA is working with **AA's** Trust Working Group to find ways to restore consumer faith in advertising and marketing.

Together with the **AA**, the DMA is working to address concerns raised around the use of personal data with a particular focus on promoting industry awareness and adoption of good data practice. The action plan also sets out support for the **ICO's** campaign 'Your Data Matters' to educate consumers around the role the **ICO** and their rights under GDPR. Ultimately, as the **Trust Working Group** pointed out in their recent report, organisations must become more transparent and give consumers the information they need.

The research states:



“People’s data privacy is important, even though not everybody takes steps to protect it. Sometimes people say it is important, but then do not take the action required. DMA tracking shows that around 50% of the population can be described as ‘pragmatists’ in the use of their data, with 25% ‘fundamentalists’ wanting no third-party use and 25% ‘unconcerned’ about the use of their data.”

In essence, individuals that did not feel that advertising personally benefitted them were more likely to distrust advertisers. People included myriad kinds of marketing in their definition of advertising.

The GDPR requires companies to change their corporate culture, while consumer trust in advertisers is at an all-time low. Companies must seize the day and tirelessly work to engender trust with consumers. The spirit of GDPR is to be upfront and honest with your customers.

The Value of Data

Trust has proved to be a key tenet in the DMA's Value of Data work stream. The campaign born in Scotland – led by DMA Scotland – is joining forces with partners and advocates across the UK to reshape the understanding of the true worth of information.

Personal data is a driver of added value in the economies of developed nations. Knowledge of human behaviour, habits and tastes is a competitive market and one that is driving technological innovation. Machine learning and artificial intelligence allow businesses to process vast quantities of personal data and gain a great deal of insight into their customers. Marketing is becoming ever more finely tuned and efficient as a result. However, with this rapid technological change comes serious ethical challenges. Accountability and responsibility are more important than ever before as businesses must engender trust with consumers. The line between what is acceptable or considered privacy intrusive is evolving and means organisations must be nimble and able to quickly react to the changing needs of society.

The aim of the Value of Data campaign is to help marketers and their customers appreciate the true value of personal data to a business. How do you value data? Once you value it, how do you protect it? **University of Edinburgh** academics Chris Speed and Ewa Luger have written a [whitepaper](#) 'Shifting values: An introduction to the value of data in the digital economy'.

We want to challenge perceptions among marketers and getting them to consider the long-term value of data. Creating long-term value comes from creating a positive culture of respect for data. This is best done by instituting an ethical framework for the processing of personal data.



“GDPR is a positive first step in trying to rebuild trust with customers but if brands want to fully leverage the opportunity, they’re going to have to go way over and above that. Especially as we head into a world that will be more and more governed by algorithms, ethics is one of the biggest areas brands need to get right to build better products, services, experiences and societies.”

Firas Khnaisser

Chair of DMA Scotland, and Head of Decisioning, Standard Life



“There is a dichotomy around GDPR. The DMA’s research identified that most marketers consider themselves to be fully compliant. However, other research suggests that the temptation to do as little as possible remains overwhelming in the pursuit of commercial advantage.

“Similarly, when it comes to whether the consumer experience has improved or suffered as a result of GDPR the results are mixed. Indeed, while the DMA research suggests consumers feel the emails they receive are more focused than before, research by Ipsos Mori for Marketing Week revealed that “just 31% of consumers think their overall experience with companies has improved”. Given this was a key focus of introducing the regulation, this should be a stark warning to brands that now is the time to do more.



“With the Ipsos Mori research revealing that 37% of consumers tend to spend more money with the companies they trust as a result of how they let them control their personal data, there is a clear opportunity for the brands that double down on doing the right thing around customers’ data.”

Mark Evans
Marketing Director, *Direct Line Group*

At the launch of the whitepaper in the Scottish Parliament the Minister for Business, Fair Work and Skills, Jamie Hepburn MSP said:



“We must ensure we operate in an environment in which we have faith. Rarely a day goes by when we see data in the news. But all often, we see data in the news for



negative reasons. But we can help change this by bringing the public with us, through getting the respect for the safe and ethical use of data. Using data ethically isn't a barrier to using data effectively. Indeed, it is a prerequisite for such. It is the only sustainable way of maintaining public trust as the only way to secure the benefits of big data.”

Jamie Hepburn

*MSP Minister for Business, Fair Work and Skills, **Scottish Parliament***

/ Teething problems

GDPR was the biggest shake-up in data protection law in a generation and with such a large-scale change, it was always going to take time for GDPR to become business as usual.

Many organisations have struggled to understand the aims of the GDPR. This is because the law is principles-based and, therefore, companies must carry out risk assessments and make a decision based on their own evaluation of the risks to an individual's personal data. The risk-based approach adopted by GDPR is flexible but has often resulted in organisations not knowing what compliance looks like.

Bad GDPR advice and contradictory legal advice compounded the sense of frustration in the marketing community. It was hard to even know what the right course of action was.

In particular, the marketing sector has struggled with the notion of legitimate interest, how to carry out a legitimate interest assessment (LIA), and have confidence they have gone through the process correctly. Consent is easy, from a legal perspective: either someone says yes or no to marketing. Whereas, legitimate interest is defined by the company, with an individual given the chance to object. Organisations have been reluctant to use legitimate interest for fear of the regulator disagreeing with their assessment.



“GDPR has undoubtedly put privacy and data protection at the forefront of the minds of consumers, advertisers, agencies and ad tech alike. It is clear though, a year on, that a lot of work still needs to be done, as many companies still find the different legal bases for processing somewhat confusing, to say the least.”



Stephen Woodford,
CEO, Advertising Association

Legitimate interest is not the only topic causing confusion. There are growing problems in the world of digital advertising, in particular, regarding the collection of cookies for marketing. Websites usually have a cookie banner that lets individuals know that their personal data may be used for a number of purposes, including marketing. It was known as implied consent. However, under the GDPR consent cannot be implied and must be given by an individual in response to a crystal clear call to action. Digital advertising remains in an odd limbo where the use of cookies does not comply with the law but nothing changes. The advertising funded model of the internet relies on the use of cookies and tracking technology. The **ICO** have formed their own digital advertising taskforce to search for potential solutions.

Case law for GDPR is only just beginning to emerge so our shared understanding of the law and what best practice looks like is going to be constantly evolving, even years from now.

Speaking about how the DMA can help organisations to navigate these challenges, Rachel Aldighieri, DMA Managing Director, said:



“The DMA is undertaking a range of different activities to support its members in complying with GDPR. We are closely working with FEDMA – the trade body for Europe’s DMAs – to create a code of conduct certified under GDPR. This would allow members to more easily exchange personal data, which is especially important for UK businesses with Brexit in mind.

“In addition to ongoing guidance, we will also be showcasing the best case studies from across the industry at our flagship conferences, events, and webinars, and offering GDPR training courses and qualifications via the IDM.



We’re also continuing our positive working relationship with the ICO, which as case law develops may necessitate more marketing specific guidance.”

Rachel Aldighieri
Managing Director, DMA

/ Best practice

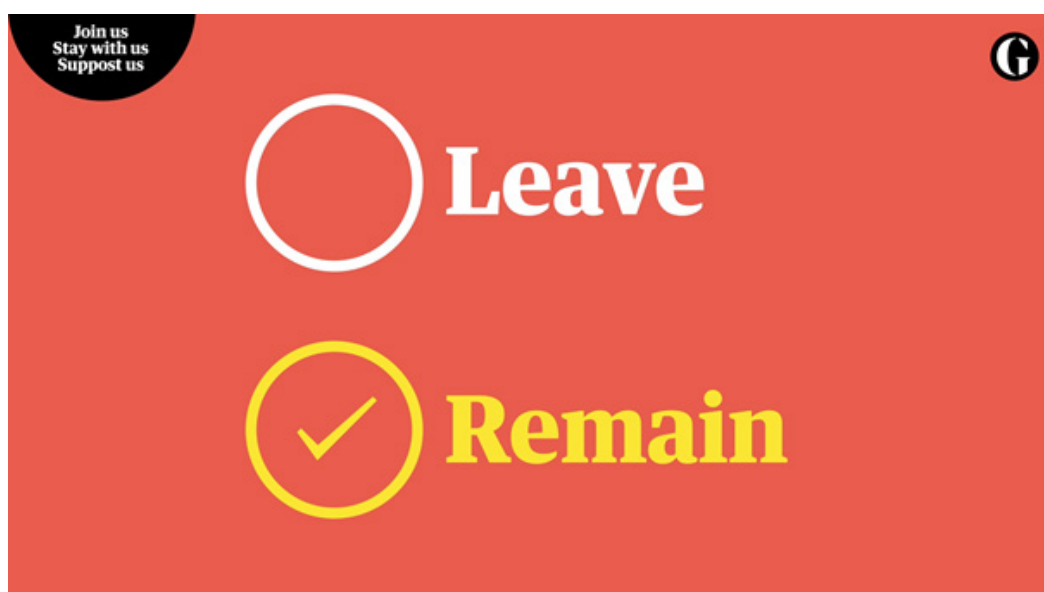
It has only been a year since the GDPR came into force but already there are some incredible case studies in how to make privacy and data protection a brand asset.

Our own best practice is formulated with the help of the DMA's councils and committees comprised of expert practitioners from across the gamut of marketing. Our council structure is focussed upon marketing channel but for GDPR output we are supported by the Responsible Marketing Committee and the Privacy Taskforce.

To generate the right content for the right channels, the DMA Team, Responsible Marketing Committee and the Privacy Taskforce work in collaboration with our Councils. This focuses our work onto the immediate needs of the marketers we serve. Fortunately, the DMA community is rich in GDPR success stories and great examples of marketing best practice in action.

The Guardian won gold at the **DMA Awards** for their GDPR communication campaign that linked issues their readers cared about with the GDPR. For example, they linked opting in to receive marketing from the **Guardian** to voting remain in the referendum. A creative attempt to engage with their readers.

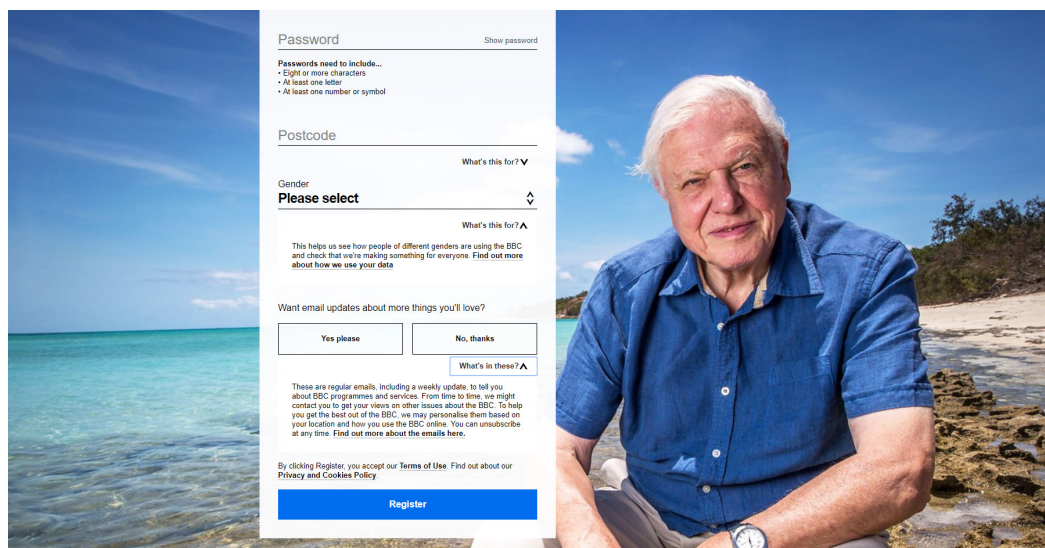
It worked too as readers responded very positively. The campaign exceeded marketing and editorial permissions targets by 110%. Readers were cross-sold onto additional preferences with a third of editorial subscribers signing up to marketing communications. Email click-through rates were strong, with the launch beating industry benchmarks by 226%. Meanwhile, 61% of new reader opt-ins came from channels other than email, proving the effectiveness of an integrated strategy. Some 62% of editorial lists grew compared with pre-campaign levels, as did **Guardian Holidays** which increased by 73%.



One of the greatest challenges has been how best to display data protection information to individuals in a way that articulately and concisely explains how someone will be affected if they share their personal data. This information must be accessible and not simply buried in a convoluted 120-page terms and conditions or privacy notice.

The **BBC** is a great case study on how to layer privacy information. Its privacy policy gives individuals the most important pieces of information straight away and offers more detail at a different stage. For example, the **BBC** is careful to explain why they need personal data from people registering on their website. It is not necessarily obvious to someone why they would need to tell the **BBC** their gender and age to access content. It pays to explain these things to people.

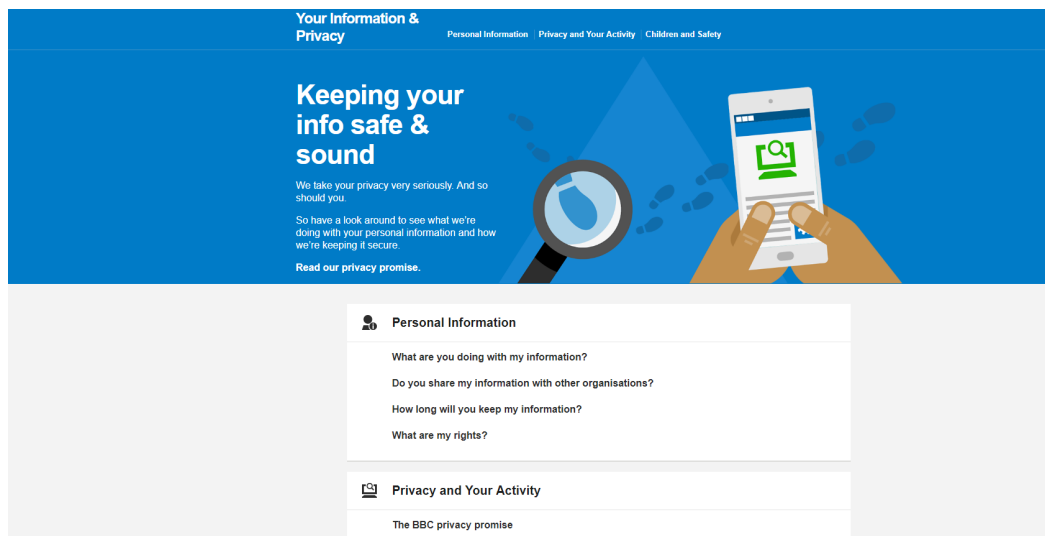
The **BBC** uses dropdown boxes to explain why they are requesting someone's personal data:



The image shows a registration form from the BBC website, overlaid on a background photograph of David Attenborough sitting on a beach. The form includes the following sections:

- Password:** A text input field with a 'Show password' link. Below it, a note states: 'Passwords need to include...' followed by a bulleted list:
 - Eight or more characters
 - At least one letter
 - At least one number or symbol
- Postcode:** A text input field with a dropdown arrow icon.
- Gender:** A dropdown menu with the text 'Please select' and a dropdown arrow icon. Below the menu, a note explains: 'This helps us see how people of different genders are using the BBC and check that we're making something for everyone. Find out more about how we use your data.' There is a 'What's this for?' link with a downward arrow.
- Email updates:** A section titled 'Want email updates about more things you'll love?' with two buttons: 'Yes please' and 'No, thanks'. Below these buttons is a 'What's in these?' link with an upward arrow.
- Footer:** A small note: 'These are regular emails, including a weekly update, to tell you about BBC programmes and services. From time to time, we might contact you to get your views on other issues about the BBC. To help you get the best out of the BBC, we may personalise them based on your location and how you use the BBC online. You can unsubscribe at any time. Find out more about the emails here.' Below this is a link to 'Terms of Use' and another to 'Find out about our Privacy and Cookies Policy'.
- Register:** A prominent blue button at the bottom of the form.

If you click on the link in the dropdown boxes, you are taken to a more detailed area of the **BBC** website. This new section has more detailed information about people's rights, who the **BBC** share your personal data with, and their privacy promise. They use videos and infographics but, crucially, the same tone of voice is maintained between the registration process and the more detailed website section.



The BBC Privacy Promise

Layering your privacy information is key and ultimately what your customers want from you. People want to be able to quickly find out how their personal data will be used and take control of that relationship. Companies that make it as easy possible for their customers to take control of their data will be rewarded with longer and more fruitful customer relationships.

Layering privacy information has been one of the most important lessons for marketers. In the past, many businesses used a privacy notice to ensure they were protected from legal challenge and not to inform consumers. However, marketers have realised that privacy notices are another opportunity to engage with customers and highlight brand values.

There is no need for privacy information to be explained in a turgid and strict legal sense because if you layer information, you can highlight what is most important to your customers. Most of your customers will not want to read a full privacy policy but they will likely want to know whether you will use their personal data for marketing or whether you share it with other organisations. Giving individuals this information first creates trust and demonstrates an organisation's commitment to the spirit of GDPR.



“We should not forget that the GDPR was brought into force with the primary aim of putting individuals front and centre when it comes to the gathering and use of their personal data. This focus is encompassed in the twin pillars of Transparency and Accountability. Brands that embrace these pillars naturally, as an integral part of their DNA and not as an afterthought, will be the brands that thrive in an increasingly competitive, data-driven world”

Fedelma Good,
Director of Data Protection Strategy, PwC



/ Enforcement

Google was fined €50 million by the French data protection authority (**CNIL**) because the company failed to comply with the transparency and information requirements of the GDPR.

The landmark case is the first large fine issued by a data protection authority under the GDPR.

The decision was specifically in relation to **Google's** Android operating system. The **CNIL** ruled that the privacy policy for Android was not clear, with users unable to find concise information about the use of their geolocation data and for targeted advertising.

This is not the first time that the use of geolocation data has been raised by the **CNIL**. In a 2018 enforcement action against **Vectuary**, it ruled that users of an app were not made aware of the fact that the app would collect their location data. The **CNIL** required **Vectuary** to delete the data that they had illegally collected. **Google** could have a similar ruling imposed upon them.

The use of geolocation data was particularly important to the development of this case. The **CNIL** judged that geolocation data presents a far greater level of risk to an individual's data protection rights. This is because **Google** would be able to make accurate inferences about someone, which in some circumstances means they were processing special categories of data. For example, if an individual's device was being used from inside a church every Sunday then their religious belief could be inferred.

Consequences of this nature were not made readily available in the privacy notice and processes were not explained in detail or in terms that users would readily understand.

Furthermore, the legal basis that **Google** was relying on for the use of the data and for targeted advertising was not clear. The lack of clarity around the legal bases was an aggravating factor in the case.

The use of pre-ticked boxes was criticised by the **CNIL**, who found that consent to receive targeted advertisements was not on the main sign-up page for Android and was, in fact, pre-ticked. In effect, users were already opted-in to receive targeted marketing. However, GDPR states that consent cannot be implied and explicitly bans the use of pre-ticked boxes as a method for gathering consent.

Google will almost certainly challenge the decision and will likely claim that they had tried to make information readily available to users and will clarify their legal basis for a number of different processes.

The case has brought wider issues into the limelight and importantly the tension between the advertising-funded model of the internet and data protection rights. People often expect to use a myriad of online services for free, in most cases exchanging their personal data in return for using a service. If regulation makes this business model unworkable then far more online services will become chargeable. This tension is one that regulators have fundamentally failed to address so far.

The principles raised in both of the **Vectuary** and **Google** cases could be applied to many other organisations involved in digital advertising. They must take heed and aim to improve transparency with their customers and users.

Unfortunately for **Google**, it may face similar enforcement action from other data protection authorities (DPA) as this case was not carried out under the one-stop-shop mechanism. Although **Google** does have its European headquarters in Ireland, the **CNIL** and **Irish DPA** ruled that **Google Ireland** did not have responsibility for the Android operating system which the enforcement case was against. **Google** may well receive more fines in the coming months.

There have been other cases emerge but this was by far the most significant. The tech giants look to be under increasing scrutiny as a result of GDPR, with regulators unafraid to mount fresh enforcement cases.

Information Commissioner, Elizabeth Denham, has warned against complacency as GDPR is an ongoing obligation and one that still requires plenty of work as case law and our shared knowledge evolves.

Many of the more well-known enforcement cases in the UK have been for data protection breaches under the old law, the Data Protection Act 1998. It takes time for regulators to build cases and gather evidence so there was always going to be a degree of overlap in the first year or two.

For example, in October 2018 the **ICO** imposed a £500,000 fine on **Facebook**, the maximum penalty under the old Act. Their investigation found that between 2007 and 2014, **Facebook** processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had.

The case arose from the furore surrounding **Cambridge Analytica** which created a dataset for political advertising services from Facebook apps as described above. **Cambridge Analytica** was thought to have unduly influenced the political process in the UK because the personal data used for their campaigns had been gathered illegally.

Looking to the future, the use of machine learning and artificial intelligence in marketing will pose fresh challenges. Ethical frameworks for the use of these new technologies will have to be developed to ensure their responsible use.



“The fourth industrial revolution – the data revolution – is driving technological and societal change at an extremely rapid pace. The data and marketing sector is at the forefront of that revolution. It is difficult for regulators to keep up to pace with change and so organisations must help ensure that the right balance between privacy and innovation is struck. Industry solutions in the form of ethical frameworks and best practice guidance must be adopted by marketers.

“The DMA-ISBA advertising technology taskforce is to foster a consensus for what brands need from the digital advertising ecosystem. Industry must work together to create solutions for challenges that affect us all. Businesses must be proactive in the new GDPR era and work together.”

John Mitchison,
Director of Policy and Compliance, DMA



/ Technology

The fourth industrial revolution has resulted in huge technological changes. Innovations in data and technology are the main drivers of economic growth in the UK today. GDPR sets the parameters in which these new technologies will develop.

However, it is becoming increasingly clear that GDPR alone is not sufficient to deal with the societal questions posed by new technology. The distinction between the online and offline worlds is becoming increasingly blurred and as it does so people are ever more connected to the technology they use.

It is easy to view technological change with suspicion, as policy makers often do, but it also offers the opportunity for profound social good too. Artificial intelligence may drive efficiencies and help flag new trends that humans have missed, such as the power to transform healthcare or to create highly targeted marketing.

Highly targeted political advertisements could potentially undermine people's rights if the artificial intelligence was unfairly nudging people towards a particular political decision. The **Cambridge Analytica** and **Facebook** scandal shows how sensitive the area of political advertising can be.

Marketing more broadly is also susceptible to sometimes overstep what many consumers may consider reasonable or fair. People may find those very precise insights about their behaviour to be overly intrusive. There is no law that gives detailed instructions, rather these are philosophical questions that marketers, individuals and whole societies are navigating, often haphazardly.

This is where ethics come in and must be used to ensure the fair application of new technology, like AI. What are the fundamental ethical principles that should inform the development and use of AI? These are big societal questions and ones that need to be thoroughly debated.



“Across the business community, GDPR has sparked a mindset change in how firms approach data privacy. The race for compliance has evolved into a focus on embedding privacy as a competitive advantage and driving greater consumer awareness and agency over how their data is used. Looking to the future, GDPR will underpin how businesses build trust in the technologies that will transform the UK economy.”

Felicity Burch,
Director of Innovation & Digital, CBI



The greatest challenge for data and marketing is the use of advertising technology. An area with immense innovation and rapid change. New technology poses new risks but by virtue of it being innovative, it is less well understood and this creates new risks for individuals and for society.

Digital advertising is a prime example of this dilemma. The use of technology to send out advertising online and generate revenue for publishers has developed very quickly and without clear oversight. It has been an organic process but this does not mean that it is in the best interests of individuals or publishers. A fresh look at the advertising technology that underpins the industry is underway and the **ICO** has been leading the way.



“In recent years, technology has completely transformed the way advertising is bought, sold and delivered. Many advertising techniques use people’s personal information, in the form of a personal profile, to decide which advert is delivered to them. Publishers then utilise real-time advertising methods to sell the advertising space.

“The speed, scale and complexity of real-time bidding is both technologically impressive and a cause for concern, but we understand that at the same time, this technology facilitates the sale of advertising space that generates a certain level of income for publishers, and value for advertisers.”

Simon McDougall,
Executive Director for Technology Policy and Innovation, ICO



There are no easy answers to the ethical questions posed by new technology and solutions will only be found as a result of rigorous debate across society. The DMA recognised this but especially how publishers must decide what they need from advertising. Ultimately, it is online publishers that rely on advertising revenue to create and share content online so the advertising ecosystem must work for them.

The DMA teamed up with **ISBA** – who represent UK advertisers – to bring together leading brands to agree a consensus on what to demand from the online advertising ecosystem. There are myriad problems from a brand perspective, the chief one being a lack of transparency and the risk that this lack of transparency may result in them breaching data protection law.

The **ICO** recently led a fact-finding forum of their own so they could understand the often complex world of digital advertising. Only by bringing together stakeholders from across private and public sectors, and consumer groups will a solution be found.

/ Conclusion

One year on from the introduction of GDPR and there are many success stories, companies making privacy a brand asset for them and building trust. However, that is not the whole story and while there have been successes, there has also been confusion and serious challenges. Businesses have often found the GDPR a difficult piece of legislation to grasp and contradictory GDPR advice has not helped the issue.

Overall, consumers are feeling more positive about GDPR, and the DMA's [consumer email tracker](#) found that two in five consumers (41%) say they are more comfortable and confident that brands are handling their data correctly thanks to the introduction of the GDPR. In 2018, consumers believe they received less email than ever before, estimating this at around 57 per week to their personal inboxes – down from 73 in 2017 – and less than half of these (44%) are actually from brands.

The GDPR has been a catalyst for businesses to reconnect with their customers and begin a dialogue around data protection issues. Brands that made privacy a brand asset are already starting to engender a greater level of trust with their customers. One of the key motivators for GDPR in the first place was waning consumer trust and a sense of frustration that citizens had lost control of their personal data.

The majority of marketers reported an increase in email open rates (74% agree) and click-through rates (75%) in the past 12 months, evidence that a more engaged and trusting audience is much more likely to respond positively to marketing.

However, some big challenges hover on the horizon for the data and marketing sector in the UK. In particular, digital advertising is in the limelight, with a number of legal challenges under GDPR claiming the advertising technology is not compliant.

The **ICO** has launched a digital advertising taskforce in response, but its findings will need to be timely and give clear guidance to online publishers who rely on advertising revenues and want to comply with the law.

While there have been many successes over the past year, there are still a great many challenges ahead for the marketers.

The data and marketing sector must continue striving to make data protection a brand asset and building a culture of deep respect for people's personal data.

/ Discover more about GDPR

Latest news and updates

For the latest news and updates, visit the [Responsible Marketing](#) section on our site.

Improve your GDPR know-how

In keeping with our mission, we're working to make sure every marketer is prepared to progress in their careers. Increase your GDPR knowledge with our specially designed [GDPR course portfolio](#), powered by the IDM.

/ Campaign sponsor

About OneTrust:

OneTrust is the largest and most widely used technology platform to operationalise privacy, security and third-party risk management. More than 2,500 customers, both big and small and across 100 countries, use **OneTrust** to demonstrate compliance with privacy regulations including the GDPR, California Consumer Privacy Act, Brazil LGPD, and hundreds of the world's privacy laws.

OneTrust's size and scale allows it to offer the easiest-to-use and most affordable solution for implementing use cases including: Privacy Maturity Benchmarking, Data Protection by Design and Default (PbD), Data Protection Impact Assessments (PIA/DPIA), Third-Party Vendor Risk Management, Incident and Breach Response, Data Mapping (Records of Processing), Customer Preference Management, Consent Management, Website Scanning & Cookie Compliance, Mobile App Scanning, Data Subject/Consumer Rights Management and Policy & Notice Management.

The platform's intelligence comes from DataGuidance by **OneTrust**, an in-depth and up-to-date source of privacy and security regulatory summaries, guidance, templates, case law, and analysis. The database is updated daily by over 20 in-house privacy researchers, along with a network of 500 lawyers across over 300 jurisdictions.

OneTrust's 700 employees are located across co-headquarters in Atlanta and in London with additional locations in Bangalore, Melbourne, San Francisco, New York, Munich and Hong Kong. To learn more, visit OneTrust.com.



/ About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should be done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our [customer-focussed principles](#).

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

/ Copyright and disclaimer

GDPR: A year on is published by the Data & Marketing Association (UK) Ltd Copyright © Data & Marketing Association (DMA). All rights reserved. No part of this publication may be reproduced, copied or transmitted in any form or by any means, or stored in a retrieval system of any nature, without the prior permission of the DMA (UK) Ltd except as permitted by the provisions of the Copyright, Designs and Patents Act 1988 and related legislation. Application for permission to reproduce all or part of the Copyright material shall be made to the DMA (UK) Ltd, DMA House, 70 Margaret Street, London, W1W 8SS.

Although the greatest care has been taken in the preparation and compilation of GDPR: A year on, no liability or responsibility of any kind (to the extent permitted by law), including responsibility for negligence, is accepted by the DMA, its servants or agents. All information gathered is believed correct at May 2019. All corrections should be sent to the DMA for future editions.