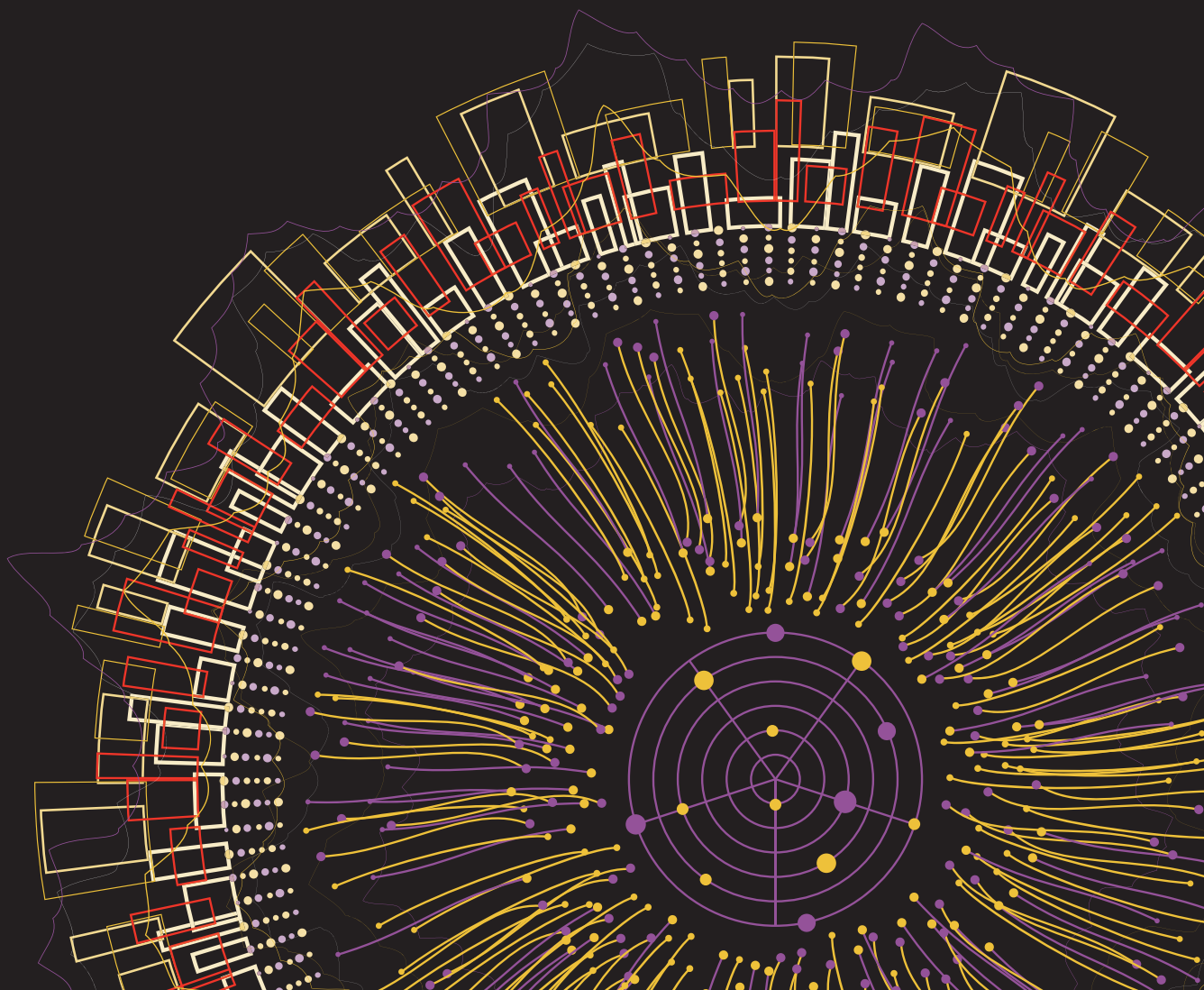
gma© Global Marketing Alliance
INSIGHT FOR DATA DRIVEN MARKETERS

Data Protection Network

OneTrust
Privacy Management Software

Data Impact 2019:

GDPR: 1 year on



Foreword

OneTrust
Privacy Management Software

We are living through a transformative time in privacy. Personal data, big data analytics and artificial technology are being used to solve everything from small daily inconveniences to tackling the world's biggest problems. At the same time, consumers are aware more than ever about the human impact of abuse or over-use of their personal data.

Adhering to data privacy regulations like the GDPR is no longer just a checklist compliance item, but instead a moment where businesses can be transparent about data collection and build customer trust that they will use and process data in a responsible manner. The GDPR was a moment in time where the world collectively had a conversation about privacy, and today we are seeing the results of this dialogue.

Countries and regions across the globe are proposing and passing similar data privacy legislation, while companies are continuing to innovate and users are still consenting to the responsible use of their data.

OneTrust is proud to sponsor the Global Marketing Alliance and the Data Protection Network on the Data Impact 2019 report highlighting the importance of a sound data strategy. As the world's leader in privacy, security and third-party risk software, OneTrust provides the technology for companies to deliver transparency and trust to their consumers as well as reporting to regulators with the GDPR and other global privacy laws.

Together with partners like the Data Protection Network and the Global Marketing Alliance as well as our base of 2,500 customers, we are enabling business innovation and consumer trust in this transformative time in privacy, delivering solutions to help solve the world's problems, both big and small, with the fair and responsible collection and use of personal data. To learn more about how OneTrust can help operationalise privacy, security and third-party risk programs, visit **onetrust.com.**

Ian Evans Managing Director, EMEA OneTrust

gma© Global Marketing Alliance
INSIGHT FOR DATA DRIVEN MARKETERS

OneTrust
Privacy Management Software

Contents:

Introduction

The introduction of GDPR forced organisations of all sizes to reassess their procedures for gathering, using and storing personal data. The scramble towards compliance as May 25th approached proved that many were unprepared for the new obligations placed upon them and were struggling to comprehend the appropriate course of action.

So where are we now?
For those organisations responsible for personal data, gaining a clear understanding of what constitutes GDPR compliance has posed an ongoing challenge. The **ICO themselves admit** that GDPR does not set a checklist of rules which can simply be ticked off:

"Every organisation is different and there is no one-size fits-all answer. Data protection law doesn't set many absolute rules. Instead it takes a risk-based approach, based on some key principles. This means it's flexible and can be applied to a huge range of organisations and situations, and it doesn't act as a barrier to doing new things in new ways."

In this report, we'll explore what we've learnt about data governance and GDPR since it came into force by drawing on insights from key GDPR rulings, the expert view of data protection consultants and the first-hand experiences of organisations which use data extensively.

Finally, we'll consider how Brexit and the upcoming ePrivacy regulation may –
or may not – impact on the way that marketers and organisations handle data.

GDPR-in-action: key rulings so far

An initial period of leniency followed GDPR's enforcement with regulators seemingly giving organisations extra time to get their data processes in order. But now, one year on and several enforcements later, what have we learnt about GDPR and its enforcement?

Though regulators across Europe have begun showing their teeth, the scare stories surrounding GDPR have so far proven to be false. Those who ignored the click-bait headlines and instead paid attention to the mundane yet significant reassurances of the ICO should be unsurprised.

The ICO's Information Commissioner, Elizabeth Denham, **outlined back in 2017** that although maximum fines would be increased, their preferred approach would remain guiding, advising and educating organisations - as was previously the case under the Data Protection Act 1998.

Nonetheless, GDPR is designed to better protect the rights of citizens and their personal data. 'Business as usual' is not its objective. So keeping track of how it's being implemented is important for all CMO's and organisations.

Here we'll detail some of those key rulings which have helped us move us towards a better understanding of what we – as businesses that handle personal data - ought to be doing.

Rulings and investigations

6 July 2018 – AggregateIQ enforcement action by the ICO

Case summary: The **first ICO action** came against AggregateIQ, a Canadian firm which had provided data services to organisations campaigning for the UK to leave the EU. It was accused of misusing individuals' personal data by processing it in a way that the subjects were not aware of, for purposes they would not have expected, and without a lawful basis for doing so. Furthermore, the processing of the data was not in line with the purposes for which it was originally collected.

Action taken: The ICO's July notice ordered AggregateIQ to stop processing any EU or UK citizens' personal data for the purposes of data analytics, political campaigning or other advertising purposes.

It also gave the company 30 days to 'audit, assess, implement and document' its data processing practises or potentially face the maximum GDPR fine of £17 million or four per cent of annual global turnover. Those 30 days are set to commence after the Canadian regulator completes its separate investigation of AggregateIQ's privacy practices.

Dispute: AggregateIQ has appealed against the verdict arguing that the ICO has no jurisdiction over them as a Canadian company and that it wrongly applied GDPR to alleged conduct which took place prior to the regulations coming into force. Furthermore, AggregateIQ argues that the action blocks them from working in Europe which is disproportionate to the alleged offence.

Key takeaways:

1. If the ICO believes data has been improperly accessed or used from individuals in the UK, it will seek to bring companies to account wherever they are in the world.
2. Brands should ensure third-party providers of data services are GDPR compliant - or risk reputational damage.
3. Personal data must be must be collected in a transparent way and for a specific and legitimate purpose.

The ICO's enforcement notice was rather short in detail. Expect more information to come to light following the Canadian regulator's investigation and AggregateIQ's appeal.

Rulings and investigations

21st January 2019 – Google fined £44m by French regulator CNIL

Case Summary: French regulator **CNIL adjudged that Google** had "not sufficiently informed" people about how they collected data to personalise advertising. The regulator said Google had not obtained clear consent to process data because "essential information" was "disseminated across several documents".

Action taken: Google was fined £44m for the infringement. The severity of the fine hung on several factors. Firstly, a vast amount of revealing data could be gathered about individuals' private lives across multiple services in "almost unlimited combinations." Secondly, these violations were continuous and ongoing; not the result of a single event or action. Finally, the number of French citizens exposed raised the significance of the breach. Google are set to challenge the decision.

Key takeaways:

1. Transparency matters: The more difficult you make it for users to understand how their data is being used, the less transparent your processes, and the bigger the GDPR breach.
2. Consent requires action: GDPR requires an unambiguous and "clear affirmative action" from an individual to indicate consent, which precludes the use of pre-ticked settings for example.
3. Be specific: Wrapping up multiple "consents" into a privacy policy and other hard-to-access documents fails to meet the GDPR's requirement for separate consent requests for each specific processing purpose.
4. Google (and other companies) have assumed that "needing" this data to carry out their business would be accepted, at least in the short term. The regulator does not concur.

9th November, 2018 – CNIL ad network 'consent' ruling

Case Summary: The **CNIL issued a formal warning** against ad network company Vectaury for illegally gaining the consent of 67 million users. There were four elements to this:

1. When downloading applications, users were prompted to give consent for the processing of geolocation data, but not explicitly told what it would be used for.
2. When the app was launched, the information displayed to users was too complex, unclear and imprecise. Users were not informed of the identity of the companies with whom their data would be shared before being prompted to make a choice - unless they searched around for this information.
3. Data processing purposes were pre-ticked to "accept" by default.
4. The use of personal data from bid requests was not consented to until after it had been used for advertising profiling.

Action taken: The CNIL ordered Vectuary to change its consent practices and delete all data collected from the invalid consent previously obtained. It has been given three months to comply. Failure to do so may result in a fine.

Key takeaways:

1. Built-in mobile app consent prompts are not sufficient for consent
2. Specific and easily understandable information must be provided before a user is prompted to express a choice.
3. A list of all third parties with whom the data may be shared must be shown to the user in a clear and easily accessible way before he/she is prompted to make a choice (hyperlink or hover over)
4. Consent of the user must be given by an affirmative action

A more in-depth analysis of this case can be found here.

Rulings and investigations

22nd November 2018 – LfDl ruling on Knuddels.de

Case Summary German state regulator **LfDl fined social media company Knuddels.de** after hackers stole personal information, including emails and passwords from approximately 330,000 users.

Action taken: Knuddels.de were fined €20,000 by LfDl on account of storing passwords in plain text. This ran against GDPR's requirement to encrypt and pseudonymise personal data (ensure data is not linked to an identifiable person). The relatively small fine was due to the company's swift action in notifying the appropriate authority and taking the necessary action to tighten security.

Key takeaways:

1. Encrypt passwords: passwords must be stored encrypted - not in plain text.
2. Respond quickly: Knuddels.de's swift response - in reporting the breach and tightening security procedures - minimised the fine
3. Be transparent: It wasn't just the speed of their response, but also the transparent way the company cooperated with the LfDl.
4. Proportionate fines: The small fine also took into account the financial burden placed on the company.

Other recent data protection rulings outside of GDPR

1st February 2019 - £120,000 combined fine for Leave.EU and Eldon

Case Summary: The **ICO issued fines** to campaign group Leave.EU and Eldon Insurance after breaching UK's PECR (Privacy and Electronic Communications Regulations 2003) which governs electronic marketing. The personal details of insurance customers were used for unauthorised political messaging, while Leave.EU subscribers were targeted by the insurance company.

Action Taken: The ICO issued fines totalling £120,000 'for serious breaches of electronic marketing laws.' The ICO investigation found that Leave.EU and Eldon Insurance were closely linked. Systems for segregating the personal data of insurance customers from that of political subscribers were ineffective.

This resulted in Leave.EU using Eldon Insurance customers' details unlawfully to send almost 300,000 political marketing messages. Leave.EU has been fined £15,000 for this breach.
Eldon Insurance carried out two unlawful direct marketing campaigns. The campaigns involved the sending of over one million emails to Leave.EU subscribers without sufficient consent. Leave.EU has been fined £45,000 and Eldon Insurance has been fined £60,000 for the breach.

Key takeaways:

1. Data segregation: when data has been gathered separately, and for a specific expressed purpose, it must be stored securely and without risk of being mixed up with other unrelated subscriptions.
2. Consent: individuals must give appropriate and clear consent for the email and SMS communications they receive.

Rulings and investigations

7th February 2019 - Bundeskartellamt rules against Facebook's plans

Case summary: The German competition authority, Bundeskartellamt, investigated how **Facebook merged user data** across its own platforms: Messenger, WhatsApp and Instagram. While this action wasn't taken under GDPR, it further clarifies how businesses should (or should not) gain consent for merging personal data across separate platforms.

Action taken: Facebook were banned from combining data across Messenger, WhatsApp and Instagram without users' providing voluntary consent. Consequently, individuals cannot be forced to provide consent as a precondition for setting up a Facebook account.

Key takeaway:

1. Consent: Once again the issue of consent is central to a case. An individual cannot be forced to provide consent for their data to be used across platforms.

GDPR: the industry experience since 25 May

In this section we set out to provide a comprehensive overview of how the industry has adapted to GDPR since its inception.

So what has been the industry's experience since GDPR's inception? How have they managed the process of becoming compliant? And what constitutes best practice now and in the future?

While the sky hasn't exactly fallen in since GDPR came into being, it's certainly had a significant impact on the data marketing industry. The difficulty of achieving compliance and the administrative burden it has placed upon businesses, is a familiar pain point. What's more, the job is never done: compliance is an ongoing challenge which requires robust processes across the whole organisation and not simply within a marketing department.

The industry is continuing to find its way when it comes to the broad issue of data ethics. Uncertainty will continue for some time yet, particularly with the ePrivacy Regulation continuing to loom on the horizon. Those organisations which continue to seek a tickbox approach are likely worst-placed to meet the data governance challenge. While a proactive 'customer-first' approach represents the best course of action. This issue is effectively summarised by Jed Mole, Vice President Marketing at data specialists **Acxiom** suggests that the increased importance of data governance propels the need for a dedicated 'Data Strategy':

"Companies have business strategies, sales and marketing strategies, facilities, IT strategies and more. But today, data and customers are symbiotic and a strategy to ensure you have the right data - that you manage and use in the right way - one that is underpinned by data ethics, is essential."

The upcoming ePrivacy Regulation provides further evidence GDPR isn't an end in itself. It's designed to be the start of a new dawn for digital marketers and citizens where the latter takes back control of their personal data and organisations are tasked with making it thus.

In many ways, the journey has only just begun.

GDPR compliance: Common problems and misinterpretations

Mix-ups and misunderstandings

The misunderstanding of GDPR by marketers and organisations is a common theme when discussing its short-term impact with data marketing specialists. In the lead up to - and in the immediate aftermath of - GDPR's enforcement, this misunderstanding lead to widespread panic in the industry. Tabloid headlines and hyberbole no doubt exacerbated a sense of paranoia and drove many companies to go above and beyond requirements and hinder their own marketing efforts in the process.

The response has been classic baby and bathwater: ceasing direct mailing and purging all personal data in order to be absolutely sure of compliance.

"The most radical measures by clients have been to stop their direct mailing or email marketing activities for prospecting completely for a certain period to avoid any risk. Of course, this led to a lack of new customers for them. The panic caused by the potentially high fines has been dominating their decisions, although the way they acted before would still have been legal under GDPR."
Stephan Merz, D2M.

The wholesale jettisoning of user data by companies in a rush to become compliant was worryingly widespread. Internal research by data specialists **1PlusX** found eight out of nine market leading data management platforms (DMPs) conflated the exercise of consumers' GDPR Opt-out with Data Deletion rights. Consequently whenever they received an opt-out request from a user, they also deleted their data.

Multiple surveys in the lead up to, and in the immediate aftermath of GDPR's enforcement, reflected the struggle towards compliance. So it should hardly come as a surprise that marketers took a safety first approach. For example:

- **Research** by TransUnion showed that only 50% of marketers felt confident they were compliant by 25 May and 23% removed nearly a quarter of records in an effort to be compliant.
- An August 2018 survey by **Dimensional Research** highlighted that only 20% of UK companies surveyed believed they were GDPR compliant, while 53% were in the implementation phase and 27% had not yet started their implementation.
- 40% of organisations **reported** not being compliant according to Cisco in a January 2019 data privacy study.

The overall picture shows that achieving compliance remains an ongoing project and a degree of self doubt remains.

Inevitably, marketers are improving their understanding of GDPR and progressing on the path towards compliance. The number of marketers who have received GDPR training has risen by more than **30%** in the last year according to data driven industry body, the DMA. In the DMA's September 2017 survey only 58% of marketers had received GDPR training but fast-forward to September 2018 and that number has risen to 89%.

In many ways this reflects how companies have been sluggish to get to grips with GDPR, and how the date of its enforcement has focused minds.

The biggest compliance challenges

What have been the biggest challenges for marketers and organisations as they strive to become GDPR compliant?

In our discussion with data professionals we discovered that the administrative burden was, unsurprisingly, top of the list. But digging deeper we can see there are four main elements to this:

- The rise in SARs (Subject Access Requests)
- The need to update data processing protocols
- The ability to adapt to different jurisdictions
- The ability to understand and interpret the legislation correctly

The rise in SARs remains one of the biggest single challenges provided by GDPR. While an individual could make a request before GDPR, the £10 charge dissuaded most people. However, now they are free of charge it has led to a rise in SARs - and businesses are struggling to keep up with demand. **Research by Talend** revealed that 70% of companies surveyed couldn't fulfill data access and portability requests within the GDPR-specified one-month time limit.

GDPR presents a question over efficiency. If someone requests access to their personal data, businesses are required to pull everything together within one calendar month. Meanwhile, if there's a data breach which poses a risk to an individual's privacy, businesses must inform the ICO of the breach within 72 hours. Time is of the essence.

Luke Godfrey, Head of Marketing at **Adare SEC**, confirmed that companies have reported an increase in SARs since the enforcement of GDPR:

"...It can be very time-consuming for an organisation to collate all the necessary information, especially larger organisations when this is multiplied by hundreds of customers with documents in multiple locations. Imagine all those hundreds of thousands of documents to trawl through – it would be a very time consuming task, especially if you are hit with numerous SARs in one go."

The increase in SARs - along with the general increased consumer understanding of their data privacy rights - has been the biggest impact of GDPR so far, according to Lorcan Lynch MD at **lead generation experts** DataXcel. Yet he's positive about its implications describing it as a "good thing for the industry":

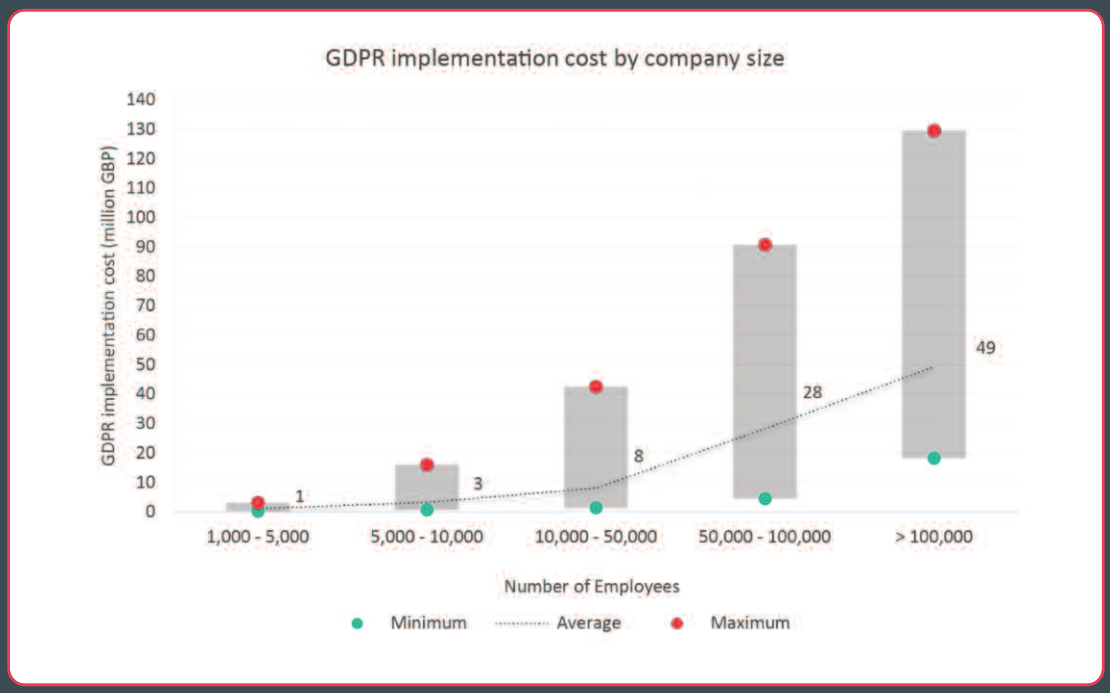
"It enables data controllers to receive both positive and negative feedback on the methods they use to process data which in turns assists us to further shape our data marketing strategies going forward."

SAR requests are just one aspect of the heightened administrative burden placed upon marketers and organisations by GDPR. Putting together the correct data processing protocols, across the organisation can be a costly - and confusing - exercise. It reiterates the importance of correctly understanding the legislation and how it relates to your specific business processes.

In other words, drawing correct guidance. Unfortunately, this is not as easy as it should be, with phoney advice a regularly reported concern. GDPR requires costly and time-consuming changes to data governance frameworks for many organisation. If those changes are based on poor or bogus advice, then that cost is exacerbated. The larger the company, the greater the scope of the compliance challenge and subsequently the higher the cost.

This graph from **SIA partners** reflects how the cost of implementation rises according to the size of the company:

GDPR compliance: Common problems and misinterpretations



A lot of money is being spent on GDPR compliance and it has created a hugely profitable industry. But amidst the sound advice and trusty assurances; not all so-called 'data protection experts' are necessarily fitting of the title.

"...There is so much conflicting advice out in the marketplace. A whole new industry has sprung up capitalizing on the fear around compliance especially from those making a lot of money from it, such as consent platforms, consultancies, lawyers etc, that it has created a confusing landscape, which has resulted in an abundance of expenditure and caution. The DMA UK and ICO have tried to temper this by distributing solid, business friendly information, but the data market has suffered immeasurably, and numerous clients have been challenged to implement and manage GDPR effectively."
Karie Burt, Vice President International at **multi-channel marketing solutions provider MeritDirect.**

As we can see, sourcing appropriate guidance was clearly a key part of the compliance challenge right from the beginning. This emphasises the danger of simply relying on third parties for guidance, and the need for individuals and companies to attain a certain level of GDPR knowledge themselves.

The right(eous) path to GDPR compliance

Approach the issue 'customer-first'
Because there is no tick-box solution to GDPR, it requires organisations to ensure they understand - and are committed to - embracing the spirit of the law, not just the letter of it. This has been described by Marketo as taking a **marketer-first** rather than legal-first approach. It entails putting the customer at the heart of the compliance strategy and according to Marketo's research it pays off: 72% of those who put the customer front and centre say they expect to exceed target this year, opposed to just 28% who approach it as an exercise in legal compliance.

Make data protection a key part of your corporate goals and training:
Formulate a dedicated data strategy to sit alongside the other key business strategies. Debbie McElhill, Associate at **data protection** consultancy Opt-4 stresses the growing need to take data governance more seriously:

"Make data governance a key priority, get it on the boardroom agenda as part of the customer strategy, and keep educating your people, be creative in how you do that. If your business is unfortunate enough to become the subject of an ICO investigation, then you can bet they will ask you how you trained your staff and will want to see evidence of that training. Having a sound data governance framework requires you to fully train everyone in the organisation who processes personal data. Looking after individuals' personal data compliantly needs to be embedded as part of your company culture, it needs to be second nature for your people, just like great customer service should be."

Be proactive and diligent - continually:
The job of compliance is never done, so the need to keep abreast of legislative changes and update training and processes where appropriate will continue. Those who create an ethical data driven culture, which places the needs of consumers and individuals first, will be better able to adjust to legislative changes as and when they occur.

Take ownership of third-party data providers:
Third parties are often the weakest link in a company's data security, and were implicated in about 63% of all data breaches pre-GDPR. Some of the largest financial penalties for data control failures were a consequence of third party actions.

Due diligence of third party providers is now key, as Ian Evans, VP at **global data protection specialists, OneTrust**, explains:

"You now have the obligation to ensure that the people you contract with - and who undertake processing on your behalf - are also going to represent you and your views on privacy as well."

The question you need to ask is: do they have the right processes in place to be GDPR compliant?

Take the time to understand GDPR for yourself:
Whether or not you decide to employ an expert data protection consultant, equipping yourself with a solid understanding of GDPR (and future privacy legislation) remains important. Those who had a basic grasp of GDPR and how it would be applied, would have avoided the unnecessary purge of data and abandoning of marketing activities which took place on 'G-Day'. The ICO provides a useful **self-assessment toolkit.**

GDPR compliance: Common problems and misinterpretations

Emphasise quality customer data over quantity:
Even without GDPR fines, poor quality data hits the bottom line. Marketers recognise this, estimating the **average cost of poor quality customer data at 6% of annual revenue**. For major brands this is measured in millions of pounds – and even this may not be the complete picture. Poor quality data impedes overall marketing performance, impacts response rates and reduces conversion rates, making the overall cost potentially much higher.

Put efficient processes in place:
Time is of the essence - particularly when individuals make data access requests under SAR or a request to erase data. Therefore, having efficient processes in place is vital. It may require upfront costs but it will pay off long-term:

"As a third-party processor of data, we needed to put significant engineering resources into working on the ability to erase individuals' data across our system in order to comply with the Right To Be Forgotten for our customers. This was the primary problem for tech companies with the introduction of GDPR - technology is innately designed to store data, and deleting it in compliance with GDPR was far more complicated than simply removing a contact. Compliance with GDPR is antagonistic to most of the security and reliability objectives of companies - so we, among many other companies, had to input a process so we can laser-focus delete individuals' data, contact info, etc".
Nina Church-Adams, Senior VP of Marketing at **Act-On Software.**

GDPR's impact on marketing efforts

Apart from the deletion of contact lists and other data sets, how else has GDPR impacted marketing efforts? While there's a range of views expressed by marketers, there have been a number of general trends which have been reflected by our discussions with the data marketing community and as revealed by a number of studies.

Short-term damage to sales efforts
Deleting contacts unnecessarily and wrongly translating opt-out requests as a demand to delete data, has undermined efforts to drive sales at many companies. In this respect, it can be argued that GDPR wasn't to blame but instead a combination of misinformation, misunderstanding and, perhaps, lack of thorough preparation. (Though clear guidance from the ICO was slow in coming.)

However, there are other ways that GDPR has damaged sales efforts short-term. For example, direct marketing efforts have taken a big hit:

"...It is a more challenging market as a lot of brand owners have reduced their use of external data for DM campaigns as they are not sure if they can use it or not but this hopefully will become clearer in 2019 and the market should regain momentum with the credible data providers that are left operating in the marketplace."
Lorcan Lynch, MD at **DataXcel**

"The short-term impact on the marketing industry has been mainly negative directly after GDPR was in effect. In addition to the temporary suspension of any direct marketing activities, another good example is the tons of emails received to reconfirm subscriptions for newsletters. By doing so, many companies "burnt" a high percentage of their email lists without any need. Some reported of reconfirmation rates between 10 and 20% only and thus lost the majority of their mailing lists, although they had collected opt-ins fully compliant with GDPR before already."
Stephan Merz, Founder, d2m.

More than half of marketers (57%) believe that the new laws create a more difficult sales environment, while just 10% say it will make it easier, **according to the DMA's latest report.**

GDPR compliance: Common problems and misinterpretations

A shift to higher quality contacts
While contact lists have shrunk short-term, and the need for compliance has somewhat shifted CMO's laser guided focus on sales and company growth for now; GDPR has forced companies to take a more qualitative approach to their marketing efforts. While a high volume of contacts looks great on a database, and marketers get a warm fuzzy feeling as the numbers grow; it's ultimately the quality of leads which really matters, and there are some signs that GDPR will force a change in mindset which will inform sturdier marketing models geared towards real strategic growth rather than eye-catching metrics.

This view is best articulated by Debbie McElhill, at **Opt-4**: "The assumption that a vast database equals lots of valuable marketing contacts doesn't carry as much credence any longer. With the principle of data minimisation, GDPR provided the impetus for many organisations to examine their legacy databases and it was not uncommon to find that these customers or prospective customers had not opened an email, responded or in any way engaged with the brand for many years.

"I think one of the key learnings has been to look beyond the headline numbers and take notice of how engaged your customers really are. Traditional marketing KPIs, for example, conversion rate to sales, average order value and channel attribution, that show what works and what doesn't, had been a little neglected in the world of digital marketing. Many brands are now returning to these fundamentals as they respond to the challenge of rebuilding their marketing databases that may have been reduced significantly following pre-GDPR re-permissioning exercises.

"We are finding that the more creative, forward thinking organisations, many of which have long embraced data privacy as an intrinsic part of good customer practice, are finding that they are having success with more targeted campaigns to smaller but better engaged customer audiences. These audience are spending more of their time and money with the brand.

Organisations exhibiting best practice are enriching their relationship with customers by introducing innovative ways to collect marketing permissions, gathering insight via customer preferences and behaviours using many different customer touchpoints - not just at the point of sale."

No doubt some marketers who are struggling to get to grips with compliance will find it difficult to look beyond the short-term damage, such as shrinking leads and a time-consuming administrative burden.

Industry surveys reflect something of a divide between business leaders and marketers, perhaps because leaders are more likely to see the longer-term picture amid a wider corporate strategy.

Research commissioned by Ricoh Europe, based on a survey of 2,550 business leaders from across 24 countries, shows a shift from the traditional mindset that regulation is a bottleneck and barrier. Over half (52%) agreed that regulation is an enabler in the digital age – a sentiment echoed further with 55% seeing privacy regulations, such as GDPR, as a basis from which to achieve organisational success.

However, **according to the DMA** only 32% of marketers believe the long-term benefits to their business will more than make up for the cost of complying. Clearly those that have directly felt the impact of GDPR on their day-to-day activities are not so positive. Yet perceptions are shifting as this number has doubled since April last year when the figure was just 16%. Meanwhile those believing the effect will be negative has dropped from 56% to 41% over the same period.

These are still early days. Uncertainty still exists and the short-term hit on data sets and outreach activities will understandably inform marketers' perceptions. As a new data culture evolves and the short-term upheaval subsides, it may be expected that positive sentiment will increase. At which point they may have ePrivacy Regulations to worry about instead.

ICO enforcements: how worried should you be?

The ICO is more than just an enforcement body; it's also there to offer guidance. It already provides a toolkit of advice and guidance and it's set to expand on that with an updated Data Sharing Code of Practice and a **Direct Marketing Code of Practice**. Any organisation serious about GDPR should be continuing to monitor such releases as part of their ongoing 'due diligence' and self-assessment protocols.

While the ICO is still largely in its guidance phase, we should expected to see a gradual shift towards enforcement. To a certain extent, we're still in a 'wait-and-see' period.

The majority of the people we spoke to for this report were not unduly concerned about ICO investigations, certainly short-term. However, those who expressed trepidation highlighted the fear of human error and the need for constant diligence.

"The honest answer for any Data Controller is yes as you feel no matter how diligent you are as an organisation the fear of some data slipping through the rigid compliance process is always possible particularly by an employee."
Lorcan Lynch, MD at DataXcel

However, companies who take all the necessary steps and are striving hard towards achieving a ethical data culture, probably have little to fear from the ICO at this point:

"...We have dealt with the ICO and have found them to be helpful and informative. I do feel this is a great concern for clients due to the negative publicity and the fear of fines, but I think it is important to note that the ICO have been judicious rather than actively handing out fines to all and sundry. I also think it is important that you can demonstrate that you worked hard to fix the issue and are doing your best to uphold the law. That seems to go a long way with the authorities."
Karie Birt, MeritDirect.

John Mitchison, Director of Policy and Compliance at the **DMA supports this view**:

"The ICO has always said that it is a pragmatic regulator and will use its enforcement powers proportionally. The Commissioner, Elizabeth Dunham, said that she will save serious fines for organisations that are negligent or wilfully ignoring their legal responsibilities to GDPR compliance.

"Companies that take data protection seriously and have taken steps to comply with the regulations, and have processes in place for continuous review and accountability, should not be concerned."

It's important to remember that the ICO is just one enforcement body and under GDPR it needs to work closely with other EU regulators as part of a harmonised approach. Furthermore GDPR is itself part of a growing trend worldwide to tighten up data protection laws.

Amory Wakefield, Director of Product at **personalisation platform, True Fit**, explained how the lengthy process of becoming a formally ISO-certified data processor was just one part of its global data compliance responsibilities.

"As we expand globally we are really working closely to make sure we're meeting the data requirements of every country we expand into. A big expansion for us in 2019 is into Asia where there is a whole different set of things to consider on the transferring and storing of data, and privacy.

"But also California has new privacy laws coming on board and we have the ePrivacy regulations, for example. As more consumers become increasingly concerned about the privacy of their data, the biggest challenge is staying compliant because there's a web of regulations out there."

ePrivacy and Brexit: getting ready for the next compliance challenges

ePrivacy: more onerous than GDPR?

The Data Protection Network believes that the ePrivacy Regulation could have a more significant impact on data driven marketing than GDPR. ePrivacy is set to cover both traditional communications - such as telephone, phone and SMS - as well as instant and social media messaging services, such as WhatsApp and VoIPs like Skype.

The new ePrivacy Regulation was originaly due to come into force on the same day as GDPR, but reaching a consensus on the final text has proved incredibly challenging.

So should marketers be concerned? According to the **DMA's 2018 report** the most common concerns that marketers expressed about potential changes were a required opt-in for B2B marketing (34%), consent requirement for cookies (26%) and an opt-in for all telemarketing (24%).

John Mitchison from the DMA is concerned that the legislation provides the right balance between protecting privacy and innovation: *"The ePrivacy is not just about online tracking and confidentiality of communications. The most recent proposal provides a fundamental framework for the personalised marketing and advertising industry. This framework must be balanced to reflect the interest and the protection of users, as well as enable the direct marketing industry to grow."*

The first draft of the new ePrivacy Regulation was published back in 2017 and many amendments have been proposed since then. Data protection consultancy Opt-4, anticipates that the new law could be delayed until 2020:

Debbie McElhill, Associate, Opt-4: *"When it comes to marketing, the main areas that could impact organisations in the UK are whether B2B marketing will be regulated in the same way as B2C and whether the 'soft opt-in exemption' mechanism for gathering marketing permissions for electronic marketing communications will remain and if so whether its use will be restricted."*

"The UK's interpretation of the current ePrivacy directive is less strict than some of our EU neighbours."

While the regulation is yet to be finalised, organisations should prepare for it now. As Stephan Merz from **d2m** observed: "Companies will want to avoid the last minute compliance panic of April and May 2018. Furthermore, we already have a good idea how it will look."

Ian Evans from OneTrust explains:

"When we look at the ePrivacy Regulation a lot of companies are saying 'I've still got ages to wait yet' but why wouldn't you get ahead of the curve? We know it's ninety-five per cent to where it's going to be. There will be fine tweaks to the regulation but it won't massively change from the documents that have been published already."

It's heartening that the majority of data specialists we spoke to confirmed that clients were cognisant of ePrivacy - supporting DMA research which said 88% of marketers were aware. Unsurprisingly, most are worried about its implications.

More guidance on the ePrivacy Regulation can be found here.

A note on Brexit

With uncertainty remaining over the UK's future inside or outside of the EU, it's important that organisation's are ready for the possibility of 'no-deal'. The ICO has set out the six steps you should take to prepare for data protection compliance in the event of a no-deal Brexit. (See appendix.)

The **DMA's 'Data privacy – an industry perspective' report**, found half of marketers were concerned about Brexit's impact on the free flow of data.

As things stand, personal data can flow freely and unrestricted within the EU, but once the UK leaves the EU it will become what is termed a "third country" and will be subject to restrictions on the transfer of personal data outside the European Economic Area.

The DMA fears that no-deal would "cause immediate and complete ceasing of UK data-flows with EU countries."

While the UK would seek 'adequacy' in the event of no-deal. The EU sets a rigorous test to ensure third countries have equivalent data protection standards - and this could potentially take years.

If there is a "transition" deal, the UK will remain subject to EU law (including data protection laws) until December 2020, and possibly beyond. Even if there is such a deal, organisations will still need to prepare for the end of any "transition." For that reason it is important to understand where your international data flows go and whether you need to take action.

As with ePrivacy, continued monitoring of the situation is recommended. There are many parallels: concern about added administrative burdens, potential compliance costs, and that universal business bugbear: uncertainty.

"Britain has mirrored the EU and their concerns about online privacy and so anything we've done to be GDPR compliant I think will transfer really well to continuing to meet Brexit's concerns. One concern is about whether one contract will still suffice for doing business both in Britain and the EU, and whether we need to market differently to people in the UK and really treat it as a separate region."
Amory Wakefield, Tru Fit.

"At the moment we still have to fear a no-deal Brexit. This would have a massive impact on the transfer of data between the EU and the UK. Any company transferring personal data of EU citizens to the UK will have to prepare for this scenario straight away. It is unsure if there will be an agreement with the EU confirming that the UK provides an adequate level of data protection as the EU countries under the GDPR. So standard contractual clauses approved by the EU could be the best solution which results in additional bureaucracy. Alternatively, companies will have to relocate their servers to EU countries, working with data processing companies in the EU."
Stephan Merz, D2M.

For more information:

- **DPN's 'Brexit Data Response' plan.**
- **ICO's Data Protection and Brexit resource page.**

Leaving the EU – six steps to take

gma© Global Marketing Alliance
INSIGHT FOR DATA DRIVEN MARKETERS

www.the-gma.com

Follow us on Twitter @gmainsight

Join our Linkedin Group for data driven marketers

Data Protection Network

www.dpnetwork.org.uk

Follow us on Twitter @dpntweet

Join our Linkedin Group

OneTrust
Privacy Management Software

www.onetrust.com

Follow us on Twitter @OneTrust

Join our Linkedin Group