dataIQ™

Research report

General Data Protection Regulation 2017

Identifying its impact on marketers and the consumer's moment of truth

In association with TEALIUM®

Contents

Section 1 - Consumers and personal data

Section 2 - Consumers and data preparation

Section 3 - Businesses and personal data

Section 4 - Businesses and Personalization

Overview

Following the introduction of the European Union General Data Protection Regulation (GDPR) in 2016, a two-year transition period was granted before enforcement begins on 25th May 2018. During that time, organizations involved in the control and processing of personal data about EU citizens need to review their strategy, policies and procedures for compliance. At the same time, EU consumers will become aware of a new set of rights which they have been granted by GDPR.

DataIQ undertook a twin-track research project in the UK to examine both sides of the data-value exchange in light of these new obligations and rights. Research has been carried out in two waves in 2016 and 2017 allowing for year-on-year comparisons. The project had three key objectives:

- To understand the consumer perspective on data collection, consent, context and control.
- To understand the business/marketer's processes, opportunities and challenges in adjusting to the new Regulation.
- To identify any mis-alignments between the two sides' views of the data exchange and their root causes.

The research was built around four key areas of data protection and privacy management: permission (the consent requested and granted for data use), personal (the use of digital identifiers to personalize content and services), preparation (the standard to which data needs to be held in order to be effective and how this is recognized by consumers) and protection (the effort made by companies to keep sensitive data secure and the expectation of individuals that this will happen). Results from the research are presented in a series of four whitepapers, each of which looks at one of these areas.

This whitepaper specifically focuses on the research segment conducted by DataIQ in association with Tealium. It looks into how aware consumers are of the way data is collected from their digital footprint, as well as how businesses rely on these data streams to deliver personalized services and a better customer experience.

In association with TEALIUM

Sponsor's comment

Jeff Lunsford, CEO, Tealium

The focus of the General Data Protection Regulation (GDPR) may be European data, but its reach extends much further, applying to any company (including those in the US) collecting, storing and processing the data of EU citizens. This means its key aim of improving and protecting consumer rights is set to raise the standard of data processing transparency, globally. Giving users the right to access, correct, delete, and transfer the data held about them, GDPR will provide consumers with a deeper understanding of the way brands perceive them and how to realize the value of their personal data.

For digital businesses, GDPR is a sign that our industry's focus must shift to be customer-centric. Instead of taking a data-only view of consumers and only seeing them as profiles, aggregates or members of segments, it's time to look at them as people. Consumers are individuals and, for them, a greater commitment to privacy and responsible data handling is a necessity, regardless of regulation. Organizations must prioritize the protection of individual rights and recognize that using consumer data to deliver personalized conversations and build relationships is a privilege.

The results of this report show that consumers are more aware than ever about how their digital activity is leveraged to obtain data and how it is used to build tailored experiences. A willingness to share data is also on the rise - nearly two-thirds of consumers are happy to share personal information, a significant increase since 2016. However, this is dependent on a clear understanding of the purposes for which that data is being requested, the choices available to the consumer, or their trust in the brand.

Yet, there are still many checkpoints to cover on the journey to GDPR compliance. Companies need to begin preparing: creating data governance panels, auditing data flows, ensuring data access and ownership are not siloed, and creating central data control points where rules can be administered and compliance can be monitored. Education will be vital to make sure a strong value exchange is communicated, understood and established.

The countdown is on. Companies must get their data practices in line. But they should also see GDPR as an opportunity to provide what today's consumers want - clarity and processes that put their individual rights first.

Key findings

Consumer attitudes towards sharing their personal information have become significantly more positive - for every one person who says they prefer not to share (the Cautious, 36%), there are two who are either happy to if the need is explained (the Rational, 42%) or are happy to share if they trust the company (the Trusting, 21%).

Only one in ten UK consumers (10%) say they are fully aware of a new law that will protect their data and grant them new rights over it. By contrast, six out of ten are only vaguely aware (24%) or not aware at all (38%)..

Four out of ten consumers (39.4%) say they would prefer not to be tracked online and by apps and avoid opting-in (as is their right under the ePrivacy Directive). On top of this, nearly one in six (17.2%) say they avoid sites and apps which they know are tracking them.

Consumers notice when their devices and the services they are accessing seem to reflect who they are. For nearly two-thirds (64.4%), it is awareness of their location which is most evident.

Consumers rate personalized services most highly which are based around convenience, such as autofill (3 out of 5), personalized offers (2.93), personalized content (2.92), interest-based content (2.91) or being recognized by the brand (2.91). Location-aware services scored lowest with a score of just 2.59.

Half of consumers (48.7%) adopt a rational attitude that personalization is ok if they have a choice. However, negative feelings are expressed by a significant minority of four in ten consumers, with one in ten (10.2%) saying personalization feels creepy if taken too far, 15.5% feeling worried, but unable to do anything about it, and 17% maintaining that they dislike personalization.

One-third (36%) of consumers already make use of ad blocking software and more than half (55%) are considering it. However, while using a private browser window may have the same effect as ad blocking software, only one quarter of consumers (25%) currently make use of this option.

Awareness of GDPR continues to rise among businesses with half (50%) now very conscious of the new Regulation and 36.3% somewhat aware of it - a combined rise of 7.3%. The proportion who are very prepared has doubled to 14.6%, while the number who are not at all prepared fell sharply from 8% in 2016 to just 1.9% in 2017.

One in six companies (16.5%) now rate themselves as Advanced in their adoption of data and analytics. This is a significant rise since last year, although overall, there has been a slight softening in self-confidence.

Third-party analytics (in other words, Google Analytics) are deployed by 75.7% of organizations, with 55.8% using first-party analytics and 55.8% first-party cookies. It is notable that companies which are still developing, in the early stages or planning their adoption of data and analytics are more dependent on free third-party tools (44.9% in total) than other, more complex options.

Four out of ten organizations are potentially at risk of non-compliance with GDPR, given that 43.6% say their use of digital tracker data is limited and they only use some of it. By contrast, just one in ten say their tracker data usage is so deeply embedded that they could not operate without it (10.3%).

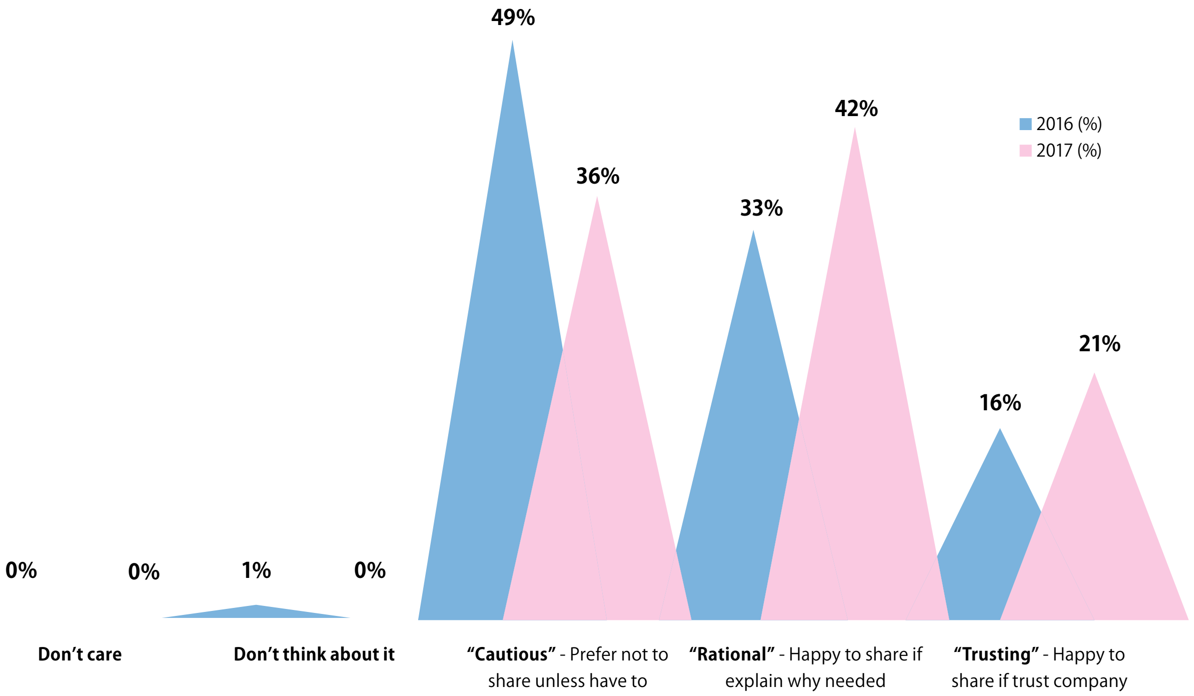
A paradox - and potential compliance risk - has been created by the gap between functions having access to digital tracker data, but not controlling it. This is most evident in sales (41% access, but only 20.5% control). Controllers who do not have access cannot, by contrast, deliver value - this is clear within insight and analytics where 31.4% own the data, but only 10.9% can access it.

The primary benefits of digital identifiers sit right at the heart of marketing - measuring performance (44.7%) and optimizing the customer journey (41.8%). Behind the scenes, organizations are expecting to fuel analytics through digital identifiers (38.3%) in order to support the customer experience and product design (38%).

The range and complexity of digital identifiers causes problems - 30.8% of organizations worry about storing the data collected and 28.2% have concerns about whether they or the system vendor own that data. A further 22.4% worry whether the data will be shared by vendors with third-parties and 21.8% are concerned directly about GDPR compliance.

Section one - Consumers and personal data

1.1 - Consumer attitudes towards sharing personal information



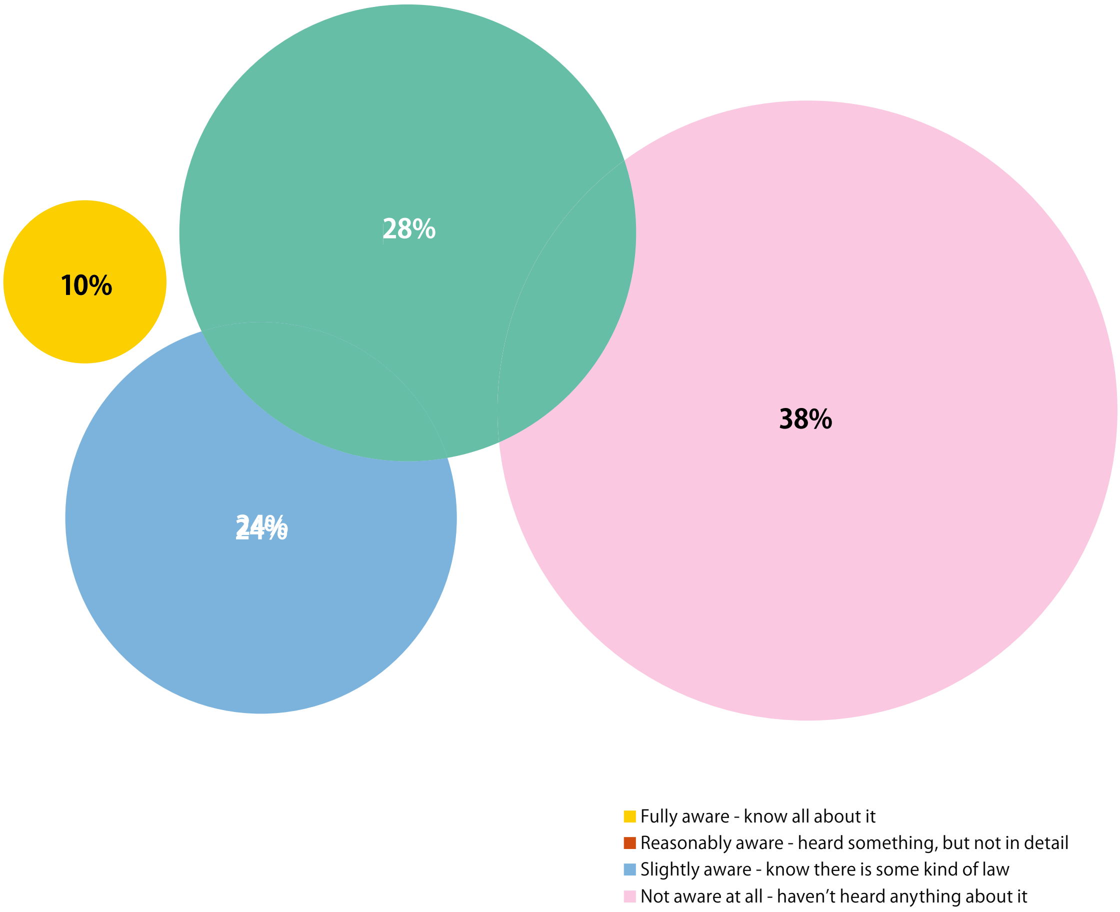
Attitudes towards sharing personal information

With enforcement of GDPR, new rights for consumers will move center stage. Transparency, consent and control will combine to make the balance of power in the data-value exchange more equal. The good news for organizations that rely on personal information is that, even in the last 12 months, attitudes towards sharing data have become significantly more positive. For every one consumer who prefers not to share personal information, there are now two who are happy to do so in the right circumstances.

Under GDPR, organizations that are unable to make clear their legitimate interest in processing data have to gain informed consent - difficult when half of the population in 2016 (49%) were starting from a position of caution. But, by 2017, there had been a 40% drop in the number who hold this attitude, leaving just over one-third (36%) in the Cautious segment.

Two-thirds of those who have changed their minds are now Rational about sharing personal information - 42% will do so if the need is explained, up from 33% last year. One-third have migrated into the Trusting group, creating a 21% segment who are happy to share if they trust the company, up from 16% in 2016.

1.2 - Consumer awareness of data protection law



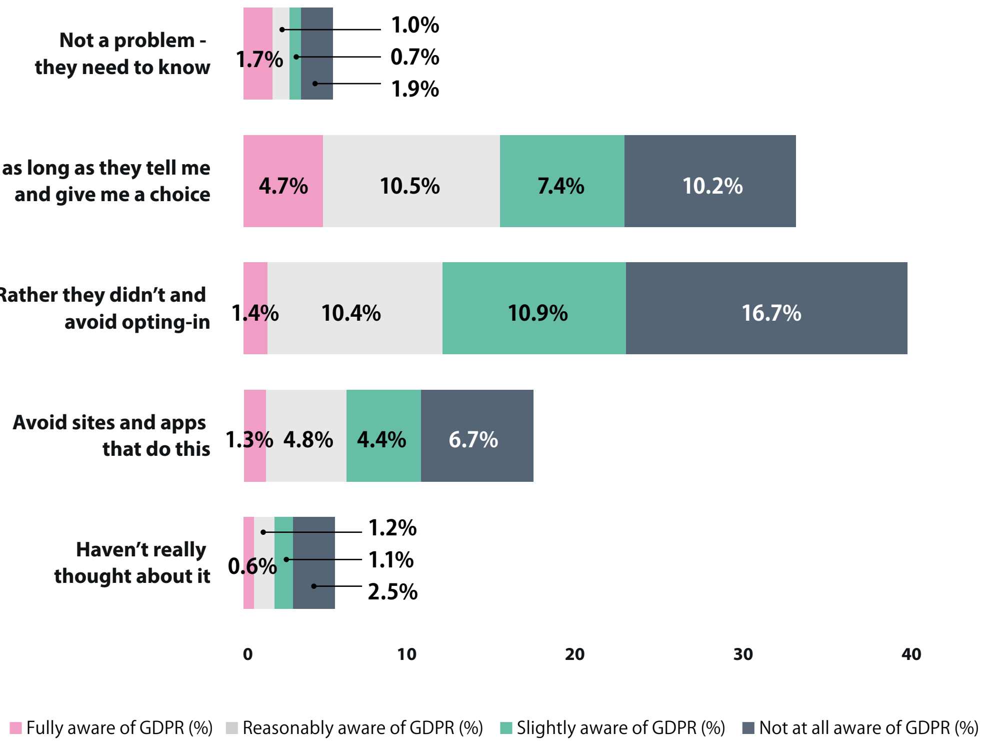
Awareness of data protection law

For GDPR to have the effect intended by its architects, consumers will need to take advantage of the rights it grants them. That will require awareness and education - but the existing base is currently low, with only one in ten consumers (10%) claiming to be fully aware of a law that protects their data and privacy. When prompted, only an additional 28% claim a degree of awareness, even if not in detail.

That leaves more than six out of ten consumers with, at best, a vague sense that there is a law protecting them or, at worst, a complete lack of knowledge. The group who haven't heard anything about it is the largest segment at 38% - the same size as all of those with a level of awareness and half as big again as the group with just some knowledge that there is a kind of law (24%).

Section 2 - Consumers and Personalization

2.1 - Attitudes towards online tracking and awareness of GDPR



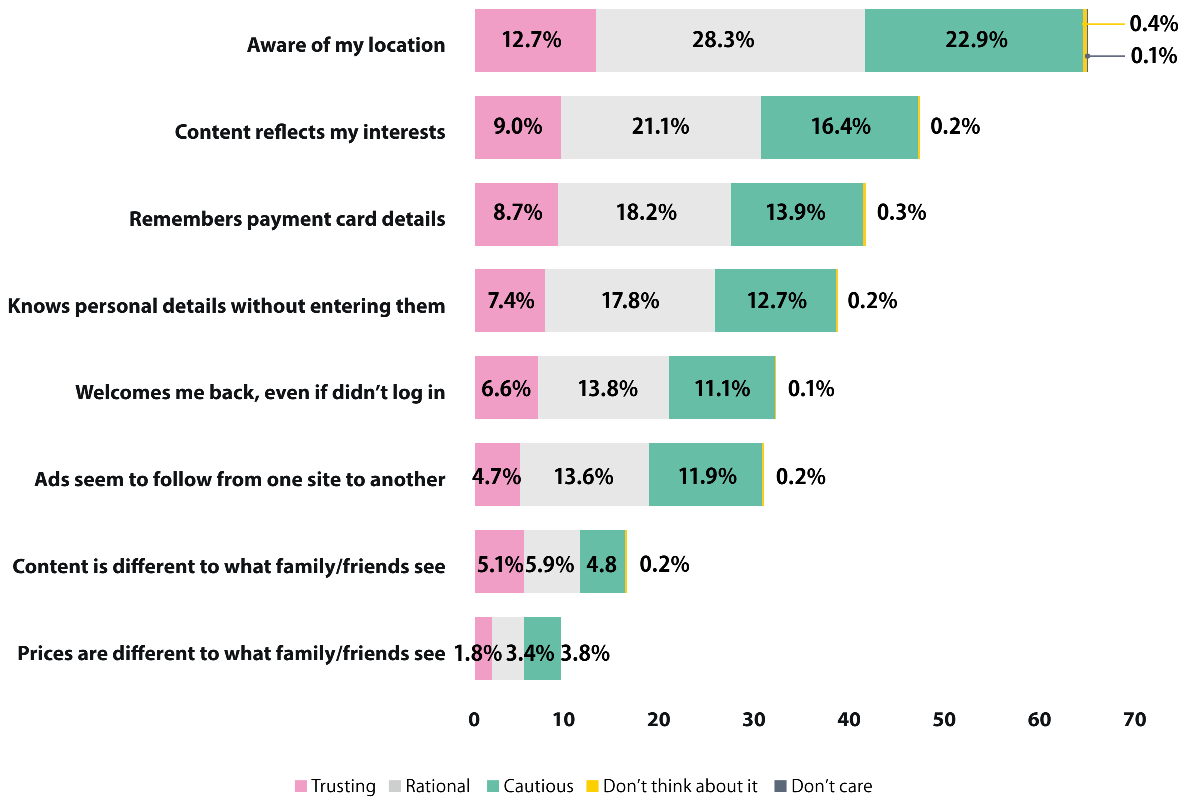
Attitude towards website and app tracking vs Awareness of GDPR

Tracking consumers online and via mobile apps is a fundamental aspect of digital marketing and the customer experience. At least, that is how businesses view it - for consumers, the story is a little different. Only 5.3% accept that companies need to know and are not troubled, virtually the same proportion say they have not really thought about it (5.4%).

In total contrast, four out of ten consumers (39.4%) say they would prefer not to be tracked and avoid opting-in (as is their right under the ePrivacy Directive). On top of this, nearly one in six (17.2%) say they avoid sites and apps which they know are tracking them. It is worth noting that this exceeds the level who have a conscious resistance to sharing their personal data.

In fact, rising awareness of GDPR appears to lead to a more rational view of data sharing. While one-third of consumers (32.8%) say they are ok with being tracked as long as they have a choice, there is a significantly higher proportion holding this attitude who claim to be fully aware of GDPR. Transparency and education about controls and rights therefore appear to be valuable tools to increase acceptance of digital data tracking.

2.2 - Experiences of personalization and attitudes towards data sharing



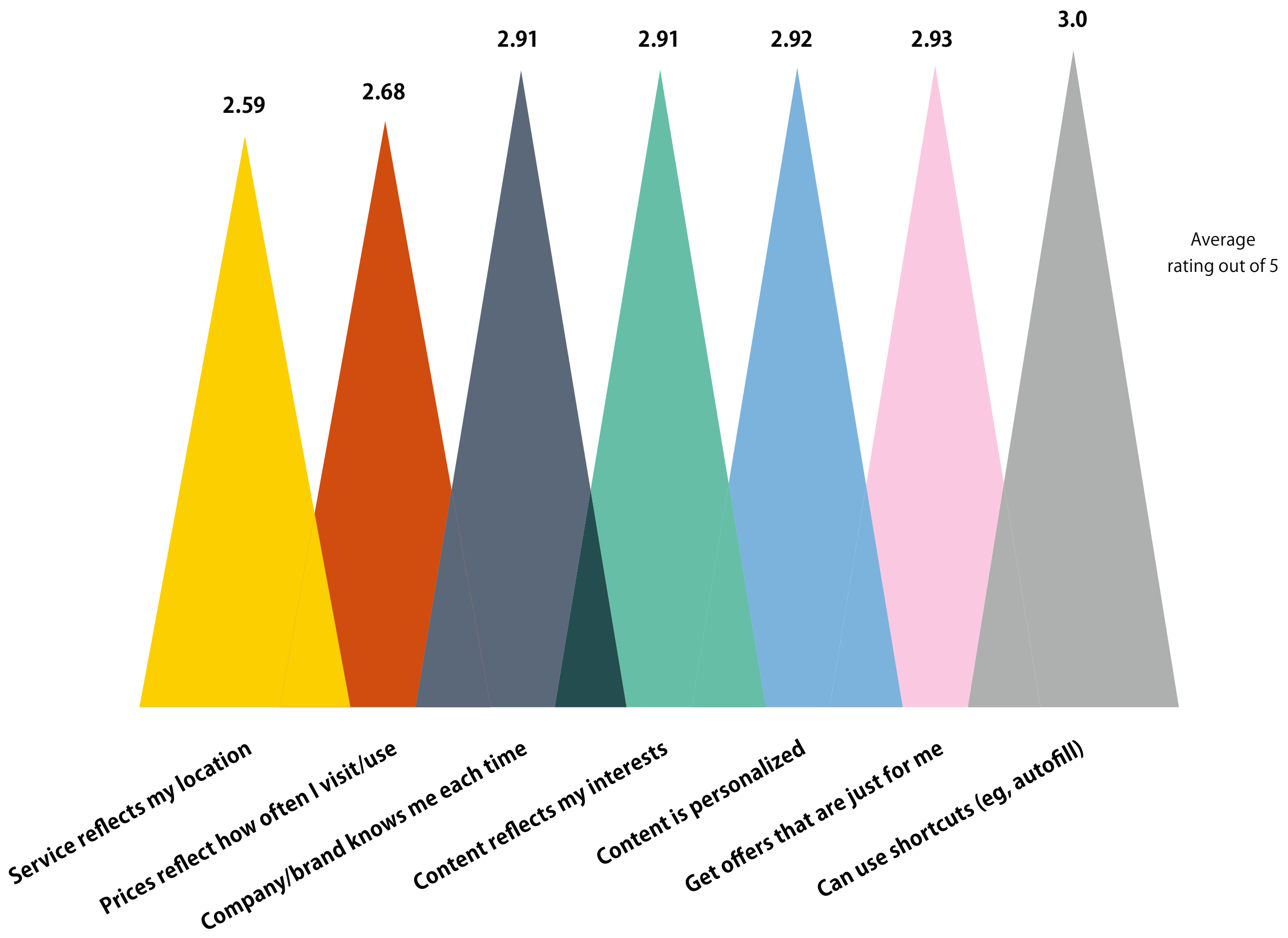
Experience of personalization vs Attitude towards sharing personal data

Consumers notice when their devices and the services they are accessing seem to reflect who they are. For nearly two-thirds (64.4%), it is awareness of their location which is most evident and this is even more strongly visible to consumers who will share data with brands they trust as well as those who are happy to share if given a reason to do so. Geo-location is clearly a persuasive and recognized benefit of data tracking.

Convenience factors play a strong secondary role, led by content which reflects the individual's interests (46.7%), followed by services which reduce the effort needed by consumers to use a service, such as remembering payment card details (41.1.%) and personal details (38.1%). These are noticed across all three mindsets towards sharing personal data, suggesting that offering a personalized service that is easy to use overrides other considerations.

However, only three in ten consumers notice some of the digital marketing techniques which are assumed to drive engagement and conversion, such as welcoming an individual back (31.6%) or behavioral tracking across websites and apps (30.4%). Differentiation of content and pricing only resonates with a minority (16% and 9% respectively).

2.3 - Consumer ratings of online personalized experiences



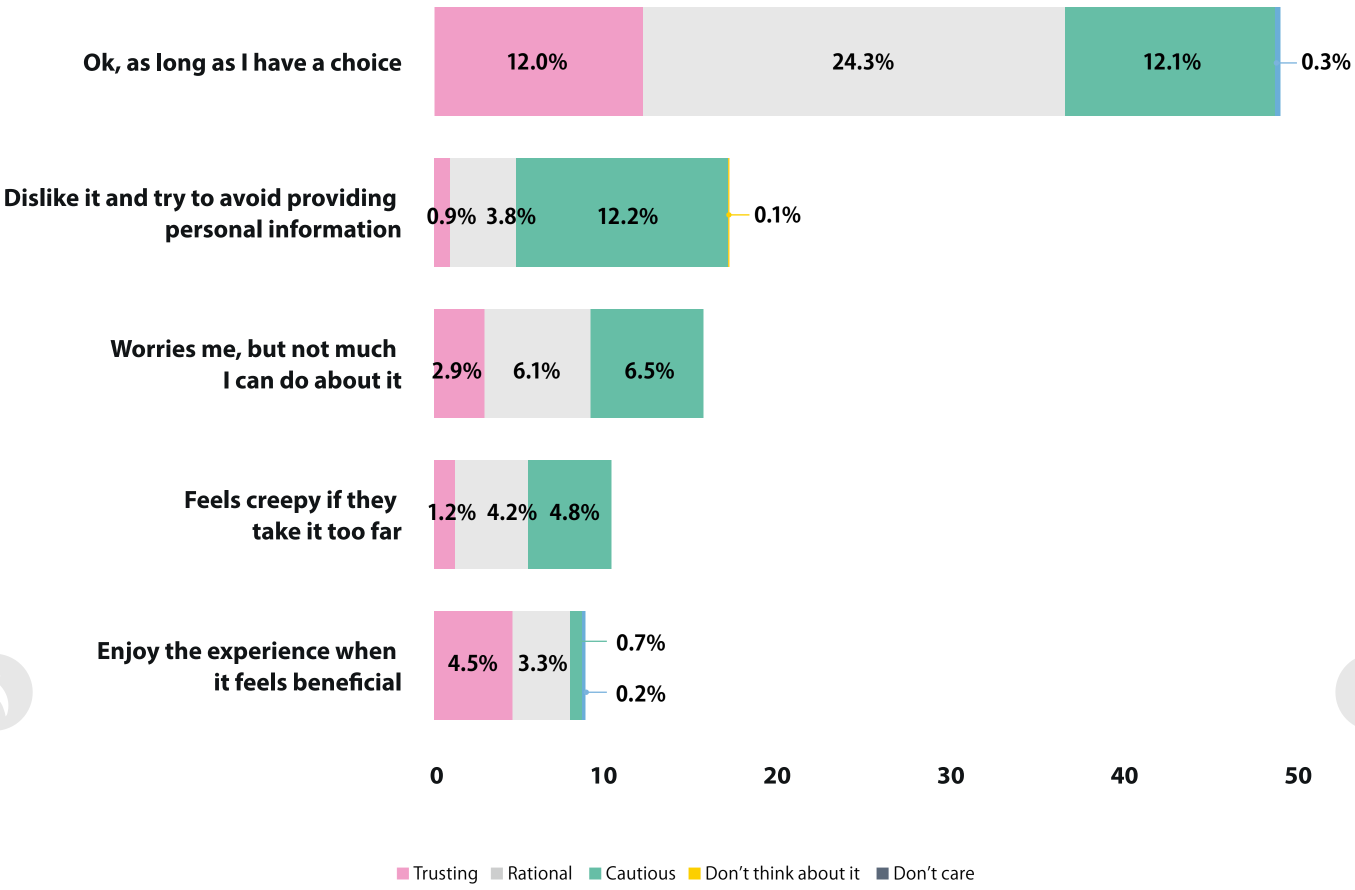
Rating of online/app personal experiences

Noticing that online and app-based experiences are taking place is one thing - valuing them is quite another. While all seven of the services considered were rated above average on a scale from 0 to 5, they only achieved weakly positive scores. Location-aware services, which were the most widely noticed, scored lowest with just 2.59 out of 5, despite the convenience of mapping, "where's my nearest" and other location-based experiences.

Most highly rated, but still only achieving modestly positive scores, are those based around convenience, such as autofill (3 out of 5), personalized offers (2.93), personalized content (2.92), interest-based content (2.91) or being recognized by the brand (2.91). There is a marginally positive attitude towards behaviorally-adjusted pricing (2.68).

The upside of these consumer ratings is that all of them fall on the positive side of the scale, even though they involve data collection and tracking which currently happens behind cookies consent. With GDPR moving these data types onto informed consent, the depth of this positive view will be tested.

2.4 - Attitudes towards personalization and data sharing



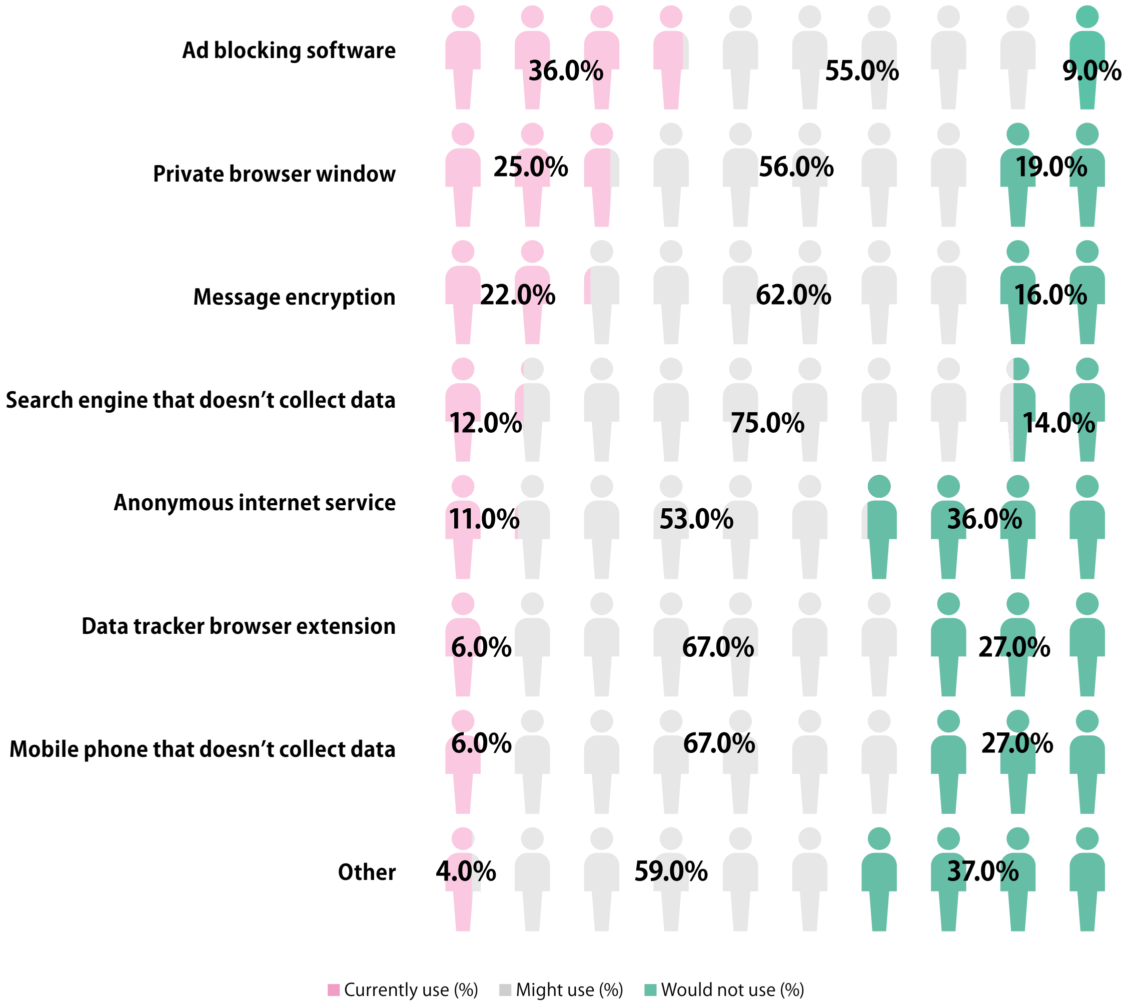
Feelings about personalization vs Attitude towards sharing personal information

If consumers notice that the services they use are being personalized and are generally positive towards the experience, does that mean they think it is ok to use their personal data this way? Notably, half of consumers (48.7%) adopt a rational attitude that personalization is ok if they have a choice.

Consumers who are Trusting about sharing their personal data fall most strongly into this group (12.0%), suggesting that trust can be built on rational grounds as much as emotional ones. This is strongly visible in the fact that as many Cautious consumers feel this way about personalization as say they dislike it (12.1% v 12.2%).

However, negative feelings are expressed by a significant minority of four in ten consumers, with one in ten (10.2%) saying personalization feels creepy if taken too far, 15.5% feeling worried, but unable to do anything about it, and 17% maintaining that they dislike personalization and try to avoid providing the personal information that drives it. While these individuals do not avoid the digital world - they have experienced it in order to form these attitudes - their concerns should be taken into account, especially in the light of enhanced rights under GDPR.

2.5 - Consumer usage of data minimization services



Data minimizing services used

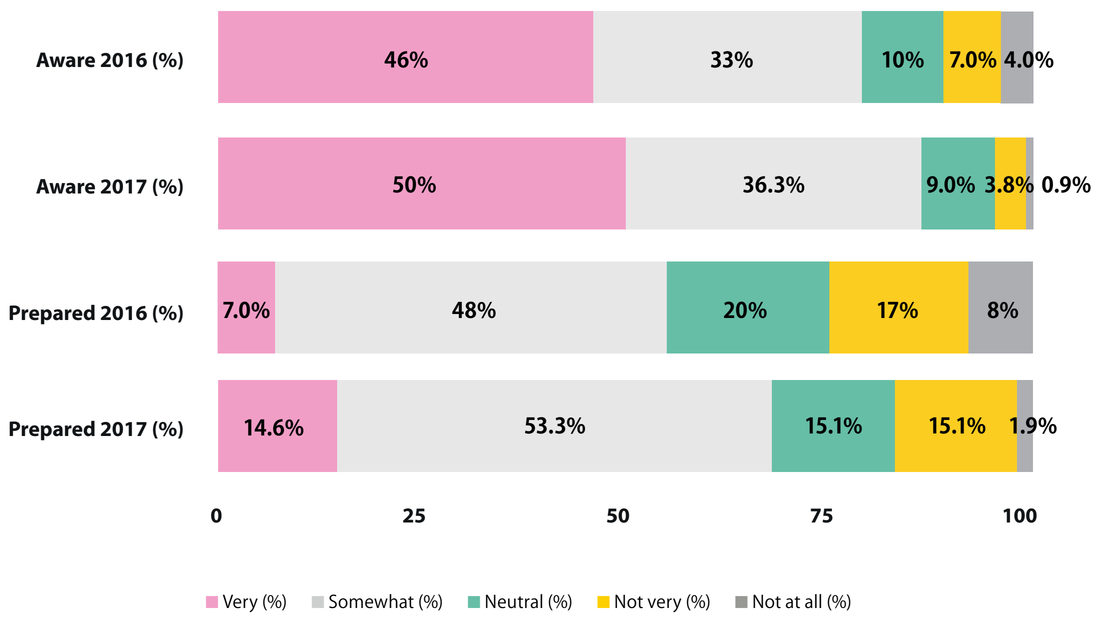
If personalized services and convenience are one way in which personal data is put to use by websites and apps, on the other side of the equation are services which actively intervene in data sharing and collection. Ad blocking has risen rapidly to the top of the list of these services, with one-third (36%) of consumers already making use of this software and more than half (55%) considering it.

Using a private browser window may have the same effect as ad blocking software, but only one quarter of consumers (25%) currently make use of a facility already built in to this core internet application. More technically-demanding, message encryption is being used by 22%, although the appification of this via WhatsApp and Snapchat has reduced the cognitive burden involved.

Only one in nine consumers have adopted the most aggressive tools to avoid their personal data being used while they are online, such as search engines which do not collect data, like Safe Page, or an anonymous internet service provider, like Tor (12 and 11% respectively), although the idea of anonymous search has the highest potential uptake at 75%. Mobile handsets which do not harvest personal data, like the Blackphone, are the preserve of a very dedicated minority, as are browser extensions that make data identifiers visible, like Ghostery
(6% each).

Section 3 - Businesses and personal data

3.1 - Awareness and preparation for GDPR

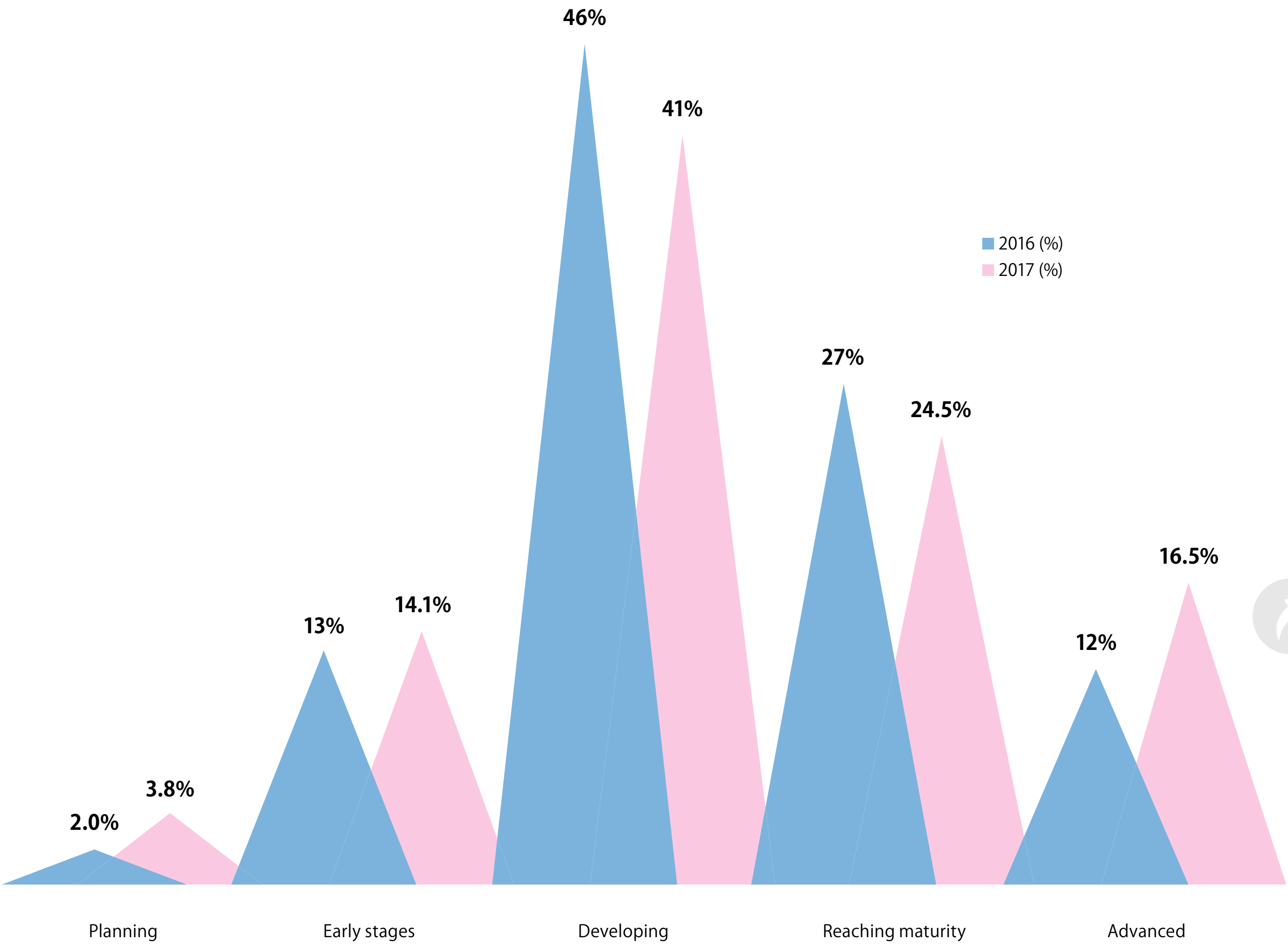


Awareness and preparedness for GDPR

In the year since DataIQ last surveyed UK companies about their awareness of GDPR, there has been a modest increase in the numbers saying they are very aware (50%) or somewhat aware (36.3%) of the new law. While encouraging, if this rate of change remains constant, there will still be around 6% of companies who have no idea that the way they handle personal information is about to change by the time enforcement starts.

More encouraging is the pace at which preparations for the Regulation are being undertaken. The number of companies who are very prepared has doubled to 14.6%, while 53.3% are now somewhat prepared. Perhaps most significant is the steep fall in those who are not at all prepared, which now stands at just 1.9%, down from 8% in 2016. It is to be hoped that this pace of change will accelerate over the coming 12 months until there are no more UK businesses who are unprepared for the new legal framework.

3.2 - Maturity level of data and analytics



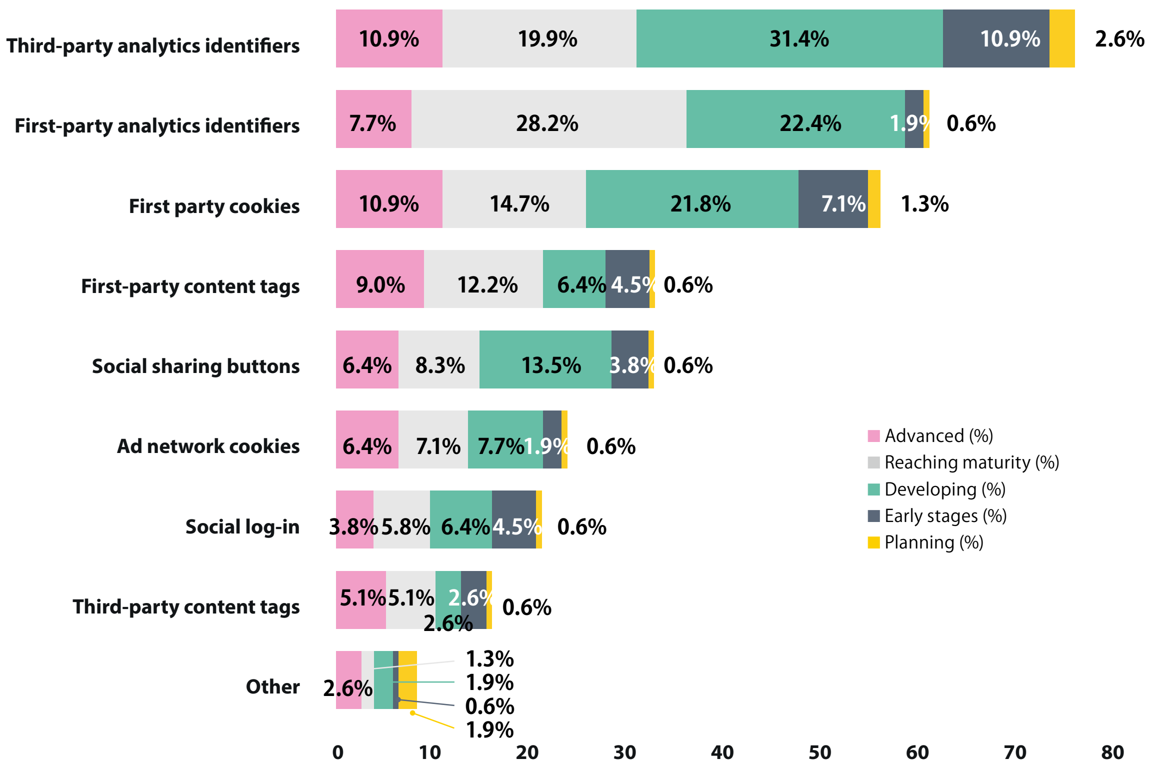
Adoption of data and analytics

The ability of organizations to adapt to GDPR is in part a reflection of their level of maturity in the adoption of data and analytics. Four out of ten place themselves either in the advanced segment (16.5%) or reaching maturity (24.5%). Although this number has not significantly changed overall since 2016, it is notable that more programs have now reached full maturity, placing one in six organizations into the leading group.

By contrast, almost the same proportion find themselves still on the launch pad with 3.8% planning - nearly double the number found last year - and 14.1% in the early stages - up slightly on 2016. For these organizations, the time remaining until GDPR starts to be enforced is likely to be a rush to understand and master the personal data they are relying on, with a strong potential to fail given the short timescale.

Section 4 - Businesses and Personalization

4.1 - Data identifiers used and maturity of data adoption



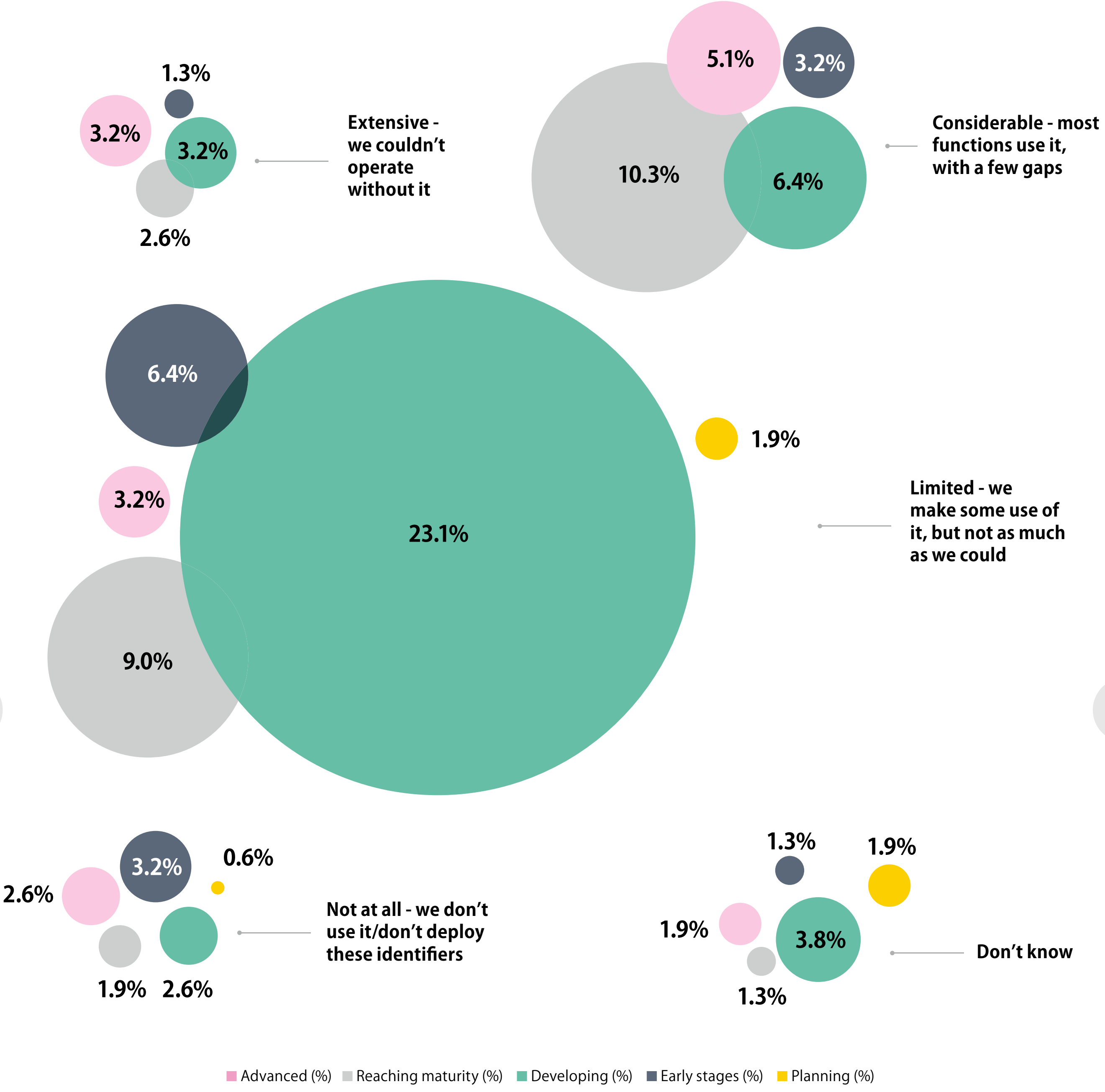
Data identifiers used in digital assets vs Maturity

Three sources of personal data collected via digital identifiers dominate current practice - third-party analytics (in other words, Google Analytics) which are deployed by 75.7% of organizations, with 55.8% using first-party analytics and 55.8% first-party cookies. It is notable that companies which are still developing, in the early stages or planning their adoption of data and analytics are more dependent on free third-party tools (44.9% in total) than other, more complex options.

First-party content tags are being used by one-third (32.7%), with the advanced and those reaching maturity having a significantly higher rate of deployment (21.2%), although only half this number allow third-party content tags (16%).

Social tools are not being used by the majority, but they are found across all levels of maturity. Social sharing buttons are in place at 32.6% of organizations, while social log-in is used by 21.1%. Surprisingly, the seemingly ubiquitous ad network cookies are only identified by one-quarter of companies (23.7%) - it is possible that others are simply not aware of the extent to which these are being dropped on their websites.

4.2 - Data usage from digital identifiers and data maturity

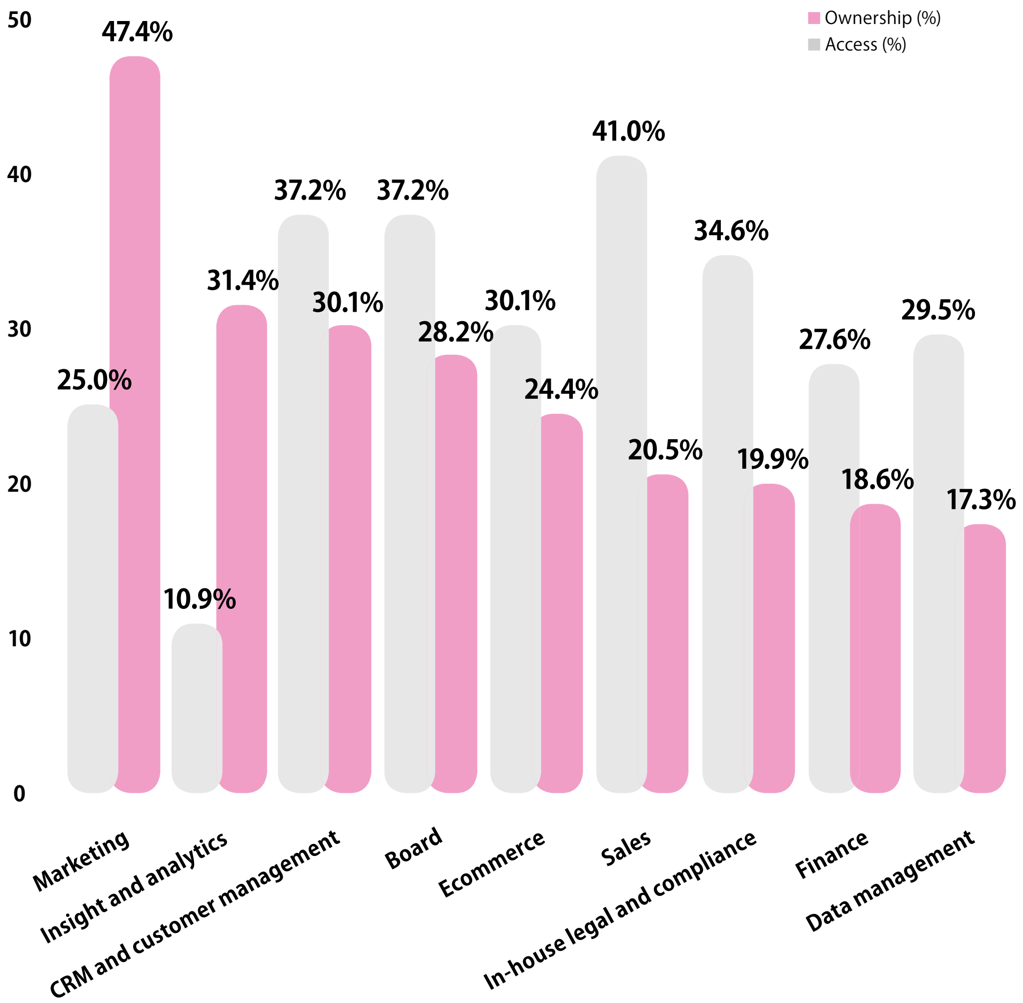


Use of data from digital identifiers vs Maturity

A guiding principle of GDPR is that data should only be collected for a clear purpose, rather than just for the sake of it. This means that four out of ten organizations are potentially at risk of non-compliance, given that 43.6% say their use of digital tracker data is limited and they only use some of it.

By contrast, just one in ten say their tracker data usage is so deeply embedded that they could not operate without it (10.3%). That is likely to be a good basis for claiming legitimate interest for processing this data. The one-quarter (25%) who say their usage is considerable, but with a few gaps, should be able to reach compliance with limited effort.

4.3 - Functions owning and accessing digital tracker data



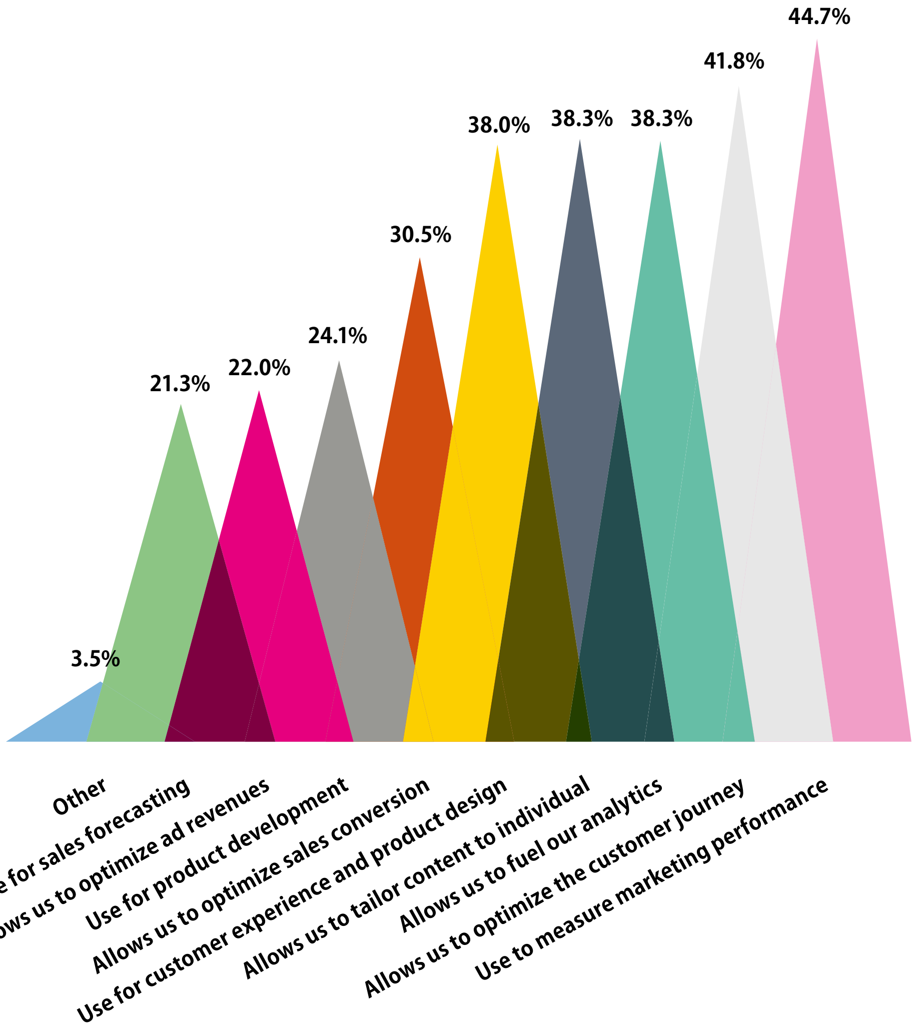
Functions owning and accessing data from digital identifiers

In nearly half of organizations (47.4%), it is the marketing department which owns the data captured from digital identifiers. Surprisingly, only one-quarter (25%) have access to this information. Instead, it is the sales department which has the highest degree of access at 41% of companies, even though it only owns this data in 20.5%.

This paradoxical gap between ownership and access is at its greatest in the insight and analytics function - 31.4% of organizations give this department ownership, yet only 10.9% allow it access. The reverse is true of in-house legal and compliance, which only owns the data at 19.9% of companies, but has access at 34.6%. Similarly, nearly twice as many data management teams have access to digital tracker data (29.5%) compared to those who own it (17.3%).

From a GDPR perspective, these disparities between access and ownership create risks. If a function is using data which it does not control, it could deploy it outside of what it has the right to do. In terms of gaining value from digital data, owners who do not have access are being constrained unnecessarily.

4.4 - Benefits derived from digital tracker data

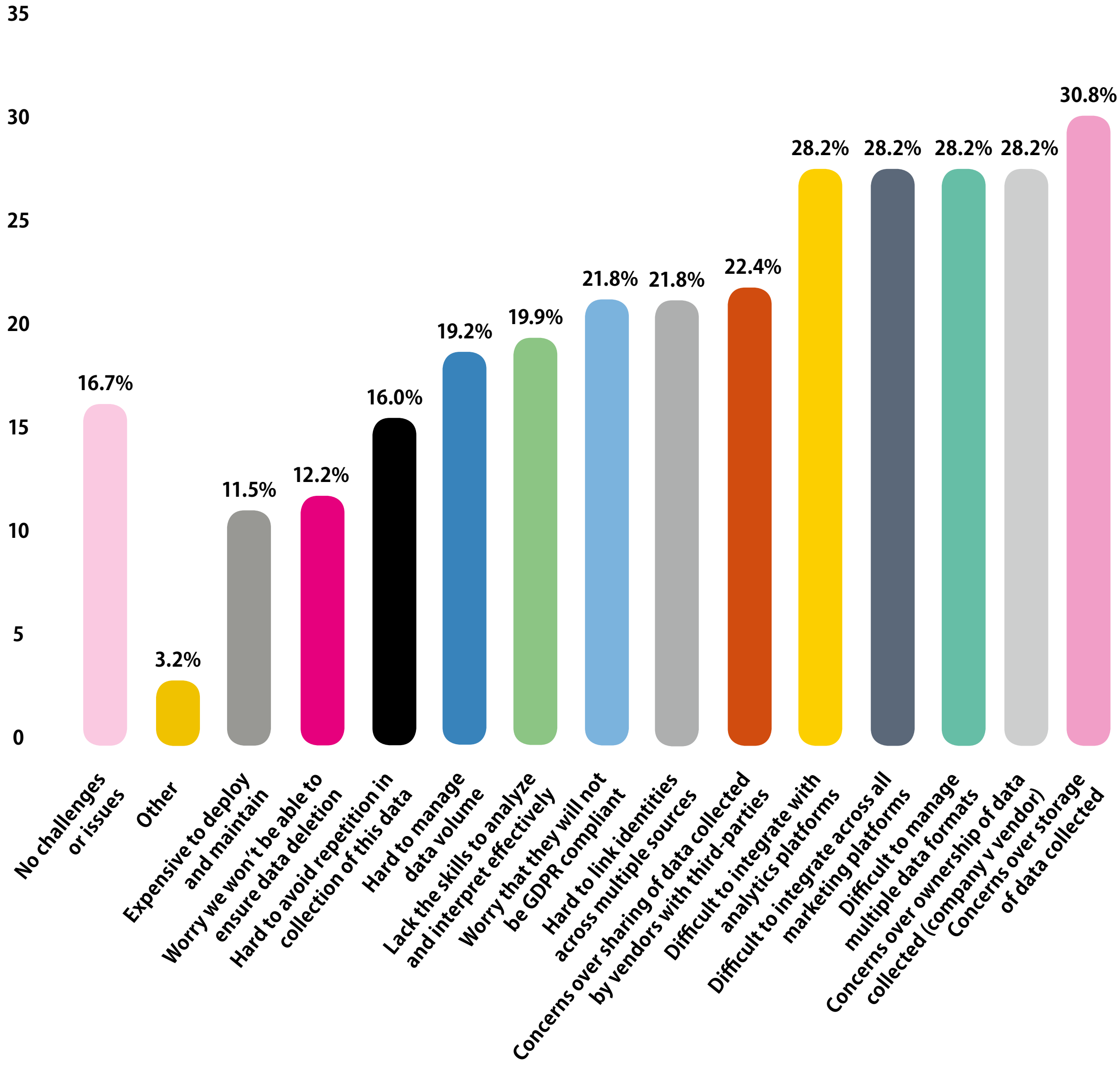


Benefits gained from digital identifiers

It is clear from the benefits which organizations expect to gain from digital identifiers that their access needs to be as widespread as possible. The primary benefits sit right at the heart of marketing - measuring performance (44.7%) - and CRM - optimizing the customer journey (41.8%). These are also uses which convert into personalization and convenience that are visible to the consumer, as is tailoring content (38.3%).

Behind the scenes, organizations are expecting to understand their processes and make improvements across sales and product development. Fueling analytics through digital identifiers (38.3%) helps to support the customer experience and product design (38%), with a further 30.5% looking to optimize conversion and 24.1% to develop products. But optimizing ad revenues is only a benefit for 22%, in line with the number who say they have ad network cookies on their site.

4.5 - Organizational issues with deployment of digital identifiers



Issues with the deployment of digital identifiers

Moving beyond free and easy-to-use digital identifiers like Google Analytics places pressure on internal resources. It also creates challenges for GDPR compliance and these top the issues identified - 30.8% of organizations worry about storing the data collected and 28.2% have concerns about whether they own that data or the system vendor does. A further 22.4% worry whether the data will be shared by vendors with third-parties and 21.8% are concerned directly about GDPR compliance. A highly-specific compliance issue - that of data deletion - is identified by 12.2%.

Technical issues also rank highly, with managing multiple data formats, integration across marketing platforms and integrating into analytics platforms named by 28.2%. Given the range of digital identifiers in use, it is no surprise that 21.8% worry how to link identities across these sources. Managing data volume (19.2%) and avoiding repetition (16%) stem from the same issue of having multiple collection sources operating. Only 16.7% run digital tracking without problems, reflecting just how complex this data infrastructure can be.

About Tealium

Tealium revolutionizes today's digital businesses with a universal approach to managing the ever-increasing flows of customer data - spanning web, mobile, offline and Internet of Things devices. With the power to unify customer data into a single source of truth, combined with a turnkey integration eco-system supporting more than 1,000 vendors and technologies, Tealium's Universal Data Hub enables organizations to leverage real-time data to create richer, more personalized digital experiences across every channel.

Founded in 2008, Tealium was recently named to the Inc. 500, which recognize the fastest-growing private companies in America. The company's award-winning solutions are used by hundreds of global enterprises, including Domino's, Cathay Pacific Airways, Priceline, Univision, TUI, Vodaphone and Eddie Bauer.

Tealium has offices worldwide. Phone numbers and addresses are listed on the Tealium website at tealium.com/contact.

Global Headquarters
11095 Torreyana Road
San Diego, CA 92121
(858) 779-1344
tealium.com

INSPIRE | CONNECT | ENGAGE

About DataIQ

DataIQ aims to inspire and help professionals using data and analytics intelligently to drive business performance across their organization and in every industry sector.

Specifically, DataIQ helps business professionals to understand the benefits of adopting data-driven strategies, develop compelling business cases, implement best practice, ensure they comply with data regulation, and understand how to use the latest tools and technology to deliver sustained business improvement.

DataIQ achieves this by providing essential insight, help and know-how from proprietary research, analysis, best practice and comment from industry leaders and data experts. All made easily available through high-quality events and digital channels.

Our unique community of business decision-makers and influencers - working across functions in FTSE 100, large and mid-market organizations - is growing rapidly as a consequence of this unique focus. Importantly, DataIQ provides the bridge for ambitious vendors, agencies and service providers to ifluence this hard-to-reach and unique community.

DataIQ is committed to championing the value of data-driven business and best practice through focusing on the success stories of data-driven professionals with initiatives including the DataIQ 100 and DataIQ Talent Awards, plus many other events and programmes. We contribute actively to trade and government bodies, including the DMA, IDM, PPA, techUK and UKTI.

For the latest information on how DataIQ can help your organization go to www.dataiq.co.uk.

For information on how to become a commercial partner to DataIQ, call Adrian Gregory or Adam Candlish on +44 (0)20 3829 1112 or email adrian.gregory@dataiq.co.uk and adam.candlish@dataiq.co.uk

Methodology

Research for this series of whitepapers was carried out in two parts. Consumer research was commissioned by DataIQ from Research Now in both 2016 and 2017 among an online panel representative of the UK population. All respondents were aged over 18, UK residents and were served a self-completion questionnaire. A total of 1,001 surveys was completed in 2017 and 1,000 in 2016. Business research was conducted in two parts in 2017. A self-completion questionnaire was served to members of the DataIQ community and also to decision-making marketers in an online panel operated by Research Now. A total of 212 responses was generated during February 2017. For the 2016 survey, DataIQ surveyed only its own community during April, generating 187 responses.