

Deloitte.




A new era for privacy
GDPR six months on



Contents

Executive summary	5
Consumer opinion on GDPR	6
Organisations and ongoing investment	7
GDPR and the Brussels effect	10
The prominence of the DPO	11
Privacy notices and consumer data rights	12
Do consumers value their privacy?	16
Do consumers trust organisations to handle data?	18
Cookie management	19
The importance of trust	20
Active regulation of GDPR	21
What's next?	22



Our survey indicates that GDPR is having the desired effect with a largely positive impact on consumer opinion in relation to personal data being collected and stored by organisations.

About the survey

Deloitte's General Data Protection Regulation ("GDPR") survey was based on 1,100 responses from individuals with involvement in GDPR within their organisations and 1,650 responses from consumers. The survey was conducted across 11 countries to get a view on consumer perceptions and organisations' responses to GDPR inside and outside the EU. The countries surveyed were the UK, Spain, Italy, Netherlands, France, Germany, Sweden, USA, Canada, India, and Australia.

Executive summary

The General Data Protection Regulation (“GDPR”) has now been enforceable for six months, but so far has it had the impact the regulators desired, and the public appear to crave, in enhancing individuals’ privacy?

Deloitte conducted a survey across a sample of both consumers and organisations to gain insights into attitudes towards privacy since GDPR became enforceable on the 25 May 2018. The survey was run across eleven countries, both inside and outside the EU, to understand what impact GDPR

has had on organisations and how consumer perceptions and behaviours have changed as a result.

The good news is the results indicate consumer awareness has risen. 58% of respondents reported that they took more caution when providing

organisations with their personal information than pre-GDPR, and organisations have invested to improve their compliance with 48% of organisations claiming to have made “significant” investment. However, our survey brought out some interesting observations:



Privacy is a global concern

A significant change under GDPR is its reach beyond the EU to place requirements on all organisations handling personal data on EU data subjects. This has clearly had an impact, with the results showing that there has been equal focus by organisations inside and outside the EU on the topic. Consumer perception is similar, with attitudes broadly aligning.



Trust is key

Individuals share data more openly with organisations they trust. They are also less likely to leave, challenge or exercise their rights against an organisation they trust if it has a breach. The ethical use of data, which can reside in the grey area between regulatory compliance and a higher standard, is seen as an increasingly important driver in this level of trust.



Consumer centricity is not yet there

Individuals’ level of trust is increased through being put in control of their data; however, most people do not feel that GDPR has done enough to increase the control they have over their data, and they still pay little attention to privacy notices. Programmes may have been too focused on internal compliance rather than taking a consumer-centric view.



Consumer action doesn’t follow perception

While the perception and importance of privacy is on the increase, consumer actions are still slow to follow suit. With the continued surge in personalisation and personal data being used in ever more complex ways, the increasingly tangible impact that the misuse of data can have at a consumer level is likely to drive a stronger reaction.




Talent matters

Most organisations have recruited or trained people to increase their capabilities to manage privacy compliance, but many still see challenges in headcount and capacity of these individuals. Continued effort is needed to address the talent shortage.

Our survey indicates that GDPR is having the desired effect with a largely positive impact on consumer opinion in relation to personal data being collected and stored by organisations. The impact on an organisational level is mixed; the majority

of organisations report successful compliance with GDPR policy, but it’s important to note that some can’t see this being maintained with their current resourcing levels whilst others may already be contravening the regulation.

Consumers continue to be more driven by the value and rewards they receive in exchange for sharing their personal data than the potential adverse impact it may have on them. 

Consumer opinion on GDPR

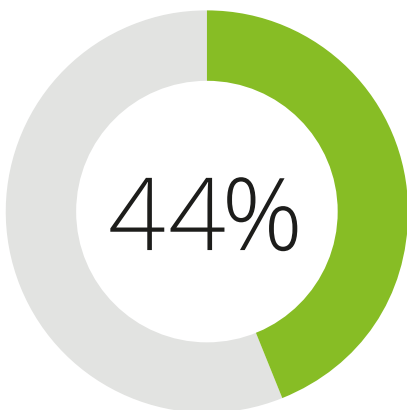
Do organisations care?

The results of the survey indicate that a perceptual change has taken place in consumers' minds. 44% of respondents believe that organisations care more about their customers' privacy now that GDPR is in force, a sentiment shared by participants from within and outside the EU. Although no significant difference was measured between EU and non-EU respondents on this particular question, participants from Australia (54%) and the US (56%) scored highest.

In fact, consumers from the EU appear to be most sceptical about organisations' intentions with 19% saying that organisations do not care about their privacy, while this sentiment is shared by only 7% of respondents outside the EU. Participants from the Netherlands, Germany and France were found to be most wary, which could be attributed to the relatively strict interpretation of the previous Data Protection Directive at a national level before the enforcement of GDPR. German employment laws and the French and Dutch data protection authorities are notorious for being some

of the strictest in the world. This appears to have empowered their populations to have a broader understanding of privacy which could naturally have led to more scepticism where it comes to organisations claiming good intentions.

Participants from India were most undecided on whether organisations cared more about consumers' privacy as a result of GDPR, with 59% of the respondents being neutral. Moreover, participants from non-EU countries were more likely to share this view, compared to participants from EU countries. This could be attributed to less exposure to the Regulation in non-EU countries. Taking into account the countless GDPR awareness campaigns that have flooded Europe over the past year, this does reinforce the finding that a better informed consumer becomes more sceptical of how organisations protect their data. It will be interesting to see how regulatory developments change this in the future, for example with California and India being two particularly hot examples of new regulations coming into force.



44% of respondents believe that organisations care more about their customers' privacy now that GDPR is in force



A prompt to be vigilant?

However, more scepticism needn't be a bad thing. Since GDPR has come into effect, consumers have become more cautious about sharing their personal data with organisations. This behaviour was found to be consistent across participants globally, with 61% of respondents outside the EU agreeing they have become more cautious as a result, versus 55% from respondents in the EU. Europe's GDPR awareness campaigns and strong regulation has definitely sparked an interest outside its borders, with respondents from India (62%) and the US (63%) in particular showing more caution since GDPR came into effect. For those organisations who have chosen to adopt a GDPR friendly approach across their global operations, this could very well be used as a competitive advantage to gain trust from consumers, regardless of whether GDPR applies to them or not.

Organisations and ongoing investment

Our results show that almost half of organisations surveyed have made significant investment in their GDPR compliance capabilities, with 33% continuing to invest and embed privacy practises into their business processes beyond the 25 May.

This was not influenced by the geographical location of the organisations, with near identical results inside and outside the EU. Interestingly, just 15% of organisations that invested significantly in their GDPR programmes now consider

their GDPR readiness programmes complete. This may indicate the vast majority have recognised the need for continued effort to embed and sustain the changes they have made. On the other hand, almost 1 in 5 organisations

aimed for bare minimum compliance, with similar results inside and outside the EU, highlighting that some organisations still see this as more of a compliance burden than a way to change how they handle personal data more broadly.



Organisations recruit for GDPR

70% of organisations surveyed have seen an increase in staff that are partly or fully focused on GDPR compliance. Only 21% have kept a steady headcount, while another 7% reported a headcount decrease, which albeit small, is surprising to see and may be more reflective of the challenge to retain Privacy expertise. Of the 70% of organisations who increased their headcount to cater for GDPR, 36% reported a significant increase, 41% reported a moderate increase and 23% reported a small increase with little difference between EU and non EU countries.



GDPR's reach beyond Europe is once again apparent

Interestingly, none of these statistics are influenced by geographical location. Comparisons between EU countries and non-EU countries are limited to differences of 1 or 2%. For example, 22% of organisations from EU countries maintained the same number of staff, compared to 20% from non-EU countries. This illustrates the global impact that GDPR has had, despite the current lack of precedence of how it will be enforced outside the EU.



The majority of organisations believe they will be able to comply with GDPR in the long-term

92% of organisations surveyed in the EU claimed a level of confidence in demonstrating their ability to comply with GDPR in the long term, with near identical results outside the EU. Of the 92%, 42% were very confident, 35% were confident and 23% were somewhat confident which is encouraging to see given the breadth and depth of the regulation. The results of both EU and non-EU respondents are largely consistent and give a clear indication of the willingness of non-EU countries to align their standards to those of the European Union.



Almost two-thirds of organisations feel they have enough resources to comply

65% of the respondents across all countries feel they have sufficient resources to sustain GDPR compliance. 49% of these respondents use a combination of internal and external resources, and 16% are exclusively resourced internally to ensure compliance. However, 32% of respondents feel their organisations are not adequately resourced to sustain GDPR compliance. 24% are actively seeking or recruiting, while the remaining 8% have no budget or resources available. Interestingly, more organisations in EU countries indicated they do not have the budget to meet the resourcing requirements, with 10% of organisations surveyed in the EU indicating this, compared to only 6% from countries outside the EU.

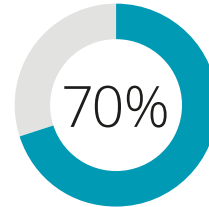
This illustrates one of the most significant challenges many organisations have faced over the last two years with a relatively small experienced labour market and explosion in demand. This has led to new positions being created at organisations that may have historically not focused on the topic, as well many new entrants to the labour market. While experience will take time to build and this imbalance is not likely to be resolved in the short term, the increased focus on the topic has to be a welcome boost in the long term to the amount of skilled people in the privacy profession.



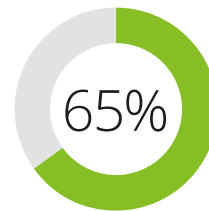
Tools used for GDPR compliance

Respondents were asked if their organisations had made technology investments to support their GDPR programmes. The majority of respondents – over 70% for each of the listed technology areas – claimed to have used internal or external tools to support their compliance activities. The most implemented solution among respondents is Data Loss Prevention technology (78%). The areas least invested-in were DPIA Execution and unstructured data scanning (both 71%). This result correlates with the explosion in vendors offering GDPR-related tooling in the last two years and organisations wanting to use technology to enhance the end-user experience and gain efficiencies where possible.

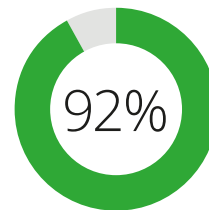
One notable pattern derived from the survey is the difference between external versus internal solutions that are being used for GDPR compliance. Where organisations outside the EU lean towards external tooling, EU based organisations show a preference for internal tools.



of organisations surveyed have seen an increase in staff that are partly or fully focused on GDPR compliance



of respondents across all countries feel they have sufficient resources to sustain GDPR



of organisations surveyed in the EU claimed a level of confidence in demonstrating their ability to conform to GDPR in the long term





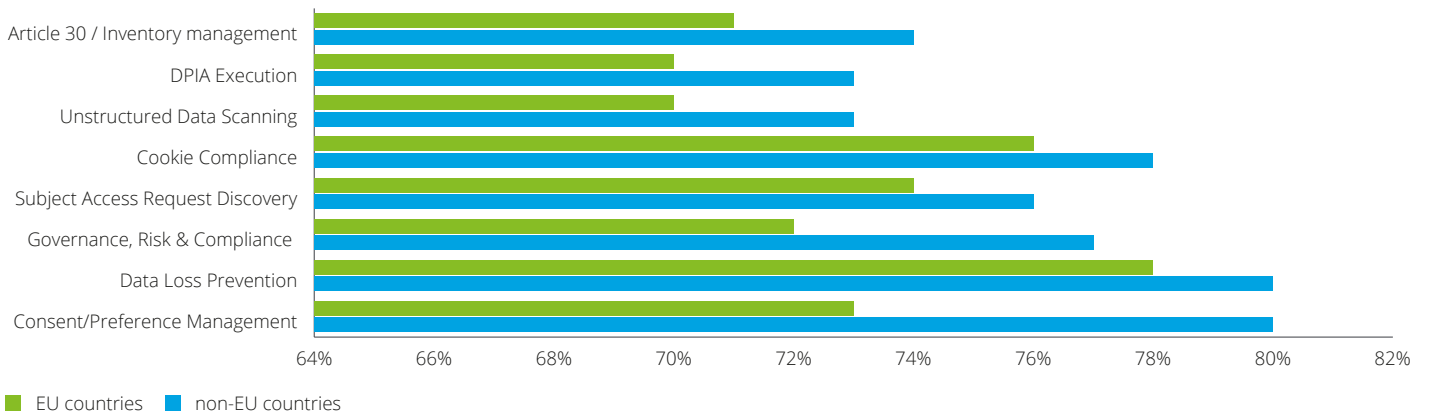
India leads the preparedness charts while Germany needs more work

In terms of Unstructured Data Scanning, there was almost parity amongst all countries with India seemingly being the best prepared. Indian respondents also report to have invested the most in other technologies to support Subject

Access Requests, DLP and Preference management scoring highest in these areas too. This could be attributed to Indian firms handling large amounts of EU citizen data as processors due to the offshoring trend that has been visible in the last 20 years and the drive to be at the forefront of technology. On the other

end of the spectrum, respondents from German firms painted an impression that their organisations were the least prepared and had no plans to make further investments, potentially pointing towards a more process-focused approach as well as a cautious approach to new tooling.

Percentage of respondents that use tools for GDPR compliance



GDPR and the Brussels effect

The survey clearly shows that GDPR's impact goes beyond Europe's borders, contributing to the so-called Brussels effect, where EU regulations have a global effect due to Europe's large market and the pressure for global organisations to adhere to the highest standard. This effect can be observed in many other outcomes of the survey.

Non-EU countries are more reactive in some areas

To deal with the increasing data requests, respondents have claimed their organisations are employing additional staff, outsourcing elements of the service and using redaction tooling. In the majority of cases, non-EU countries are making bigger changes; 44% of businesses from these countries have already allocated additional staff resources while only 36% of businesses in EU countries have done the same. Similarly, 28% of organisations in non-EU affected countries have already implemented outsourcing solutions while only 18% of EU countries have outsourced the service or elements of the service. Whether these organisations are simply more on the forefront of compliance or whether they are coming from a less mature starting point and having to invest more, is unclear. However, what is clear is that non-EU countries are quickly improving their compliance position.



In the majority of cases, non-EU countries are making bigger changes; 44% of businesses from these countries have already allocated additional staff resources while only 36% of businesses in EU countries have done the same.



Control and personal autonomy

When questioned whether the introduction of GDPR gave individuals more control over their personal data, respondents agree that GDPR has given them more control over their data, with a total of 51% of participants agreeing to some extent. Results also show that 42% of those surveyed responded they 'somewhat agree', with a further 30% stating they felt neutral towards this increase in control. This could be attributed to participants being unaware of the greater control they can have over their data, or organisations not yet embracing the possibilities of consumer dashboards, preference centres or more customer-centric approaches to how they handle personal data.

Respondents from non-EU countries gave a more positive response. On average, 6% more respondents from non-EU countries were likely to think GDPR gave them more control over their data, compared to those inside the EU. However, the countries that had seen the least change in this regard were Germany and France; this may highlight the existence of good control in these countries pre-GDPR due to a relatively high regulatory bar, rather than a lack of control since.

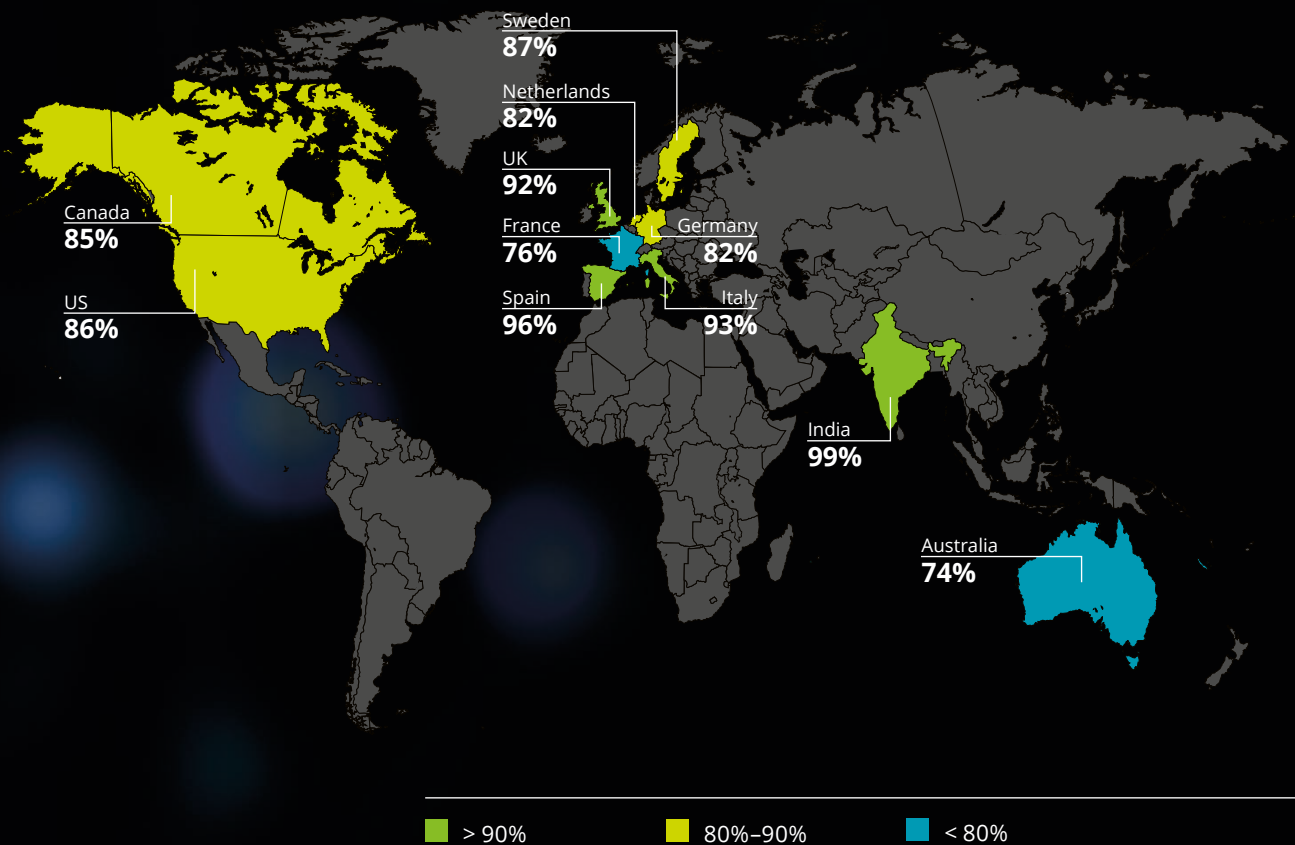
The prominence of the DPO

A large majority (87%) of organisations now have a Data Protection Officer (“DPO”) in place.

Of countries surveyed, 99% of Indian businesses have appointed a DPO, followed by Spain (96%), and Italy (93%). In contrast, only 76% of businesses in France and 74% of businesses in Australia have assigned a DPO for their organisation. Noting that appointing

a DPO is not mandatory for all organisations depending on the personal data they process, these are considered relatively high numbers, but highlight the importance that organisations have placed on having senior accountability for Privacy in their organisations.

Percentage of organisations that have appointed a DPO



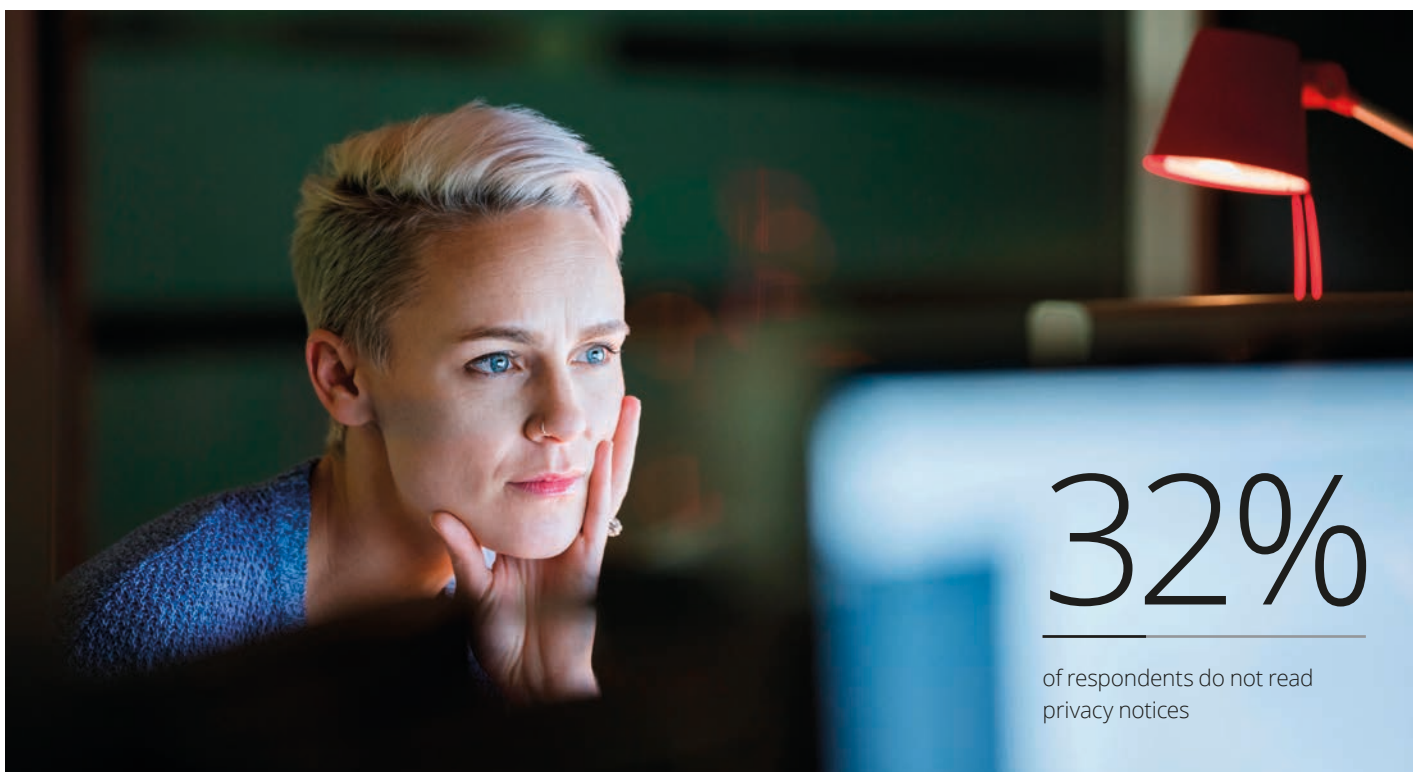
Privacy notices and consumer data rights

One of the key requirements of GDPR is providing individuals greater transparency on how their personal data is handled through the “right to be informed.” This is largely driven by an obligation to provide consumers with clear and transparent privacy notices that highlight how their personal data is being collected, stored and used.

Even with greater transparency, consumers are not necessarily dedicating more time and attention to reading privacy notices. 32% of respondents indicated they still do not read privacy notices, with a higher rate from EU countries – 34% versus 28% outside the EU. Does the knowledge of being protected by strong legislation create a sense of security or are consumers outside the EU simply more careful with their personal data?

Regardless of geographical differences, since the introduction of GDPR, 41% of respondents claim they are paying more attention to privacy/cookie statements generally. 15% of respondents only pay more attention to privacy notices when they are from organisations that they do not know well or trust. Some were negatively affected by GDPR, with 6% of respondents stating they pay less attention to cookie and privacy notices now that the regulation has been put into force.

In addition to this, 42% of respondents remained undecided as to whether privacy notices have become clearer as a result of GDPR, highlighting that some further simplification of privacy notices may be required. Despite this, more than half of the respondents to the survey agree that privacy notices have become clearer as a result of GDPR, which is a positive step, with 17% strongly agreeing with this statement. Only 3% of individuals feel that privacy notices are now considerably less clear.



The introduction of GDPR has strengthened existing rights for individuals, such as the right of access, the right to erasure, and the right to opt out of direct marketing. We have also been introduced to the right of data portability. But how aware are individuals of these rights?

Observations from our survey show that individuals generally have a very high level of awareness, with 78% on average being aware of the key rights that they have. Consumers from EU countries more aware of their rights than those outside the EU, however this varied depending on the right. The EU results indicate the most commonly used and well-known right is the right to opt-out of direct marketing, with 23% of respondents having exercised this right already and with 84% of respondents claiming to know of the right. In non-EU countries, the most well-known right is the right of access (78%).

Right of access

79% of respondents are aware of their right of access, with near identical levels of awareness inside and outside the EU. 10% of respondents have already submitted access requests to organisations that hold their personal data. 21% of respondents had not heard of the right of access and 29% confirmed they have no intention to use it. However, there is a strong likelihood that individuals' awareness of their rights and their propensity to exercise those rights will increase over time as further scenarios that take advantage of these rights emerge and are used to enforce consumer rights.

Right to data portability

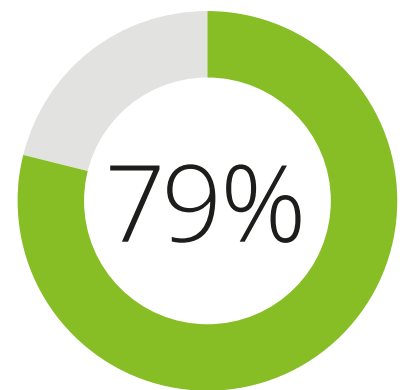
76% of respondents are aware of the right to data portability. 9% revealed to have already submitted portability requests whilst 23% had not heard of the right and a further 24% stated that they have no intention to use it.

Interestingly, we saw 81% of respondents from EU countries are aware of the right to data portability, with the Netherlands and France leading the way in terms of awareness, both at 83%. Only 68% of respondents in non-EU countries were showing awareness of this particular right, where Australia and Canada recorded the lowest awareness; 60% and 62% respectively. This could be attributed to it being the only new data right that consumers have, and therefore less practised before now.

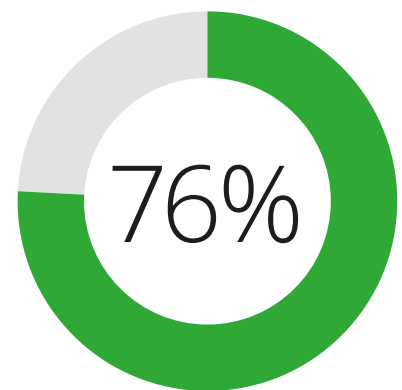
Right to erasure

The right to erasure has already been used by 12% of our respondents making it the second most exercised right from our survey. The trend of increased awareness of rights within the EU continues here, with 79% of EU respondents reporting awareness, compared to 72% from non-EU participants. Netherlands had the highest awareness of this right, with 86%, whereas Canada only had 67% awareness of this right.

Conversely, people from non-EU countries claim that they are more likely to exercise this right in the future (21%) compared to their peers in EU countries (17%).



79% of all respondents are aware of their right of access, with near identical levels of awareness inside and outside the EU



76% of all respondents are aware of the right to data portability

How do consumers use their data subject rights?

Respondent's answer	Right of access	Right to opt-out of direct marketing	Right to data portability	Right to erasure
1. Aware of this right	79%	80%	76%	76%
2. No intention of using this right	29%	21%	24%	26%
3. May use this right in the future	16%	20%	20%	18%
4. Have already used this right	10%	20%	9%	12%

Right to opt-out of direct marketing

Results for the right to opt-out of direct marketing show 80% of respondents are aware of this right with an average of 19% having used it already. Around one fifth of individuals have not heard of this particular right, and a similar number have no intention to use it and likewise, do not mind their data being collected for direct marketing purposes. This would indicate the vast majority of respondents are uneasy about how their data is being used for direct marketing.

Dealing with data requests

Since GDPR came into effect, organisations have had to deal with more stringent requirements surrounding the data requests from clients and consumers. Organisations have seen a large rise across all request types.

The most commonly received request has been access requests with 38% of respondents reporting a doubling or more. Given that a relatively small number of individuals have exercised this right so far, and that others intend to do so in the future, this presents a potential challenge for organisations in how they respond to future increases.

The least common requests received were those opting out of direct marketing, although much of this will be done via self-service functionality. Requests for data portability were stated as having increased by more than five times by 13% of the respondents, making it the most significantly increased data request type, however this is from a very low baseline given that individuals didn't have this right before GDPR was introduced in most cases.



Increasing pressure to respond

Only 30% of those surveyed were able to respond to the data requests received within one month. 37% were either unable to keep up with the volume or only able to respond to just a few within one month. This didn't differ whether the request was for access, portability, erasure or marketing opt-out. With only one third of the requests being answered within the set timelines, organisations might need to reconsider the procedures they have put in place to deal with this part of the regulation. The trend for start-up websites to cater for consumers who want to exercise their right of access requests to multiple organisations via one portal is one to watch in terms of whether these gain any traction, or even if organisations are obliged to respond. With such tools becoming more common and known to consumers, organisations may further fall behind in their struggle to keep up with the volume of data subject requests coming their way.

Do consumers value their privacy?



Limited improvements to personal data management

58% of respondents claim that GDPR has had no or minimal impact on how they perceive organisations to handle their data, despite a large percentage of organisations indicating they had invested heavily in their GDPR programmes. Only 26% felt that organisations had fundamentally changed the way personal data was being handled. This could be due to GDPR programmes placing more focus on internal governance and compliance than being customer-centric programmes, which are typically more costly and complicated to achieve. This also aligns with results of our previous benchmarking survey that showed many organisations were striving for a “defensible” position short-term, and not yet seeing privacy as a true differentiator with their customers.

Deviations were noticed when comparing different countries. Businesses in India (32%) were the most likely to report how they made fundamental changes, while businesses in Australia were the least likely (21%), despite the recently introduced Notifiable Data Breach Scheme in Australia.

Data breaches

Data breaches have received a significant amount of media attention in recent years with a range of flagship multinationals being named for losing large amounts of consumer data, but there is a risk of consumer breach fatigue. Survey results show 17% of respondents claim they would stop using a service or buying from an organisation if a data breach was to occur. Nevertheless, consumer trust and the value the organisation is delivering appear to matter most, with an additional 35% of respondents stating that their decision to stay or go would be dependent on these factors. As with a lot of issues organisations can face, having a solid reputation helps to safeguard your consumer base, re-enforcing the need for strong anti-breach mitigations, timely, confident responses and general consumer trust in handling personal data.

There is no doubt that data breaches are likely to impact consumer trust. 25% of respondents confirm their level of trust with an organisation would decrease if the organisation was involved in a data compromise. Combined with another 35% stating their decision to stay or go depends

on how much they trust an organisation, this serves as a warning to organisations that suffer repeated data breaches, or those less established organisations that may not yet have a trusted brand in the market place.

History of data breaches

Where a history of data breaches is present, 70% of respondents identified this as being a concern and having an impact on their level of trust. 23% remained neutral while 7% disagreed that their level of trust would be impacted.

And more telling is 1 in 10 customers would contact the organisation to find out more if it suffered a data breach, which for a multi-national organisation with millions of customers can represent a significant undertaking. Therefore, catering for response mechanisms such as automated breach response, call-centre overflow and having professional forensics expertise at hand will soon be more commonplace as publicly reported breaches become the norm.

Treat your consumer

The need to respond to consumers' demands in an increasingly competitive environment has become more important than ever, but also more difficult due to a stricter regulatory environment. However, our survey did show that 60% of consumers are willing to share more data to receive personalised benefits and discounts.

Clearly consumers are beginning to understand the value of their data and are more willing to share their personal data if they are rewarded in some way or if they are getting something in return – such as discounts, personalisation, loyalty schemes or other perks.

This demonstrates the growing need for organisations to be customer-centric and to place consumers at the heart everything they do. Organisations should ask themselves what benefit their customers are receiving through the collection of their data, and whether this benefit is significant enough for them to be forthcoming with their information. "Quid pro quo" seems to be the way to the consumers data heart.



58%

of respondents claim that GDPR has had no or minimal impact on how they perceive organisations handle their data



17%

of respondents claim they would stop using a service or buying from an organisation if a data breach was to occur



60%

of consumers are willing to share more data to receive personalised benefits and discounts

Do consumers trust organisations to handle data?



Quality and transparency of privacy policies

Organisations who are transparent about how

they use personal data are rewarded with consumers' much-wanted trust. The survey results clearly show that the majority of respondents (67%) take into account the quality and transparency of privacy policies when deciding the level of trust to place in an organisation to handle their data correctly. This illustrates the importance of privacy notices as part of the consumer journey, and the opportunity to make them a differential element of it rather than a legal necessity. However, this also highlights the current disparity between consumer perceptions and actions; as previously highlighted, many individuals simply don't read privacy notices, so organisations need to find a way to engage in an open, transparent way outside of lengthy written policies.



Ease of control of personal data

Organisations are starting to invest in consumer

preference centres where cookie, marketing and other types of consent can be easily managed. The results of our survey show this investment pays off. Similar to the transparency results, 67% of all respondents agree that easily being able to control their personal data has an impact on the level of trust they have in an organisation. However, as discussed earlier, only 51% of individuals feel GDPR has actually put them more in control of their personal data, so organisations have an opportunity now to increase their level of consumer engagement through more thoughtful, customer-centric data management.



Potential misuse of personal data

An overwhelming majority of respondents agreed this was

an important factor that would concern them (73%), and this was an obvious pattern globally. Where misuse of personal data has always been an ethical concern, GDPR reinforces the prohibition of the use of personal data for other reasons than those communicated and agreed by the consumer. Recent developments have even taken this further and for the first time, misuse of personal data, identified as a data protection issue, has been criminally prosecuted by the UK data protection authorities. This particular case, combined with our results, clearly shows how the misuse of data is turning into an absolute no-go area for organisations, and that the emergence of data ethics will be a key trend in the future.



Data being shared with third parties

Our survey found that 68% of respondents agreed that

sharing of personal data with third parties is a concern. Considering the difficulty of controlling data once it has been shared with a third party, this insight re-enforces the importance of having model clauses, data processing agreements and transparent notices in place.



Excessive collection of data

The excessive collection of data was a significant concern for our respondents with 70%

agreeing that this would impact the level of trust they have in an organisation. This shows a growing concern that organisations collect more data than is required and puts an emphasis on developing ways to implement data minimisation.



Cookie management

Many websites have amended their cookie policies in accordance with GDPR. It's therefore no surprise that consumers are also becoming more aware of how cookies are used by websites to track preferences and activity. 49% of the respondents in our survey claim to actively manage cookies when visiting websites.

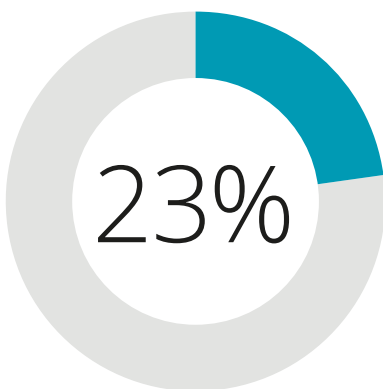
Interestingly, the frequency of how often consumers actively managed their cookies was determined by a number of factors, including their trust in the website, the accessibility in managing the cookies and also how easy the process was. The level of trust was the largest determining factor; 23% of respondents base their cookie management practices on trust and knowledge of the company involved.

30% of respondents claim to manage cookies without any particular factor influencing in their decision, whilst 15% claim to actively manage them on all websites that they visit.

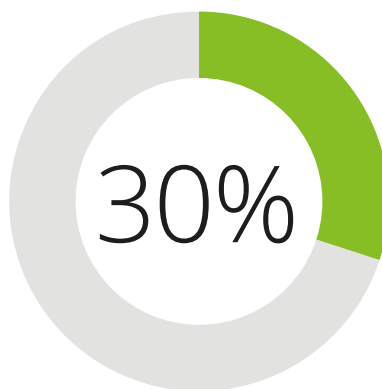
The management of cookies was not influenced by geographical location; percentages of answers submitted were almost identical. This shows consumers globally are becoming increasingly aware of how their information is being processed, as we move towards an ever-advancing technological society.

Excessive use of cookies

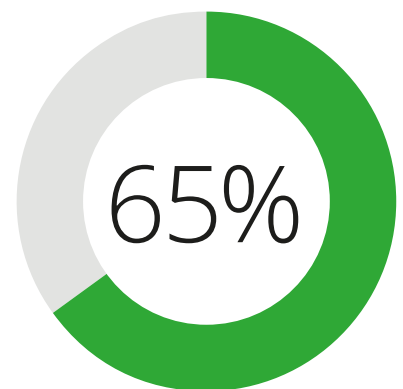
In the EU, more transparent cookie notification requirements have been in place since 2011 and a total of 65% of respondents agree the excessive use of cookies is a concern for them. Again this demonstrates the challenges that both organisations and consumers face given the apparent apathy or reluctance to delve into privacy notices to understand more about them. It is expected that the incoming ePrivacy Regulation will raise further awareness on the use of cookies on websites.



23% of respondents base their cookie management practices on trust and knowledge of the company involved



30% of respondents claim to manage cookies without any particular factor influencing their decision



65% of respondents agree that the excessive use of cookies is a concern for them

The importance of trust



Improving consumer trust seen as biggest driver

On average 59% of organisations observe improving consumer trust as a highly important driver for GDPR compliance activities, with 66% in non-EU countries compared to 56% in EU countries. 24% of organisations claim that this is a medium importance driver. The emphasis on the importance of improving consumer trust seems to be well placed; 43% of consumers in the EU and 45% of consumers in non-EU countries feel as though organisations care more for their privacy since GDPR came into effect. However, our results show that while there is some increase, many consumers have become more aware of how their data is being handled since GDPR has come into effect, but this has translated into more questioning of how organisations handle it, rather than more trust.

Your general reputation as an ethical organisation

With consumers becoming increasingly aware of how ethical organisations behave overall, it is no surprise that 69% of respondents feel that an organisation's general reputation as an ethical organisation plays an important factor in their level of trust in that organisation. Only 24% of respondents neither agreed nor disagreed whilst only a mere 7% overall disagreed.

In particular, respondents in non-EU countries felt more strongly about this issue. As mentioned before, the regulatory environment in Europe is generally more developed with significant potential for repercussions since the introduction of GDPR. This highlights respondents in non-EU countries show more concern about ethical practices of an organisation. This may indicate where country regulations do not enforce ethical behaviour, consumers do not shy away from demanding it themselves.

69% of respondents feel that an organisation's general reputation as an ethical organisation plays an important factor in their level of trust in that organisation

Active regulation of GDPR

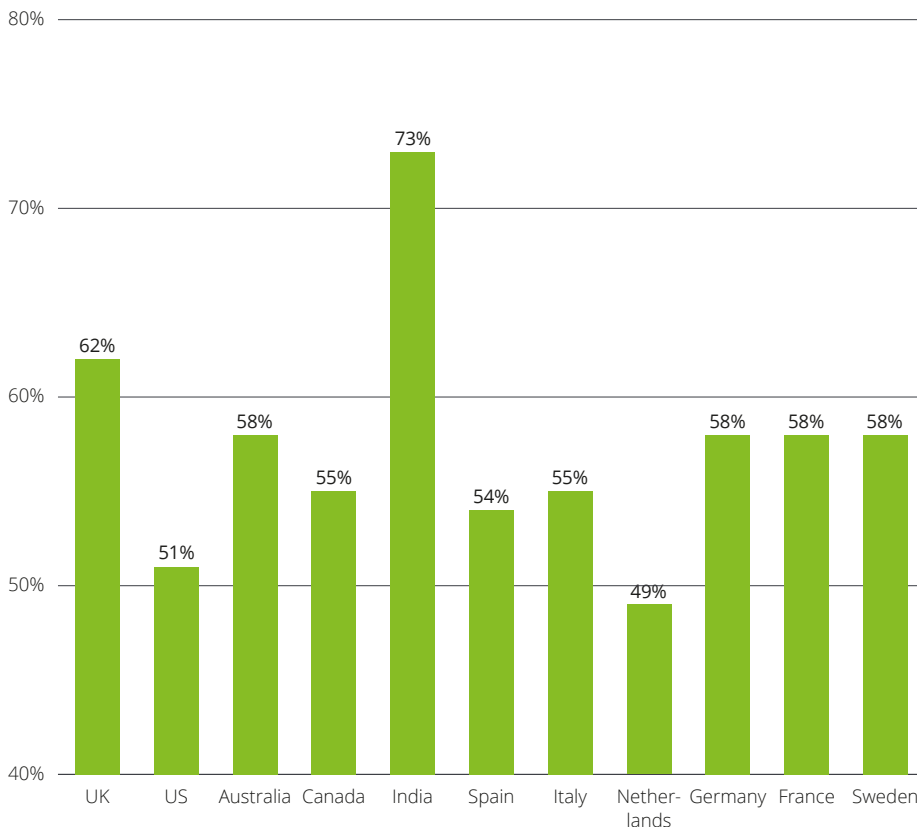
Non-EU countries receive regulatory requests

With the introduction of GDPR, the data protection authorities now have more powers than ever before. According to our survey, they are making good use of their increased regulatory enforcement abilities,

with 57% of respondents indicating their organisations have received regulatory requests from their Supervisory Authority.

The highest number of regulatory requests have been seen by organisations in India (73%), and the UK (62%).

Percentage of respondents that have received regulatory requests



The future of enforcement

Six months in, the level of published regulatory enforcement has been relatively low, but this is not a big surprise. Data breaches continue to receive significant press coverage, but many pre-date GDPR and will be enforced under previous regimes, so it's too soon to get a clear picture on the types of enforcement we can expect to see longer term. The threats of fines of up to four percent of global turnover have grabbed many headlines, but regulators may be reluctant to impose such large fines as they will undoubtedly be met with significant challenge from the recipients. This may lead to long, protracted enforcement procedures that could impact regulators' abilities to uphold the regulation in other areas due to capacity constraints. Regulators will have a fine balance to strike between the frequency and scale of enforcement action.

In addition to regulatory enforcement, GDPR has provided individuals the right to receive compensation where they have suffered material or non-material damage. Organisations now need to be mindful of the potential for class action law suits to be filed against them in these cases, and the coming year will be key in understanding how big an impact these could have.

While these two scenarios represent significant potential impacts, the reputational damage and clean-up costs that can result from a breach cannot be forgotten. Before the introduction of GDPR they presented a significant incentive for organisations to take their privacy obligations seriously and will continue to do so.

What's next?

The results of our survey show organisations have stepped up and invested heavily in their internal compliance activities, and consumers are more aware than ever of their rights, which reflects the positive impact that the EU was aiming for.

Six months, however, is not sufficient to assess whether GDPR will have a lasting impact. Organisations must continue to embed and sustain the changes they have made as consumer sensitivity towards the consequences of data misuse becomes more heightened. The regulatory landscape will also continue to evolve, with more precedent being set on the nature and severity of enforcement to help guide organisations on where to focus.

Below we have set out three key insights that we believe will shape the privacy agenda over the coming year and what organisations can do in response:



1. Customer-centricity and ethics

Greater awareness from consumers of their rights and how their data is used will provide an opportunity for organisations to differentiate themselves by putting customers at the centre of everything they do with their data. There will be greater focus on the ethical use of personal data as well as complying with the regulation.

Organisations have the opportunity to build on their current programmes and identify more sophisticated ways to offer personalised services, putting their customers more in control of how their data can be used. This includes clearer and more innovative privacy notices and increased use of preference centres, as well as more positive reinforcement of their own beliefs and standards around data.



2. Board level scrutiny

Given the significant impact that non-compliance can have, coupled with mandatory breach notification, Privacy is going to remain a board-level risk. This means more scrutiny over business as usual activities and how compliance is being managed, sustained and proactively demonstrated.

Organisations will benefit from clear reporting lines and governance structures to manage their privacy risk. This should include the use of concise reporting tools such as dynamic dashboards that present executive-level summaries on how privacy risk is being managed and trends over time. The reporting has to present privacy risk in the context of the wider organisation to engage the board on what the tangible impacts could be and move away from legalese and theory.



3. Technology and automation

The benefit that technology can bring to streamline existing processes is a well-trodden path across many compliance areas. The current vendor market for GDPR related tooling is very crowded, with dozens of new entrants and existing vendors turning their hand to GDPR tooling. We expect to see some consolidation in the market and a clearer picture on the vendor landscape emerge, with more integration between existing solutions and refinement of current technology offerings.

Many organisations have put in place robust, manual process to manage their privacy risk. These are commonly positioned as a first step in a longer term programme of work that will see more use of automation and technology to make the processes more efficient and reliable. As privacy processes and controls mature, organisations should assess where technology can have the greatest impact and determine which internal or third party solutions, or combination of solutions provide the greatest return on investment.

Organisations must continue to embed and sustain the changes they have made as consumer sensitivity towards the consequences of data misuse becomes more heightened.

Contacts



Peter Gooch
United Kingdom
pgooch@deloitte.co.uk
+44 20 7303 0972
+44 7803 003849



Beth Dewitt
Canada
bdewitt@deloitte.ca
+1 416 643 8223
+1 416 919 0784



Erik Luysterbourg
Belgium
eluysterbourg@deloitte.com
+32 2 800 23 36
+32 497 51 53 95



Manish Sehgal
India
masehgal@deloitte.com
+91 124 679 2723
+91 9818 544 900



Annika Sponselee
Netherlands
asponselee@deloitte.nl
+31 882 882 463
+31 610 999 302



David Batch
Australia
dbatch@deloitte.com.au
+61 2 8260 4122
+61 401 133 033



Daniel P. Frank
USA
danfrank@deloitte.com
+1 312 486 2541
+1 312 401 0125



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2018 Deloitte LLP. All rights reserved.

Designed and produced by Deloitte CoRe Creative Services, Rzeszow. 197705