IDC Executive Brief

Sponsored by: **Symantec**

Author:
Duncan Brown

May 2018

Ready or Not, Here Comes GDPR: The State of European Readiness

Executive Brief

GDPR changes the game for any organisation handling personal data.

The General Data Protection Regulation (GDPR) is one of the most talked-about pieces of new legislation being introduced by the EU. One of the (many) characteristics of GDPR is its extra-territoriality scope, meaning that it applies to organisations in all countries that deal with data relating to people in the EU. Thus, it is often interpreted as a de facto global standard for data protection.

GDPR changes the game for any organisation handling personal data. The rise in business risk associated with personal data, including but not limited to substantial fines, means that organisational behaviour will change irrevocably, and IDC believes that that change is positive. Much attention is given to the high fines, but our research shows that organisations are more worried about the loss of reputation from mishandling data.

Such is the extent of changes required of organisations by GDPR that many will not be ready when the new law enters into force in May 2018. IDC, in conjunction with Symantec, has developed a GDPR Readiness Assessment tool, designed to give a high-level indication of where organisations are in their journey towards compliance. The results show that most have a long way to go: 43% still do not know what GDPR is and how it is going to affect them, or are just starting to learn about the new requirements (*Source: IDC's GDPR Readiness Assessment, Question 1: Which of the following best describes your organisation's approach to GDPR compliance?*).

Organisations fall broadly into two categories: those that aspire to implement enough policy change in order to avoid sanctions from the regulator; and those that identify an advantage to being as compliant as they can be. There is nothing inherently wrong with either of these approaches, as long as they are informed and are a result of a comprehensive business risk assessment.

Some of the more interesting (and controversial) aspects of GDPR include the right to be forgotten (RTBF) and the prospect of a rise in data protection activism. RTBF is one of the most misunderstood requirements in GDPR, and it is difficult both for individuals to understand the rights and for organisations to implement. In the end, we hope that the principle of RTBF will apply, even though this may require some data to be retained for operational reasons. Activist groups are likely to provoke scrutiny of companies that transgress GDPR or are particularly heavily dependent on personal data. Such bodies will be as active as the regulators in holding organisations to account. They may also be engaged in representing multiple

individuals in the case of infringements, leading to the prospect of what are effectively class-action lawsuits.

Don't panic. Organisations first need to increase their awareness of and preparedness for GDPR. Partnering with an expert in information security is a big step in securing personal data. And companies that create a cross-organisational task force stand a much better chance of success than those who do not.

GDPR Overview

GDPR represents the biggest shakeup in data protection and privacy legislation in over two decades. It is one of the most controversial, and most misunderstood, pieces of European legislation in living memory. IDC also thinks that the long-lasting impact of GDPR will be considerably more profound than most observers believe.

It is important to understand the origins of GDPR. The European Charter on Human Rights, formulated in 2000, states in Article 8 that every living human being has the right to have their personal data protected. It is this statement — that data protection is a human right — that underpins GDPR. There are several implications that follow from this:

- Since human rights are not limited to countries of residence, but extend to all living persons, GDPR aims to protect the human rights of all people, not just those resident in the EU.
- GDPR is not negotiable, or a nice to have benefit of living in a developed economy. It is a fundamental underpinning of society.

Whether or not one agrees with the status of data protection as a human right, what is clear is that the EU has the strength of mind to drive its agenda as far as possible. The consequences of this situation are clear to see in GDPR: extra-territoriality in geographical scope, the instantiation of new rights of access, rectification and erasure, and so on.

Previous data protection regulation, agreed in 1995, was identified as having two fundamental flaws:

- It was implemented as the Data Protection Directive (95/46/EC), which was implemented differently in all 28 member states. This led to a patchwork of data protection regimes across the EU, resulting in variable implementation of data protection rights for citizens, and increased complexity and cost of doing business.
- It predated both the widespread adoption of the World Wide Web as a universal information platform and the emergence of social media and other mechanisms for capturing and sharing personal data.

The Data Protection Directive was therefore regarded as being dysfunctional and out of date. One of the common misconceptions around GDPR is that it is vague and therefore difficult to implement. In fact, it is deliberately vague, in order to protect it as far as possible from further technology developments that would otherwise undermine the legislation. This is important because many companies

have struggled to understand the full implications of GDPR, because GDPR relies primarily on a principle-based approach to legislation, and essentially leaves the details to companies to work out, according to their assessment of the risk to individuals' data protection rights. GDPR is also drafted as a regulation, which means that it applies to all member states as it stands, and does not require transposition into local legislation (although there are several opportunities for derogations).

One of the most talked about features of GDPR is its apparently draconian administrative fines for non-compliance (See Article 83). There has been a lot of focus placed on the level of fines, which — IDC believes — is distracting and can be counter-productive. The broad structure of fines is:

- For infringements of the operational aspects of GDPR, €10 million or 2% of worldwide annual revenue, whichever is the higher;
- €20 million or 4% of total worldwide annual revenue, whichever is the higher, for breaches of basic principles, data subject rights, data transfers to non-EU countries, and failure to comply with previous sanctions imposed by a regulator.

Regulators have a toolkit of sanctions that they can use, including imposing a ban on data processing.

The main misconceptions surrounding administrative fines are twofold. The first is that stiff penalties will be levied from the start of the enforcement period, to set an example. However, based on our discussions with regulators, IDC does not believe that heavy fines will be levied in most cases. In fact, companies will have to be egregious in their non-compliance in order to attract the most severe financial penalties. Fines are designed to be "effective, proportionate and dissuasive." In other words, they are designed to hurt companies, in order to change their behaviour, but that pain should be commensurate with the damage caused. And regulators will want to keep their powder dry, should a series of infringements by the same offender occur.

Instead, regulators are likely to use other non-financial levers, in combination with financial penalties, to enforce compliance. This is the second misconception: that it is fines alone that will enforce the law. In fact, regulators have a toolkit of sanctions that they can use, including audits, orders to communicate breaches to affected data subjects, restrictions on processing, and constraints on data transfers (see Article 58). In extreme cases a regulator can impose a ban on data processing, which could put a company out of business.

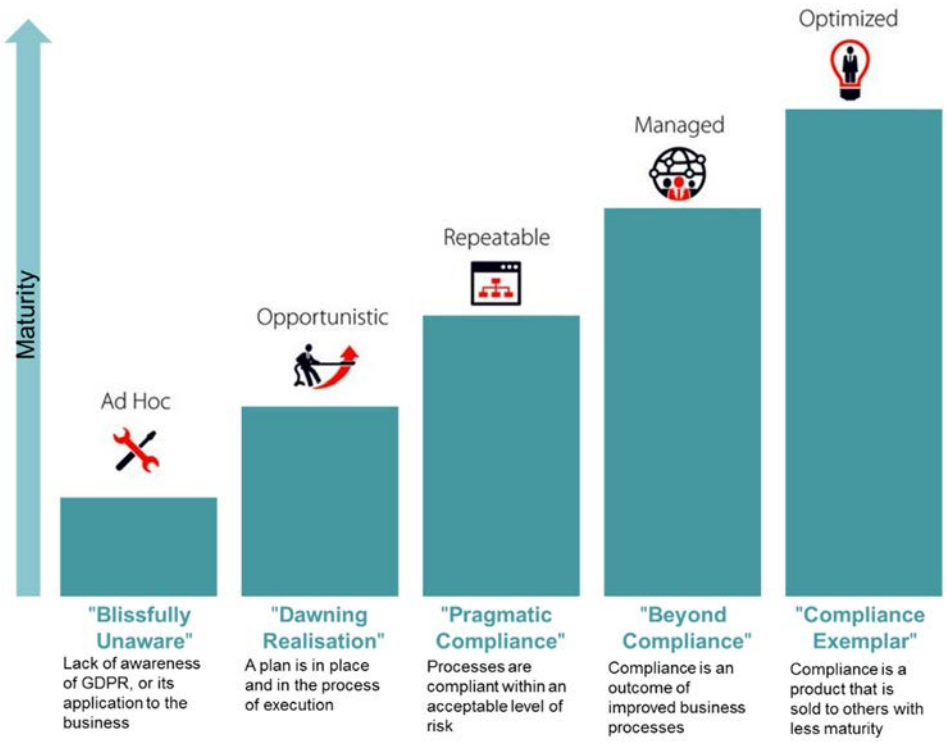
In addition to regulatory powers, individuals may also seek compensation from an organisation infringing their data protection rights (see Article 82). The ability to combine such actions into what is essentially a class action proceeding is also included in GDPR and, as we discuss later in this paper, there are no financial limits specified in GDPR to the extent of compensation that may be sought (see Article 80).

Ready or Not?

In order to help companies assess their state of readiness for GDPR, and to gather insight into the overall state of readiness in Europe, IDC developed a GDPR Readiness Assessment (GRA) tool, in conjunction with Symantec. The tool features a short set of questions, each identified as indicators of understanding, of actions taken, and of overall intentions with respect to GDPR. Although not a definitive assessment of an organisation's state of compliance, it yields substantial insight into how companies are approaching the new regime of data protection.

The tool arranges companies into one of five stages of readiness, with organisations just starting out at stage one, and those that are achieving a high degree of compliance at stage five (see Figure 1). One of the key questions the tool attempts to answer is, what does "ready" look like? Based on other IDC research, and looking at the responses provided in the tool, it appears that readiness is a function primarily of aspiration and assessment of risk.

FIGURE 1
IDC's GDPR Readiness Model



Source: IDC 2018

There are two broad categories of aspiration with regards to GDPR compliance. There are those companies that seem to regard GDPR as an obstacle to overcome, and aim to implement sufficient processes in order to avoid sanctions from a regulator. As long as a full business risk assessment has been done, and compliance is within an acceptable level of risk to executive management, then we think this is an appropriate business strategy. Data captured from the tool tells us that 35% of companies aim to implement GDPR primarily to avoid audits and fines. Organisations that are at stage three in our readiness model fit this profile, and

those that are at stages one and two can reasonably be expected only to aspire to stage three. For example, 26% of organisations using the tool are just beginning to learn about GDPR requirements.

Then there are those companies (26%) that seek to go beyond any minimum standards and aim to achieve comprehensive compliance, or possibly even best in class compliance. These are organisations that, for a variety of motivations, are taking a more opportunity-based approach to GDPR. Again, this is an appropriate business strategy, and companies that are in stages four and five in our model fit this profile.

GDPR is All About Risk

At IDC, we like to say that GDPR is all about risk. The tool examines organisations' approaches to risk related to personal data and reveals some interesting aspects of GDPR that carry specific sources of risk.

The number one identified risk is data protection by design and default.

As Figure 2 shows, the number one identified risk is data protection by design and default. This is a new requirement in GDPR and mandates that organisations must consider data protection at the time at which processing is being considered: that is, at the innovation stage of the business process. Proving that data protection is built in to the business process will be difficult, and organisations are clearly struggling with the concept of embedding data protection considerations into everyday processes.

The second most feared risk relates to defining use cases and managing consent. The rules on consent are often poorly understood. For example, consent is not required in all cases: it is one of six legal bases for lawfully processing personal data. Companies struggle to determine when consent is required, how to ask for and manage consent, and how to set customer expectations.

FIGURE 2

Which Risks do Companies Perceive to be the Greatest Under GDPR?

Question 3: Which of the following GDPR requirements will pose the greatest challenge to your organisation?

Source: IDC 2018

The third biggest risk concerns encryption and/or pseudonymisation of data. Encryption obfuscates data so that only those with authorisation to view the data can do so. But here are many ways to encrypt data, and encryption may break

business functionality, such as analytics, searching and sorting. Importantly, key management is a core discipline, and few companies have skills in this area. Pseudonymisation is the process of decoupling data from identifiers so that it can be processed securely, without individuals being identified. The identifying attributes are kept separately, but can be added back to the data if identification of an individual is required. Pseudonymisation is a relatively new term introduced in GDPR, and as a result is not widely understood.

FIGURE 3

Firms Are More Worried About Reputation Risk Than Administrative Fines

Question 8: To what extent are you worried about the potential consequences of GDPR?

Source: IDC 2018

The punishments for infringements of GDPR are various, as we said earlier. Interestingly, organisations appear to be worried less by administrative fines and more by reputational damage (see Figure 3), most likely stemming from a data breach (although other sources of infringement may also carry reputational risk).

FIGURE 4

Understanding of GDPR is low overall

Question 9: What is limiting your ability to establish full GDPR compliance across your data management environment?

Source: IDC 2018

Organisations are also worried simply about the understanding they have of the data they are processing: 71% of firms think that a lack of knowledge about GDPR is limiting their compliance (see Figure 4). One of the key requirements of GDPR is to know what data exists in the organisation, why it exists, who owns the data and can access it, and how long it needs to be kept. As we can see in Figure 5, most organisations are not confident in their abilities to achieve these basic requirements: of most concern are the 69% of organisations that are not confident that they know where their personal data is. But overall, adherence to the core principles of GDPR, as stated in Article 5, is low.

FIGURE 5

Adherence to the Core Principles of GDPR is Low

Question 4: How confident are you that you can identify and locate every instance of an individual's personal data in your systems?

Question 5: At a high level, does your organisation have insight into each of the following types of data today?

Source: IDC 2018

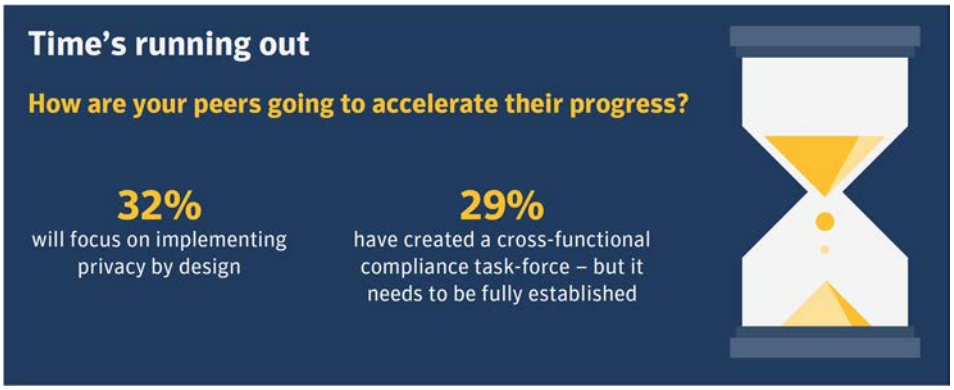
If the vast majority of organisations are ill prepared for GDPR, what should they do? 32% of firms will focus on implementing privacy by design concepts, in an attempt to embed data protection principles into their organisations (see Figure 6). This is a noble aim but one that will be implemented only over a substantial lapse of time: privacy by design is not a quick fix for GDPR. IDC thinks that one of the critical success factors for a successful GDPR program is to create a cross-functional compliance task force that spans all parts of the business that deal in personal data. But only 29% have done this, meaning that the majority of programs will sit in silos, and risk missing key elements of operations that touch personal data.

FIGURE 6

Good Intentions, Not Much Action

Question 2: Which of these GDPR-specific areas do you think your organisation will need to focus on the most? (Response: Implement privacy by design and privacy by default)

Question 7: Regarding leadership of your GDPR programme, has your organisation established a cross-functional compliance taskforce or governance board that involves GRC, IT, and operational stakeholders?



Source: IDC 2018

RTBF is easy to misinterpret and it may also lead to unintended consequences.

The (Infamous) Right to Be Forgotten

One of the most misunderstood articles in GDPR is the right to erasure, commonly referred to as the right to be forgotten (or RTBF, see Art 17). The principle behind RTBF is sound: data should only be held for as long as it is needed to fulfil the purpose for which it was gathered. If data is no longer required by an organisation, we should delete it. If organisations forget to do this, then it is reasonable to allow an individual to have the right to request the data's deletion.

However, RTBF is easy to misinterpret and it may also lead to unintended consequences. Consumers may read RTBF as the right to demand that an organisation forgets everything about them, including useful or legally required information. Similarly, organisations may believe that they are obliged to forget information that may be required in the performance of the contract, such as customer account details and records of transactions. Neither of these situations applies under GDPR.

In fact, RTBF is not an absolute right — data controllers can decline requests, for example in cases where data is required in legal obligations or is held in the public interest. In most cases, we think that RTBF will apply where a data subject withdraws consent, having previously provided this as the lawful basis for processing. In most other cases, where consent is not depended upon for lawful processing it is less likely that an RTBF request would be successful.

RTBF may also be difficult to implement technically. There has already been a court case in the Netherlands where a data subject tried to have his data removed from an immutable blockchain application. It's also unclear whether RTBF requests also apply to backup and archiving copies that may exist on old tape storage devices.

Do data subjects understand the full implications of an RTBF request? A request to be forgotten entirely will remove all references to that data subject, including those that may prevent further contact from being made. For example, a do-not-call list may have to retain some data in order to know not to call a data subject. In other words, some data may have to be retained in order to implement the spirit of a report request. Pragmatically, we think that most data subjects will understand and accept this situation, but there may be instances where this is not true, leading to confusion and frustration on both sides.

The Impact of GDPR on Consumers

So far, most of the impact from GDPR has been experienced by the corporate sector based on revisions of business processes, risk reappraisal and mitigation strategies, and the implementation of new technology. If this represents wave one of GDPR, then wave two will be focused on consumers and citizens.

The first question then is, do consumers care about personal data? It is arguable that they do not: they seem happy to create and distribute their own personal data at scale without regard for its intended destination or purpose. It's clear that no one reads terms and conditions for services provided. This is verifiable: PayPal's

terms of service are longer than Hamlet at over 30,000 words. Consumers are happy to agree to WiFi terms and conditions that demand rights to a first-born child, painting snail shells, or oblige people to unblock sewers.

Do consumers understand the impact of sharing personal data? There is little evidence to suggest that this is the case, but there are sufficient instances that may predict a different situation in the future. The recent turmoil surrounding Facebook, Cambridge Analytica, and AIQ has been well publicised and shines a light on the third-party use of data for purposes unknown to the data subjects. Healthcare data seems rarely to be properly protected, despite its highly sensitive nature. The sector regularly tops the tables of data protection offenders produced by regulators and privacy watchers.

Financial information is also highly sensitive, and is also frequently spilled. The Equifax breach in 2017 leaked millions of data records. The recent TSB Bank outage may also transgress GDPR: Article 32 obliges organisations to ensure the "availability and resilience" of data processing. And the rise in ransomware attacks also affects GDPR compliance, with the definition of a data breach including "unlawful destruction, loss, (or) alteration" of personal data.

Slowly and gradually, consumers are becoming more aware of the sensitivities surrounding their personal data, and the risks associated with it. They are also increasingly aware that organisations have a moral and legal responsibility to protect that data. As this awareness grows, and more companies are scrutinised for their failure to adequately protect personal data, we think that the balance of power will shift from organisations to consumers.

The end game is a rise in data liquidity, where consumers confer rights (via consent) to use personal data to named suppliers, or possibly data brokers. Effectively, consumers are giving a license to selected data controllers to process the data, for which consumers may receive monetary recompense and/or additional services. Organisations will need to treat consumers not only as customers of their core service but also as suppliers of the data that enables them to provide that service in the first place.

The key concepts in creating data liquidity is Data portability (See Article 20). Data portability enables transfer of data between suppliers, allowing consumers to move their data wholesale from one provider to another, at no cost to them. This ability unpicks the stickiness of providers' offerings, and should lead to an increase in customer churn. Churn is a well-recognised concern in some markets, such as mobile telephony, but is very rare in others, like financial services. IDC thinks that data portability will at the very least drive high levels of personal data protection. If consumers believe that the data is not being adequately protected it will be easier for them to defect.

The barrier to data portability is the network effect, which states that the usefulness of a service is proportional to the square of the number of users. Thus, consumers may be reluctant to switch to an alternative provider if their friends and contacts are not on the new service. Primarily, this affects social media providers, which are dependent upon network effects. But it is possible that activist engagement could sway this balance.

Class-action lawsuits pose a greater financial risk than fines.

The Rise of GDPR Activism?

The consequences for infringements of GDPR have tended to focus on the substantial fines which can be levied by regulators. While these are indeed significant, there is a potentially greater financial risk from the prospect of class-action lawsuits on behalf of data subjects.

While the term "class action" is not used officially, GDPR allows not-for-profit bodies to represent data subjects in the case of an infringement (See Article 80). This representation can apply to the rights of data subjects in their pursuit of recourse if they are a victim of an infringement. This recourse ranges from a simple complaint to regulator, to a complaint against the judgement of a regulator, and to a complaint of an infringement by a data controller or processor. The right to representation is important, because it includes the rights to receive compensation (see Article 82) which then opens the prospect of multiple financial claims for damages. Article 82 confers a right for any person "who has suffered material or non-material damage" to claim compensation from the controller or processor. There are several interesting dimensions to this part of GDPR:

- Damage does not need to be material, but can simply be the fact that an infringement has occurred. Although it is likely that non-material damages will attract lower levels of compensation than material claims, this is not codified in the legislation. Such non-material actions could include claims for distress, anxiety or reputation damage.
- Compensation is payable as a result of an infringement. Infringements are not limited to personal data breaches, but could, for example, relate simply to the failure of an organisation to process a data subject access request (see Article 15) or RTBF request within the time allowed (typically one month).
- There are no limits on the compensation payable by controllers or processors. This means that, potentially, such multiple claims may exceed the limits of administrative fines levied by regulators.

We expect not-for-profit bodies that are appropriately informed on data protection matters to represent data subjects. It is widely argued that such representative actions will be pursued by nefarious groups seeking to do harm to organisations, particularly those they may disagree with on a basis of differing principles or ethics. GDPR pre-empts this type of action to a degree: it mandates that such representing bodies must have "statutory objectives which are in the public interest, and (be) active in the field of the protection of data subjects' rights". In other words, representing bodies cannot be commercial operations, or be engaged in activities that are not in the public interest. The types of bodies we think will engage in such representation activity will be consumer rights outfits and privacy advocacy groups.

Nevertheless, interested bodies could affect substantial financial damage upon infringing data controllers and processors. It is conceivable that they may corral groups of data subjects and pre-empt an infringement by coordinating individual data subject access requests to a single company. Such a coordinated approach could swamp a target and subsequently strain the resources of the firm, meaning it

would be unable to service all requests and thus be in a position of non-compliance. At the very least, such action would test the resilience of a company to demonstrate its GDPR compliance, but in many cases would result effectively in a denial of service attack from a deluge of relatively trivial requests.

It remains to be seen whether activist organisations do, in fact, orchestrate campaigns against specific companies. However, the prospect is real and organisations need to assess the risk and take appropriate preparatory action.

Conclusion

GDPR is a force for good. It updates existing data protection law that is hopelessly out of date, and tidies up legislation across EU member states into a cohesive set of rules. It also reinforces data protection as a human right, and prompts organisations to treat personal data with the respect it deserves. GDPR is designed to change the behaviour of organisations in the treatment of personal data: eventually, we think, it will also change the attitude of individual data subjects towards how our own data is handled.

FIGURE 7
Actions to Speed up Progress

Source: IDC 2018

Organisations cannot ignore GDPR. They must embrace it, organise for it, and embed it in the business processes. Data protection is not something that is extra: it is integral to everything that organisations do.

In order to make rapid progress in GDPR compliance, we think organisations can focus on three fundamentals (see Figure 7).

- Understand where you are in readiness for GDPR. Self-awareness is the first step to enlightenment, so try our self-assessment tool to give you a starting point.
- GDPR is not just about IT or security, but we also believe that organisations cannot be compliant without the application of technology. In particular, the requirements for information security are key, not just in the adherence to security requirements (see Article 32) but also more broadly in

controlling access to personal data, and the use of encryption and other pseudonymisation techniques to remove data from GDPR scope.

- GDPR is not an IT issue, or even a legal issue. It is a business concern, and multiple areas of the organisation will be affected by GDPR. Typical GDPR programs involve sales, marketing, human resources, accounts and customer service. Make sure you involve all of your stakeholders in a GDPR program, and establish this as a continuous review process.

Investment in GDPR processes and solutions will pay off in the long term.

Finally, remember that GDPR is here to stay. It is not a one-time effort to become compliant, after which we can return to old habits. Any investment in GDPR processes and solutions will pay off in the long term. Good luck!

About the Research

IDC developed a short questionnaire comprising nine key questions, each identified as indicators of understanding, of actions taken, and of overall intentions with respect to GDPR. These questions were developed based on a deep understanding of GDPR requirements and also of prevailing attitudes to GDPR as revealed in IDC's GDPR Readiness survey 2017.

We compiled the nine questions into an online tool, the IDC GDPR Readiness Assessment (https://symantecgdpr.idcready.net), which is free to complete and which provides an indicative assessment of the respondent's organisational preparedness for GDPR. The tool is available in English, French and German. Respondents can optionally download a tailored report detailing IDC's assessment of GDPR readiness.

The figures cited in this report are based on the responses of 1601 participants who completed the assessment between November 2017 and April 2018. Responses from Germany numbered 150, France 211, and the UK 499, with balance of responses coming from other countries. All statistics were correct at the time of writing.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.