IDC PERSPECTIVE

10 Myths Regarding GDPR: Sifting Fact from Fiction

Kuan Hon Duncan Brown

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: 10 Myths Regarding GDPR: Sifting Fact from Fiction

This IDC Perspective aims to clear up some common myths, particularly – but not only – those relating to security. The prospect of big fines under the General Data Protection Regulation (GDPR), which applies in all EU member states beginning May 25, 2018, has motivated a scramble to implement compliance programs before the deadline, including those related to security. However, many misunderstandings and misconceptions about GDPR seem to be prevalent.

Key Takeaways

- GDPR is important to address the increased risks associated with processing personal data.
- GDPR is one of the most significant pieces of legislation ever to impact the technology industry, but there is a substantial amount of misunderstanding regarding the new law's scope, applicability, and enforcement.
- GDPR increases the obligations on both technology buyers and suppliers, and so it is critical that both parties understand the new requirements. In particular, the extension of liability from data controllers to third-party processors means that understanding the impact on customer-supplier relationships is critical.

Recommended Actions

- Information and advice on GDPR are abundant, but much of it is mistaken, some dangerously so. Only use sources that you deem reliable — and accountable.
- One of the best sources of information on GDPR enforcement are the enforcers — the regulator community. Regulators are surprisingly open to discussion and advice, so use them as valuable sources of input.
- Ultimately, GDPR is all about risk. Any decision made regarding GDPR should be set in the context of a holistic risk assessment, which should drive each company's compliance activities.

Source: IDC, 2017

June 2017, IDC #EMEA42628217

SITUATION OVERVIEW

The prospect of big fines under GDPR, which applies in all EU member states beginning May 25, 2018, has motivated a scramble to implement compliance programs before the deadline, including those related to security.

In particular, service providers that store or process personal data, such as cloud services providers, will for the first time be subject to certain obligations as data processors, including the requirement to implement appropriate security measures. GDPR will oblige both controllers (those that control the "purposes and means" of processing personal data) and processors (such as service providers) to take measures to ensure a level of security for the personal data they process that is appropriate to the risk to individuals. Both types of firms will also be subject to certain breach reporting requirements under GDPR.

However, many misunderstandings and misconceptions about GDPR seem prevalent. This IDC Perspective aims to clear up some common myths, particularly — but not only — those relating to security.

One very important issue to clear up is that in this study, "security" and "security breach" are used in the same broad sense. Under EU data protection laws, "security" is used in the broad sense of "information security," meaning not just technical security but also security through people and processes. In the words of the legislation, "security" requires "appropriate technical and organizational measures" to protect personal data as commensurate with the risks, particularly from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. A "security breach," for data protection law purposes, includes data breaches, not just technical security breaches. For example, leaving papers containing personal data in a plastic bag on the train would be considered a "security breach" by data protection authorities under EU data protection laws, just as much as if a hacker uses SQL injection to access personal data in a database behind a badly coded website.

ADVICE FOR THE TECHNOLOGY BUYER

Information and advice on GDPR are abundant, but much of it is mistaken, some dangerously so. Only use sources you deem reliable — and accountable. There is much bad advice coming from those who think they understand the law just because they can read the GDPR, and organizations are relying on their advice. The myths we have encountered demonstrate how tricky and difficult it is to understand and interpret the legal issues, even among people who are data protection experts. While nonlegal professionals can be a useful source of information, it would be a mistake not to at least get advice from a law firm from time to time, ideally working in conjunction with other engaged parties.

One of the best sources of information regarding GDPR enforcement are the enforcers — the regulator community. Regulators are surprisingly open to discussion and advice, so use them as valuable sources of input. It is notable, however, that the regulators seem to be as overwhelmed by GDPR as the rest of the market. They are scrambling to issue guidance on a variety of ambiguous areas in GDPR (of which there are many), and their bandwidth is extremely limited. Nevertheless, they are keen to engage with the data protection community, and several are running briefing sessions, workshops, and full-scale conferences to try and guide companies.

Ultimately, GDPR is all about risk. Any decision made regarding GDPR should be set in the context of a holistic risk assessment, which should drive companies' compliance activities. If in any doubt as to the intended outcome of GDPR compliance, we suggest referring to the core principles included in Article 5. Any course of action that is consistent with these principles is likely to be on the right course toward compliance (and the converse is also true).

IDC'S POINT OF VIEW

Myth 1: GDPR is Like Y2K

Some firms are tackling GDPR with the same hysteria prevalent when addressing the Y2K millennium bug. In other words, they are approaching GDPR as a single project with a defined end date, where success is binary — you are either successful, or planes will fall out of the sky. This is a myth.

GDPR will entail a new way of working, not just a "point in time" activity. Just like the common saying (coined by Steve Lipner in 2002) "security is a journey, not a destination," data protection law compliance should also be viewed as an ongoing, never-ending process.

Much of the current compliance focus seems to be (in the security world, at least) on avoiding breaches (data or security). This is dangerous, as it ignores a host of other issues in which noncompliance could lead to a huge fine (further discussion next). In other words, security is not the only compliance issue.

There is another aspect to the Y2K comparison — many firms now believe that Y2K was overblown, at best overstated, and at worst a hoax to drive IT revenues. Skepticism is rife regarding GDPR, as proven by several other myths discussed later. IDC's view is that compliance with GDPR — as a law — should be the default position for legitimate firms, and those deviating from this stance must understand the associated risks.

Myth 2: No One Will get Fined

Some consider the risks of heavy fines as over-exaggerated, and that GDPR will be proven in time to be a storm in a teacup.

Regulatory Resources are Limited, So No One Will get Caught

It is true that, under GDPR, it will be harder for the national data protection authorities supervising compliance with data protection laws to investigate and sanction infringements. GDPR is more prescriptive than current laws and expands data protection obligations. This means there will be more for authorities to oversee. They will have more work to do, yet they are likely to have less money to do it with. GDPR will do away with the filing/registration fees payable by controllers that process personal data fees that many authorities have relied on for funding hitherto. This means some authorities will struggle to get enough funding to resource their regulatory activities fully. Hence, in March 2017, data protection authorities — in what is known as Article 29 Working Party or WP29 — collectively wrote to EU member state governments, urging them to provide their national authorities with sufficient financial and human resources to conduct their duties (see the letter on Article 29 available at http://ec.europa.eu/newsroom/document.cfm?doc_id=43668). However, even if more funding is provided to authorities, it is never likely to be enough, given the scale of personal data processing in the EU.

Targeted Enforcement is Likely

Authorities will probably have to take a strategic, targeted approach to enforcement. They won't have enough resources to go after everyone; they can't possibly investigate or act on every single complaint. This means they are likely to go after the most high-profile firms and/or firms engaging in personal data processing practices they consider particularly egregious. In that sense, the biggest firms may act as "shields" for smaller firms; however, if smaller firms engage in seriously infringing practices, they might still be fined to "make an example."

Consequences Could be Dire for Enforcement Targets

For those targeted for enforcement, the ceiling for fines could be 4% of the total worldwide group turnover in the past financial year (or €20 million if higher), depending on their status under data protection laws (as data controller or processor) and exactly which rule has been infringed. There could also be reputational damage if the infringement and fine are publicized.

Furthermore, national non-governmental organizations (NGOs) may be able to claim compensation on behalf of individuals, depending on each EU member state — not class actions as such, but similar. The potential total compensation if such claims are brought could be enormous, and a firm could potentially find itself facing both regulatory fines and lawsuits.

Thus, every firm will have to make its own GDPR risk assessment in the context of its own business operations. Taking the "ostrich head in sand" approach of assuming no one will get fined is a risk with potentially very high impact.

Myth 3: Everyone Will get Fined 4%

First, there are two tiers of fines that apply. The higher tier has a ceiling of 4% group turnover in the past financial year (or €20 million if higher), while the lower tier has a ceiling of 2% group turnover in the past financial year (or €10 million if higher). Which tier applies will depend on exactly which rule has been infringed.

Generally, only controllers — firms that control the "purposes and means" of processing personal data — risk higher-tier fines, although for a few rules, lower-tier fines apply. Generally, processors, such as service providers, are only subject to lower-tier fines, with one important exception — if they make international "transfers" without following GDPR's restrictions and conditions.

Certain Factors Affect Whether and How Much to Fine

The figures or percentages concerned are ceilings, not floors. They constitute the maximum amount that an authority could issue a fine for. It could decide to issue a lower fine, or not fine a firm at all, depending on the circumstances.

In deciding whether to fine and how much, authorities are required by the GDPR to take into account certain factors:

- Categories of personal data affected (e.g., how sensitive was the affected data, such as health data or data about sex life)
- The nature, gravity, and duration of the infringement, taking into account the nature, scope, and purpose of processing, number of individuals affected, and how much damage they suffered
- Whether the infringement was intentional or a result of negligence
- Whether any action was taken by the firm to mitigate the damage suffered by individuals
- The firm's degree of responsibility, taking into account the measures it implemented under the new obligation of data protection by design and default, as well as its security measures
- Any relevant previous infringements
- Extent of firm's cooperation with the authorities to remedy or mitigate the infringement's possible adverse effects
- How the authority find out about the infringement, particularly whether the firm notified authorities about the infringement, and if so, to what extent
- The extent to which the firm complied with any previous orders against it on the same subject matter

- Adherence to approved codes of conduct or approved certification mechanisms
- Any other relevant aggravating or mitigating factor, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement

This means if a firm owns up to an infringement and reports it to the authority, the authority might reduce the fine, whereas if the firm tries to hide the infringement and is later found out, the authority could increase the fine in consequence. Similarly, if a firm deliberately tries to save costs (gain financial benefits) by skimping on security measures to protect personal data, that would be an aggravating factor. However, it also means firms can take precautions in advance to try to minimize or even avoid fines in the event of future infringements, such as by implementing appropriate security measures and security by design. Evidence of effort and intent to comply — such as properly documenting how security decisions were reached and maintaining adequate records, logs, and audit trails — will always be regarded favorably by regulators. The absence of evidence of steps taken for compliance will equally count against the firm.

Note that noncompliance with a supervisory authority's order to do or not do something, such as to implement certain security measures, always risks a higher-tier fine.

Myth 4: Noncompliance is Equivalent to a Security Breach

Security Breaches Often Result in Fines

It is true that currently, many fines are for security breaches. For example, in the U.K., majority of data protection law fines have been for security breaches, most of them involving human error rather than technology. However, the higher tier of fines applies — under GDPR Article 83(5) — to breaches that are considered fundamental principles of data protection law — such as fair processing, data minimization, purpose limitation, and data retention — or processing personal data without a recognized legal basis such as consent or legitimate interests.

In the U.K., fines for security breaches have been increased because personal data that were no longer needed were not deleted or anonymized and were affected by a breach, whereas if obsolete data were deleted, obviously the breach would not have put those individuals at risk.

Authorities View Compliance with Basic Principles as Critical

Furthermore, compliance with all the fundamental personal data processing principles will be important, not just security measures.

As those principles are considered critical under data protection laws, it is likely that some authorities will seek to send a message by imposing high fines on firms that infringe those principles (or particular principles), especially if they are doing so systematically and/or deliberately — whether or not a security breach is involved.

A Data Breach is not the Same as an IT Security Breach

It is worth reiterating that a data breach, which will be treated as a "security breach" under data protection laws if it involves personal data, can be caused by a wide variety of actions, not all of which pertain to technical security of IT systems. Clearly, an IT security breach might lead to a data breach, but this is not necessarily the case. In fact, the detection of an IT security breach and subsequent prevention of a data breach should be regarded as a success.

Myth 5: For Security Breaches, the Fine is Only 2%

Controllers are Subject to Higher-Tier Fines for Security Breaches

If a firm is a controller, personal data security (particularly confidentiality and integrity) will be considered a fundamental principle under GDPR Article 5(1)(f). Accordingly, a higher-tier fine applies if a controller fails to implement appropriate security measures for personal data. This means both technical and organizational measures (i.e., people, policies, and processes as well as technology/systems), including steps to protect against insider threats. GDPR's security requirements extend, as appropriate, to measures for confidentiality, integrity, availability, resilience, business continuity and disaster recovery, encryption and pseudonymization of data, and regular testing to evaluate the effectiveness of these measures. A data breach is the clearest indicator that appropriate security measures have not been implemented, but other factors or situations could lead authorities to conclude that a firm has not taken appropriate security measures, such as a regulatory investigation following a customer complaint or on the authority's own initiative.

Processors are Subject to Lower-Tier Fines for Security Breaches, but Could Still be Sued

In contrast, if a firm is a processor, then security breaches only carry a lower-tier fine. However, as with controllers, it is still exposed to the risk of compensation claims for the security breach (see further discussion next), which could be very large if NGOs sue on behalf of numerous affected individuals.

Myth 6: All Security Breaches Have to be Reported Within 72 Hours

Only Personal Data Breaches are Reportable

First, only "personal data breaches" must be reported, which is narrower than security breaches generally, and narrower than "data breaches." Essentially, this means breaches of confidentiality or integrity affecting personal data rather than availability — although of course in some situations, incidents affecting availability may also compromise confidentiality, integrity, or both.

Reporting Obligations Vary with the Firm's Role

Second, breach notification obligations depend on the status of the firm under data protection laws, as controller or processor.

Note that the status of a firm will depend on particular factual circumstances. The parties' labels and what is stated in their contracts will not be determinative.

Controllers' Reporting Obligations and Timing Depend on the Risk

If a firm is a controller, personal data breaches may have to be notified, separately, to authorities and individuals. It must notify the data protection authority of personal data breaches, unless the breach is "unlikely to result in a risk" to individuals' rights/freedoms, which is a very low threshold. It must notify the authority without undue delay, and where feasible, within 72 hours after the firm becomes aware of the breach. Thus, the deadline is not 72 hours after the breach occurred, but 72 hours after the firm knows about it. If it is not feasible to report to the authority within 72 hours, the firm can take longer to notify, as long as it does so without undue delay, and explains the reasons for the delay to the authority.

A controller must also notify individuals of personal data breaches without undue delay, but only where the breach is likely to result in "high risk" to their rights/freedoms. Furthermore, it does not have to notify them, even of a high-risk breach, if it had applied appropriate security measures to the affected data, particularly so as to render the data unintelligible to unauthorized persons (e.g., by properly encrypting the data, taking steps after the breach to make that high risk "no longer likely to materialize," or if notifying them would involve disproportionate effort, it must inform them equally effectively through a public communication or similar).

Processors are Required to Notify Their Controllers

If a firm is a processor, it must notify personal data breaches, without undue delay, to the controller that engaged it. This is the time for the controller to notify authorities and individuals. No indicative time limit is given for processors.

Myth 7: It is Safest not to Report Security Breaches

Some firms may think that if they conceal security breaches from authorities, they will not get fined.

The Authority Could Find out Anyway

The risk of course is that the authority may find out about the breach from other sources, whether via data dumps, members of the public (e.g., complaining customers), whistleblowers, or even the media. If so, the authority could fine the firm for the security breach, increasing the fine because the firm did not self-report.

Firms Could be Fined for Failing to Report Personal Data Breaches

Furthermore, if the security breach involved a "personal data breach," the authority could impose a lower-tier fine on the firm for not reporting it when it should have. In other words, the requirement to notify personal data breaches itself carries a lower-tier fine if infringed.

Myth 8: To Comply with GDPR, We Have to Encrypt Everything

This myth is wrong. The requirement is to implement measures to ensure a level of security appropriate to the risks among individuals (both likelihood and severity) for every situation, including storage and transmission, taking into account the state of the art and implementation costs as well as the nature, scope, context, and purposes of processing. In other words, the approach to security measures is risk-based, and factors in both what technology is available at the time and the costs involved.

Encrypt Only Where Appropriate

Encryption is specifically mentioned, but it is not necessarily essential. It only needs to be applied to personal data where it is appropriate, considering the risks. Thus, stronger security measures should be applied to sensitive data (e.g., health data), such as encryption with more secure algorithms and longer keys. Encryption of transmissions is likely to be considered appropriate in many situations.

Encryption may Have Disadvantages

Bear in mind that key management is never easy, advanced decryption technologies may emerge (e.g., based on quantum computing), and encryption can reduce business functionality (e.g., searching, sorting, analytics), although format-preserving encryption is being used for cloud data to prevent cloud providers from accessing intelligible customer data while maintaining full functionality for the customer. Furthermore, encryption could reduce security functionality in that encrypted traffic cannot be read by many detection technologies.

Myth 9: You can Outsource GDPR Liability for Security to Third Parties

GDPR will significantly increase supply chain risk in which any personal data processing is involved.

Controllers Generally Remain Liable for Security and Other Compliance Issues

A controller remains liable for the security of personal data under the GDPR, even if it chooses to outsource some, or all, of its processing to third-party processors. It could still be fined for security breach in the supply chain, although if its own security measures were appropriate and the controller itself is not at fault, this may help reduce or avoid a fine.

Furthermore, a controller could also be sued if individuals suffer damage — financial or otherwise — from the security breach or other noncompliant processing. If so, unless it can prove that it is not in any way responsible for the "event giving rise to the damage," it must compensate them for all the damage.

The key legislative policy objective is to ensure that individuals are fully compensated. They can effectively decide to litigate against anyone in the supply chain, as is most convenient for them. How the different parties in the supply chain sort out the fault and liability among themselves is a much lesser policy concern. Note that it will be for the controller to prove its own lack of responsibility (if that is the case). It needs to make sure it can evidence its own compliance, so records, logs, and audit trails will be much more important. Having a code of conduct or certification that has been approved for GDPR purposes can help demonstrate compliance, including in relation to GDPR's security requirements. Guidance on codes/certifications is expected from regulators in the summer of 2017, and obviously, vendors that can offer a product or service that adheres to an approved code or certification may have a market advantage. It is still early days in terms of sectors or industry organizations putting forward codes/certifications for approval under the GDPR, although the Cloud Infrastructure Services Providers in Europe (CISPE) has indicated its intention to do so for cloud infrastructure services.

Controllers will have rights against their processors under their contracts, which according to GDPR will be much more detailed and must include security obligations on the part of the processor, for breach of which the controller could sue the processor. Also, a controller that has paid full compensation is entitled to claim from others in the supply chain in proportion to their responsibility for the damage. To clearly demonstrate who is responsible for what aspects, it will be important for the contract to set out their respective responsibilities in much more detail than hitherto, to help make it easier to determine the allocation of liability, with appropriate indemnities. This is particularly because, in reality, it is often difficult to ascertain and prove who was responsible (and at fault) for what aspect, especially where a complex supply chain is involved such as in layered cloud services.

Processors Also Generally Remain Liable for Security and Other Compliance Issues

A service provider that is a processor also has direct obligations under the GDPR to take appropriate security measures, even when the processor in turn uses subprocessors (i.e., subcontractors). This means the processor will be directly subject to fines for security breaches, even if caused by its third-party subcontractor or vendor. However, as with controllers, there may be mitigating factors that can help reduce or avoid a fine.

The processor will also have contractual obligations (and liability) to its controller regarding security measures and many other aspects, even if the true fault lays with the subcontractor that it chose to use. GDPR requires processors' contracts with their subprocessors to contain provisions that effectively mirror those that must be in the contract between the controller and processor. This means the processor should also have contractual rights against its subcontractors in relation to security breach. However, as with controllers, it will be important for the subcontract to be sufficiently detailed regarding who is responsible for what exactly, with adequate liability allocation and indemnities.

As with controllers, processors will also be exposed to supply chain risks on another front. Individuals, including NGOs on behalf of multiple individuals, could decide to take legal action against a processor for their damage from a security or other breach. For example, they may perceive a large processor to have bigger pockets than the controller, or the processor's subcontractor, or a multinational processor that has an office or other presence in their country may be simpler to sue in practice. Again, this is in addition to potential fines.

Unlike with controllers, processors will only be liable for compensation if they have not complied with their own GDPR obligations as processors. GDPR's processor obligations are less far-reaching than controllers' GDPR obligations, but include requirements on security measures. While not stated in the GDPR, so that it remains for regulatory guidance and perhaps courts to clarify this issue, it seems there has to be some element of causation (i.e., the noncompliance by the processor should have contributed to the security breach in order for the processor to be liable for compensation). If the processor infringed the GDPR in a minor way that was unrelated to the security breach (e.g., failed to keep all the records required), hopefully that would not be enough to expose it to compensation claims.

Again, processors can escape liability for compensation if they can prove they are not responsible for the damage caused. This underlines the importance of clear allocation of responsibilities in contracts both up and down the supply chain, with both controllers and subcontractors, and the importance of records, logs, and audit trails to provide evidence.

There is a strange requirement under GDPR that seems to be a direct obligation on processors, exposing them to fines. Processors are given a new "policing" role, and must tell the controller "immediately" if the controller gives them any instructions that, in the processor's opinion, infringe the GDPR or other EU or member state data protection laws. Hopefully, regulatory guidance will clarify the position, as it cannot be right that processors should be required to make themselves familiar with the GDPR and all EU laws on data protection, including security measures, and be exposed to fines if their controllers do not comply with their own obligations (e.g., by instructing the processor to implement security measures that are substandard).

Therefore, it will be critical to make sure that contracts — both upstream and downstream — cover the risks sufficiently. Processors will want to carry out due diligence on their customers as well as their subcontractors. The possibility of insurance merits investigation — not just cyber-insurance but also liability insurance, but bearing in mind that it is unclear whether regulatory fines may be insurable.

Myth 10: Data Location is not a Security Issue

While data location may not be a technical security issue, it is one factor that may be relevant to overall security. The security measures applied, such as encryption, access controls, and privileges, ought to matter more than data location. For example, some firms may think that properly encrypted personal data may safely be stored outside the EU as long as they alone can access the keys.

However, the geographic location of personal data is highly regulated under data protection laws as a legal compliance matter. Also, bear in mind that many EU regulators take the view that data location is a security issue (e.g., the U.K. Financial Conduct Authority in its cloud guidance, and Germany's Federal Office for Information Security or BSI in its Cloud Computing Compliance Controls Catalogue or C5). Whether this view is driven by political, emotional, or other motivations, the fact is that the geographic location of personal data (i.e., the countries where datacenters used to process personal data are sited) is closely controlled under data protection laws and some other regulations. The same applies to remote access by someone outside the EU to personal data that are stored in the EU. GDPR will generally tighten the rules on data location even further. In addition, this is the only area in which processors are subject to the higher-tier fine.

Therefore, it will be important for firms, whether they are controllers or processors, to consider data location when processing personal data. If any personal data are to be stored or otherwise processed outside the EU (known as international transfers), ensure that recognized tools are used, such as the EU-U.S. Privacy Shield or popularly termed as "model clauses," or that an exception applies. There are a lot of legal uncertainties about location issues now because of court cases challenging the validity of recognized tools such as the Privacy Shield and model clauses. Therefore, a watching brief should be kept in this area.

There is one aspect where GDPR may assist here. It will allow international transfers to recipients who have signed up to a code of conduct or obtained a certification, in cases in which the code or certification has been specifically approved for that purpose under the GDPR. Again, it will be up to industry bodies or even individual firms to put forward codes or certifications for approval.

LEARN MORE

Related Research

- *The Impact of GDPR on Cloud Service Providers – Part 2: Security, Data Transfer, and Other Considerations* (IDC #EMEA42627917, June 2017)
- *The Impact of GDPR on Cloud Services Providers – Part 1: General Considerations for Contracts and Liability* (IDC #EMEA42627817, June 2017)
- *Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe* (IDC #EMEA42512717, May 2017)
- *European GDPR-Related Activity Appears to Follow a Rough North-South Maturity Line* (IDC #EMEA42460617, April 2017)
- *Western Europe GDPR Survey, 2017: Mobility Results* (IDC #EMEA42426817, April 2017)
- *The Road to GDPR Compliance: Higher Levels of Data Management Maturity Will Help* (IDC #EMEA42420117, March 2017)
- *Is Test Data Management a Blind Spot for GDPR Compliance Activities?* (IDC #EMEA42407217, March 2017)
- *IDC PlanScape: EU General Data Protection Regulation (GDPR) Compliance for IT Security in Healthcare* (IDC #EMEA42309917, March 2017)
- *Rule 41 Adds Potential Complications to GDPR and Privacy Shield – But Don't Panic* (IDC #IcEMEA42209417, January 2017)
- *Which GDPR Requirement is the Most Challenging?* (IDC #EMEA42215117, January 2017)
- *Which Key Preparations are European Service Providers (IT/Telecom) Making for GDPR?* (IDC #EMEA42266217, February 2017)
- *Which Security Technologies Are Key to Getting Ready for GDPR in 2018?* (IDC #EMEA41907216, November 2016)
- *Does Encryption Solve All Your GDPR Compliance Problems?* (IDC #EMEA41907116, November 2016)
- *GDPR Countdown: How to Make a Mobile Strategy Compliant* (IDC #EMEA41869616, November 2016)

Synopsis

This IDC Perspective dispels 10 common myths about the EU General Data Protection Regulation (GDPR):

- GDPR is Like Y2K
- No One Will get Fined
- Everyone Will get Fined 4%
- Noncompliance is Equivalent to a Security Breach
- For Security Breaches, the Fine is Only 2%
- All Security Breaches Have to be Reported Within 72 Hours
- It is Safest not to Report Security Breaches
- To comply with GDPR, We Have to Encrypt Everything
- You Can Outsource GDPR Liability for Security to Third Parties
- Data Location is not a Security Issue

Note: For the avoidance of doubt, this study does not purport to provide legal advice.

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.

IDC U.K.

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