EU GDPR: A CORPORATE DILEMMA

A Study on Corporate Readiness To Remove Customer Data
## Contents

- **European Union General Data Protection Regulation: An Overview**  
  3

- **Corporate IT Survey: Methodology & Objectives**  
  5

- **Key Survey Findings: The 5 Biggest Trends Influencing EU GDPR Compliance**  
  6

- **Corporate IT Survey: Full Results & Discussion**  
  7

  - Corporate Pressure Intensifies to 'Forget' Customer Data  
    9

  - Lack of IT Processes, Documentation & Tools Increases Likelihood of GDPR Violations  
    10

  - Departmental Silos Heighten Corporate Security Risks  
    12

  - Companies Accept Accountability for Responsible Data Management  
    13

  - Data Erasure Software Tops List of Most Valuable Technology to Comply with EU GDPR  
    14

  - EU GDPR Is Seen as Model for Security Legislation in Other Countries  
    15

- **Final Thoughts**  
  16

- **Recommendations For Organizations To Prepare For Compliance**  
  17

- **About Blancco Technology Group**  
  18

- **Contact Us**  
  18
On December 15, 2015, the European Commission, the European Parliament and the European Council reached an agreement on the General Data Protection Regulation (GDPR). Four years in the making and the subject of much debate among governing bodies, industry pundits and the media, the new data privacy law will give individuals greater control over their personal data. At the same time, once ratified and implemented, it will tighten control and impose accountability on organizations that collect, store and use customer data.*

Notably, the data privacy law’s jurisdiction will apply not only to businesses based in the EU, but also to those outside the region. Companies based outside of Europe will have to abide by the same rules when offering services in the EU. In early 2016, the European Parliament and the European Council will formally adopt the new law and the new rules will become applicable two years thereafter, in 2018.

*Applicable to Businesses, and Governments

Regulation (EC) No 45/2001, which applies to the processing of personal data by EU institutions, bodies, offices and agencies, will be adapted to include GDPR principles “in order to provide a strong and coherent data protection framework” across the entire EU. There are exceptions for the Judiciary, national security and “social good” like handling epidemics, and natural or man-made disasters.
Some of the key points outlined in the GDPR include the following:

**APPLICABILITY**
The new law applies to both data collectors and data processors, and both businesses and governmental organizations; accommodations are made for micro small and medium-sized businesses.

**RIGHT TO BE FORGOTTEN**
The legislation also enshrines the right to have personal data erased “without undue delay” under certain circumstances.

**BREACH NOTIFICATION**
Supervisory authorities must be notified within 72 hours of learning of a data breach; impacted individuals must be notified “without undue delay.”

**PARENTAL CONSENT**
Requires organizations to verify consent from “holder of parental responsibility for children under 16, or 13, if allowed by a member state.”

**WITHDRAWAL CONSENT**
Per the newly enacted legislation, prior to giving consent, data subjects must always be informed of their right to withdraw consent.

**FINES**
The maximum fines will be set at 4 percent of an organization’s worldwide turnover, or €20 million, whichever is higher. Infractions will be grouped into tiers, attracting different maximum fine levels.
We surveyed 511 corporate IT professionals in the United States, Canada, Mexico, United Kingdom, Germany, Singapore, Malaysia and Australia to understand their level of awareness, preparation and capacity to comply with the ‘right to be forgotten’ and the General Data Protection Regulation. The survey was fielded during Fall 2015 and targeted IT professionals across a variety of businesses (up to 10,000 employees) and represents 20 industries.
### Key Survey Findings

#### The 5 Biggest Trends Influencing EU GDPR Compliance

1. **Lack of documentation, processes and tools** increases the likelihood of GDPR violations. **41 percent** of IT professionals don’t provide written documentation about the defined processes/technology used to remove outdated or irrelevant customer data. **25 percent** of the surveyed respondents do not know how long it would take to implement the necessary IT processes and tools to pass a “right to be forgotten” audit.

2. Corporate pressure to forget customer data won’t dissipate any time soon, with **46 percent** of global IT professionals receiving **customer requests to remove outdated or irrelevant data in the last 12 months**.

3. While **awareness of GDPR is high (48 percent)** among global IT professionals, their level of preparation is much lower. **40 percent** admit to being less than fully prepared – with **16 percent still needing to find the right data removal software, 9 percent uncertain of how and where to start**, and finally, **15 percent not even knowing if they are prepared**.

4. **IT professionals inside and outside of Europe (65 percent)** are keen to implement data protection laws similar to the framework of EU GDPR.

5. **Data erasure software (48 percent)** tops the list of the **most valuable type of technology** to ensure GDPR compliance, followed by encryption key removal tools (26 percent) and malware removal tools (10 percent).
Awareness Is Not Equivalent to Preparation for EU GDPR

28% 14% 59%

1 2 3 4 5 6 7 8 9 10

Little/No Knowledge (1-4)  Highly Aware (6-10)

Note: Figures may not add to 100 due to rounding.

We asked IT professionals around the world to rate their level of awareness about the proposed General Data Protection Regulation. 28 percent of IT professionals ranked their level of awareness as low. In comparison, 59 percent of IT professionals identified themselves as being highly aware of the legislation.
Although 60 percent of the IT professionals surveyed have been proactive in preparing for the new legislation, others are not in the same position of readiness. 40 percent admitted to being less than fully prepared – with 16 percent still needing to find the right data removal software, 9 percent uncertain of how and where to start and 15 percent not even knowing if they are prepared.

A data breach can hurt a company’s brand reputation, reduce customer loyalty, result in legal repercussions, impose heavy fines as high as 4 percent of an organization’s worldwide turnover, or €20 million, whichever is higher – and even damage stock prices. Proactively planning for the removal of data not only helps organizations meet the “Right to be Forgotten” requirements, but also decreases the chances of organizations being investigated and potentially fined by the Supervisory Authorities.
Nearly half (46 percent) of IT professionals have received a customer request to remove outdated or irrelevant data in the last 12 months. As consumers become more informed and concerned about their data protection and privacy, companies will likely see an increase in the quantity and frequency of data removal requests. As a result, best-of-breed organizations should prepare for a seamless, automated data removal process to efficiently handle those requests and substantiate regulatory compliance.

Many companies today invest heavily to attract new customers. When companies experience a data breach, it complicates things and leads to lost business costs\(^1\), which include abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished good will. Rather than look at customer requests for data removal as an operational and financial burden, organizations should view it as a golden opportunity to improve customer retention and offer verifiable proof that data has been removed permanently as a point of differentiation against competitors. As a result, customers will be more trusting and loyal – reducing the likelihood that they will walk away and spend their time and money elsewhere.

---

1 Ponemon Institute, 2015 Global Cost of a Data Breach, April 2015
Lack of IT Processes, Documentation & Tools Increases Likelihood of GDPR Violations

Despite growing customer and regulatory pressure, 41 percent of the global IT professionals surveyed don’t maintain documentation of the defined processes/technology for the removal of outdated or irrelevant customer data. Written policies are an important component of a healthy business model and empower businesses to properly manage data across the entire lifecycle – from creation to storage to transfer to removal.

To understand why this is a cause for concern, consider the circumstances surrounding the Ashley Madison data breach in 2015. The online dating site sold registered users a $20 “Full Delete” service with the promise that their data would be removed completely and permanently. However, this was not the case and the personal information of over 32 million registered users was leaked. Failing to provide written documentation that data has been completely erased – and can never resurface – can have serious consequences for businesses that go beyond the exorbitant legal fines imposed by the Supervisory Authorities. It can also result in diminished sales, customer lawsuits, diminished customer loyalty, damaged brand reputation and reduced stock prices.

In order to avoid these consequences, organizations need to establish a comprehensive data lifecycle process, which includes secure data removal when needed. Once this process is thoroughly tested and documented, organizations should request certification (proof) that data has, in fact, been permanently removed. As with any other process within an organization, transparency and proof should not be taken for granted. By doing so, organizations will see an increase in customer trust and loyalty and have the potential to make a profound impact in the marketplace.
Timeline Required for Organizations to Develop and Implement IT Processes & Tools to Pass a “Right to be Forgotten” Audit

25% Don't Know
11% Less Than 3 Months
19% 3-6 Months
15% 7-9 Months
15% 10-12 Months
10% 1-2 Years
3% 2-3 Years
3% Over 3 Years

Note: Figures may not add to 100 due to rounding.

Twenty-five percent of IT professionals surveyed had no idea how long it would take to develop and implement the processes and tools to pass a "right to be forgotten" audit. Meanwhile, 60 percent stated that it would take their organization up to 12 months, with the rest putting it at one or more years. This suggests that organizations need to begin planning immediately in order to meet the GDPR requirements when they become enforceable in 2018.

If a company is investigated by the Supervisory Authorities, it will be critically important to be able to provide documentation to prevent legal fines and court actions from being taken against the company. It's important to remember that the European Parliament and European Council will formally adopt the new law at the beginning of 2016 and the rules will then become applicable two years thereafter, in 2018.
We asked IT professionals to confirm which stakeholders within their organizations care most about data privacy. 29 percent stated that their C-level executives and board-level directors care most. This indicates a gradual shift in how C-level and board-level executives approach data security as more than just an IT priority, but a component of their overall company strategy.

However, our survey findings also point to a large mismatch in the level of interest taken by different internal groups and a lack of cross-team collaboration. On the one hand, 29 percent of the respondents said the IT department is the most concerned stakeholder. But only 2 percent cited the marketing department as caring most. It’s also interesting to note that the CTO (7 percent), compliance (7 percent) and legal departments (7 percent) are relatively low on the list of stakeholders who care most about data privacy. In the days, weeks and months following a data breach, organizations typically focus on investigating the source/root of leaks and do a full assessment of their existing operational processes, security protocols, technology solutions/tools, internal and external risk levels and documentation maintained. While these figures are not as high as many would hope, they represent yet another opportunity for each of these groups to collaborate with one another to build out tighter, more defined internal processes, shore up new technology solutions and finally, educate, train and communicate processes to all employees within the organization.
Companies Accept Accountability for Responsible Data Management

Although there may be some areas of improvement for organizations to prepare and develop IT processes, documentation and tools, they understand and accept their own responsibility in the matter. In fact, 77 percent of the respondents believe it’s fair to hold companies responsible for the removal of customer information, when requested.

This contradicts a common misconception that companies want to shirk their data protection responsibilities. Clearly, companies are willing to acknowledge their responsibility for removing customer data. But it’s not sufficient to simply acknowledge a problem exists and accept responsibility for the methods used to collect, process, manage, store and remove customer information. Businesses need to proactively plan for success by developing a process that covers the entire data lifecycle – from creation to collection to processing to storage to removal.*

Is It Fair to Hold Companies Responsible for Removal of Irrelevant Information?

- **Yes**: 77%
- **No**: 23%

*Four Data Lifecycle Management and Protection Considerations*

1. Cover all phases of the data lifecycle – acquisition, use, storage, transfer and removal.
2. Establish appropriate protections at every phase – and while not all data are the same, they all need to be protected.
3. Ensure robust access controls and monitoring – consider especially the negligent or malicious insider.
4. Obtain input and consent from all stakeholders to ensure secure enablement of current and future business initiatives.
While each type of security technology has a specific purpose and role in protecting organizational data, our study indicates that data erasure software has, by far, the most value in addressing the “right to be forgotten” and complying with the GDPR’s requirements. In fact, 48 percent of the IT professionals surveyed put data erasure software at the top of their compliance lists, followed by encryption key removal tools (26 percent) and malware removal tools (10 percent).

With the approval of the GDPR legislation as of December 15, 2015, it’s important for businesses to conduct an internal audit of all third party technology solutions, tools and databases being used. When doing so, businesses should build a checklist that confirms if and how their existing solutions/tools support privacy and data protection initiatives. If any gaps are found in the existing technology solutions, tools and databases, organizations should immediately begin the process of researching and evaluating new solution providers for purchase and implementation.

Of course, there are multiple types of data security/privacy products and solutions that exist – encryption key removal tools, malware removal tools, anti-virus software, file deletion programs and data erasure software, just to name a few. As part of an organization’s due diligence, it’s vital to understand each potential provider and verify that their products/solutions are certified by the appropriate governing bodies and will assure compliance with the most stringent international regulatory standards.

It is important to understand the difference between simply ‘deleting’ data and removing it completely and permanently. Typical file deletion commands do not, in fact, eradicate the data and prevent it from resurfacing; they merely remove pointers to the disk sectors where data resides. As a result, data that businesses may assume has been ‘deleted’ can easily be recovered with common software tools.
EU GDPR Is Seen as Model for Security Legislation in Other Countries

We asked IT professionals across North America, Europe and Asia Pacific if they believe other countries/regions should implement data protection laws similar to the EU GDPR and the responses were enlightening. Nearly three-quarters (65 percent) of the IT professionals answered ‘yes.’ This confirms our other findings – IT professionals around the world, not just in Europe, are willing to accept and own responsibility for how data is collected, processed, stored and removed.

Do You Believe Other Countries/Regions Should Implement Data Protection Laws Similar to GDPR?

- Yes: 65%
- No: 14%
- Don’t Know: 23%
While no organization today can discount the importance of data protection, what is up for debate is just how prepared companies are to comply with the new legislation, specifically regarding an individual’s right to be forgotten. From operational and financial burdens to the legal requirements that could be enforced and the level of accountability – this new legislation will change how organizations operationally manage their customers’ data.

The new EU General Data Protection Regulation (GDPR) will force organizations around the world to reconsider – and in some cases, redesign entirely – their data collection and data protection programs. If organizations want to ensure GDPR compliance by 2018, they will need to develop end-to-end data lifecycle management processes, create transparent processes and customer communications on their methods for data removal, and finally, improve their security posturing as a whole to include detection and response and the gathering and sharing of threat intelligence.
Recommendations for Organizations To Prepare For Compliance

DEVELOP END-TO-END DATA LIFECYCLE MANAGEMENT PROCESSES

Consider what constitutes protected data, how to meet data residency requirements, if and how to fully anonymize data, how you will handle 3rd parties (e.g., data processors, business associates, cloud storage vendors, etc.), what your data retention / lifetime needs are and how you will enable the “right to be forgotten.” Consider how you will provide protection during all phases of data lifecycle, and whether creating a strong Data Protection Officer (DPO) role is a good idea.

ENABLE TRANSPARENCY

Consider how you will provide “positive consent” from customers and enable constant communication about status / use of personal data. Ensure you have the ability to correct inaccuracies, obtain parental consent when children are involved, and notify customers when changes in your processes occur.

IMPROVE SECURITY POSTURE

This is obviously a very wide area, but some considerations include encrypting data-at-rest and data-in-motion, and providing security for data-in-use; and round out your capabilities to move beyond prevention to include detect & respond, and getting threat intelligence to inform on your security triage. Finally, consider insider risk.

Because of the new law’s stringent requirements, corporate compliance will require a considerable investment of time, resources and budgets. To help businesses prepare, we have created a detailed list of recommendations to ensure EU GDPR compliance by 2018.
Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients’ customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk by xCaliber Technologies, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers’ experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk (or Xcaliber Technologies) provides world-class support, pre and post implementation, allowing our customers to derive measurable business results.

Contact Us
For Sales & Marketing, Please Contact:
Email: marketing@blancco.com

For Corporate Communications & PR, Please Contact:
Email: press@blanccotechgroup.com