



GDPR: Preparing For Change

Building further trust with
our customers

Imprima White Paper #2

Published 14 May 2018

The contents of this document are limited to general information and not detailed analyses of law or legal advice and are not intended to address specific legal queries arising in any particular set of circumstances.

GDPR Deadline

The clock is ticking

Preparing for change

With just under 2 weeks until the GDPR comes into effect, many organisations are still ill-prepared to meet its requirements. Given the importance of this topic, Imprima has started running a series of articles on GDPR, designed to help our clients deal with the new regulation in the context of information sharing via secure data storage and collaboration platforms.


Last month, in our first published White Paper on this key topic, we looked at GDPR in context of the wider data protection landscape and how it relates to the UK (Brexit) and the US (Privacy Shield). In this 2nd article on the GDPR we:

- **Analyse how prepared companies are for the new regulation**
- **Explain how Imprima has prepared for the GDPR**
- **Offer straightforward advice to companies who are still working towards meeting the requirements**

What is the GDPR?

The General Data Protection Regulation (GDPR) represents the most important data protection regulation change in Europe in the last 20 years. The GDPR, approved and adopted by the EU Parliament in April 2016, replaces the Data Protection Directive 95/46/EC. The GDPR is designed to both update and harmonise data privacy regulation, and the various laws surrounding it across Europe. Its primary intent is to provide further data privacy protection for, and empowerment of, all EU citizens. As a result, the new regulation reshapes the way organisations across the region approach data protection and data transfers in a uniform and consistent manner.

Furthermore, as the GDPR reduces 28 sets of different national data protection laws into a single regulation; with the aim of reducing compliance costs, complexity, risk and uncertainty within reporting for organisations. It should be seen as a benefit not only to EU citizens, but also for companies that fully embrace the change.

A background image for a callout box featuring a person's hand typing on a keyboard. Overlaid on the image are glowing blue lines and the words "Data Protection" in a large, light blue, sans-serif font. A small yellow square with an exclamation mark is positioned to the left of the text.

! Once the GDPR comes into effect on 25 May 2018, all companies processing and holding the personal data of subjects residing in the EU must be compliant, regardless of where they are based.

How ready are organisations for the change?

Over the last 18 months, businesses across the world have been scrambling to get their organisations GDPR compliant ahead of the 25th May deadline.

The scandal surrounding Cambridge Analytica, and its improper use of Facebook's user data, brought this issue of data protection and privacy to the fore in an extremely timely fashion.

In many recent articles, it has been reported that organisations are far from ready for the EU's imminent General Data Protection Regulation (GDPR) compliance deadline. According to a recent report from Forrester Research, European companies are very pessimistic about their readiness, with just 26% saying they are fully compliant and another 22% expecting to be fully compliant within 12 months.

GDPR and secure data-storage, sharing, and collaboration platforms

With the explosive growth of the Internet and the Cloud as a data storage mechanism, the creation and processing of personal data has become ubiquitous and far-reaching. The GDPR aims to update data privacy

standards to address these new technologies, while remaining true to original privacy principles established in 1980. Without question, the ease of access to information (personal or otherwise) on a global scale - and in real time - has transformed how business is conducted. However, this transformation comes with huge risks that are associated with the use - or misuse - of personal data. The utilisation of less secure file sharing platforms that do not adequately protect and manage information, now comes at a heavy price. Not only is there the adverse reputational damage caused through data breaches, the new regulation can also lead to significant fines and penalties on any offending data owners. Therefore, data owners are well advised to only use data processors, such as data-storage and data-sharing providers, that ensure GDPR is fully complied with.

Imprima, as a market leading Virtual Data Room provider, focused on providing customers with due diligence and asset management solutions, welcomes the new regulation. Imprima sees the GDPR as an opportunity for SaaS providers, in particular Virtual Data room providers, to further improve trust and transparency with clients on how their personal data is stored and used.



Imprima's existing security framework

ISO 27001

As an organisation that has always been focused on earning our customers' trust whilst handling their documentation with care and confidentiality, Imprima has developed a strong compliance culture and robust security safeguards. Imprima has been ISO 27001 certified (ISO 27001:2013 standard) since 2010, and its scope of applicability covers our entire business – our people, processes, platform and data centres.

The ISO 27001:2013 accreditation ensures information security is integrally managed within both the platform and the processes of IROOMS, and to a consistently high and rigorous standard. To that end, its list of controls has been updated and enhanced to fully encompass the growing security threats to organisations.

At Imprima we believe that ISO 27001 is the most appropriate certification for providers of highly secure Virtual Data Rooms. As an internationally recognised

accreditation, based on best practice, it measures a company's ISMS (Information Security Management System) against requirements set by the ISO (International Organisation for Standardisation). Moreover, ISO 27001 is a continuous process: to maintain the compliance certificate, organisations must submit to rigorous and mandatory audits and review processes on an ongoing basis, multiple times per year. As a result, the ISO 27001 certification is demanding for an organisation to achieve and maintain, as well as rigorous in its scope.

The ISO 27001 standard is an excellent framework for compliance with the EU GDPR. Given Imprima has already implemented the full scope of ISO27001, we have a significant advantage over many other secure data storage and collaboration platforms. Our priority has always been to assist our clients to comply with all data protection obligations. This is underpinned by having the most stringent technical security measures and personnel standards in the industry.



How is Imprima preparing for the GDPR?

Our technical and organisational security measures include:



Active Protection and Passive Monitoring

Firewalls, “least privilege user access control” with user IDs and passwords with limited lifetimes, intrusion detection and prevention systems, encryption of portable data storage devices and encryption of personal data in transit with 256Bit AES encryption, real-time anti-virus protection, anti-malware and anti-spyware software.



Segregated Protection with bespoke setup

Data separation, restricted remote access with multi-factor authentication, logging and monitoring of user activity (without access to data room content).



Continued review and adherence of procedure

Compliance with hardware and software manufacturer instructions, regular software updates, regular network penetration testing, secure wiping of decommissioned devices, data backup with regular testing and disaster recovery procedures.



Personnel vetting, screening and compliance

On top of our technical security measures, our administrative security measures include personnel vetting on all new employees, as well as regular and continuous security training for existing staff.

Further measures Imprima has taken to comply with the new regulation:

SPECIFIC MEASURES:

1. GDPR-compliant data processing terms to each client (this gives each client control over the processing of their data and confirms the client's instruction to Imprima to process data in connection with our services).
2. Updated our platform end-user (click-through) agreement to give our clients more control over end-user conduct.
3. Issued GDPR-compliant data processing terms to our suppliers and contractors.
4. Updated our website privacy notice.
5. Prepared and distributed a GDPR Q&A to help our clients comply with the GDPR in relation to client data held in their Imprima data room, or otherwise processed by Imprima on their behalf.

Key recommendations

What advice would Imprima give other organisations in terms of ensuring GDPR compliance?

Much has been made about the headache GDPR is causing organisations. However, in its simplest form, this regulation is a reasonable and sensible set of rules which organisations should be endeavouring to implement.

Moreover, it provides a monumental opportunity for businesses to really understand their data, know where it resides, and use it to improve operations and enhance the increasingly important customer experience.



We recommend you implement the following measures to help ensure compliance:

■ KEY RECOMMENDATIONS:

1. Implement **GDPR training programmes** in your organisation so that employees are aware of the data protection compliance they must follow
2. Ensure mechanisms are in place within your organisation to ensure that, by default, only personal data necessary for each specific purpose is processed, and the data is stored for no longer than necessary.
3. Review all **privacy notices** used by your organisation and put in place a plan for changing these notices to comply with the GDPR.
4. Consider whether your organisation should appoint a **Data Protection Officer** to comply with the GDPR.
5. And last but not least: make sure that you only contract providers for handling and storage of your data that are already fully GDPR compliant

Summary

Essentially, the GDPR specifies best practices for how your organisation should handle personal data. In addition to avoiding fines for non-compliance, specifying processes and procedures to ensure compliance with those rules will help your organisation overall. By establishing a framework that puts protection of personal data at the heart of your business and by protecting an individual's ability to control this data, companies will be able to ensure customer trust.

Compliance with the EU's data protection laws, including both customer and data security, is enhanced and improved by adding an extra layer of security and rigour to business operations.

Choosing Imprima, as opposed to non-EU based or non-GDPR-compliant SaaS Providers, will be hugely beneficial for businesses looking for a safer, more robust data protection partner. It ensures data protection to the highest level, while both data storage and data transfer remain fully compliant.

If you would like more information on how Imprima is ensuring we maintain our position as the most secure platform for due diligence and asset management, please get in touch.

Gary McKeown (Chief Executive Officer)
May 2018

Contact us

To find out more about how GDPR will impact your business, please visit
our website or contact your local Imprima office:

www.imprima.com



Imprima global offices

London

Imprima iRooms Limited
30 Crown Place
London EC2A 4EB
Tel: +44 20 7965 4700
E: londonsales@imprima.com

Frankfurt

Imprima (Deutschland) GmbH
Barckhausstraße 10
60325 Frankfurt am Main
Tel: +49 69 915 0980
E: frankfurt@imprima.com

Paris

Imprima (France) SARL
32 Avenue de l'Opéra
75002 Paris
Tel: +33 1 76 75 32 91
E: paris@imprima.com

Amsterdam

Imprima (Nederland) B.V.
De Boelelaan 7
1083 hj Amsterdam
Tel: +31 207 155 600
E: amsterdam@imprima.com

New York

Imprima (USA) Inc.
135 East 57th Street
New York
NY 10022
Tel: +1 646 844 2993
E: newyork@imprima.com

Sydney

Imprima Australia
Level 12, Plaza Building
95 Pitt Street
Sydney, NSW 2000
Tel: +61 283 110 266
E: sydney.sales@imprima.com