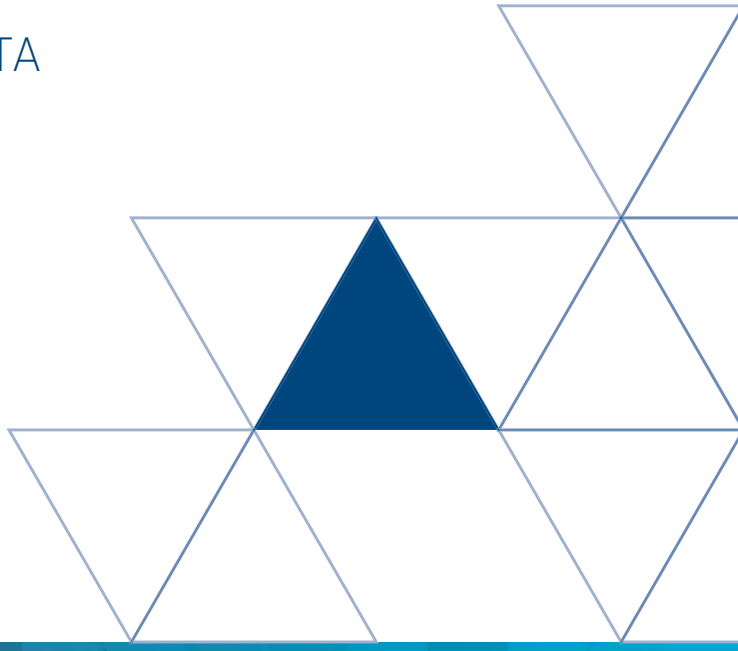
IRON MOUNTAIN®

THE IMPORTANCE AND STATUS OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

AND RESULTING REQUISITES FOR DATA TRANSFER COMPLIANCE



WHITE PAPER

SEE INFORMATION DIFFERENTLY

CONTENTS

INTRODUCTION

WHY READ THIS DOCUMENT?

The protection and privacy of an individual's Personally Identifiable Information (PII) is more imperative than ever. Data breaches, both major and minor, occur with increased frequency and consequences. Laws and regulations covering the acquisition, use, transmission, storage, destruction and breach of PII are implemented and enhanced regularly.

This document will be beneficial to readers concerned with upcoming privacy laws and regulations in the European Union (EU) as the General Data Protection Regulation (GDPR) is on the cusp of approval. The GDPR addresses privacy issues on an imposing scale and its methodology will most likely be used by other governments and agencies around the world. These entities, and indeed any corporation that may access and transfer the personal information of an EU individual, should remain aware of the upcoming GDPR changes.

PRIVACY PROTECTION TODAY

Meeting and maintaining the privacy expectations and data of all individuals is perhaps one of the greatest struggles seen by governments, federal agencies, and other entities today. They are responsible for its protection having spent the beginning of this millennium strategizing and issuing regulations with the goal to protect the world's personal information now and in the foreseeable future. This is not an easy fete.

The laws and regulations must allow for the transfer of vast amounts of digital personal information, but in a safe, controlled environment. The data must be protected not only from external hackers, but employees, the media, and other governments, including our own.

The collection, retention, distribution, and loss of personal data has reached a critical peak as our abilities to manipulate, collate, and store pieces of digital data have reached prolific levels. With this in mind, the European Union (EU) is about to approve the latest and farthest reaching legislation in the form of the General Data Protection Regulation (GDPR)[1]

With the ultimate goal of protecting the personal information of all, corporations and governments alike must invent valuable time and resources in their quest to:

- obtain, retain, and process data
- maintain physical and digital security measures
- maintain necessary documentation in relation to consent, legitimate interest, etc.
- coordinate safe disposal or destruction of the data
- assess risk and maintain compliance
- contend with reporting and repercussions of any breached information

GENERAL DATA PROTECTION REGULATION (GDPR)

PROPOSAL AND STATUS

The proposal for the GDPR was issued in 2012 by the European Commission (EC) and will replace the outdated Data Protection Directive originally issued in 1995. It is important to note from a legal view point that the GDPR, being a regulation, carries much stronger legal requirements than the 1995 directive: the regulation is a mandate, whereas the directive was guidance. These regulations will apply not only to the member states of the EU, but to all non-European companies that operate in the EU (currently governed by the laws of the country in which they are corporately based), along with significant fines for non-compliance.

[1]EUROPEAN COMMISSION - Proposal for a Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data and On The Free Movement Of Such Data (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

The GDPR proposal was originally greeted with positive response. The appeal of additional protection for citizens, compliance by non-EU countries (referenced by the EU as "third countries"), and an easier approval process for cross border data transfers appeared to be a win-win situation. However, multiple Articles within the GDPR have come under deep scrutiny; dissatisfaction with Safe Harbor is rife and disgruntlement between member states over dissimilar views on data protection levels have undermined the already lengthy approval process.

The GDPR requires approval on multiple levels. The Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the EU Parliament adopted it in October 2013 with a multitude of amendments after which it was resoundingly approved by the EU Parliament on March 12, 2014[2]. The proposed regulation will now go through discussions between the European Parliament, Commission, and the Council.

On June 6, 2014, Viviane Reding, Vice President of the European Commission (EC), confirmed that the Council has agreed on two pillars of the GDPR: cross-border data transfer rules and territorial scope. In relation to Safe Harbor, she stated that of the 13 recommended improvements, only 12 have been agreed upon; the 13th being the national security exception[3].

Safe Harbor:
An agreement between the United States Department of Commerce and the European Union (EU) to regulate the personal data exportation of European citizens by U.S. companies.

On January 7, 2015, Jan Phillip Albrecht, Vice-Chair of the Committee Civil Liberties, Justice and Home Affairs (LIBE), member of the European Parliament and their rapporteur for the EU's GDPR as well as the EU-US data protection framework agreement, issued an explanation of the GDPR's ten main issues[4]. In relation to items affecting compliance for cross border data transfers, Mr. Albrecht indicated these items were in a stale-mate amongst member states.

Even with controversy between EU governmental entities, third countries, and pressure from multiple industries for specific revisions, the overall opinion is that resolution and approval of the GDPR should be obtainable by end of year 2015, after which the member states will have two years to bring their regulations up-to-date. (Article 91) As for Safe Harbor Agreement certifications (US/Swiss Treaty) and Standard Contractual Clauses (Model Clauses) currently in use by non-EU entities, there appears to be no "official" documented deadline but the current expectation is within five years after the Regulation enters into effect.

RESULTING REQUISITES FOR COMPLIANCE

In anticipation of the GDPR approval, companies that transfer any type of personal data (customer, vendor, employee, etc.) across borders should have their operating procedures, documentation competencies, and Data Protection Officers (DPO's) prepared for implementation and ready for possible cross border approval requirements. Because the GDPR has several substantial differences in comparison to the Data Protection Directive, the following should be kept in mind[5]:

[2] A New Milestone Toward Adopting Enhanced Data Protection Rules in the EU 3/2014; Jones Day: http://www.jonesday.com/European-Parliament-Votes-in-Favor-of-General-Data-Protection-Regulation-and-Threatens-Suspension-of-Data-Transfers-to-US-03-21-2014/?RSS=true
[3] Progress on the EU General Data Protection Regulation and the Status of Safe Harbor, Jan Dhont and Katie Woodcock: https://www.privacyassociation.org/news/a/progressontheeu-generaldataprotectionregulationandthestatusofsaf
[4] EU General Data Protection Regulation State of Play and 10 Main Issues, Jan Phillip Albrecht: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf
[5] EUROPEAN COMMISSION - Proposal for a Regulation Of The European Parliament And Of The Council On The Protection Of Individuals With Regard To The Processing Of Personal Data and On The Free Movement Of Such Data (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

- Legally enforceable rights apply for controllers, processors, sub-processors, etc. regardless of transfer type or location: controller to controller, controller to processor, and so forth;
- It is applicable regardless of where the personal data is processed;
- As the GDPR is a regulation for all member states, substantial fines will be imposed for non-compliance. Penalties: 5% of annual world turnover or EUR 100 million, whichever is greater. The DPA may request deletion of the data, suspension of data flow, and a temporary or permanent ban on processing actives.
- Consent may only be given explicitly. Consent and data may be withdrawn under the "right to erasure" and companies must ensure "data portability";
- The definition of personal data has expanded;
- Only one Data Protection Authority (DPA) will be required for the review and approval (through a multi-step process) of the cross border transfer and they will additionally have enforcement authority (known as One-Stop-Shop).
- Transfers involving a "Third Country" (non-EU) will still require contractual obligations through Binding Corporate Rules (BCR), Standard Contractual Clauses (also known as model clauses), or the Safe Harbor agreement (US/Swiss Treaty).

> ...substantial fines will be imposed for noncompliance;
> ... with sanctions in fines of up to 5% of annual world turnover or EUR 100 million...

KEY DATA ASPECTS

The issues that remain open between the EU Parliament and Council could substantially alter the drafted rules of the Regulation as they stand today. This means global companies preparing for the impending Regulation are faced with shifting obstacles. Focus, therefore, should start with the applicability and fundamentals of providing, maintaining, and documenting adequate levels of data protection, along with the creation of or revision of procedures and policies in relation to key data aspects such as:

1. DATA SUBJECT PERSONAL DATA AND TERRITORIAL SCOPE

The definitions of "data subject" and "personal data" are key in determining the applicability of the regulation. Article 4 of the GDPR indicates that a data subject is "a natural person who can be directly or indirectly identified by the controller or a third party using reasonably likely means."

Personal data is data relating to a data subject. Any data that are not personal data are outside the scope of the proposed regulation. Common misconceptions regarding the term include the belief that data must be linked to a name to be personal data; however, with the increasing ease of re-identification, even removing further items from sets of data will not necessarily render it anonymous or de-identified. Third parties can match the pieces of information within their own databases allowing them the ability re-identify individuals.[6] LIBE has expanded the definition of personal data to include data that has the possibility of identifying or singling out an individual, directly or indirectly, and will include device identifiers, IP addresses and location data.[7]

> Personal data is data relating to a data subject. Any data that are not personal data are outside the scope of the proposed regulation.

[6] "Key Aspects of the Proposed General Data Protection Regulation Explained...", European Digital Rights, Sec 1: https://edri.org/files/GDPR-key-issues-explained.pdf
[7] "The Draft EU General Data Protection Regulation: Where We Are Now and Where We Are Going", Karin Retzer and Joanna Łopatowska of Morrison Foerster, Nov. 2013: http://media.mofo.com/files/Uploads/Images/131113-draft-eu-data-protection.pdf

2. DATA PRIVACY IMPACT ASSESSMENT (DPIA)

As part of a company's privacy risk assessment, and prior to the start of every project that will involve personal data that is sensitive, on a large scale or with intensive records, an organization should perform a preliminary threshold analysis (initial assessment) to determine if a DPIA is necessary.

Direction for companies that need to complete a DPIA can be found in Chapter 3 of "Recommendations for a Privacy Impact Assessment Framework for the European Union" prepared for the European Commission November 2012.[8] It should be noted that this recommendation states that a senior executive officer should be held accountable for the quality and adequacy of a DPIA and should approve the final results.

> A senior executive officer should be held accountable for the quality & adequcy of a Data Privacy Impact Assessment (DPIA)

3. LEGITIMATE INTERESTS

The change in legitimate interest involves the inability to transfer data outside the EU on a legitimate interest basis and will rely on contractual arrangements entailed with BCRs, model clauses, and Safe Harbor. If processing is to be based on legitimate interest of a controller, it cannot override the fundamental rights and interest of the data subject.

Under the LIBE amendments, legitimate interest widened out to cover secondary processing purposes, i.e. where necessary for the legitimate interests of third parties provided that meets the reasonable expectations of the relevant data subject.[9] In addition, consent cannot be used to justify legitimate interest for third party processing if processing is an incompatible purpose (not related to the original purpose).

4. CONSENT

Consent, though agreed upon for the most part, is still under revision to add specificity. Overall, consent for data processing must be freely given, specific, informed and explicit by default. It applies to both sensitive and non-sensitive data, and will cease to be valid when the original purpose of data collection ceases to exist or when used for a secondary purpose. Consent will only justify processing if that consent is "purpose limited," i.e. for one or more specific purposes. Consent should be as easy to withdraw as it is to grant it and data subjects should be made fully aware of the risk of termination of the services if they withdraw their consent to processing.

> Consent will be explicit by default

5. PRIVACY NOTICE

LIBE created a two- step process for notification[10]. The new notification requirements will require measurement and documentation of the applicability of each category required in the notifications.

The first step of the additional privacy notice requirements will include a standardized table with text and symbols. The table is meant to allow an individual to easily view whether personal information will be transferred to commercial third parties, sold, rented out or encrypted. To date, there are six items in the table, each with their own icon. The first three items are mandatory to address. The entity issuing the notification will need to carefully review the Article requirements as there are at least 12 items that are required to be included in the written portion of the notification.

[8] "Recommendations for a Privacy Impact Assessment Framework for the European Union" prepared for the European Commission, Nov. 2012
[9] "Draft EU General Data Protection Regulation: Update & Impact On Insurance Sector", eversheds.com: eversheds.com/global/en/what/articles/index.page
[10] "The Draft EU General Data Protection Regulation: Where We Are Now and Where We Are Going", Karin Retzer and Joanna Łopatowska of Morrison Foerster, Nov. 2013: http://media.mofo.com/files/Uploads/Images/131113-draft-eu-data-protection.pdf,
and "EU draft Data Protection Regulation: the LIBE Committee amendments", a Hogan Lovells Briefing Paper 2013: http://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf
and "Update on Draft EU Data Protection", King&Wood Mallesons: http://www.sjberwin.com/insights/2013/11/07/update-on-draft-eu-data-protection-regulation#

6. DATA PORTABILITY AND RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

Data portability has two aspects: 1) if a data subject's data are processed in a commonly used electronic format, they can obtain a copy of the data in a format that allows for further digital use by them, and 2) if data is processed based on consent, the data subject should be able to take the data they have supplied with them when changing service providers. The information must be free of charge unless the request is "manifestly excessive". If so, a reasonable fee may be charged but the controller will be responsible to prove why they considered it excessive.

That same data subject can ask for the data to be erased. If the controller no has longer has a viable reason for holding the information, request for erasure will need to be granted. There are exceptions when a controller is legally obliged to retain data.

7. DATA PROTECTION OFFICER (DPO)

Where previously a controller was required to appoint a DPO if their enterprise employed 250 persons or more, the LIBE amendments to the GDPR (Articles 35-37) now require companies with personal data for more than 5,000 individuals in any consecutive 12 month period[11], or that process sensitive data such as health data, to appoint an independent DPO with extensive experience who shall report directly to the executive management of the controller or the processor.

Multinationals may appoint a "main responsible" DPO, provided the DPO is easily available from each location/ establishment. There is a minimum term of appointment of 4 years for employees and 2 years for external contractors. The DPO will have specific tasks to be completed in accordance with the GDPR.

8. DATA BREACH NOTIFICATION

With the LIBE amendments (GDPR Articles 31-32), the 24 hour deadline for security breach notification has been removed. Replacing it is the need to report with "undue delay," taken at this point in time to mean 72 hours. When reporting to the supervisory authority, the controller will need to describe the nature of the breach, including categories, number of data subjects, and number of records involved; the identity and contact details of the DPO; measures to mitigate possible adverse effects; consequence of breach; and measures proposed or taken.

[11] "Retailers need to prepare for the new EU Data Protection Regulation", DLA Piper: https://www.dlapiper.com/en/us/insights/publications/2015/02/law-a-la-mode-edition-15/retailers-need-to-prepare-for-the-new-eu-data/

ISSUES WITH CROSS BORDER APPROVAL PROCESSES

ONE-STOP-SHOP (OSS) FOR DATA PROTECTION AUTHORITY (DPA) APPROVALS

The EU is trying to establish the OSS – One-Stop Shop. The thought behind the OSS is positive: organizations doing business in more than one country will be able to deal with one DPA. The OSS will have regulatory authority to resolve disputes and enforce authority to ensure compliance. The mechanism of the OSS is intended to deliver enhanced legal certainty, efficiency for businesses, and effective proximity for individuals. It will rely on an enhanced cooperation and coordination between a "lead DPA" and other concerned DPAs.

This raises concerns that (1) regulatory authorities without lead supervision may lose influence over data protection issues that affect citizens in their Member States, (2) the regulatory authority with lead supervision may be removed from individuals affected by the data controller's processing activities, (3) businesses may 'forum shop,' to obtain their preferred lead regulatory authority and (4) orders by lead regulatory authorities may be unenforceable in other Member States.[12]

> Organizations doing business in more than one member state will only require approval from one DPA. For ten or more countries, two DPAs are required.

THIRD COUNTRY (NON-EU) USE OF SAFE HARBOR, BINDING CORPORATE RULES, AND STANDARD CONTRACTUAL CLAUSES: THREE INSTRUMENTS USED BY TO IMPORT DATA.

The source of contention between the EU governments and businesses in the United States are the three main instruments of cross border data transfer: The Safe Harbor Agreement (US/Swiss Treaty), Standard Contractual Clauses (Model Clauses), and Binding Corporate Rules.

» Safe Harbor

The US-EU Safe Harbor's controversy stems from its self-certification. It is an agreement formed to allow transfer of EU personal data to a country without "adequate" privacy standards as described in the Data Protection Directive of 1995. Only organizations under the U.S. jurisdiction of the Federal Trade Commission (FTC) or air carriers and ticket agents in the Department of Transportation's jurisdiction may self-certify. This leaves out certain financial institutions, non-profits, and others.[13]

» Standard Contractual Clauses (SCCs)

The EC has approved three decisions for SCCs: Two for transfers from data controllers to data controllers and one for transfers from data controllers to data processors. One of the main problems with using SCCs is the prior approval required by the DPAs to ensure compliance with the EC Model Clauses, as the DPA in one member state may find them acceptable whereas the DPA in another may not.

The Article 29 Working Party (WP29) issued a Co-Operation Procedure in November 2014[14] to address the use of SCCs with regard to international data transfers. In the context, they describe an approval process that appears to be based largely on the OSS principle. The use of the Co-Operation Procedure would be a boon for companies operating out of multiple member states, allowing for greater ease in using ad hoc contracts or intragroup agreements.

» Binding Corporate Rules (BCRs)

BCRs are binding codes of conduct, checked and enforced by EU national authorities, to implement in multinational data transfers, in order to make all internal transfers lawful at once. BCRs have been in use for over a decade. BCRs can be described in two separate categories: BCR-C for data transfers from an EU controller to a US controller (traditional use), and a BCR-P for data transfer from an EU Controller to a US processor.

[12] "One-Stop-Shop" Under the Proposed EU Regulation: A Way Forward", Hunton&Williams: https://www.huntonprivacyblog.com/2014/11/articles/one-stop-shop-proposed-eu-regulation-way-forward/
[13] "Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks-Eligibility for Self-Certification", export.gov: http://www.export.gov/safeharbor/
[14] Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clauses; adopted 11-26-2014, Article 29 Working Party: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf

CONCLUSION

Having an "overall view" of the required measures should enable companies to recognize the areas that need attention. The following chart gives that overall view and comparison as to what it required now and what will be required shortly. To ensure your future compliancy, review each item that will need addressed and begin setting your course of action for transition with plans and procedures directing employees and consultants, vendors and third parties as to their expectations and requirements. Keep in mind, however, that the GDPR is still under consideration and the rules they have proposed may still be revised. Consult your legal counsel or privacy professional to ensure all regulatory requirements have been met.

OVERALL VIEW: CHANGES FROM DPD TO GDPR

Data Protection Directive (DPD)	**Genereal Data Protection Regulation (GDPR)**
EU Member States use as guide	Regulation applies to all member states
EU only	Global Long Reach
For Data Controllers	For Data Controllers, Processors, Sub-Processors
Penalties for noncompliance per Member State	Sanctions are massive
Approval through DPA of each Member State	Approval through one DPA (or two for ≥10 Member States)
DPO not required	Regulation applies to all member states
Varying types of consent	Explicit consent only
Protected: Personal data when name included	All personal data, regardless, and encrypted
Limited definition of PII	Expanded definition of PII
Copy request allowed by data subject	Copy, deletion, and data portability request allowed by data subject
Data Privacy Impact Assessment Suggested	DPIA required: sensitive or great in number
Legitimate interest used as basis for processing and sub-processing	Cannot be used as transfer basis or sub-processing, consent cannot be used as legitimate interest
Privacy Notice required with suggestions	Privacy notice requires table and specific wording
No breach notification requirements	Breach notifications with time limits
No breach penalties	Breach non-compliance fines substantial

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN

Iron Mountain Iron Mountain Incorporated (NYSE: IRM) is a leading provider of storage and information management services. The company's real estate network of over 67 million square feet across more than 1,000 facilities in 36 countries allows it to serve customers around the world. And its solutions for records management, data management, document management, data center management, and secure shredding help organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including business documents, backup tapes, electronic files, and medical data. Visit www.ironmountain.com for more information.