PREPARE NOW FOR THE NEW EU DATA PROTECTION LAW

Map your organisation's personal data and future-proof your Records Retention Schedule

IRON MOUNTAIN®

WHITE PAPER

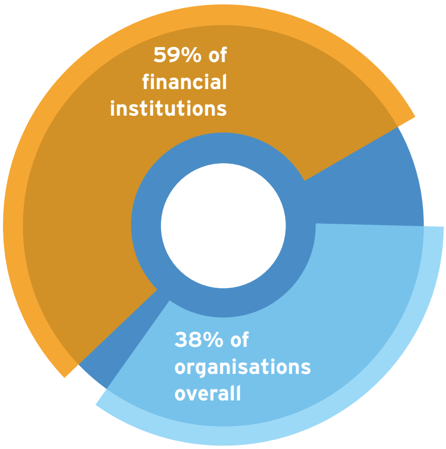
WHY READ THIS

BECAUSE HAVING A SOLID RECORDS AND INFORMATION MANAGEMENT PROGRAMME IN PLACE NOW WILL PUT YOU IN A GOOD POSITION TO COMPLY WITH THE IMPENDING GENERAL DATA PROTECTION REGULATION (GDPR).

AN INCREASINGLY COMPLEX EU REGULATORY ENVIRONMENT

The European regulatory landscape as it affects records retention and disposition is complex. Not only do you need to adhere to local laws governing records retention in every market where you conduct business, you also need to consider operational and business requirements and your organisation's risk appetite. Entire teams of lawyers may be focused on keeping track of regulations. Recent figures from **Thomson Reuters**[1] suggest that over a third of organisations (38%) and 59% of global financial institutions dedicate one whole day a week to analysing regulatory developments.

Organisations spending one day a week keeping up with regulations



The process of creating rules to govern your organisation's information is complicated further by the exponential growth in volume and variety of data created and processed by organisations; and the ever-increasing need to harness its value. Indeed, **IDC**[2] expects annual data creation to reach 40ZB by 2020 – a 50-fold increase from 2010. In addition to all of this, companies face a new challenge driving the need to get retention and disposition right in the form of the new **EU General Data Protection Regulation**[3] (GDPR), which comes into effect in 2018.

While the new regulation is focused on protecting European residents' constitutional right to privacy and does not set out any specific retention requirements, failure to comply with it can have far-reaching financial and reputational implications, making it important to get records retention right. With a greater focus on the comprehensive treatment of personal data and increased risks and fines comes a heightened need to make sure your data policies, rules and location information are up to date, especially for personally identifiable information (PII). Failure to act now will leave you rushing to catch up at a time when a mistake or oversight may be punishable by law and cost your organisation dearly.

[1] http://searchcompliance.techtarget.com/feature/Firms-face-regulatory-fatigue-higher-cost-of-compliance
[2] http://searchdatamanagement.techtarget.com/feature/Big-data-growth-increases-data-integration-degree-of-difficulty
[3] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

THE IMMINENT ARRIVAL OF THE GDPR

Designed to protect personal information in an increasingly digital world, the GDPR is a heavyweight, EU-wide legislation that will have far-reaching implications for organisations and their use and storage of personal data – in whatever form that might be.

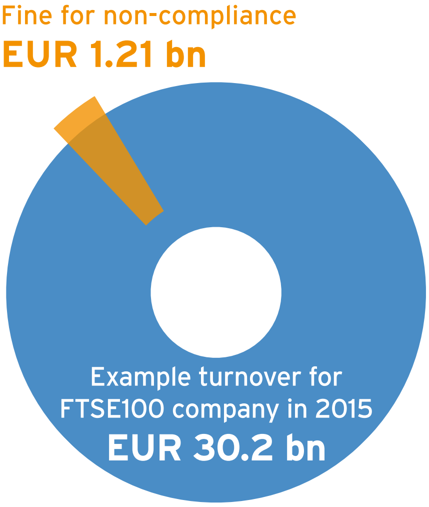
It protects the right of a European resident to determine whether, when, how and to whom his or her personal information is revealed and how it can be used. It will apply to EU-based organisations as well as the data processing activities of those who target EU data subjects, covering the acquisition, use, transmission, storage, destruction and breach of personal data. Failure to comply with the regulation will result in swift and severe punishment, with fines of up to **4% of annual world turnover or EUR 20 million**[4] – whichever is greater.

> THE DAYS OF KEEPING EVERYTHING, FOREVER JUST IN CASE ARE WELL AND TRULY OVER IF ORGANISATIONS AIM TO PROTECT PERSONAL DATA ACCORDING TO THE LAW.

However, despite the risk of severe fines and the deadline to comply only two years away, a **fifth of businesses**[5] across Europe remain unaware of how the changes will affect them and the impact they will have upon the storage and processing of personal data.

Now is the time to make sure you know where PII lives in your organisation, your business suppliers' organisations and what obligations you carry in terms of its retention and destruction.

Example fine for non-compliance for FTSE100 company



QUESTIONS TO ASK NOW

- **Do you understand enough about the new regulation to know whether or not you're ready?**
- **What is meant by 'personal data', where does it sit in your organisation, who has access to it and how do you keep retention rules up to date to govern it? This includes data on corporate systems, employees' personal devices, offsite archives and filing cabinets as well as information stored by suppliers, subcontractors and business partners.**
- **Is there an Information Governance council in your organisation? How are Records and Information Management and Privacy leaders coming together with other colleagues to address how your organisation will prepare for the new regulation?**

Share these questions with your colleagues

[4] http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf (Article 79)
[5] https://www.ipswitch.com/blog/european-businesses-feel-the-financial-burden-of-preparing-for-gdpr/

THE CRITICAL GDPR TERMINOLOGY CHECKLIST

1 Personal data and territorial scope, data subject access requests

Understanding what is meant by personal data is the first step in deciding which parts of the regulation will apply to your information and how. ‘Personal data’ is defined as data relating to a ‘data subject’ (a person) who can be directly or indirectly identified on the basis of that data by an organisation’s ‘data controller’. Such data also includes device identifiers, cookies or IP addresses. Under the GDPR, data controllers should be aware of all personal data under their control and able to demonstrate that they understand the risks facing data protection.

2 Data protection impact assessment (DPIA)

As part of a privacy risk assessment and in advance of any project that is likely to increase risks to the information belonging to data subjects, an organisation is required to perform an initial assessment to determine if a DPIA is necessary. This assessment is much easier once you know where your personal information lives.

3 Data subject’s access request

The right of an individual to see and receive a copy of his or her personal data that an organisation (and its business associates) process.

4 The right to erasure and data portability

Better known as the ‘right to be forgotten’, organisations need to be able to quickly identify and delete or transfer personal data if asked to do so by the person whose data it is. You can only do this if you know exactly what information you hold and where it is.

5 Notice and consent

In recent years, we have seen the rise of the citizen or increased public citizen concern and demand for transparency in how personal data is used. Authorities are also challenging organisations to show you have provided notice and collected consent in cases where it is needed. Consent for data processing must be freely given, specific, informed and explicit by default. If individuals are to knowingly and willingly provide permission, organisations in return should be transparent about what they are processing the data for and how long they intend to keep it, especially as they are required to show proof of notice and consent.

COMPLIANCE IN PRACTICE: SHOW THAT YOU KNOW

In order to meet your statutory obligations (granting access, rectifying wrong personal data, or deleting outdated personal data), you first need to know where it lives. A data map of physical and digital information, including personal data, provides a helpful organisation-wide view of where data is located to ensure its risk can be assessed and monitored on an ongoing basis.

Once you know where your information is, you need to know what you can do with it and how long you must keep it. This requires making sure that your retention policies are up to date so that you are only keeping and destroying personal data (and all other records) when you are required to for legal, regulatory or contractual obligations in a defensible way.

Further, information your organisation may want to mine for big data or analytics purposes will need to have personal data removed and then stored not as records but aggregated into a data repository.

MANY GLOBAL ORGANISATIONS USED TO KEEP THE SAME RETENTION PERIOD FOR ALL RECORDS FOR OPERATIONAL CONVENIENCE. WITH THE STRICTER REGULATION, A THOROUGH REVIEW OF RETENTION POLICIES AND PROCEDURES[6] IS NECESSARY TO ENSURE THEY MEET OBLIGATIONS AND TO AVOID OVERRETENTION OF PERSONAL DATA.

[6] http://www.ironmountain.co.uk/Knowledge-Center/Reference-Library/View-by-Document-Type/Best-Practices/D/Mini-Document-Retention-Guide-United-Kingdom-2015.aspx

VISUALISING THE REGULATORY CHALLENGE

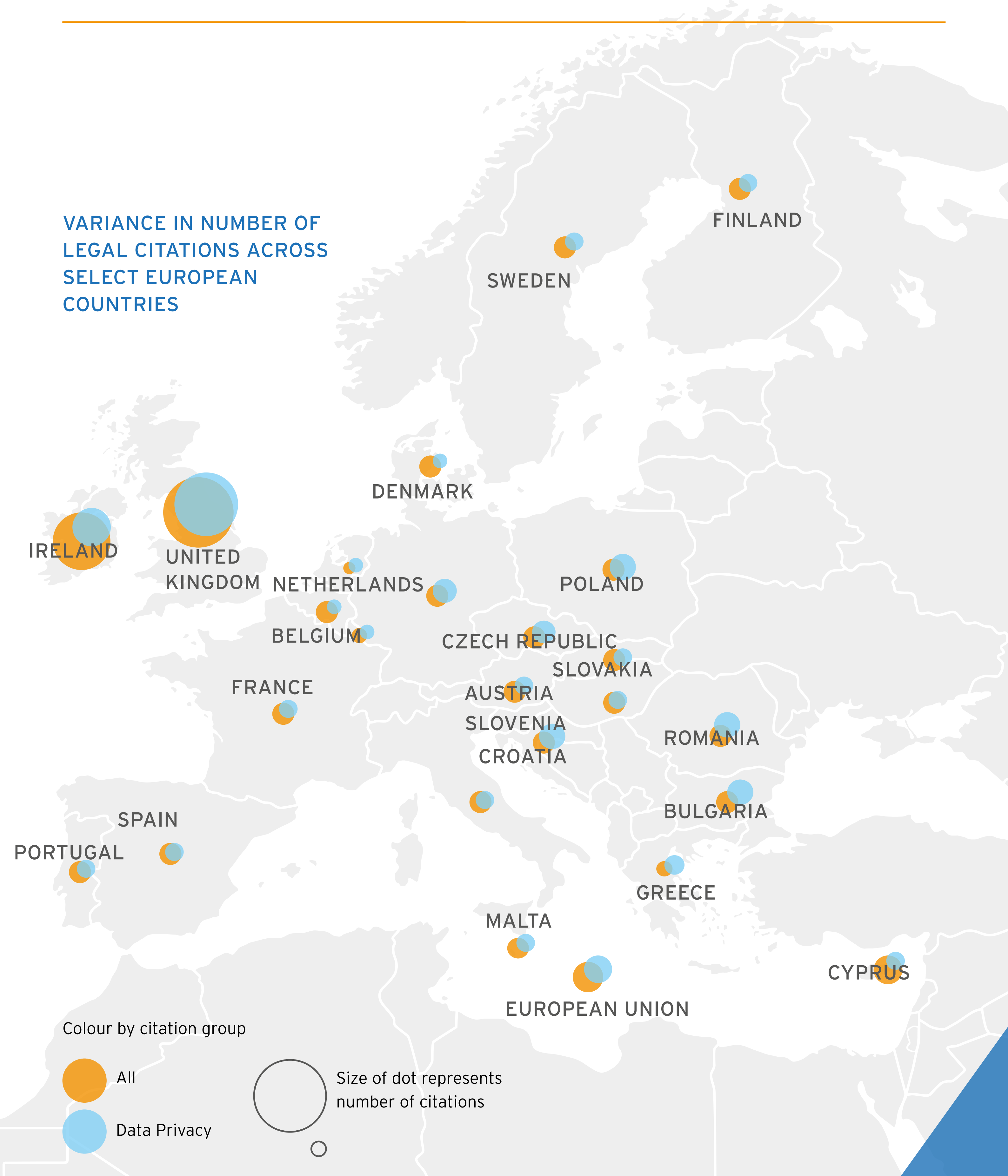
One of the challenges for organisations is in understanding the full extent of where personal and potentially sensitive information exists across their entire data estate. Some record types, such as customer account records and employee files, will inevitably contain PII, but other less obvious types such as contracts and shareholder records may also be subject to the scope of GDPR.

To understand and demonstrate how existing laws and regulations across any industry can affect the retention of personal information, we analysed a sample of our **Iron Mountain Global Research**[7] database containing 30,000 fully summarised and cited retention requirements.

The following map shows the spread of the sample of data we used for the analysis and illustrates the proportion of regulation that could apply to personal data in each country.

[7] http://www.ironmountain.co.uk/Services/Records-Management-And-Storage/Global-Research-and-Policy-Center/Global-Research-Service.aspx

VARIANCE IN NUMBER OF LEGAL CITATIONS ACROSS SELECT EUROPEAN COUNTRIES



***Please note** data used for visualisations is a representative sample set of European countries and industries drawn from the Iron Mountain Global Research database

PUTTING THEORY INTO PRACTICE

2018 is not the time for surprises

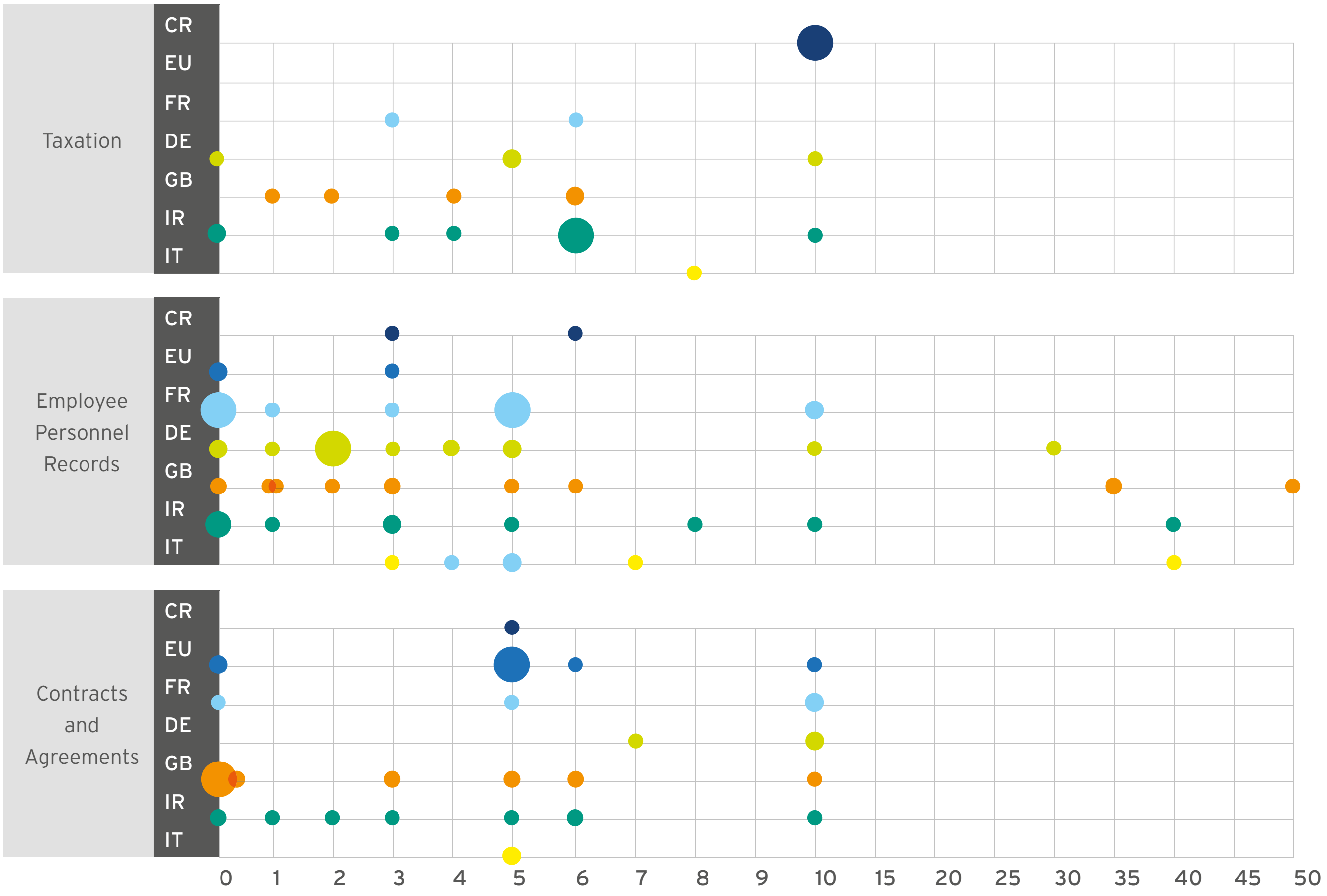
Records retention is not a new challenge for organisations. The introduction of the GDPR and associated penalties for non-compliance means that it has become mission-critical to get data retention right. Knowing what records – both digital and physical – you have across all business units, and in particular which of those contain personal data is the starting point for avoiding the wrath of the regulators.

Arranging records by function, class and type makes it easier to apply robust retention rules for each and avoid the sudden discovery that you have lost data you should have kept or retained information that you are no longer entitled to hold.

Information that passes through the hands of employees, contractors and suppliers must also comply with the same retention policies.

Just as regulations change and impose new sanctions on organisations over time, your retention policies should remain dynamic and responsive, adaptable to evolving business and regulatory landscapes.

VARIANCE IN MAXIMUM RETENTION PERIOD FOR SELECT RECORD TYPES ACROSS SELECT EUROPEAN COUNTRIES



The graphs demonstrate that there is a broad spread of retention periods assigned to similar record types throughout different countries across Europe.

The complexity of retention requirements and the range of retention periods that could apply is illustrated for selected EU countries. It also shows the extent of EU wide regulation.

Colour by country

- ● Croatia
- ● Europe
- ● France
- ● Germany
- ● Great Britain
- ● Ireland
- ● Italy

Size by count

○ Size of dot represents number of citations with the corresponding retention period

Hover on the title of each graph for more indepth retention information

HOW WE CAN HELP

Taking a broad-brush approach to meeting GDPR obligations is not an option. **Iron Mountain's Global Research service and Policy Centre solution**[8] can help your organisation automate the development and maintenance of your retention schedule. Our Professional Services experts use a proven consulting methodology to define and build a research library tailored to your organisation's risk profile and sized to your global footprint. As part of this process we can capture a data map for your information estate, highlighting where critical, sensitive and personal data exists. This will allow you to respond more quickly to requests for information, accurately identify candidates for destruction or tackle a breach in a more contained way.

Once your library and data map have been created and retention schedule developed or refreshed, you'll receive go-forward, up-to-date retention guidelines from the localities you operate through our **Policy Centre solution**, a cloud-based portal where your retention schedule lives. Then you can update your policies accordingly to stay continually current and confidently destroy information when it reaches the end of its retention period. Experts are on hand to help explain what the changing regulations mean and empower you to keep control and mitigate risk at every stage of the information lifecycle – enabling you to meet GDPR obligations and beyond.

GET HELP NOW

If you want to learn more about this topic, Iron Mountain's Professional Services experts and the **Global Research service and Policy Centre** solution can help your organisation prepare to fully comply with the regulations that govern you.

For more information please call:

08445 60 70 80

or visit our **website**.

[8] http://www.ironmountain.co.uk/Services/Records-Management-And-Storage/Global-Research-and-Policy-Center.aspx

ABOUT 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 69 million square feet across more than 1,100 facilities in 37 countries allows it to serve customers with speed and accuracy. And its solutions for records management, data management and document management help organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information for business advantage. 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.co.uk for more information.

Iron Mountain®