IRON MOUNTAIN®

GDPR FREQUENTLY ASKED QUESTIONS

CONTENTS

GENERAL QUESTIONS

CAN YOU PROVIDE AN OVERVIEW OF YOUR GOVERNANCE STRUCTURE FOR IMPLEMENTATION OF THE GDPR?

For many years, Iron Mountain has been supported by dedicated teams that focus on privacy, technology and information security in all the markets where we operate. In early 2016, these teams started the process of preparing Iron Mountain for the GDPR. . Our executive leadership team is actively engaged and has appointed our Chief Technology Officer to lead the efforts to ensure compliance within our processes, infrastructure and service offerings.

The Privacy and Information Technology teams have conducted a comprehensive assessment of our compliance with the GDPR. The results have been shared with the leadership team and subject matter experts and any material gaps have been or are being addressed to ensure compliance with the GDPR.

CAN YOU PROVIDE YOUR PROJECT PLAN AND TEAM STRUCTURE FOR YOUR GDPR PROJECT?

Our project plan is an internal document that is managed by Privacy and Compliance. We are happy to respond to any specific questions related to our GDPR project.

WHAT DID YOU EXPERIENCE TO BE THE KEY ISSUES OR STUMBLING BLOCKS TO YOUR BUSINESS WHEN IMPLEMENTING ALL THE NECESSARY GDPR PROCESSES?

We have not identified any major obstacles. While the GDPR introduces a few new concepts, Iron Mountain's existing privacy program ensures that we are well prepared to comply with the GDPR.

DOES THE GDPR RESULT IN ANY CHANGES TO OUR WORKING RELATIONSHIP?

There are no changes in the way we provide our services or our relationship with you. However, we introduced new data processing agreements with customers to comply with all GDPR requirements. Accordingly, we have prepared such a document that we are happy to provide for your review and signature.

WHAT IMPACT DOES THE NEW LEGISLATION HAVE ON THE SCOPE OF SERVICES PROPOSED UNDER THE FRAMEWORK?

There are no changes to the way we provide our services or our relationship with you. However, we introduced new data processing agreements with customers to comply with all GDPR requirements. Accordingly, we have prepared such a document that we are happy to provide for your review and signature.

WHAT SYSTEMS DO YOU CURRENTLY UTILIZE TO MANAGE BOXES AND DOCUMENTS YOU CURRENTLY HAVE ON-SITE? WHAT CHANGES DID YOU PROPOSE TO YOUR SYSTEMS TO COMPLY WITH THE NEW GDPR LEGISLATION?

We use SKP/O'Neill or other solutions depending on the country location. Our IT assessment project has not identified any material gaps in these solutions.

CAN IRON MOUNTAIN IDENTIFY THE TYPE OF PERSONAL DATA IT PROCESSES AS DATA PROCESSOR?

NO.

Iron Mountain does not know and is not authorized to identify what information it processes on behalf of its customers. Therefore, the customer must provide the necessary details as part of the data processing agreement with Iron Mountain.

DO YOU REVIEW ON A REGULAR BASIS YOUR DATA PROTECTION FRAMEWORK AND POLICIES, AND HAVE YOU COMPLETED A REVIEW TO ENSURE COMPLIANCE WITH THE GDPR?

Iron Mountain reviews its compliance with applicable laws and regulation on a regular basis and makes the necessary changes.

ARE YOU PROPOSING TO APPLY FOR CERTIFICATION UNDER THE GDPR?

At the moment, Iron Mountain does not plan to apply for a certification.

IS THE ACCESS TO PERSONAL DATA LIMITED ONLY TO THOSE PERSONNEL WHO REQUIRE ACCESS TO PERFORM THEIR ROLE?

Yes. Personnel are required to be positively authenticated and authorized prior to being granted access to Iron Mountain facilities and systems. Access based on an employee's role is limited to the minimum necessary to perform their job function. Access to information resources is controlled through a managed process that addresses authorizing, modifying and revoking access.

DATA PROTECTION IMPACT ASSESSMENTS

HAVE YOU IMPLEMENTED A DATA PROTECTION IMPACT ASSESSMENT/PRIVACY IMPACT ASSESSMENT (DPIA/PIA) PROCESS?

Yes. We have a privacy risk assessment procedure in place that must be completed before developing, introducing or purchasing any new solutions that processes personal data or engaging any new vendor that processes personal data on behalf of Iron Mountain.

DO YOU HAVE AND MAINTAIN DPIA GUIDELINES AND TEMPLATES?

Yes. We have a privacy risk assessment procedure in place that must be completed before developing, introducing or purchasing any new solutions that processes personal data or engaging any new vendor that processes personal data on behalf of Iron Mountain.

IN WHAT CIRCUMSTANCES ARE DPIAS COMPLETED? PLEASE PROVIDE EXAMPLES OF DPIAS COMPLETED.

Our Data Protection Impact Assessment must be completed for all 'High' risk rated applications or projects by the relevant business owner or project lead. A 'High' risk classification means that a more detailed Data Protection Impact Assessment must be completed. A 'Low' classification means that a shorter Privacy Questionnaire must be completed.

AUDITS

HAVE THE REQUIREMENTS FOR AUDITS CHANGED UNDER THE GDPR AND IF SO HOW?

With respect to audits there is no fundamental change under the GDPR. The GDPR does not contain very detailed rules regarding audits; it grants the data controller the right to audit its data processors. Details are subject to the agreement of the parties.

VENDORS/SUBCONTRACTORS

HOW WILL YOU ENSURE THAT ALL OF YOUR SUB-CONTRACTORS WHO PROCESS PERSONAL DATA WILL COMPLY WITH THE GDPR BY 25 MAY 2018, AND WHAT OVERSIGHT ARRANGEMENTS DO YOU HAVE IN PLACE?

Our process contains the following steps:

1. Identify which of our existing vendors process personal data and which of those qualify as data processors based on the service they provide to Iron Mountain. (excluding global vendors – these are being dealt with by P&C at the Enterprise level).

2. Assess whether a vendor is qualified under the GDPR.

3. Send out the vendor DPA template to the processors for signing.

Risk relating to the use of third parties is considered as part of an initial third party selection process, whereby all suppliers are risk assessed as part of a due diligence process prior to any engagement. We reviewed (and update) all our existing vendor agreements to meet the GDPR requirements. We use a new vendor agreement template with future vendors, which complies with the GDPR requirements. Our new vendor agreement template has been designed to include typical customer "flow-down" provisions.

IF IRON MOUNTAIN ENGAGES ANOTHER VENDOR (SUB-PROCESSOR) FOR CARRYING OUT SPECIFIC PROCESSING ACTIVITIES ON BEHALF OF ITS CUSTOMER, WILL THE SAME DATA PROTECTION OBLIGATIONS BE IMPOSED ON THE SUB-PROCESSOR AS SET OUT IN THE CONTRACT BETWEEN IRON MOUNTAIN AND OUR COMPANY?

As the global leader in information management solutions, Iron Mountain is honored to work with about two hundred thousand customers.

We are confident that our vendor data processing agreements comply with the GDPR requirements and in all material aspects reflect our customer data processing agreements.

We are executing these data processing agreements with all of our processors to make sure that they are subject to the same principles as set forth in our agreements with our customers.

CAN WE REVIEW THE CONTRACTS BETWEEN IRON MOUNTAIN AND ALL SUB-PROCESSORS LISTED IN THE APPENDIX TO THE DPA?

We would share with you our vendor facing DPA template. Otherwise, we represent that the terms of our standard vendor DPA are incorporated into our vendor DPAs.

WHICH CATEGORIES OF PERSONAL DATA ARE BEING TRANSFERRED TO THE SUB-PROCESSORS?

The vendors that Iron Mountain typically uses do not have direct access to your company's personal information as they handle the assets (i.e. the box or backup tape) and not the information. To the extent they transport or securely destroy an asset, that asset may contain your company's personal data.

Please note that Iron Mountain in its capacity as data controller also uses data processors, that process limited personal data about our customers' employees for customer relationship management, invoicing and other administrative purposes.

DATA SUBJECT ACCESS REQUESTS (UPDATE, DELETE, DATA PORTABILITY ETC.)

DO YOU RESPOND DIRECTLY TO A DATA SUBJECT ON BEHALF OF A CUSTOMER?

In the case of receiving any requests directly from a data subject regarding their personal data (update, deletion, export) we will inform the customer and provide assistance for responding to the data subject according to the customer agreement.

DO YOU PROVIDE INFORMATION TO SUPPORT CUSTOMER'S RESPONSE TO THE DATA SUBJECT?

No. In case of receiving any request directly from data subjects regarding their personal data (update, deletion, export) we will inform the customer and provide assistance for responding to the data subject according to the customer agreement.

PLEASE DESCRIBE HOW PERSONAL DATA WILL BE AMENDED, DELETED, OR PORTED IF REQUESTED BY A CUSTOMER?

We will act according to your instruction, and in accordance with the customer agreement.

RECORDS RETENTION

FOR HOW LONG ARE CUSTOMER INFORMATION AND RECORDS RETAINED?

1. The customer information we process as processor on behalf of our customers will be retained according to the customer's agreement and instructions.

2. The information we hold about the customer (i.e. contact details of their employees) will be retained according to the applicable retention periods contained in our retention schedule.

ACCOUNTABILITY

HOW CAN YOU SHOW COMPLIANCE WITH THE ACCOUNTABILITY PRINCIPLE?

We have a comprehensive GDPR Project Plan that focuses on the key topics such as data inventory, data mapping, data exports, data protection officers, privacy notices and policies, data protection impact assessments, privacy by design & default and data breach management.

DATA PROTECTION OFFICER (DPO)

DO YOU HAVE A DPO IN PLACE AND DOES THAT PERSON MEET THE REQUIREMENTS OF THE DPO UNDER THE GDPR? IF SO, PLEASE PROVIDE THEIR CONTACT DETAILS.

Iron Mountain decided to appoint one centralized DPO.
Our centralized data protection officer can be contacted as follows:

Iron Mountain Data Protection Office
Global.privacy@ironmountain.com
Iron Mountain Europe
Czuczor utca 10
1093 Budapest
HUNGARY

Iron Mountain's Global Privacy and Compliance Team will work in close cooperation with the DPO.

ARE YOU REQUIRED TO APPOINT A DPO UNDER THE GDPR?

Yes. Iron Mountain decided to appoint one centralized DPO.
Our centralized data protection officer can be contacted as follows:

Iron Mountain Data Protection Office
Global.privacy@ironmountain.com
Iron Mountain Europe
Czuczor utca 10
1093 Budapest
HUNGARY

IF THERE IS NO MANDATORY REQUIREMENT TO APPOINT A DPO UNDER THE GDPR, DO YOU INTEND TO APPOINT ONE? IF SO, PLEASE PROVIDE THEIR CONTACT DETAILS WHEN AVAILABLE.

Iron Mountain decided to appoint one centralized DPO.
Our centralized data protection officer can be contacted as follows:

Iron Mountain Data Protection Office
Global.privacy@ironmountain.com
Iron Mountain Europe
Czuczor utca 10
1093 Budapest
HUNGARY

IF YOU DO NOT HAVE OR INTEND TO APPOINT A DPO, PROVIDE DETAILS OF HOW WILL YOU EVIDENCE OF WHICH FUNCTIONS AND STAFF HAVE THE REQUIRED SKILLS, KNOWLEDGE AND RESOURCES TO COMPLY WITH THE GDPR.

Iron Mountain decided to appoint one centralized DPO.
Our centralized data protection officer can be contacted as follows:

Iron Mountain Data Protection Office
Global.privacy@ironmountain.com
Iron Mountain Europe
Czuczor utca 10
1093 Budapest
HUNGARY

RECORD OF PROCESSING ACTIVITIES (DATA MAPPING)

HOW WOULD YOU SHOW THAT YOUR INFORMATION ASSET REGISTER (INCLUDING DATA FLOWS AND CROSS BORDER DATA TRANSFERS) IS UP-TO-DATE?

In relation to the personal data we process for our own purposes such as HR, marketing, or CRM we use (and update) a segment of our commercially available Iron Mountain® Policy Center solution.

PLEASE CONFIRM AND EXPLAIN HOW YOU MAINTAIN A RECORD OF ALL CATEGORIES OF PROCESSING ACTIVITIES CARRIED OUT ON OUR BEHALF IN ACCORDANCE WITH THE DATA PROTECTION LAWS.

As data processor, we know through our billing systems what services and, therefore, what processing activities we carry out on behalf of our customers.

DATA BREACH

WHAT IS YOUR INTERNAL PROCESS FOR BREACH REPORTING, AND HOW DO YOU INTEND TO COMPLY WITH THE GDPR?

Protecting customers' information is of paramount importance to us. Our Event Reporting Procedure was developed to support that.

Additionally, Iron Mountain is using an event reporting solution (ERMS) to record all incidents. In order to comply with the GDPR we revised and updated both our procedures and reporting platform.

DO YOU HAVE A PROCESS IN PLACE TO NOTIFY DATA SUBJECTS OF DATA BREACHES, AND IN WHAT CIRCUMSTANCES WOULD YOU NOTIFY DATA SUBJECTS?

Iron Mountain is only responsible for notifying customers about data breaches regarding customer material. Customers may be obliged to notify the regulators and/or data subjects.

DATA TRANSFERS

DO YOU HAVE CONTRACTS IN PLACE WITH THE OFFSHORE PROVIDERS (THIRD PARTIES OUTSIDE THE EU) THAT INCLUDE APPROPRIATE CONTRACT CLAUSES (INCLUDING DATA PROTECTION AND INFORMATION SECURITY) THAT MEET THE GDPR REQUIREMENTS?

For transfers to countries that do not provide an adequate level of data protection, we rely on Model Clauses, or on the Privacy Shield certification for US based entities. Both transfer mechanisms are compliant with the GDPR requirements.

IN THE EVENT THAT DATA IS PROCESSED OR STORED OFFSHORE (OUTSIDE OF THE EU), DO YOU OBTAIN THE WRITTEN CONSENT OF THE CUSTOMER TO DO THIS?

Our customer contracts contain the necessary authorization to transfer personal data to third parties outside of the EEA. Iron Mountain does not export the customers' physical assets (articles, files, images, media, and deposits).

STAFF COMMUNICATION AND TRAINING

WHAT STAFF COMMUNICATIONS, AWARENESS ACTIVITY, OR TRAINING HAVE YOU COMPLETED/PLANNED IN ORDER TO RAISE AWARENESS OF THE GDPR AND INFORMATION SECURITY IN THE BUSINESS, AND HOW WILL THIS BE DELIVERED, AND BY WHEN?

Iron Mountain completed a series of GDPR trainings for its staff and provides annual privacy and security trainings. In case of any internal request or additional needs, the Privacy and Compliance Team will deliver further privacy sessions.

WHAT TRAINING AND AWARENESS DO YOU PLAN TO DELIVER ON A REGULAR BASIS TO EMBED THE GDPR? HOW WILL THIS BE DELIVERED? HOW FREQUENTLY WILL THIS BE DELIVERED?

Iron Mountain completed a series of GDPR trainings for its staff and provides annual privacy and security trainings. In case of any internal request or additional needs, the Privacy and Compliance Team will deliver further privacy sessions.

800.899.IRON
IRONMOUNTAIN.COM

WE PROTECT WHAT YOU VALUE MOST™

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

USDM-FAQ-041918A