IRON MOUNTAIN®

GDPR FOR INFORMATION GOVERNANCE PROFESSIONALS

DEFINITION OF TERMS

BINDING CORPORATE RULES (BCRS)

Rules within a multinational group of companies that determine how they will transfer personal information to their entities that are in countries that do not ensure an adequate level of protection for personal data. BCRs that the European Commission approves under the European Commission's EU cooperation procedure provide for the legal transfer of personal data between the entities of such multinational groups.

DATA PROTECTION AUTHORITIES (DPAS)

National data protection authorities are independent public authorities tasked with overseeing the operation of data protection law within their territory. They have the authority to investigate an organization's handling of personal data, intervene before processing or transfers of personal information, participate in and bring legal proceedings for privacy violations, and hear grievances of individuals who believe their personal data has been misused.

WHAT IS THE GDPR?

The General Data Protection Regulation ("GDPR") is a European Union ("EU") regulation adopted in April, 2016, aimed at strengthening privacy protections for individuals residing in the EU, harmonizing EU states' data protection laws and creating a standardized mechanism of enforcement. While it does not come into effect until May 25, 2018, its impacts are so overarching and applicability so broad, that organizations are currently scrambling to prepare to meet its mandates in 2017 before they come fully into effect next year. As detailed in this Guide, fines and penalties for failure to comply could cripple a business and compliance is not a simple matter to achieve.

WHY READ THIS GUIDE?

This Guide is intended to support a business's Information Governance (IG) team prepare to meet the firm's obligations under the GDPR. Some members of the team who are privacy professionals or attorneys may already be very familiar with the GDPR but complying with the GDPR will require a firm to reach into its Information Technology, Records Management and Line of Business functions to make compliance a reality. This Guide is intended as an introduction to the GDPR that the lawyers and privacy specialists as well as the members of the IG team can all understand and use as a project plan for GDPR compliance.

As any lawyer will tell you, a law or regulation is only partially about the words as written; it is only when the law begins to be enforced by regulators and courts that one can truly tell what factors the authorities will consider critical, so we have provided insights from our work with our clients to tell you what they are doing now to prepare for GDPR. If you are outside the norm in your level of preparedness for the GDPR, you are putting your firm at an additional risk.

Finally, if you think you can ignore the GDPR because your company is not incorporated or physically located in the European Union, think again. The GDPR is applicable to any firm which has the PII of any EU citizen and the EU is preparing to enforce the GDPR world wide – particularly against 'deep pocket' targets.

DEFINITIONS CONTINUED

DATA PROTECTION OFFICER (DPO)

Data Protection Officers ensure that an organization is both aware of and complies with relevant data protection responsibilities. A DPO must be appointed if the core activities of the company involve "systematic monitoring of data subjects on a large scale" or large scale of special categories of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric information, sexual orientation, or data regarding health or sex life). Small-medium enterprises (SMEs) may be exempt from appointing a DPO if certain requirements are met.

PERSONALLY IDENTIFYING INFORMATION (PII)

Information that can be used on its own or together with other information to determine a person's identity, locate an individual, or contact a particular person. Information that is unique to a person or that can de-anonymize anonymous data can be considered PII.

RISKS OF NONCOMPLIANCE

Under the GDPR, EU Data Protection Supervisory Authorities will have an array of both investigative and corrective powers – including the ability to issue warnings of noncompliance, perform audits of organizations housing EU's residents' personal data, demand specific remediation within a specific time frame, order erasure of certain data, and suspend data transfers to a third country.

In addition, the GDPR grants Supervisory Authorities the ability to issue administrative fines for noncompliance. Breached organizations will find the fines they face increasing dramatically. From a theoretical maximum of £500,000 (over $664,000) that the Information Commissioner's Office (ICO) can currently levy, penalties will reach an upper limit of £20 million (over $22.4 million) or 4% of annual global turnover – whichever is greater. The 4% of annual global turnover is the maximum fine that can be imposed; i.e., for serious infringements in which there was not sufficient consent provided by the customer to process data.

Decided on a case-by-case basis, these fines will take into consideration a variety of factors including, but not limited to:

- the nature, gravity and duration of the infringement;
- whether the infringement was intentional or negligent;
- attempts by the controller or processor to mitigate damage sustained;
- **level of responsibility of controller or processor in terms of the technical or organizational measures in effect at the time;**
- record of previous breaches/infringements by the controller or processor;
- demonstrated effort(s) to work with the Supervisory Authorities to remedy or mitigate the impact of the breach/infringement;
- the type(s) of data impacted by the breach/ infringement;
- manner in which the infringement becomes known to the Supervisory Authorities;
- whether the controller or processor had previously taken any corrective measures over the subject matter at issue in the instant breach/infringement;
- record demonstrating past compliance to improve codes of conduct or certified data privacy mechanisms; and
- other factors such as possible financial benefits gained/losses avoided directly or indirectly by the infringement.

While the variety of factors considered suggests a more "totality of the circumstances" approach, the risk posed by the upper limit of these penalties is unprecedented and could have a severe economic impact on an organization's future. Understanding the risks of noncompliance and having the appropriate security safeguards, breach planning, privacy information destruction, privacy policies and procedures, privacy retention schedules and competent related personnel in place are critical to ensure smooth sailing at the GDPR comes into effect.

HISTORY OF EU/U.S. PRIVACY LAWS/FRAMEWORK

It is important to look at the history of Privacy laws and framework to understand the ideals that serve as the foundation for the GDPR and the EU-US Privacy Shield.

EU PRIVACY DIRECTIVE

In 1995, the EU adopted Directive 95/46/EC, commonly referred to as the EU Data Protection Directive (the "Directive"), with the twin objectives of both protecting the personal information of individuals within its jurisdiction and harmonizing the laws of its member states to allow free flow of such information between said states. This Directive was not self-executing and required implementing legislation to be passed by all member states.

This patchwork of laws is what currently constitutes data protection within the EU and what will be largely replaced when the self-executing GDPR takes effect. Note that the GDPR is a regulation rather than a directive like the former EU privacy Directive, and, as a result, is immediately enforceable when it takes effect and does not require that member states pass implementing legislations to enforce it.

DEFINITIONS CONTINUED

MODEL CONTRACT CLAUSES

Standard clauses that the European Commission has approved because they provide adequate privacy protection to the personal data of individuals. These clauses allow personal information to flow legally from a data controller in EU/EEA member states to a data controller or processor in a country that does not provide adequate protection to personal data.

SAFE HARBOR FRAMEWORK

Though the Directive has been useful in harmonizing cross-border transfer of personal information within the boundaries of the EU, issues have proliferated in private information transfers, processing and control of that information in countries outside of the EU and particularly in the United States. To address these issues, the U.S. Department of Commerce, in collaboration with the European Commission ("EC"), in 2000, established a Safe Harbor framework where US based companies could self-certify that they would adhere to seven privacy principles (the "Principles") encompassed in the Directive to ensure that the privacy rights of European residents would be protected. The Principles are summarized below.

NOTICE

A data subject – an individual whose personal information is being collected, processed, or controlled – must be given notice under such circumstances. This notice must be in "clear and conspicuous" language and not only inform the subject as to the purpose of the collection or use, but give information on how to contact the organization performing those activities, recourse available, and to what types of third parties the information might be available.

CHOICE

A data subject must be given the choice to opt out of allowing his or her personal information to be disclosed to third parties, or to be used for purposes other than those for which the data subject provided original authorization.

ONWARD TRANSFER

In order to transfer personal information to a third party, an organization must apply the above two principles and:

1) Ascertain that the third party adheres to the Principles;
2) Ascertain that the third party is subject to the Directive or an equivalent privacy regime; or
3) Enter into a written agreement with the organization requiring that the third party offers at least the same level of privacy protection as outlined in the Principles.

SECURITY

Organizations must take reasonable precautions in order to prevent loss, misuse and unauthorized access, disclosure, alteration, and destruction of personal information.

DATA INTEGRITY

Personal information must be relevant for the purpose(s) of its intended use and an organization cannot process such information in a manner inconsistent with such purpose. The organization should take reasonable steps to ensure the data is reliable for its intended use, and is accurate, complete and current.

ACCESS

Data subjects must be given access to their personal information and be able to correct, amend, or delete inaccurate information unless the burden or expense of such access would be disproportionate to the privacy risks to the data subject, or if such access would violate the rights of persons other than the data subject.

ENFORCEMENT

There must be readily available and affordable independent recourse mechanisms provided to allow individuals' complaints and disputes to be investigated, resolved, and remedied.

SNOWDEN REVELATIONS

In June 2013, the London Guardian, reported on the first of many U.S. National Security Agency ("NSA") documents leaked by intelligence contractor, Edward Snowden. Subsequently, the press released thousands of documents supplied by Snowden, and, in the process, uncovered many of the ways in which the NSA collected and used personal information relating to millions of individuals, including some European residents. Among those Europeans whose rights had been violated by the NSA, were leaders of European countries. NSA activities and the U.S.'s seeming indifference to individual privacy rights did not sit well with these EU leaders and their fellow Europeans who value privacy as a fundamental constitutional right. The GDPR, designed to replace the Privacy Directive was fast tracked to ensure that the U.S. understood its obligation to protect any EU resident's private information that came under U.S. control.

SAFE HARBOR INVALIDATION

On October 6, 2015, the Court of Justice of the European Union ("CJEU"), decided in Maximillian Schrems v Data Protection Commissioner, to invalidate the European Commission Decision 2000/520/EC (the "Safe Harbor Decision"), that implemented theEU commitments laid out in the Safe Harbor Agreement between the EU and U.S. The court's decision was based largely on revelations from the Snowden leaks.

Specifically, even though a U.S. organization might have self-certified under the Safe Harbor framework, that organization could be compelled by the U.S. government to disclose personal information to U.S. federal authorities if deemed to be in the interest of national security. The U.S. authorities could access such information in a manner incompatible with Safe Harbor Principles and no mechanism of remedy would exist for individuals impacted by the disclosure. In not assessing whether the U.S. government provided privacy protections equivalent to those ensured under the Directive, the E.C., in agreeing to the establishment of the Safe Harbor framework, had overstepped its authority established by the Directive. The CJEU held that the approximately 4700 U.S. companies certified under the Safe Harbor framework were not guaranteeing a sufficient level of privacy protection for European individuals.

Some companies that relied upon Safe Harbor certification to validate EU originating trans-Atlantic transfers of personal information quickly sought alternative means to prove their protection of European residents' privacy, including the execution of model contracts or the adoption of Binding Corporate Rules, both of which are discussed more fully below.

U.S. ORGANIZATIONS IMPACTED BY GDPR

Essentially, any U.S. organization that handles the data of EU residents will be affected by the GDPR. This includes information related to employees who are EU residents, to purchases from or sales to EU residents, and to monitoring the activities of EU residents, including cookies or other methods of tracking users' activities. In addition, the definition of personally identifying information (PII) within the framework of the GDPR is extremely broad, extending to any information that, if combined with another available piece of information, could identify an EU individual.

Consequently, any organization that does business with, tracks, employs, or processes any information about EU residents will be subject to sanction for failing to adhere to the provisions of the GDPR.

RESPONSIBILITIES OF U.S. ORGANIZATIONS HOUSING E.U. RESIDENTS' PII

CONSENT; RIGHT TO WITHDRAW CONSENT

Under the GDPR, valid consent must be explicit for data collected and must specify purposes for which data is used. Consent for children must be given by the child's parent or custodian, and verifiable. **Data controllers must be able to prove consent (i.e. "opting in") and consent may be withdrawn.**

RIGHT TO BE FORGOTTEN, RIGHT TO CORRECT, ERASURE RIGHTS

The GDPR also creates additional "new" rights for individuals, while also strengthening some of the rights that currently exist under the Privacy Directive. These rights are:

- **Right to be informed:** This is an obligation to provide 'fair processing information', typically through a privacy notice. It involves the need for transparency over how you use personal data (concise, intelligible and easily accessible; written in clear and plain language; and free of charge).
- **Right of access:** The GDPR will give individuals the right to obtain confirmation that their data is being processed; access to that personal data; and other supplementary information (similar to what would be provided in a privacy notice).
- **Right to rectification:** Individuals are entitled to have personal data rectified if it is inaccurate or incomplete, and receive notification about any third parties with whom this information was disclosed.
- **Right to erasure:** Also known as "the right to be forgotten", this enables an individual to request that personal data be deleted or removed when there is no compelling reason for its continued processing.
- **Right to restrict processing:** Individuals have a right to block or suppress processing of personal data in certain circumstances (similar to that seen under the Privacy Directive).
- **Right to data portability:** Allows individuals to receive or transmit personal data from one data controller to another without hindrance to that data's usability.
- **Right to object:** Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority; processing for direct marketing; and processing for purposes of scientific/historical research and statistics.
- **Rights in relation to automated decision making and profiling:** E.U. individuals have the right not to be subject to a decision that is based on automated processing and which produces a legal effect or similarly significant effect on the individual.

VENDOR/THIRD PARTY RESPONSIBILITIES

The GDPR sets forth clear lines of account ability regarding data processing by separating responsibility between two types of entities for handling personal data: controllers (principals) and processors (vendors).

The controller is the entity that makes decisions about processing activities. It is responsible for carrying out data protection impact assessments, protecting data subject rights (including erasure, reporting and notice requirements), and maintaining records of processing activities. In addition, the controller entity assumes duties related to data breach notification and consultation prior to processing. The GDPR also places strict requirements on controllers to maintain their own detailed records of processing activities, but will not require them to register such activities with the Data Protection Authority in each member state. By contrast, the processor is any entity contracted by the controller for carrying out processing. Processors have a duty to process data only as instructed by controllers, and implement both the technical and organizational steps needed to meet the GDPR's requirements. Processors are also required to delete or return data to the controller once processing is complete, and agree to specific conditions for engaging other processors. Should the processor act outside the scope of that authority, it will effectively be viewed as a controller – subject to all of the controller's responsibilities as identified above.

CROSS BORDER TRANSFERS

The GDPR will allow transfers of personal data outside the EU where the European Commission has decided that the third country, a territory or one or more specified sectors within that country, or the international organization in question has ensured an adequate level of protection for the personal data. Previous adequacy decisions made under Directive 95/46/EC will remain in effect, and the European Commission will routinely monitor developments in third countries and international organizations that could impact recent adequacy decisions.

NOTIFICATIONS OF BREACH REQUIREMENTS

In the event of a breach, an organization may need to notify the relevant supervisory authority as well as the individuals whose personal information is involved in the breach itself. The decision to notify the relevant supervisory authority can be assessed on a case-by-case basis – losing customer details would be worth reporting (as it exposes individual to identity theft) whereas losing a staff telephone list would not need to be reported.

Under Article 33 of the GDPR, controllers are required to report a personal data breach to the relevant Supervisory Authority within 72 hours of the organization first becoming aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If the notification is not made within that time frame, the organization must provide reasons for the delay. The breach notification should state:

- nature of the personal data at issue (including categories and number of the individuals as well as personal data concerned);
- name and contact details of the data protection officer (or other point of contact);
- the likely consequences of the breach; and
- the measures taken (current or proposed) to deal with the breach and, if applicable, measures taken to mitigate any possible negative effects.

If, however, the data breach is likely to result in a high risk to the rights and freedoms of a data subject, then the controller must communicate the breach to that data subject without undue delay (see Article 34 of the GDPR). In this circumstance, the organization must state in clear and plain terms both the nature of the breach and:

- the name and contact details of the Data Protection Officer or contact person;
- the likely consequences of the breach; and
- the measures taken or proposed to be taken by the controller to address the breach and/or mitigate its effects.

If the controller reported the breach to a Supervisory Authority but not the data subjects, the Supervisory Authority can mandate that the controller take additional steps to notify those data subjects.

By contrast, data processors have a much clearer mandate – they are simply required to notify controllers of a personal data breach without undue delay.

Without guidance from the new European Data Protection Board (EDPB), organizations in doubt as to whether individual rights and freedoms are at risk might best decide to play it safe by notifying data subjects and/or seek direction from the Supervisory Authority.

RETENTION LIMITS

In terms of data retention, the GDPR retains the core principle that **personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.** However, it does add that personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest or scientific, historical, or statistical purposes and be subject to the implementation of appropriate safeguards. However, this should also take into account certain rights granted by the GDPR – including the right to object and the right to erasure (also known as the "right to be forgotten"), under which data subjects have the right to either object to such processing in general and/or demand erasure of that personal data, in certain cases sooner than the end of the maximum retention period. EU Member States may decide to limit the rights granted to data subjects under the GDPR on the condition that there is no risk of breaching the privacy of the data subject and whether other appropriate safeguards have been put in place by the organization.

THE U.S. PRIVACY SHIELD

The U.S. Department of Commerce ("DOC") and the European Commission worked jointly to create the EU-U.S. Privacy Shield Framework to address requirements set by the European Court of Justice in its ruling on October 6, 2015, declaring the existing U.S. Safe Harbor Framework invalid. The new EU-U.S. agreement places safeguards on how U.S. authorities can access the data of European consumers and employees, and creates a framework for resolving cases where Europeans believe that their personal data is misused. The Privacy Shield is critical to facilitating the cross-border data flows upon which major tech companies and other industries rely to carry out trans-Atlantic business, currently the largest trade route in the world.

The EU-US Privacy Shield was adopted July 12, 2016, when the European Commission determined that, under EU law, the Privacy Shield framework is adequate to permit data transfers. The International Trade Administration (ITA), within the DOC, administers the EU-US Privacy Shield program. U.S. Organizations can visit http://www.privacyshield.gov to perform self-certification, which is a public commitment to adhere to the requirements of the framework. Self-certification with the DOC began August 1, 2016, and recertification is required annually.

WHY PARTICIPATE IN PRIVACY SHIELD?

U. S. organizations subject to the Federal Trade Commission (FTC), or the Department of Transportation (DOT) (which have agreed to enforce the Privacy Shield Principles) can join the framework via self-certification. Certification is voluntary, but U. S. organizations that do not participate must comply with EU legal privacy requirements through an alternative method if they plan to transfer personal data from the EU to the U.S. The FTC has stated that it is making enforcement a priority, even adding extra staff specifically to enforce it.

Under the EU data-protection regime, the only requirement for legal transfer of relevant data out of the EU to the U.S. is the individual's consent. However, implementation is tricky as the definition of valid consent is different in each EU country and if there is coercion, the individual has not given consent. If an organization asks an employee for consent to transfer human resources data out of the EU, many DPAs consider that coercion.

Self-certification for the EU-U.S. Privacy Shield Framework began on August 1, 2016, and as of mid-February, 2017, there are 1,649 organizations on the Privacy Shield List (a public list of participating organizations available at https://www.privacyshield.gov/list). This is about a third of those self-certified under Safe Harbor. Organizations certified under the Privacy Shield are determined to provide the "adequate" privacy protections required by the EU Data Protection Regulation. In addition, the EU member states that demand prior approval for data transfers waive this obligation or provide automatic approval for organizations with Privacy Shield certification.

PRIVACY SHIELD FRAMEWORK REQUIREMENTS

The Privacy Shield incorporates the Seven Privacy Principles (see above) and includes 16 additional supplemental principles that expound on the first seven. These principles include additional requirements to those that existed under the Safe Harbor Agreement in order to provide additional protection to the personal data of consumers and employees transferred from the EU to the US. US organizations joining the Privacy Shield Framework must ensure that they adhere to these new requirements.

Privacy Shield participants must apply Privacy Shield Principles as soon as they join the framework. However, for purposes of the Accountability for Onward Transfer Principle, an organization with pre-existing commercial relationships with third parties has nine months from the date of certification to meet requirements of contractual revisions for data transfers as long as certification is accomplished within two months of the effective date (between August 1 and September 30, 2016). During the interim, notice and choice principles apply and agents who receive transferred personal data must adhere to the levels of protection required by the Principles. An organization has a duty to take reasonable steps to stop and remedy any activity by a third party which is not in compliance with the Privacy Shield and to provide the DOC with the privacy protection contractual clauses they have with that third party upon request.

ORGANIZATIONAL RESPONSIBILITIES UNDER PRIVACY SHIELD INCLUDE:

- Requirement that additional information be provided to individuals in the Notice Principle, including:
  - a declaration of the organization's participation in the Privacy Shield,
  - the individual's right to access the personal data utilized by the organization, and,
  - identification of the organization's designated dispute resolution body.
- Contractual provisions relating to third party transfers indicating that:
  - the data can only be processed for limited and specified purposes,
  - the individual must consent to the use of their data for those purposes,
  - the third party will provide the same level of protection as the Privacy Shield Principles, and
  - the third party will notify the transferor if they are unable to provide that level of data protection;
- Transferor maintains responsibility for data protection when transferring to an agent;
- Limit maintenance of PII to information that is relevant to the necessary processing;
- Annual recertification through the self-certification process;
- Independent recourse mechanisms that will be free to the individual and will investigate their complaints;
- Requirement to respond quickly to inquiries from the DOC, including complaints from EU member state authorities;
- Requirement of public disclosure (if allowed by confidentiality) of any portions of assessment or compliance reports sent to the FTC that relate to the Privacy Shield if an organization is under an FTC order or court order due to non-compliance.

PRIVACY POLICY PROVISIONS REQUIRED UNDER PRIVACY SHIELD INCLUDE:

- Acknowledgement of the organization's participation in the Privacy Shield Framework (along with the URL or a link to the Privacy Shield List);
- Specification of the personal data types that the organization collects;
- Identification of subsidiaries of the organization that are participating in the Privacy Shield;
- A stated commitment to apply the Privacy Shield Principles to all EU personal data;
- Specification of the reasons why the organization gathers and employs personal data about individuals;
- Instructions regarding contacting the organization with questions or grievances (including providing contacts in the EU that can respond to those questions or grievances);
- Identification of third parties to which the organization divulges personal data it collects, and the reasons for such disclosure(s);
- Acknowledgement of the individual's right to access the personal data utilized by the organization;
- Specification of the ways the organization allows individuals to restrict the use and exposure of their personal data;
- Identification of the independent dispute resolution body designated to address grievances and provide appropriate recourse to individuals (at no cost to the individual)
- Disclosure that the FTC, DOT, or another authorized statutory body in the U.S. has the power to investigate the organization's adherence to the Privacy Shield Principles and provide enforcement;
- Acknowledgement that individuals may, under certain conditions, be entitled to binding arbitration;
- Acknowledgement that the organization must divulge personal data if public authorities lawfully demand it, including to meet national security or law enforcement requirements;
- Acknowledgement that the organization remains liable when it performs onward transfers to third parties;
- Provide a hyperlink to the DOC's website addressing Privacy Shield Principles and individuals' rights (at http://www.privacyshield.gov/) and a hyperlink to the applicable independent recourse mechanism where individuals can report violation complaints that have not been resolved.

COSTS OF PRIVACY SHIELD PARTICIPATION

The costs of participating in the Privacy Shield includes an annual fee for certification, an annual contribution into a DOC fund and any costs that might be attached to establishing independent recourse mechanisms. The Doc has published a Fee schedule for the annual fees that is available on the Privacy Shield website at https://www.privacyshield.gov/Program-Overview.

The Privacy Shield Framework also specifies that the DOC will create a fund to which participants will contribute annually in order to provide money to cover the costs of arbitration that are described in Annex I to the Privacy Shield Principles. Additionally, each participant will incur the costs related to the independent recourse mechanisms they are required to provide to individuals. If individuals utilize these mechanisms their services are free, and the organization must incur costs.

LIMITS TO GOVERNMENT ACCESS UNDER PRIVACY SHIELD

The US has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Individuals in the EU will, for the first time, benefit from redress mechanisms in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the U.S. under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and should be as targeted and focused as possible and details the safeguards in place for the use of data under such exceptional circumstances. The U.S. Secretary of State has established an independent Ombudsman mechanism within the Department of State as an option for redress in the area of national intelligence for Europeans.

PRIVACY SHIELD: DISPUTE RESOLUTION

Any EU resident who maintains that his or her data has been misused under the Privacy Shield scheme benefits from several accessible and affordable dispute resolution alternatives. Ideally, the company will resolve the complaint itself; or free of charge Alternative Dispute resolution (ADR) solutions are offered. Individuals can also go to their national DPAs, who will work with the FTC to investigate and settle any complaints by EU residents. If a case is not resolved by any these means, an arbitration mechanism is available as a last resort. As stated above, an Ombudsperson who is independent from U.S. intelligence services provides redress for EU residents if their personal data was utilized for national security.

ANNUAL EVALUATION OF PRIVACY SHIELD

It is essential that the EU-US Privacy Shield Framework be monitored continually to ensure that it is working properly. To this end, Privacy Shield will be evaluated by an annual joint review, including the commitments made by the U.S. Office of the Director of National Intelligence regarding personal information utilized for national security or law enforcement purposes. As part of this review, the European Commission and the US DOC will perform the review with the involvement of EU DPAs and U.S. national intelligence experts and will appraise the transparency reports of organizations who have fielded requests for information from the government. In addition, the European Commission will meet with concerned NGOs and stakeholders annually to examine the impact U.S. privacy law developments will have on Europeans. The results of the joint review will be publicly disclosed via a report to the European Parliament and the Council.

IMPLICATIONS OF PRIVACY SHIELD

At their core, the goals of Safe Harbor and Privacy Shield are identical: Participating companies must treat data originating from the EU in accordance with EU law. The real differences is in the safeguards that make sure companies and governments abide by the rules.

The changes in this respect are threefold. First, the US Department of Commerce is now responsible for ensuring companies meet the higher data privacy requirements. Second, any individual whose data originates from the EU (not just Europeans) can complain if they feel their rights have been violated. Those complaints will be forwarded to the relevant U.S. department in a timely manner, free of charge to the individual. Third, the U.S. has committed to eliminate wholesale mass surveillance on the personal information transferred from the EU to the U.S., and have agreed that bulk collection will only be performed if there are preconditions and that collection should be as refined and directed as possible. Complaints pertaining to data transferred for national security will be handled by an ombudsperson, who should work impartially and independently of all federal security agencies.

Max Schrems, a lawyer and privacy activist whose complaint against Facebook's data practices set in motion a chain of events that killed Safe Harbor. "It's the same as Safe Harbor with a couple of additions, and it's going to fail like the one before," he told Fortune.

"It's better than Safe Harbor, obviously, but far from what the ECJ has asked for." Although Schrems is unsure if he'll go after Privacy Shield in the same way, he's sure that someone will, and successfully so: " We haven't really made up our minds so far, but it's really not a problem to challenge it," he said. "There are so many options to kill it."

ALTERNATIVES TO PRIVACY SHIELD FOR PROTECTION DATA TRANSFERS

Most scholars and practitioners agree that the Privacy Shield is likely to be subject to some sort of legal challenge. Several EU data protection authorities have encouraged U.S. companies to explore the alternative arrangements available under the EU data protection regime. Model Contract Clauses (MCC) and Binding Corporate Rules (BCR) are alternatives that permit the transfer of data from the EU to the U.S.

MODEL CONTRACT CLAUSES

Under Article 26 (4) of the directive 95/46/EC, the European Commission can determine that specific contract clauses provide adequate privacy protection for data transfers. These clauses can be part of a stand-alone model contract, or they can be addendums or sections in an existing agreement.

The Commission has approved two sets of standard clauses. One set applies to transfers from inside the EU/EEA countries to outside the EU/EEA countries between two data controllers, and the other set applies to transfers from a data controller inside of the EU/EEA countries to a processor outside of the EU/EEA countries. Some EU countries require registration of these model contracts/clauses with the local data protection authority (DPA). Organizations that utilize these clauses can legally transfer personal information out of EU/EEA countries because they provide adequate protection.

The adoption procedure for a standard contractual clause includes several steps as specified on the European Commission website. In addition, any changes to the model contract terms or new clauses require approval of the local country DPA and can take significant time. In addition, if an organization wishes to made changes to the model contract clauses for transfers from several EU countries, they will need the approval of the DPA in each country.

BINDING CORPORATE RULES

Binding Corporate Rules (BCR) are a binding set of rules a company creates with respect to personal data. These internal rules specify global policies regarding the organization's international transfers of personal information to entities within its group situated in countries that do not provide adequate protection to personal data. With BCRs in place, an organization is not required to sign model contract clauses for each transfer of personal data made within the organizational group. In addition, BCRs provide a guide for employees on how to deal with personal data management.

BCRs are required to contain the seven privacy principles, tools that will ensure the effectiveness of data privacy protection, and language that ensures that the BCRs are binding. DPAs must approve the BCRs adopted by multinational organizations. To keep organizations from having to request approval from each country's DPA individually, the European Commission has set up a BCR approval process where a lead authority leads the other authorities in a cooperation procedure.

The approval process for BCRs has five steps:

- Designation of a lead authority by the organization;
- Submission of draft BCRs to the lead authority, which the authority returns with comments;
- Circulation of BCRs to relevant DPAs by the lead DPA;
- Mutual Recognition countries acknowledge they received the BCR and other countries agree that the BCRs are in compliance with requirements;
- BCRs are final according to all DPAs, so the organization requests from each DPA authorization for transfers.

The approval process takes 12-18 months and might take longer as more companies are opting for this arrangement.

WHO WILL ENFORCE PRIVACY SHIELD AND GDPR?

The GDPR is a heavyweight, EU-wide legislation that will have far-reaching implications for organizations and their use and storage of EU personal data – in whatever form that might be, and wherever it is.

The GDPR will protect 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 organizations as well as the data processing activities of those companies that target EU data subjects, regardless of location, and will control the acquisition, use, transmission, storage, destruction and breach of personal data.

US AGENCIES

The Privacy Shield augments the previous Safe Harbor Agreement in several ways, one of which is the requirement that the US Department of Commerce ("DOC") verify certain particulars of an organization conducting an initial self-certification or yearly re-certifications. Prior to placing an organization on the Privacy Shield List, **the DOC will verify that the organization has:**

- provided required organization contact information;
- described the activities of the organization with respect to personal information received from the EU;
- indicated what personal information is covered by its self-certification;
- if the organization has a public website, provided the web address where the privacy policy is available and the privacy policy is accessible at the web address provided, or if an organization does not have a public website, provided where the privacy policy is available for viewing by the public;
- included in its relevant privacy policy a statement that it adheres to the Principles and if the privacy policy is available online, a hyperlink to the Department's Privacy Shield website;
- identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy;
- if the organization elects to satisfy the requirements in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the appropriate EU data protection authorities ("DPAs"), indicated its intention to cooperate with DPAs in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when EU data subjects have brought their complaints directly to their national DPAs;
- identified any privacy program in which the organization is a member;
- identified the method of verification of assuring compliance with the Principles (e.g., in-house, third party);
- identified, both in its self-certification submission and in its privacy policy, the independent recourse mechanism that is available to investigate and resolve complaints;
- included in its relevant privacy policy, if the policy is available online, a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints; and
- if the organization has indicated that it intends to receive human resources information transferred from the EU for use in the context of the employment relationship, declared its commitment to cooperate and comply with DPAs to resolve complaints concerning its activities with regard to such data, provided the Department with a copy of its human resources privacy policy, and provided where the privacy policy is available for viewing by its affected employees.
- Work with independent resource mechanisms to verify organizations have registered with relevant mechanism for dispute resolution.

When organizations fail to adhere to duties specified pursuant to the Privacy Shield framework, U.S. federal agencies may remove them from the Privacy Shield List. If removed, an organization would be obligated to return or delete all EU personal data it has received pursuant to the Privacy Shield. The noncompliant organization would no longer be on the publicly available Privacy Shield List and the DOC would publish an announcement of its noncompliance to ensure notification to all interested parties. Civil penalties could also be imposed due to unfair and deceptive trade practices.

In addition to DOC enforcement, Privacy Shield creates a binding arbitration requirement where organizations are required to participate in binding arbitration to resolve alleged violations of the Privacy Shield Principles. A Privacy Shield Panel, consisting of 20 arbitrators designated by the U.S. Department of Commerce and the European Commission, will have the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of an individual's personal data) necessary to remedy a violation.

The Privacy Shield Team of the ITA is also conducting regular updates and reviews of participating companies, to ensure that companies follow the rules. The U.S. Department of Commerce has committed to a rigorous monitoring to weed out "free-riders", i.e., companies that falsely claim adherence to the scheme. Companies' commitments are legally binding and enforceable under U.S. law by the Federal Trade Commission and companies that do not comply will face severe sanctions.

THE VITAL ROLE OF RECORDS MANAGEMENT IN MEETING THE MANDATES OF GDPR

1. PII MUST HAVE A VALID RETENTION SCHEDULE BASED ON THE PURPOSE FOR WHICH IT IS MAINTAINED, AND MUST BE DISPOSED OF IN A TIMELY MANNER.

By its very nature, stored PII should be considered records with specified retention periods, due to the fact that Article 5 of the GDPR requires that personal data be, "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." Similarly, the Privacy Shield principle of Data Integrity and Purpose Limitation requires that information, "may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing [compatible with the purposes for which it has been collected or subsequently authorized by the individual]." In this regard, any PII held must have a business use compatible with its initial collection or subsequent authorization. **Therefore it is a record and if it fails to meet this standard the PII should be the target for defensible disposition.**

2. DATA BREACHES CAN LEAD TO STRINGENT FINES UNDER GDPR AND U.S. LAWS

Data privacy breaches are now an unfortunate component of the modern business landscape. According to the Ponemon Institute's 11th Annual Cost of Data Breach Study, the average consolidated total cost of a data breach grew from $3.8 million to $4 million. The study also reported that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from $154 to $158.

The threat is very real, with the global study putting the likelihood of an organization suffering a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent. Because of this, insurers are increasingly performing their own audits of a company's information governance framework when determining the cost of privacy breach coverage. **The resulting rising insurance costs based on weak information governance will likely increase focus on improvements, particularly in areas of information retention and classification, both areas normally best managed as part of a records and information management plan.**

IF PII IS NOT VALUABLE TO THE ORGANIZATION, THE RISK OF MAINTAINING IT IS SIMPLY TOO HIGH.

With many organizations past fears relating to e Discovery sanctions led to a default position of "keep it all, just in case." Continuing to follow this position is untenable with the advent of the GDPR and the current requirements of Privacy Shield. In addition to experiencing data clutter to the point of hindering their ability to manage daily activities, **organizations are putting themselves at risk if they keep PII past its period of usefulness.**

Organizations over retaining PII not only face tremendous information storage costs but are at risk of violating the core Principles of the GDPR and the Privacy Shield framework. Organizations are exposing themselves to sanctions, and are making it impossible to meet their responsibilities to allow access, provide security, and disclose and cure potential breaches. For these reasons it is highly advisable that organizations create or update policies and procedures to defensibly dispose of PII once it is no longer useful for the purposes for which is was collected or subsequently authorized.

In short, organizations must be able to meet the requirements of protecting PII under the GDPR and Privacy Shield, be able to produce PII under the Right to Be Forgotten, protect PII to prevent data breach and its drastic effects, and, finally, defensibly dispose of PII to reduce ongoing costs and risks.

By identifying information that qualifies as records – that is, information which is necessary for business processes, of evidentiary value, or required to be kept by regulatory or legislative mandate – an organization can begin to defensibly dispose of a great portion of its documents, reducing storage costs and preventing breaches or the necessity to retrieve and relay the deleted documents in response to access requests.

Data that is routinely collected, processed, and stored as part of regular business activity but which serves no business purpose and which is not legally mandated to be retained could also contain PII by the broad definitions assigned by the GDPR. This should serve as sufficient motive to systematize the prompt deletion of non-record data.

WHERE IS THE DATA CONTAINING PII? CAN WE ACCESS IT QUICKLY? IS IT ENCRYPTED? IS IT UP TO DATE? IS IT ACCURATE? IS IT SECURE? IF YOU CANNOT ANSWER THESE QUESTIONS, YOU CANNOT BE IN COMPLIANCE.

An organization may be required to retain different categories of information for various periods, depending on which jurisdictions apply. Determining the retention schedule through traditional methods of legal research is labor-intensive and expensive.

Organizations need to create a data map so they know what proprietary data they have, where is it physically, how sensitive it is and who has access. They should then only collect and store the information needed to remain compliant, so as not to fall foul of any data protection regulations

IMPROVING PRIVACY, RIM POLICY

As mentioned earlier, PII under the GDPR is any information that if combined with another available piece of information would allow an individual to be identified. It does not need to be assimilated with that other available piece of information to be considered PII. This means that a piece of information an organization would not normally view as a record on its own would need to be treated as PII.

This information would need to be governed according to the appropriate protection and retention requirements.

In order to retain PII in a manner consistent with the requirements of the GDPR, an organization will need to:

- Maintain consent from individuals allowing collection and use of their PII;
- Protect against the unauthorized access of PII;
- Retain PII only for the appropriate length of time and dispose of it consistent with the EU's limitations on the length of time it can be kept;
- Store PII in a manner that allows for immediate access to it;
- Maintain records of an individual's requests regarding right to erasure, right to ensure accuracy, etc.
- Maintain security of PII
- Notify individuals of PII transfers
- Ensure integrity of PII data.

THE DATA PRIVACY OFFICER

To ensure compliance with the GDPR, certain organizations must appoint a Data Protection Officer (DPO). The DPO is a person who is formally tasked with ensuring that an organization is both aware of and complies with relevant data protection responsibilities. Appointing a DPO is necessary if the core activities of the company involves "systematic monitoring of data subjects on a large scale" or large scale of special categories of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric information, sexual orientation, or data regarding health or sex life). Small-medium enterprises (SMEs) may be exempt from the DPO requirement if certain requirements are met.

Article 38 of the GDPR requires the organization to support the DPO by providing the necessary resources to carry out the designated tasks, including access to personal data, processing, and other related operations. The DPO reports to upper management, but is also expected to work independently and without direction. These duties include, but are not limited to:

- devising policies and procedures that bring the organization into compliance with the GDPR;
- monitoring the implementation of those policies;
- ensuring that all staff are fully trained in regards to protecting data;
- assigning responsibilities and handles the public's requests regarding their personal data; and,
- monitoring, notifying and communicating information about personal data breaches.

The DPO also keeps management informed regarding their obligations under the GDPR, and serves as the primary contact point for Supervisory Authorities (documenting requests by public and regulatory bodies to remove, destroy or access data). The closest analogous role in U.S.-based organizations would be the role of Chief Privacy Officer (CPO).

PRIVACY BY DESIGN/ PRIVACY BY DEFAULT

While the current EU Data Protection Directive requires data controllers to have proper technical and organizational data protection measures in place, it does not incorporate privacy by design, the GDPR goes a step further by specifically recognizing two key concepts: privacy by design and privacy by default.

First, privacy by design is an approach to systems engineering which takes privacy and data protection compliance into account throughout a project's life cycle. It requires companies to design policies, procedures and systems at the outset of any product or process development that give appropriate consideration to the latest data protection technology and the cost of implementation.

Criticized by some experts as too "vague" or "open-ended, privacy by design offers businesses a good deal of flexibility in determining how to implement such plans – taking into account the type of processing at hand and the potential risks to the rights of individual data subjects.

PRIVACY BY DEFAULT, ON THE OTHER HAND, ASKS THAT DATA CONTROLLERS IMPLEMENT SUCH TECHNICAL AND ORGANIZATIONAL MEASURES SO THAT, BY DEFAULT, ONLY THAT DATA WHICH IS NECESSARY FOR EACH SPECIFIC PURPOSE OF THE DATA PROCESSING IS IN FACT PROCESSED.

In a sense, the aim with privacy by default is to minimize the amount of data being collected, the extent to which it is processed, the period of time it is stored, and the degree to which it can be accessed. Organizations should only process personal data to the extent it is needed and then store it for only such time as is necessary (and no longer). Efforts to streamline and minimize processing of any superfluous or extraneous data should be of the utmost importance.

In order to address the requirements for each of these concepts, an organization can take the following steps:

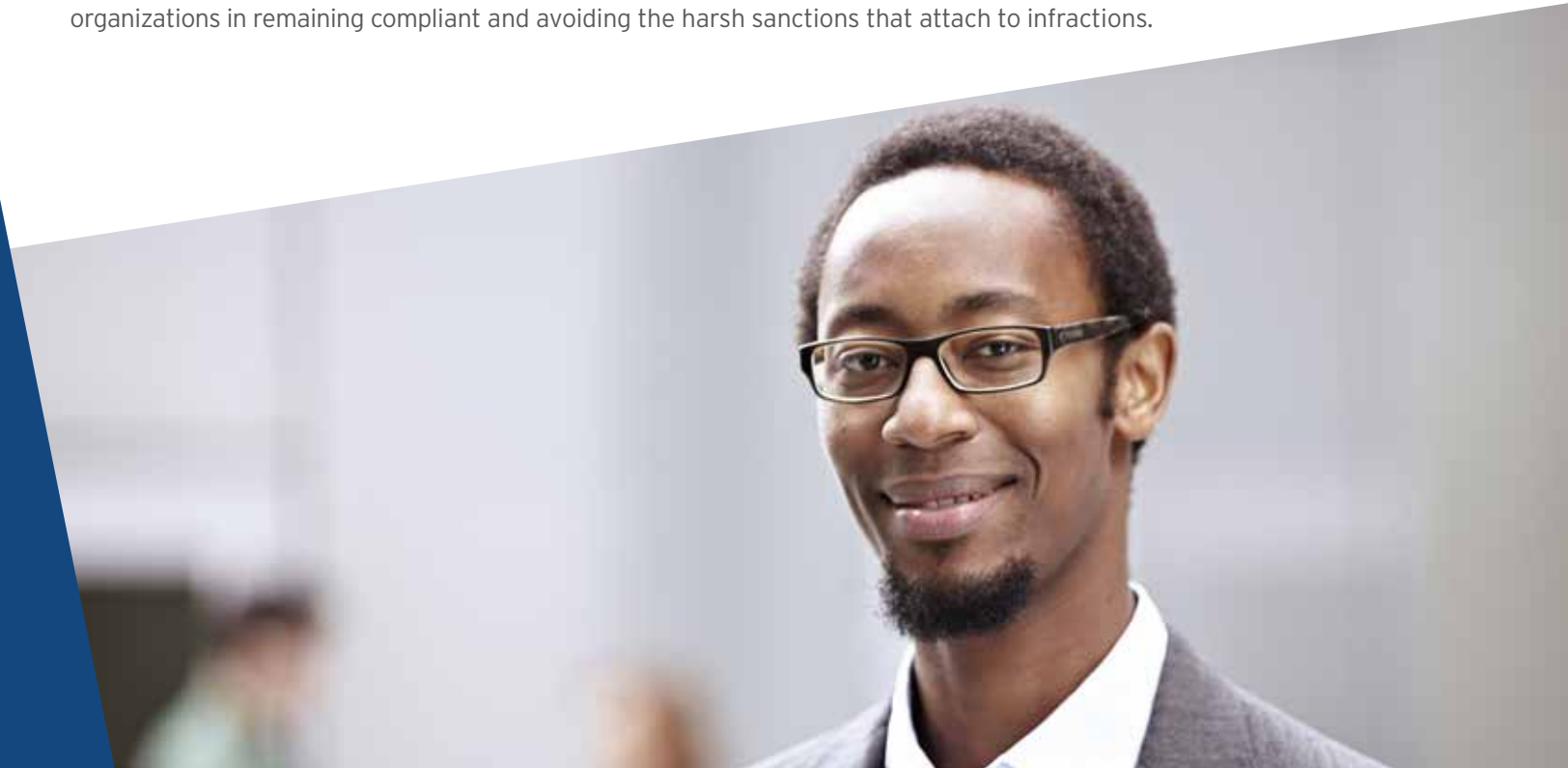
- create a privacy impact assessment template to be used for new projects and workflows;
- revise both existing and future contracts with data processors;
- review data collection policies and procedures; and,
- implement automated deletion procedures for personal data.

IRON MOUNTAIN

YOUR PARTNER FOR CREATING PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

As part of Iron Mountain's continued development of products to aid its clients in meeting the ever increasing demands in records management and information governance including the difficult challenges related to ensuring compliance with the myriad of mandates created by the EU Privacy Regulation that will impact thousands of U.S, Iron Mountain has expanded its offering in PCS to include global and US state privacy laws. By the end of 2017, privacy laws enacted around the world will be part of PCS that can be mapped to individual records.

In addition, Iron Mountain is developing privacy related retention schedules to attach to PII to ensure its timely deletion. In partnership with HPE, Iron Mountain will work with organizations to find PII and to ensure its encryption and security. Iron Mountain is introducing enhancements to PCS to aid organizations to maintain only PII or other information that is valuable to business, required to be maintained by law or on legal hold. By implementing large scale defensible deletion plans, organizations will be better able to secure data and respond to a breach which might occur. Utilizing these and other enhancements designed to meet the requirements of GDPR will aid organizations in remaining compliant and avoiding the harsh sanctions that attach to infractions.



SAMPLE GDPR READINESS CHECKLIST

- ☐ Ensure that PII is identified and treated as a record within your organization for the purpose of retention and defensible disposal
- ☐ Conduct a privacy maturity assessment and benchmark analysis to determine next steps for your organization
- ☐ Establish clear and concise GDPR compliant privacy notices with consent mechanism and age verification process for data subjects under 13 years
- ☐ Establish a data map for your organization to ensure quick access and records management practices required by GDPR
- ☐ Follow a well-researched retention schedule to ensure the defensible nature of all PII maintained
- ☐ Systematically dispose of PII that has no business purpose and does not have a legal retention period
- ☐ Safeguard all PII that is retained for a defensible purpose by encrypting it and applying appropriate security measures
- ☐ Unless you are exempt, establish a Data Protection Officer and provide him or her with all necessary support to independently perform required duties
- ☐ Implement both privacy by design and privacy by default practices through established privacy policies and procedures as required by the GDPR
- ☐ Create a thorough data breach response plan that includes mechanisms for breach reporting as required by the GDPR
- ☐ Achieve EU-US Privacy Shield self-certification (or utilize BCRs or MCCs) to ensure legal data transfers of personal information from the EU to the US
- ☐ Maintain complete records of all GDPR compliance activities.

IRON MOUNTAIN'S CURRENT PRIVACY CERTIFICATIONS

Iron Mountain, Inc. is committed to protecting the privacy of personal data and the information that it manages for its clients. One of the ways it publicly demonstrates this commitment is via privacy certifications. Iron Mountain has achieved both the EU-US Privacy Shield Framework certification and the Privacy+ certification, which together provide protection to the personal information of their employees and clients, as well as the physical and off-line computer media they manage for clients.

IRON MOUNTAIN'S

PRIVACY SHIELD CERTIFICATION

On December 7, 2016 Iron Mountain, Inc. achieved certification under the EU-US Privacy Shield Framework. It has certified both its human resources personal information and its non-human resources personal data. After the successful verification process, the DOC added Iron Mountain to the privacy shield list available at https://www.privacyshield.gov/list where types of personal information they are likely to transfer and the purposes for those transfers are specified. They have certified that Iron Mountain and its eight additional entities will comply with the Privacy Shield Principles and have made their privacy policies available to the DOC (the privacy policy regarding non-human resources data is available on the Iron Mountain website and the Privacy Shield List). In addition, Iron Mountain has specified that when grievances regarding human resources personal data occur, EU DPAs are the independent recourse mechanism and that when grievances regarding non-human resources personal information occur, a privacy independent recourse mechanism is available. Employees and clients for the organization can trust that they have adequate recourse if they believe their personal data has been mishandled.

Iron Mountain, Inc. believes that joining Privacy Shield and following its 23 principles provides its employees and clients in the EU a necessary level of data protection. In addition, Iron Mountain can successfully continue its business processes (and necessary data transfers) without needing to create Model Contract Clauses or Binding Corporate Rules. Iron Mountain is invested in protecting employee and client information and joining the Privacy Shield Framework demonstrates this commitment.

IRON MOUNTAIN'S

PRIVACY+ PRISM CERTIFICATION

On August 10, 2016 Iron Mountain, Inc. announced its Privacy+ Certification. Iron Mountain pursued this certification to show clients that they are very serious about the privacy protection they provide to the information they manage. Professional Records & Information Services Management International (PRISM International, or the "Association") administers Privacy+ certification. PRISM International is the nonprofit global trade association for the information management industry and Privacy+ certification is available to organizations who handle hard-copy records and off-line removable computer media and provide physical storage for clients. The certification does not apply to cloud storage, document imaging, and shredding services.

Iron Mountain, Inc. worked with other members of the Association to develop Privacy+, ensuring that it would provide important privacy protection for clients' information. Goals of the certification include reducing privacy breaches and sharing resources across participants so they can minimize privacy risks. Participants must demonstrate that they have met the ten control objectives of the certification via a third-party audit of the adequacy of their internal control mechanisms. According to the PRISM International website (at http://www.prismintl.org/Privacy-Certification/privacy/privacy-plus-certification-criteria.html) the ten control objectives are: Organization and Management Control, Information Security Policy, Risk Assessment, Human Resources Controls, Vendor Management Controls, Physical Access Controls, Environmental Controls, Logical Access Controls, Network Security Controls, and Electronic Access to Client Information Controls. As a quality control, PRISM International requires that all third-party auditors must be pre-approved. The certification process also includes a workshop that prepares organizations for the audit process. If an audit is performed successfully, the company will receive Privacy+ certification within 30 days.

Iron Mountain, Inc. is one of the 33 information management companies that are currently Privacy+ certified. A list of all certified organizations is available on the PRISM International website (at http://www.prismintl.org/Privacy-Certification/privacy/privacy-certified-companies.html). These companies must go through the re-certification process every 2 years. A new audit is required for recertification. Due to the time that these internal control audits take to perform, PRISM International recommends that all organizations start working towards recertification 6 months before the company's second anniversary. If an organization allows the Privacy+ certification to lapse, they must remove the Privacy+ certification from all marketing materials.

AUTHORS

Teresa Pritchard Schoch, , JD, MSLS, CRM, CIPP, IGP. Principal, Professional Services, Iron Mountain Information Governance & Digital Solutions

Kelly Huckman, JD. Consultant, Professional Services, Iron Mountain Information Governance & Digital Solutions

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Founded in 1951, Iron Mountain Incorporated (NYSE: IRM) is the global leader in storage and information management services. Iron Mountain is committed to storing, managing and transforming what our customers value most, from paper records to data to priceless works of art and culture. Providing a full suite of solutions – records and information management, data management, digital solutions, data centers and secure destruction – Iron Mountain enables organizations to lower storage costs, comply with regulations, recover from disaster, and protect their data and assets from a complex world. Visit the company website at www.ironmountain.com for more information.