DATENSCHUTZ: IHR WEG ZUR COMPLIANCE

Wie Sie Compliance in einen Wettbewerbsvorteil verwandeln

IRON MOUNTAIN®

ZUSAMMENFASSUNG

Compliance. Datenschutz. DSGVO. Nur zu oft denken wir bei diesen Begriffen an endlose Bürokratie und Formulare – und an die allgegenwärtige Angst davor, wegen nicht erfüllter Anforderungen zur Kasse gebeten zu werden. Aber die Dinge ändern sich. Denn es geht nicht mehr nur darum, formell bestimmte Auflagen zu erfüllen. Nein, in einem Zeitalter, in dem Vertrauensverlust eine große gesellschaftliche Gefahr darstellt, möchten wir **kulturelle Veränderungen** voranbringen, so dass Unternehmen die Chance haben, das Vertrauen ihrer Kunden zurückzugewinnen.

Bislang haben Unternehmen sich weniger proaktiv um die Compliance gekümmert, sondern meist nur reagiert, wenn neue Anforderungen an sie gestellt wurden[1]. Ihr Wunsch war es, mit so wenig Zeit und Aufwand wie möglich den Behörden zu zeigen, dass sie die Gesetze einhalten. Aufgrund der Vielfalt globaler, nationaler und sogar kommunaler Vorschriften ist dies heutzutage jedoch immer schwieriger zu bewerkstelligen. Niemand sollte mehr denken, dass Datenschutz nur eine lästige Aufgabe ist, die schnell erledigt werden muss. Stattdessen ist eine umfassende Strategie erforderlich, die schon im Fundament des Unternehmens beginnt. **Privacy by Design und Privacy by Default** bedeuten, dass **Datenschutz bereits technisch und durch entsprechende Voreinstellungen in einem System verankert wird**.

Betrachten wir es aus einem positiven Blickwinkel. Bei der Navigation durch die neue Datenlandschaft und der Einrichtung von Privacy und Security by Design und Default geht es um viel mehr, als nur Gesetze einzuhalten. Es ist der einzige Weg für Unternehmen, um:

- Ihre Business Continuity sicherzustellen
- Innovation zu fördern, ohne zusätzliche Risiken einzugehen
- Vertrauen in ein Wertversprechen zu verwandeln
- Daten besser auszuwerten und wichtige Einsichten zu gewinnen
- Herausforderungen der Globalisierung zu begegnen

1. https://www.complianceweek.com/best-practices-in-policy-management/2218.article

KAPITEL DIESES LEITFADENS:

„Privacy by Design und by Default hebt den Datenschutz auf eine ganz neue Stufe, denn damit müssen die Kunden nicht mehr selbst nach mehr Datenschutz verlangen – sie bekommen ihn ganz automatisch."

Ann Cavoukian, Gründerin des Global Privacy and Security by Design Centre

In unserem Zeitalter der sozialen Medien könnte man leicht annehmen, dass Menschen bereit sind, ihr Leben online zu teilen – auch wenn das bedeutet, dass sie den Anbietern der Networking-Plattformen ihre Daten preisgeben müssen. Deshalb gibt es überall diese langen Datenschutzrichtlinien, die kaum jemand vollständig liest. Sobald ein Benutzer das Häkchen setzt und sich mit einer solchen Richtlinie einverstanden erklärt, ist das Thema Compliance durch. Oft erkennt der Benutzer erst viel später, worauf er sich eingelassen hat – seine Daten werden nun für ganz verschiedene Zwecke genutzt, wie beispielsweise Werbung.

Doch zu diesem Zeitpunkt ist das sprichwörtliche Kind schon in den Brunnen gefallen. Denken Sie zum Beispiel einmal daran, wie schwierig es ist, ein Konto bei Facebook zu löschen. Meist dauert es mehrere Wochen. Das liegt zum Teil daran, dass Facebook noch mit ganz anderen Onlinediensten verbunden ist, die dieselben Daten für die Anmeldung nutzen. Viele Unternehmen verfolgen ganz deutlich die Strategie, ihre Benutzer in großen Systemen quasi einzusperren. Kurz gesagt: **Der Datenschutz wird in einer Richtlinie festgelegt, die niemand liest**. Erst später wird uns klar, welche Risiken wir eingehen und was wir hätten tun können, um sie zu vermeiden.

Dieses Szenario ist ein gutes Beispiel dafür, wie Unternehmen in Zeiten hoher Ansprüche an den Datenschutz *nicht* vorgehen sollten. Mit der DSGVO und ähnlichen Gesetzen wird bereits versucht, den Verbrauchern die Kontrolle über ihre Daten zurückzugeben. Compliance bezieht sich derzeit meist noch auf den Umgang mit unseren Daten, *nachdem* wir sie übermittelt haben. Aber die neuesten Regeln sehen **aktive Maßnahmen** vor. Das heißt, die Benutzer müssen den Unternehmen **explizit erlauben**, Informationen zu erfassen und zu nutzen. Das ist eines der Grundprinzipien von Privacy by Design und Privacy by Default.

1

Statt darauf zu warten, dass Datenschutzprobleme auftauchen, werden gemäß Privacy by Design entsprechende Schutzmaßnahmen schon bei der Entwicklung von Anwendungen und Geschäftsprozessen integriert. Als Benutzer haben wir die Tendenz, die Standardeinstellungen von Programmen zu akzeptieren, weil sie uns ja schließlich das Leben erleichtern sollen und wir alle keine Zeit zu verlieren haben. Deshalb muss **Datenschutz die Standardeinstellung sein**. Nur so bleibt er gewährleistet, selbst wenn wir als Benutzer nichts unternehmen. Erst, wenn wir auf eine Funktion zugreifen *möchten*, für die der Anbieter auf personenbezogene Daten zugreifen *muss*, sollten wir uns bewusst dafür entscheiden können. So wie wir zum Beispiel einer Foto-App auf unserem Smartphone den Zugriff auf die Kamera des Geräts gewähren müssen. Mit diesem nutzerzentrierten Ansatz wissen User stets über die Verwendung ihrer Daten Bescheid.

Fassen wir kurz die grundlegenden Prinzipien von Privacy by Design zusammen:

Datenschutz muss:

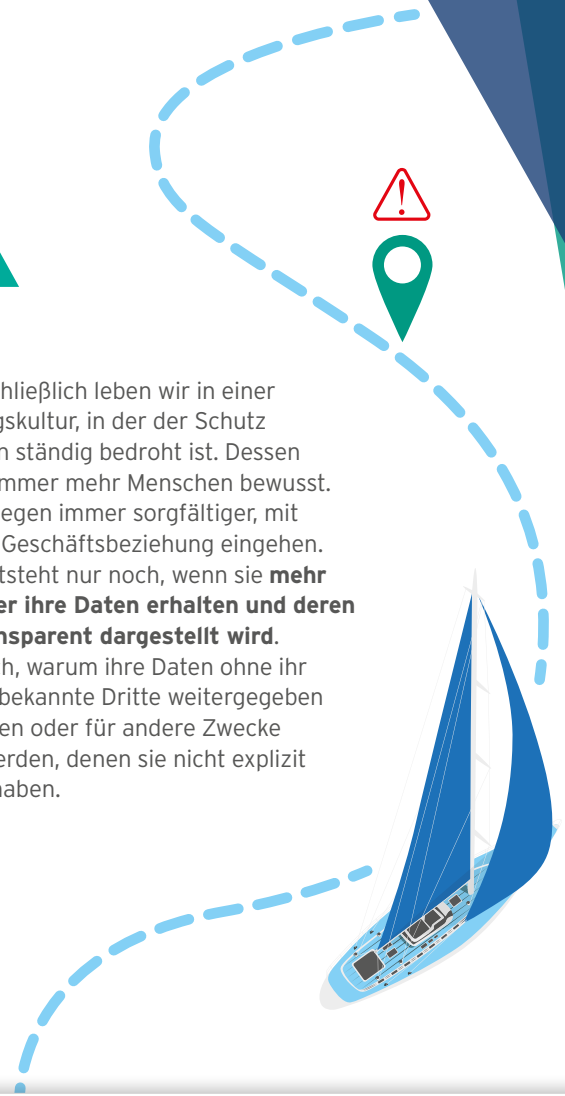
- aktiv und vorbeugend geschehen, nicht reaktiv und korrigierend.
- immer die Standardeinstellung sein.
- schon bei der Entwicklung jeder Anwendung und jedes Prozesses integriert werden. Beim Datenschutz darf es keine unnötigen Kompromisse geben.
- sich auf den gesamten Lebenszyklus der entsprechenden Daten erstrecken.
- sicherstellen, dass alle Vorgänge sichtbar und transparent bleiben.
- die Interessen der Kunden an erste Stelle setzen, nicht die des Unternehmens.

„Unternehmen können einen Wettbewerbsvorteil erreichen, wenn sie den Datenschutz aktiv in ihre Abläufe einbinden. Denn so profitieren sie nicht nur selbst, sondern schaffen mehr Kundenvertrauen."

Ann Cavoukian, Gründerin des Global Privacy and Security by Design Centre

Compliance hatte in der Geschäftswelt bislang oft einen negativen Beigeschmack. Viele Führungskräfte denken dabei nur an Bürokratie, sehen sie als Innovationsbremse oder als notwendiges Übel. Da das Erreichen von Compliance meist schwierig ist, verwundert es nicht, dass viele Unternehmen die gesetzlichen Anforderungen nach wie vor nicht erfüllen. In einer Untersuchung hat sich gezeigt, dass nur knapp über ein Viertel alle Vorgaben der DSGVO erfüllt – und das 17 Monate nachdem das Gesetz in Kraft getreten war[2]. Gleichzeitig berichten jedoch **81 % der Unternehmen**, die laut eigener Aussage alle Anforderungen erfüllen, dass sie **positive Auswirkungen auf ihr Image** bemerkt hätten. Compliance ist also kein Hindernis, sondern kommt dem Geschäft zugute.

Über **Compliance als Wettbewerbsvorteil** zu sprechen – das mag zunächst seltsam klingen. Der direkte Zusammenhang wird aber immer deutlicher. Schließlich leben wir in einer Überwachungskultur, in der der Schutz unserer Daten ständig bedroht ist. Dessen werden sich immer mehr Menschen bewusst. Kunden überlegen immer sorgfältiger, mit wem sie eine Geschäftsbeziehung eingehen. Vertrauen entsteht nur noch, wenn sie **mehr Kontrolle über ihre Daten erhalten und deren Nutzung transparent dargestellt wird**. Sie fragen sich, warum ihre Daten ohne ihr Wissen an unbekannte Dritte weitergegeben werden müssen oder für andere Zwecke verwendet werden, denen sie nicht explizit zugestimmt haben.



2. https://www.capgemini.com/news/data-protection-and-privacy-report

WIE SIE COMPLIANCE IN EINEN WETTBEWERBSVORTEIL VERWANDELN

2

YouTube musste erst kürzlich

$170 Mio.

zahlen, weil es gegen das COPPA-Gesetz zum Schutz der Privatsphäre von Kindern im Internet verstoßen hatte.[3]

Schon zu lange glauben viele Unternehmen, dass es für ihr Geschäft nur schlecht sein kann, wenn ihre Kunden die Kontrolle über ihre Daten zurückerhalten. Sie stellen ihr eigenes Geschäftsinteresse über die Interessen ihrer Kunden, obwohl es genau umgekehrt sein sollte. Denn Datenschutz ist inzwischen ein sehr **großer Pluspunkt aus Kundensicht** und sollte daher auch für Unternehmen im Fokus stehen. Auf Trusted Shops und ähnlichen Plattformen zum Beispiel zeigt sich in den Bewertungen der Kunden sofort, welche Unternehmen den Datenschutz ernst nehmen, und Privacy by Design und Privacy by Default werden zu einem kritischen Merkmal für einen guten Unternehmensruf.

Um **vertrauensvolle Geschäftsbeziehungen** aufzubauen, müssen Unternehmen einsehen, dass **Datenschutz auch ihnen selbst etwas bringt**, und mit den Daten ihrer Benutzer sorgfältig umgehen. Beide Seiten müssen profitieren, was nur gelingen kann, wenn die Unternehmen stets deutlich machen, wie sie Daten erheben und was sie damit vorhaben. Wenn sich z.B. später die Möglichkeit ergibt, bestimmte Daten für einen anderen Zweck als vorgesehen einzusetzen, können die Unternehmen ihre Kunden noch einmal um die Einwilligung bitten. **Die meisten werden diese Transparenz zu schätzen wissen**, was zu einer engeren Beziehung führen und wiederum Wachstum und Innovation fördern kann. Entscheidet sich ein Unternehmen jedoch, die gesammelten Daten nach eigenem Gutdünken ohne Einwilligung zu nutzen, schadet es dem eigenen Ruf und verstößt gegen die Compliance-Bestimmungen, was hohe Geldstrafen zur Folge haben kann. YouTube musste bspw. erst kürzlich 170 Millionen USD zahlen, weil es gegen das COPPA-Gesetz zum Schutz der Privatsphäre von Kindern im Internet verstoßen hatte[3].

Zusammengefasst: Die Einbettung von Privacy by Design und Privacy by Default in jede Geschäftsfunktion schützt nicht nur den Ruf Ihres Unternehmens. Sie ist vielmehr ein grundlegender Teil Ihres Wertversprechens an Kunden, mit dem Ihr Unternehmen in unserer **Gesellschaft, in der Datenschutz eine solch wichtige Rolle spielt**, weiterhin erfolgreich sein kann.

3. https://www.theverge.com/2019/9/4/20848949

„Die schiere Menge an Daten in verschiedensten Formaten – wobei physische Datenträger besonders problematisch sind – und die Pflicht, diese Daten in kurzer Frist zusammenzustellen, stellen Unternehmen vor enorme Herausforderungen."

Michael Zurcher, Global Privacy Officer bei Iron Mountain

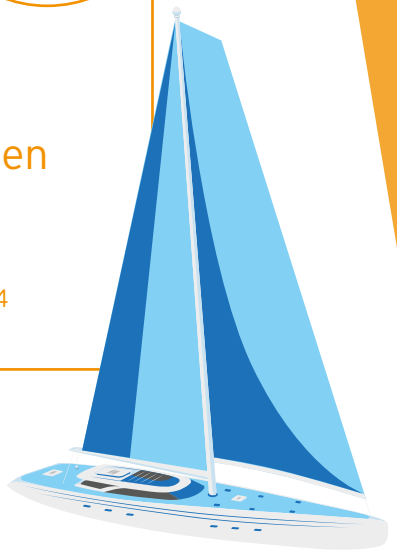
Die praktischen Aspekte von Privacy by Design und Privacy by Default sind für Unternehmen vermutlich die größte Herausforderung. Vor allem, wenn sie schon seit Jahrzehnten Daten sammeln, die nun in ganz verschiedenen Formaten vorliegen. Dass sich unsere **Technologien immer schneller weiterentwickeln**, macht diese Aufgabe auch in Zukunft nicht einfacher: Jeden Tag kommen neue Daten hinzu, die von vielen Unternehmen gar nicht mehr adäquat verarbeitet werden können. In einer aktuellen Studie hat sich gezeigt, dass weniger als ein Drittel aller Unternehmen sich selbst als datengesteuert bezeichnen, obwohl alle mehr Daten als je zuvor sammeln.

Letzten Endes **kommt es deshalb immer auf ein gutes Informationsmanagement an**. Nur wenn die richtigen Prozesse vorhanden sind, können die Daten richtig ausgewertet und Innovationen vorangetrieben werden, ohne zusätzliche Risiken einzugehen. Ein stabiles Information-Governance-Programm sollte sich an bestimmte Prinzipien halten, damit die Herausforderungen in Bezug auf Compliance und Sicherheit heute und auch in Zukunft gemeistert werden können.

Weniger als

1/3

aller Unternehmen bezeichnen sich selbst als datengesteuert.[4]

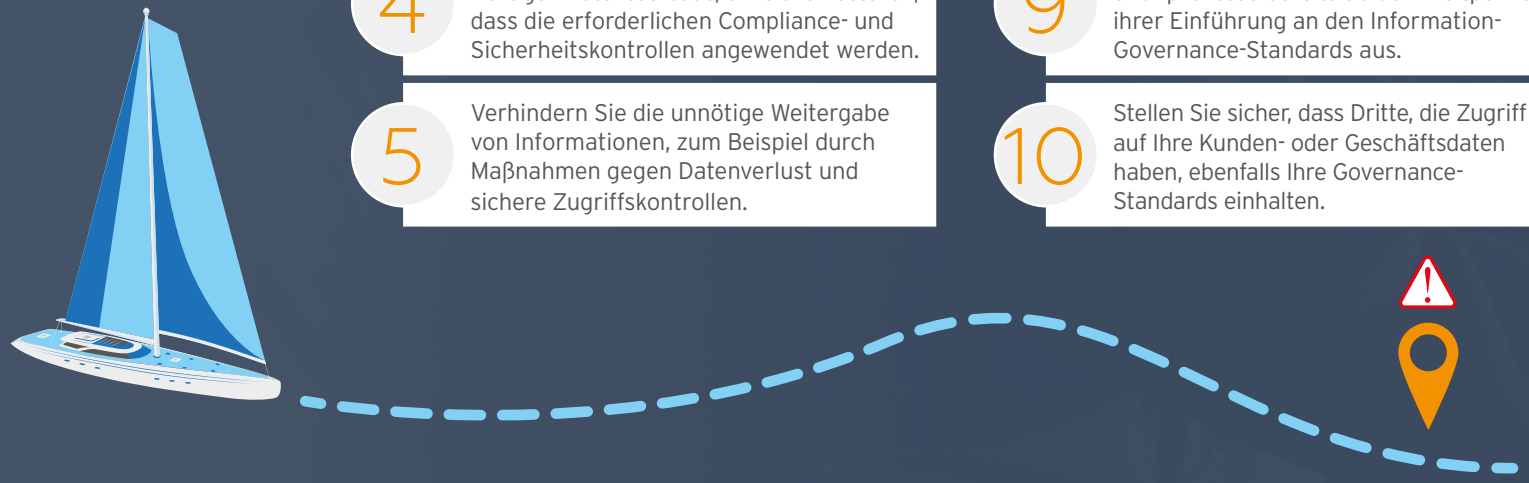


4. https://hbr.org/2019/02/companies-are-failing-in-their-efforts-to-become-data-driven

3

Zehn Schritte für ein zukunftssicheres Information-Governance-Programm

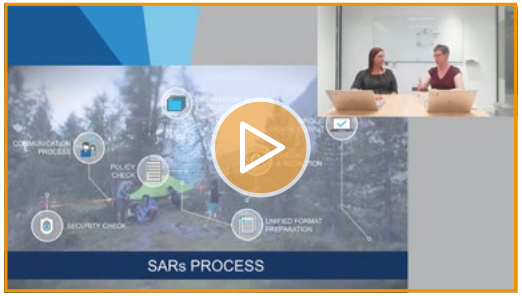
1. Informieren Sie alle Angestellten über ihre Aufgaben und Pflichten bezüglich des Datenschutzes gemäß Ihren Compliance- und Sicherheitsrichtlinien.
2. Überprüfen Sie die Authentizität und Integrität Ihrer Daten und vermeiden Sie Inkonsistenzen.
3. Archivieren Sie alle Daten an einem einheitlichen, für Ihr Unternehmen geeigneten Aufbewahrungsort.
4. Klassifizieren Sie Informationen unter dem richtigen Datensatzcode, um sicherzustellen, dass die erforderlichen Compliance- und Sicherheitskontrollen angewendet werden.
5. Verhindern Sie die unnötige Weitergabe von Informationen, zum Beispiel durch Maßnahmen gegen Datenverlust und sichere Zugriffskontrollen.
6. Vernichten Sie Daten, die keinen rechtlichen oder betrieblichen Zweck mehr erfüllen, am Ende ihres Lebenszyklus auf sichere Weise.
7. Sichern Sie alle vertraulichen Kunden- und Unternehmensdaten bei Übertragung und im Speicher mit Verschlüsselung und Multifaktor-Authentifizierung.
8. Reagieren Sie auf Auskunftsersuchen innerhalb von 30 Kalendertagen (gemäß DSGVO).
9. Richten Sie Ihre Geschäftssysteme und -prozesse bereits ab dem Zeitpunkt ihrer Einführung an den Information-Governance-Standards aus.
10. Stellen Sie sicher, dass Dritte, die Zugriff auf Ihre Kunden- oder Geschäftsdaten haben, ebenfalls Ihre Governance-Standards einhalten.

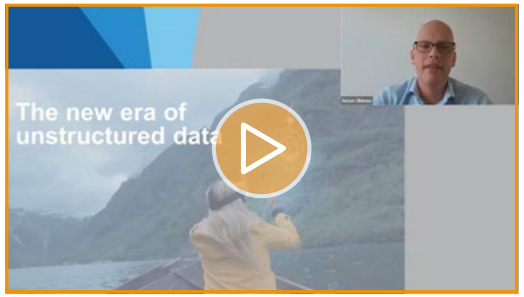


Gerade **das Beantworten von Auskunftsersuchen** erweist sich für viele Unternehmen als schwierig. Benutzer haben das Recht zu fragen, welche ihrer Daten verarbeitet werden, um welche Datentypen es geht, warum das Unternehmen diese Daten besitzt und wie sie erfasst wurden. Auch die Frage nach dem Nachweis der sicheren Speicherung ist zulässig. Alle Auskunftsersuchen müssen innerhalb von 30 Kalendertagen beantwortet werden. Das führt zu Problemen, wenn die Daten in unstrukturierten Formaten vorliegen, auf Papier oder in E-Mail-Archiven. Manchmal lagern Unternehmen sogar noch längst veraltete Formate, die nicht so leicht durchsuchbar sind wie Informationen in den mittlerweile üblichen Datenbanken.

CHECKLISTE AUSKUNFTSERSUCHEN ANSEHEN ▷

Wenn Unternehmen heute und in Zukunft diese Herausforderungen meistern möchten, brauchen sie ein **einheitliches Informationsmanagement** mit einem größtenteils automatisierten Prozess. Dabei ist es unter anderem wichtig, dass unnötige Daten erst gar nicht mehr erfasst beziehungsweise nach Ende ihres Lebenszyklus gelöscht werden und die Datenschutzrichtlinien aktuellen Ansprüchen genügen.





Dafür benötigen Unternehmen ein Programm für die Verwaltung des Informationslebenszyklus, das entsprechende Schritte automatisch durchführt. Zum Glück gibt es Technologien, die helfen. Beispielsweise kann **Texterkennung (OCR)** Papierdokumente digitalisieren, damit sie durchsucht werden können, und **künstliche Intelligenz (KI)** kümmert sich um die großen Massen unstrukturierter Daten. Gemeinsam helfen diese Lösungen Ihnen dabei, eine skalierbarere und leichter handhabbare Infrastruktur zu erreichen, die jeden einzelnen Geschäftsprozess mit Mehrwert versorgt.

DAS FUNDAMENT FÜR INNOVATION OHNE RISIKO

Einfach ist die Umsetzung des Prinzips Privacy by Design und Privacy by Default nicht, insbesondere nicht für etablierte Unternehmen und Plattformen, die erst zahllose Geschäftsprozesse und -systeme umgestalten müssen, um die Compliance-Anforderungen zu erfüllen. Aber Datenschutz ist auch ein **grundlegendes Menschenrecht** in Zeiten, in denen skrupellose Werbetreibende jede Gelegenheit nutzen, von unseren Daten zu profitieren. Zum Glück gibt es viele Möglichkeiten, wie Privacy by Design Ihrem Unternehmen einen Mehrwert bringen kann.

Wenn Sie den Datenschutz bereits technisch und durch entsprechende Einstellungen in Ihrem Datenmanagement verankern, schaffen Sie ein einheitlicheres und effizienteres System, mit dem Sie zum datengesteuerten Unternehmen werden können.

Ihre Kunden vertrauen Ihnen viel eher, wenn Sie bewusst und bereitwillig alle Compliance-Vorschriften einhalten.

Mit den richtigen Datenmanagementprozessen wird Ihr Unternehmen zudem leichter skalierbar und lässt sich besser an aktuelle und zukünftige Anforderungen anpassen.

ÜBER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) bietet Informationsmanagementdienste, mit denen Unternehmen die Kosten und Risiken bei der Verwaltung ihrer physischen und digitalen Daten reduzieren und ihre Effizienz erhöhen können.

Iron Mountain wurde 1951 gegründet und verwaltet Milliarden von Informationsbeständen für Unternehmen weltweit. Dies beinhaltet gesicherte und archivierte Daten, elektronische Dateien, Dokumenten-Digitalisierung, Geschäftsdokumente, die sichere Vernichtung von Daten und Dokumenten und vieles mehr. Weitere Informationen finden Sie auf unserer Unternehmenswebsite unter www.ironmountain.de / www.ironmountain.co.at / www.ironmountain.ch

IRON MOUNTAIN®

WIR SCHÜTZEN, WAS IHNEN AM WICHTIGSTEN IST