GDPR – DATENSCHUTZ-GRUNDVERORDNUNG

Die Herausforderung als Chance nutzen

Die Bedeutung der Datenschutz-Grundverordnung
Ab Mai 2018 können Verstösse gegen die GDPR (General Data Protection Regulation) oder auch DSGVO (Datenschutz-Grundverordnung) mit harten Sanktionen von bis zu 4 % des Gesamtumsatzes oder 20 Mio. Euro geahndet werden, dazu kommen die Kosten von Schadenersatzforderungen. Die GDPR gilt für alle Organisationen, die personenbezogenen Daten in der EU (Europäischen Union) verarbeiten. Sie ist zudem verbindlich für Unternehmen ausserhalb der EU, die Dienstleistungen innerhalb der EU anbieten und personenbezogene Daten von Personen («betroffene Personen») verarbeiten. Deshalb steht die GDPR bei vielen grossen Organisationen sowohl innerhalb wie ausserhalb der EU weit oben auf der Agenda. Am stärksten betroffen ist das B2C-Segment mit Banken, Versicherungen sowie der Gesundheits-, Rechts- und Bildungsbranche usw.

Der Ansatz der GDPR ist im Prinzip einfach: Unternehmen analysieren, inwiefern die GDPR sie tangiert, identifizieren die Lücken und schliessen diese mit geeigneten Massnahmen. Doch die Praxis ist komplexer: Analysen ergeben in der Regel, dass das Unternehmen nicht richtlinienkonform arbeitet und nicht vollumfänglich transparent ist, wo und wie die fraglichen Daten aufbewahrt werden. Dies ist sehr riskant, denn nicht zu wissen, dass Daten vorhanden sind, wird nicht als Entschuldigung akzeptiert. Die brennenden Themen sind:

- Richtlinien, Kontrollen, Prozesse, Aufgaben und Verantwortlichkeiten bei der Handhabung von personenbezogenen Daten
- Erfassung, Aufbewahrung, Abfrage, Verarbeitung, Nutzung, Änderung und Vernichtung von personenbezogenen Daten
- Verwaltbarkeit von digitalen und physischen Daten in einem strukturierten oder unstrukturierten Format
- Vertraulichkeit, Integrität, Sicherheit, Verfügbarkeit und Störfallsicherheit beim Umgang mit Daten
- IT-Plattformen, Systeme, Datenbanken
- Transparenzregeln, Informationspflicht und Prüfungsbefugnisse

Die grundlegenden Herausforderungen
Auf den ersten Blick geht es bei der GDPR einfach um regulatorische Vorgaben, doch in der Realität berührt sie etwas sehr Grundlegendes: die Struktur, die Verarbeitung und die Kommunikation von Daten. Oft sind die entsprechenden Strukturen über Jahrzehnte gewachsen, sodass diverse physische und digitale Formate (Papier, Band, Post, Akten ...) in strukturierten und unstrukturierten Daten (Briefe, E-Mails, Gespräche, Formulare) vorhanden sind, die an verschiedensten Orten (physische Archive, verteilte Datenbanken) aufbewahrt werden.

Die GDPR sorgt für viele Gespräche, doch es wurde bisher kaum etwas über Daten in Papierform gesagt – dabei sind sie es, die am ehesten operationelle Probleme verursachen und Organisationen Risiken aussetzen. Mit der GDPR wird Papier zum echten Problem. Es lässt sich überall aufbewahren und jedes Blatt Papier könnte personenbezogene Daten enthalten. Auch der Umfang stellt ein Problem dar: Sowohl in internen Aktenablagen als auch in Archivierungsunternehmen lagern Millionen von Kartons und Akten. Zu vielen dieser Daten gibt es keine Metadaten und die vorgeschriebene Aufbewahrungsfrist ist bereits abgelaufen. Mit grosser Wahrscheinlichkeit enthalten sie jedoch personenbezogene Daten und stellen somit ein Risiko dar.

Vielerorts laufen GDPR-Projekte, in die eine breite Palette an Geschäftsfunktionen und Mitarbeitenden involviert sind. Angesichts des Umfangs und der räumlichen Verteilung bringen Papierakten bei der Einhaltung der neuen Vorschriften einen grossen Zeit- und Arbeitsaufwand mit sich. Solche Initiativen sind kostspielig und bringen nur einen begrenzten geschäftlichen Nutzen. Es braucht daher Lösungen, welche die Kosten auf ein Minimum beschränken und gleichzeitig ermöglichen, personenbezogene Daten für Innovationen und die Verbesserung von Dokument- und Informationsprozessen zu nutzen. Wenn Unternehmen die Thematik

strategisch betrachten, können sie aus einer regulatorischen Bürde eine Geschäftschance machen. Die GDPR bietet die Gelegenheit, den bestehenden Datenpool verwaltbar und somit nutzbar zu machen.

Lösen Sie die Grundprobleme der GDPR
Gängige GDPR-Ansätze umfassen die folgenden Schritte:

1. Sensibilisierung und C-Level-Support
2. Identifizierung von Prozessen und Medien mit personenbezogenen Daten
3. Analyse der aktuellen Prozesse, Verträge und Datenobjekte, die mit personenbezogenen Daten in Berührung kommen
4. Identifizieren von Lücken hinsichtlich der GDPR-Anforderungen
5. Wirkungs- und Risikoanalyse
6. Definieren, Finanzieren und Umsetzen von Massnahmen und Projekten

Das Ergebnis solcher Programme sind revidierte Unternehmensrichtlinien, Kontrollen, Reporting- und Auditstrukturen sowie grössere IKT-Neuerungen im Bereich Datenbanken, Archivierung, Content Management, CRM und ERP, Zugriffsrechte und Identitätsmanagement. Dabei geht es hauptsächlich darum, als Grundlage für die GDPR-Compliance-Kontrolle über einen wachsenden Pool von physischen und elektronischen Dokumenten in strukturierter wie unstrukturierter Form zu gewinnen. Dies umfasst:

- Finden und Identifizieren von personenbezogenen Daten
- Kennzeichnen, Indexieren und Klassifizieren von personenbezogenen Daten
- Einholen der expliziten Zustimmung von betroffenen Personen zur Aufbewahrung und Nutzung personenbezogener Daten
- Kommunizieren, ändern und löschen von personenbezogenen Daten auf Anfrage
- Festlegen, Dokumentieren und Umsetzen von Nutzungsbeschränkungen und -berechtigungen

Die wenigsten Unternehmen arbeiten ohne Papier. Bei einigen gibt es einige wenige durchdigitalisierte oder einige papierfreie Prozesse, doch die Umstellung auf ein komplett digitales Modell dauert viel länger, als die Branchenexperten sagen. GDPR-Initiativen, die keine Digitalisierung umfassen, werden die Prozesskosten in die Höhe treiben und keine erhöhte Flexibilität bieten. Dies beschränkt das Kundenerlebnis, die Innovation und die Wettbewerbsfähigkeit.

Bei der Anpassung an die GDPR auch gleich digital zu werden, vereinfacht hingegen nicht nur die Compliance, sondern schafft auch einen Mehrwert im gesamten Unternehmen. Die erfolgreichsten GDPR-Ansätze gehen über regulatorische Vorschriften und Compliance hinaus, indem sie den Gesamtansatz für die Dokument- und Datenverarbeitung überprüfen und die Tür zu neuen Möglichkeiten öffnen. Dazu braucht es eine zukunftsorientierte Perspektive.

Das Problem an der Wurzel packen und daraus geschäftlichen Nutzen erzielen
Daten sind eine strategische Ressource. Nutzbare Daten eröffnen wertvolle neue Geschäftschancen, neue Welten des Kundenerlebnisses sowie neue Wege zur operativen Exzellenz und machen veraltete Systeme und Prozesse schnell überflüssig. Der digitale Versand reduziert den Aufwand für die Postbearbeitung, die Dokumentenverwaltungskosten und den Zeitaufwand für die Datenverarbeitung. Doch viele haben dabei mit unstrukturierten Daten und der grossen Bandbreite an elektronischen und physischen Medien zu kämpfen – denselben Hindernissen, mit denen auch Unternehmen im GDPR-Prozess konfrontiert sind. Daher wäre es kurzsichtig, das Thema nur aus der GDPR-Perspektive anzugehen.

Die Kosten und Herausforderungen bei der Umsetzung von GDPR-Ansätze sind ein direktes Ergebnis von Daten, die sich über viele Jahre hinweg angesammelt haben. Diese Datenansammlung wird zur Bürde, weil die Datenverarbeitung immer komplexer wird, sowohl allgemein als auch compliance-technisch betrachtet. Die wichtigen Fragen sind: Sollen wir investieren, um eine nicht konforme Datenbasis konform zu machen? Oder sollen wir investieren, um diese Datenbasis zu einer Ressource für künftige Geschäfte zu machen? Sollen wir die steigenden Kosten für die Komplexität eines veralteten Systems weiterhin tragen? Oder sollen wir einen grossen Schritt machen und in neue Geschäftschancen investieren? Der kritische Punkt ist bereits erreicht. Dieses grundlegende Problem nicht anzugehen ist zu einem ernsten Risiko geworden. Die Digitalisierung der Dokumenten- und Datenverarbeitung eröffnet diverse Möglichkeiten:

- Erhöhte Produktivität: Überall und jederzeit auf Informationen zugreifen und effizienter zusammenarbeiten
- Höhere Kundenzufriedenheit: Das Backoffice wird auf die Kundenbedürfnisse ausgerichtet und kann schnell kompetente Antworten liefern
- Besseres Kundenverständnis: Alle in der Kommunikation enthaltenen Daten sind sichtbar, was eine Rundumsicht auf den Kunden, Datenanalysen und fundierte Entscheidungen ermöglicht
- Verbesserte Compliance: Vollständige Transparenz und Kontrolle ermöglichen eine schnellere Reaktion auf Gesetzesänderungen; dies senkt das Risiko und wahrt den Ruf

Die meisten Unternehmen besitzen keine Richtlinien zur Datenaufbewahrung und kennen den rechtlichen Status der Daten in archivierten Dokumenten nicht. Die Digitalisierung alter Papierdokumente ist eine äusserst mühsame Arbeit. In der Eile, sich noch fristgerecht an die GDPR anzupassen, mag es verlockend scheinen, Dokumente zu zerstören statt zu digitalisieren. Doch Vorschriften auszuweichen, indem Akten zerstört werden, ist eine sehr riskante Option – und dazu noch eine Verschwendung von Datenkapital. Richtig durchgeführt ist der Digitalisierungsprozess ein Meilenstein auf dem Weg zum komplett digitalisierten Unternehmen, das Nutzen aus wertvollen Daten zieht.

Die GDPR ist ein Weckruf für Unternehmen, die in Sachen Digitalisierung hinterherhinken. Vielen Unternehmen mangelt es weder an der Strategie, noch am Willen oder den Möglichkeiten. Doch oft fehlen die Ressourcen, das Know-how und der Transferprozess. Dieses Problem können Unternehmen lösen, indem sie mit geeigneten strategischen Partnern zusammenarbeiten. Die Auslagerung ist eine Möglichkeit, die wichtigsten GDPR-Themen anzugehen und die Digitalisierung dazu zu verwenden, die Compliance zu gewährleisten, Auskunftsanfragen schnell zu bearbeiten und neue Geschäftschancen zu nutzen.

SPS Switzerland AG kann helfen

SPS Switzerland AG (SPS) verwaltet mit zukunftssicheren und gesetzeskonformen Lösungen und Dienstleistungen alle personenbezogenen Daten, die bei einer Organisation eingehen, unabhängig von deren Form (physisch, elektronisch) und Format (strukturiert, unstrukturiert). Mit hocheffizienten On- und Offsite-Servicezentren, Scan- und Erkennungstechnologien sowie künstlicher Intelligenz werden digitale Dokumente erstellt, relevante Daten extrahiert und Dokumente akkurat klassifiziert und indexiert. Die Verarbeitung von Dokumenten und Daten erfolgt effizient, gesetzeskonform und gemäss höchsten Qualitätsstandards. Physische Dokumente werden eindeutig identifizierbar gemacht und den Richtlinien entsprechend abgelegt oder vernichtet.

SPS verlagert Prozesse mit personenbezogenen Daten in die digitale Welt. Physische Aufzeichnungen müssen nur am Anfang und am Ende ihres Lebenszyklus in die Hand genommen werden («single touch processing»). Alle weiteren Schritte dazwischen erfolgen digital. Möglich macht dies eine digitale Poststelle in Kombination mit der intelligenten Verarbeitung von Transaktionsdaten und Dokumenten. Durch die Digitalisierung bestehender physischer Archive werden alte Datenpools aufgeräumt und die aufwendige Handhabung physischer Dokumente (auffinden, sammeln, nachverfolgen etc.) entfällt.

SPS bietet eine führende Serviceplattform für Geschäftsprozesse, die neue Möglichkeiten für die Verarbeitung personenbezogener Daten eröffnet. Dokumente und Daten sind gleich ab Prozessstart nutzbar, sodass ganze Arbeitsschritte eliminiert, automatisiert oder von Offsite-Servicezentren übernommen werden können. So gewährleistet SPS nicht nur die GDPR-Compliance, sondern bietet dank künstlicher Intelligenz (AI) und Robotik (RPA) sowie der Grundlage für Datenanalysen zusätzliche Vorteile:

- GDPR-konforme Handhabung von alten und neuen Daten
- Optimierte und schnellere Prozesse für physische und digitale Dokumente und Daten
- Kostenreduktion, operative Flexibilität und Anpassungsfähigkeit
- SLA- und Auditpfad
- Notfallwiederherstellung, Back-up und Krisenmanagement
- Vertiefte Business-Analysen dank nutzbaren Daten
- Laufende Verbesserungen und Engagement für Innovation

Die Dienstleistungen von SPS sind von Grund auf GDPR-konform konzipiert und befähigen Kunden, die Chancen der digitalen Transformation zu nutzen. Als Expertin für die End-to-End-Datenverarbeitung vom Omni-Channel-Input über die Digitalisierung und Verarbeitung bis zum Omni-Channel-Output ist SPS die ideale Partnerin, die ausserdem die traditionellen Schweizer Werten Diskretion und Sicherheit pflegt sowie durch Innovationskraft überzeugt. Die Kunden von SPS bekommen das Beste aus zwei Welten: hochwertige Dienstleistungen und Innovation kombiniert mit Sicherheit und Zuverlässigkeit in folgenden Bereichen:

- Verarbeitung von Omni-Channel-Input
- Digitale Poststelle
- Datenmanagement und Dokumentenverarbeitung
- Intelligente Prozessautomatisierung
- Verarbeitung von Omni-Channel-Output

Die GDPR in Kürze

Mit der GDPR harmonisiert die EU die Datenschutzstandards ihrer Mitgliedsstaaten. Bislang setzte jeder Mitgliedsstaat die Europäische Datenschutzrichtlinie von 1995 nach eigenem Gutdünken um, was zu unterschiedlichen Standards führte. Die GDPR ist seit März 2016 in Kraft, wobei Unternehmen zwei Jahre Anpassungszeit gewährt wurde; ab dem 25. Mai 2018 ist sie einzuhalten. Die GDPR ersetzt nationale Regelungen und stärkt die Rechte von betroffenen Personen an ihren personenbezogenen Daten. Sie fordert:

- Rechtmässigkeit, Fairness, Transparenz
- Integrität und Vertraulichkeit
- Zweckbindung, Korrektheit und –Datenminimierung
- Rechenschaftspflicht

Personenbezogene Daten sind im Sinne der GDPR alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Diese Person wird als «betroffene Person» bezeichnet. Mit der GDPR wird die Definition von personenbezogenen Daten auf eine breitere Palette persönlicher Merkmale wie Namen, Kontaktangaben, Online-Identitäten, Ausweis- und Versicherungsnummern, Adressen, Orte, IP-Adressen sowie Informationen, die eine Identifizierung ermöglichen – beispielsweise genetische, biometrische und medizinische Daten –, ausgedehnt.

Die GDPR unterscheidet zwischen Verantwortlichen und Auftragsverarbeitern. Verantwortliche und Auftragsverarbeiter haben dieselben Verpflichtungen, wobei Auftragsverarbeiter im Namen der Verantwortlichen handeln. Der Verantwortliche ist eine Organisation, die Mittel und Zweck im Hinblick auf personenbezogene Daten definiert. Bei Datenschutzverletzungen haftet primär der Verantwortliche. Typische Auftragsverarbeiter sind Dienstleister, Clouddienstanbieter, Outsourcer usw.

Die GDPR beinhaltet die Verpflichtung, personenbezogene Daten auf Anfrage betroffener Personen zu berichtigen, zu ändern oder zu löschen und Datenschutzverletzungen innerhalb von 72 Stunden zu melden. Für die Nutzung personenbezogener Daten ist die ausdrückliche Zustimmung der betroffenen Personen erforderlich. Auf Anfrage müssen betroffenen Personen elektronische Kopien ihrer personenbezogenen Daten unter Angabe von Inhalt, Aufbewahrungsdauer, Aufbewahrungsort und Aufbewahrungszweck zur Verfügung gestellt werden. Systeme, Produkte und Prozesse müssen so konzipiert sein, dass sie Datenschutz- und Sicherheitsvorkehrungen integrieren. Es gilt, Datenverarbeitungsaktivitäten angemessen zu dokumentieren und geeignete Sicherheitsstandards (technisch und organisatorisch) anzuwenden. Unternehmen, die grosse Mengen an personenbezogenen Daten verarbeiten, müssen interne Kontrollen durchführen und einen Datenschutzbeauftragten einsetzen, um das Risiko von Datenschutzverletzungen für betroffene Personen zu minimieren.