Was die EU-Datenschutz Grundverordnung (EU-DSGVO) für Sie bedeutet

Was ist die EU-DSGVO?

Die EU-DSGVO (Datenschutz-Grundverordnung) ist eine Verordnung der Europäischen Kommission zur Schaffung eines einheitlichen Mandats für jeden EU/EWR-Mitgliedstaat, zum Schutz personenbezogener Daten im Falle eines Datenverstoßes.

Das aktuelle Regelwerk der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) leitet sich aus einer 1995 in Auftrag gegebenen Richtlinie ab, die im nationalen Kontext der einzelnen EU/EWR-Mitgliedsstaaten interpretiert und gestaltet werden soll.

Das neue Gesetz ist keine Richtlinie, sondern eine Verordnung, die alle EU/EWR-Länder dazu verpflichtet, in der gesamten Union das gleiche einheitliche Recht zu befolgen, überlässt dem national Gesetzgeber jedoch ein gewisses Maß an Spielraum zur Umsetzung der Verordnung.

Die EU-DSGVO soll die Datenschutzgesetze in der gesamten Europäischen Union angleichen und die persönlichen Daten ihrer Einwohner im In- und Ausland schützen. Als weltweit tätiges Unternehmen begrüßt Therefore die neue Regelung als einen Schritt in die richtige Richtung zur Stärkung der persönlichen Rechte und Freiheiten.

> “Als weltweit tätiges Unternehmen begrüßt Therefore die neue Verordnung als einen Schritt in die richtige Richtung zur Stärkung der persönlichen Rechte und Freiheiten.”

Wie Therefore™ helfen kann:

Die EU-DSGVO ist eine komplexe Verordnung, die erhebliche Anstrengungen und Investitionen in Datensicherheit und den Schutz betroffener Unternehmen erfordert.

Therefore Corporation ist bestrebt, Sie bei der Einhaltung der EU-DSGVO zu unterstützen. Unsere Informationsmanagementlösung ermöglicht das Speichern, Finden und Kategorisieren persönlicher Daten in einer sicheren Datenumgebung. Darüber hinaus bietet Therefore™ Ressourcen, die die Überwachung und Verwaltung der im System gespeicherten persönlichen Daten vereinfachen und den Berichts- sowie Verarbeitungsanforderungen der EU-DSGVO entsprechen.

Aufgrund der Natur und des Umfangs der EU-DSGVO, geht die Einhaltung dieser Verordung weit über die Softwaregrenzen hinaus. Die Einhaltung ergibt sich aus einer Kombination solider Datenschutzrichtlinien, Verfahren, Schulungen und Berichterstattung. Therefore™ kann Ihrem Unternehmen dabei helfen, diese Ergebnisse und damit die Einhaltung der EU-DSGVO-Richtlinien, durch den Einsatz geeigneter Werkzeuge die das Finden, Verwalten, Sichern und Berichten von Unternehmensdaten ermöglichen, zu gewährleisten.

Ein korrekt konfiguriertes, gewartetes und verwaltetes Therefore™ System hilft Ihnen beim sicheren Umgang mit persönlichen Daten und bietet in Kominbation mit geeigneten organisatorischen Verfahren und Funktionsweisen besseren Schutz vor Datenverstößen.

Wie Therefore™ hilft...

- Speichern, finden und katalogisieren gespeicherter persönlicher Daten
- Einfache Überwachung und Verwaltung personenbezogener Daten
- Eine sicherere Datenumgebung erschaffen
- Werkzeuge zur Erfüllung der Berichts- und Verarbeitungs-anforderungen

Therefore™
PEOPLE PROCESS INFORMATION

Wo beginnen?

Die EU-DSGVO untersteht vielen Anforderungen, wie Unternehmen personenbezogene Daten sammeln, speichern und nutzen können. Dazu gehören:

- Wie personenbezogene Daten identifiziert, gespeichert und gesichert werden
- Wie Anforderungen an Datentransparenz entsprochen wird
- Wie Verstöße gegen die EU-DSGVO erkannt und gemeldet werden
- Wie Sie Datenschutzpersonal und MitarbeiterInnen schulen
- Und mehr

Da die Einhaltung ("Compliance") dieser neuen Verordnung mit viel Aufwand verbunden ist, empfiehlt Therefore™ mit der Überprüfung Ihrer Datenverwaltungspraktiken und -richtlinien zu beginnen. Die Nichteinhaltung der EU-DSGVO kann ernsthafte finanzielle Folgen wie auch Rufschädigung nach sich ziehen. Sanktionen können bis zu 10.000.000 € oder 2% des weltweiten Bruttoeinkommens umfassen, je nachdem, welcher Betrag höher ist. Bei der Beurteilung der Situation durch die Behörden kann jedoch der Nachweis einer soliden Reihe von Sicherheitsvorkehrungen und die Reaktionszeit für Meldungen eines Datenschutzverstoßes berücksichtigt werden.

Auf dem Weg zur Einhaltung der EU-DSGVO sollten Sie auf folgende Bereiche achten:

ERKENNEN: Prävention und Vorbereitung

- Identifizieren Sie die Art der persönlichen Daten, die Ihr Unternehmen sammelt und wie diese gespeichert werden
- Führen Sie eine Risikobewertung und Gefahrenanalyse durch, um sich ein Bild über den derzeitigen Status zu machen
- Ernennen Sie einen Datenschutzbeauftragen/Data Protection Officer (DPO)
- Schulen Sie Ihre MitarbeiterInnen um sicherzustellen, dass die DatenverarbeiterInnen über die neuen Regelungen informiert sind und diese einhalten

VERWALTEN UND SICHERN: Auswirkungen auf die Sicherheit

Implementieren Sie Richtlinien und Werkzeuge, um die Verwaltung und den Zugriff auf Ihre persönlichen Daten zu verwalten:

- Nicht autorisierten Personen Zugang auf personenbezogene Daten verwehren
- Elektronisch: Keine über das Internet oder lokale Netzwerke zugängliche Datensicherung
- Physisch: Zugriff auf Papierdaten, Server oder Speichermedien mit persönlichen Daten verhindern

In Therefore™:

- Überprüfen Sie die Berechtigungseinstellungen um ausschließlich autorisierten Benutzern Zugriff auf persönliche Daten zu gewähren
- Erwägen Sie einen Hochsicherheitsbereich in Ihrem Therefore™ Repository, wie z.B. einen Ordner mit Kategorien zur Speicherung persönlicher Daten, die in den Anwendungsbereich der EU-DSGVO fallen
- Einschränkung der Ansichtsrechte auf Indexfelder, die personenbezogene Daten enthalten
- Regelmäßige Überprüfung der Systemzugriffsberechtigungen mittels der Erstellung von Sicherheitsberichten in Therefore™
- Aktivierung der Backup-Laufwerke, Speicher- und Aufbewahrungsrichtlinien sowie Migrationszeitplänen zur ordnungsgemäßen Datensicherung
- Festelegen von Aufbewahrungsrichtlinien, um veraltete Informationen nach Ablauf lokal-geltender Aufbewahrungsfristen zu löschen
- Aktivieren Sie ggf. erweiterte Sicherheitseinstellungen im Therefore™ Solution Designer
- Für Therefore™ Web Access kann die Einstellung “Encrypt Link” für Masken Objekt-IDs in Therefore™ aktiviert werden, um die Sicherheit zu erhöhen

BERICHTEN: Datenverstöße und zu ergreifende Maßnahmen

Implementieren von Richtlinien und Verfahren für den Umgang mit und Meldungen von Datenverstößen:

- Führen Sie sorgfältige Aufzeichnungen über Sicherheitsimplementierungen Ihres Unternehmens - solide Beweise für Bemühungen zum Schutz und zur Verwaltung personenbezogener Daten erhöhen die Chancen auf Nachsicht, wenn es um Sanktionen durch die Aufsichtsbehörden geht
- Bestimmen Sie ein Verfahren oder eine Strategie, um einen Verstoß wirksam an die Regulierungsbehörden Ihres Landes zu melden - solche Verstöße müssen normalerweise innerhalb von 72 Stunden gemeldet werden

In Therefore™:

- Konfigurieren Sie einen Therefore™ Audit Trail, um Aktivitäten von Systembenutzern zu protokollieren und die Protokolle regelmäßig auf Anzeichen verdächtiger Aktivitäten zu überprüfen
- Speichern Sie Dokumentation zu Sicherheitsimplementierungen Ihres Unternehmens in Therefore™ und erstellen Sie einen Workflow rund um den Prozess der Organisationsüberprüfung

ÜBERPRÜFEN: Datenschutzrichtlinien und Zugriffsanfragen (SAR - Subject Access Requests)

Umsetzung der Verordnung und Verfahren für Datenschutzrichtlinien und SARs:

- Erstellung eines Protokolls oder Verfahrens für die Bearbeitung von Zugriffsanfragen
- Regelmäßige Überwachung der Datenschutzbestimmungen, um sicherzustellen, dass Geschäftsprozesse weiterhin gesetzeskonform sind
- Aktualisierung der Datenschutzrichtlinien des Unternehmens

In Therefore™:

- Erstellung eines Workflows zur effizienten und korrekten Bearbeitung von Zugriffsanfragen, Sicherstellung lückenloser Dokumentation und Nachvollziehbarkeit der Prozesse
- Erstellung eines Workflows zur regelmäßigen Überprüfung der aktuellsten Vorschriften, um Richtlinien und Verfahren gegebenenfalls anzupassen
- Kategorisieren persönlicher Daten in logische Gruppen, die es erleichtern, auf SARs zu reagieren; zum Beispiel, Kundendateien in Fälle zu organisieren, in denen alle persönlichen Daten einer Person (Dokumente, Metadaten usw.) zusammengefasst werden
- Erstellung von Berichten mit Hilfe von Therefore™ Business Analytics, um sicherzustellen, dass Prozesse ordnungsgemäß abgeschlossen werden
- Installieren Sie immer die neuesten empfohlenen Patches und Updates, um die Sicherheit Ihres Systems zu gewährleisten

EU-DSGVO: Umsetzung in der Praxis

Betrachten wir einen fiktiven Fall einer Versicherungsgesellschaft, die mit Therefore™ personenbezogene Daten EU-DSGVO-konform verwaltet:

Die Moya Insurance Group (kurz MIG) ist ein internationales Versicherungsunternehmen mit Sitz in der EU.

Aufgrund der Natur des Versicherungsgeschäfts speichert MIG viele persönliche Daten ihrer Kunden und ist damit ein vorrangiges Ziel der EU-DSGVO. Dazu gehören Daten wie:

- Name, Geburtsdatum, Familienstand, Wohnadresse, Telefonnummern und E-Mail-Adressen
- Medizinische Informationen und biometrische Daten (für Krankenversicherungen)
- Einkommens- und Finanzinformationen (für Hypothekenversicherungen)
- Fahrtenbücher und Fahrzeuginformationen (für Kfz-Versicherungen)

MIG verwendet Therefore™, um die genannten Daten in ihrer Organisation zu verwalten. Alle Kundendaten, einschließlich persönlicher Daten, Dokumentationen und Informationen zu Richtlinien werden zusammen in einem elektronischen Ordner aufbewahrt.

ERKENNEN

- MIG führte eine Überprüfung der gespeicherten Daten durch und erstellte eine Liste der Arten an persönlichen Daten, die sie über ihre Kunden besitzt
- MIG ist bewusst, dass die EU-DSGVO die Art und Weise ihrer Geschäftstätigkeit beeinflusst und hat sich dementsprechend auf die Verordnung vorbereitet:
- MIG wollte in keinen neuen Datenschutzbeauftragten investieren und beauftragt daher bei Bedarf einen Anwalt
- Der beauftragte Anwalt (DPO) führte ein Schulungsseminar durch, um MIG-MitarbeiterInnen über die EU-DSGVO zu informieren. Alle Anwesenden haben ihre Teilnahme mit einer Unterschrift bestätigt. Die Schulungsunterlagen wurden in einer für alle MitarbeiterInnen jederzeit einsehbaren Kategorie in Therefore™ gespeichert. Das unterschriebene Anwesenheitsblatt wurde zusammen mit allen weiteren Unterlagen, die MIG während der Vorbereitung auf die EU-DSGVO erstellt hat, in Therefore™ gespeichert

VERWALTEN UND SICHERN

MIG führte ein erstes Audit ihrer Sicherheitsrichtlinien mit ihrer IT-Abteilung durch und stellte folgende Probleme fest:

- Ein Systemadministrator hatte vor 3 Monaten gekündigt und vergessen, seinen Schlüssel für den Serverraum zurückzugeben. Das Schloss wurde aus Sicherheitsgründen ausgetauscht und der neue Schlüssel an autorisiertes Personal verteilt
- Ein zusätzliches Risiko stellten Aktenschränke mit Kundeninformationen aus den Jahren 2005 bis 2010, im Untergeschoss dar. MIG entschied sich, das Scannen und Digitalisieren dieser Papierdokumente auszulagern und später in Therefore™ zu importierten
- Eine Festplatte mit Kopien von Kundendokumenten wurde auf dem Schreibtisch eines Mitarbeiters gefunden. Die Richtlinien von MIG wurden aktualisiert, um den MitarbeiterInnen zu verbieten, Kundendaten ohne vorherige Genehmigung aus dem Netzwerk zu entfernen. MIG erwägt nun die Installation der Therefore™ Mobile App auf den Geräten ihrer MitarbeiterInnen, um einen sicheren Fernzugriff zu ermöglichen

MIG führte eine Überprüfung des Systems Therefore™ durch und nahm die folgenden Änderungen vor, um die Datensicherheit zu erhöhen:

- Um die Menge der angezeigten persönlichen Daten zu minimieren, änderten sie ihre Berechtigungseinstellungen, damit Manager nur Kundendaten ihrer Unterabteilung und nicht für die gesamte Organisation einsehen konnten
- MIG verringerte die Inaktivitätszeit bis zur Abmeldung von Benutzern, die vergessen hatten sich auszuloggen

BERICHTEN

- MIG hat eine zusätzliche Kategorie in Therefore™ geschaffen, in der die Dokumentation der Sicherheitsverfahren, die Durchführung von Schutzmaßnahmen und der Nachweis der Ausbildungsaktivitäten rund um das EU-DSGVO gespeichert werden
- Desweiteren hat MIG einen Workflow erstellt, der regelmäßig Checklisten an die Abteilungsleiter sendet, um die Datenverarbeitungsprotokolle mit ihren Teammitgliedern zu überprüfen. Der Abteilungsleiter unterzeichnet diese Überprüfung, um den Workflow fortzusetzen
- Zusammen mit dem DPO hat MIG ein Protokoll zur Meldung von Datenverstößen an die zuständigen Behörden innerhalb von 72 Stunden erstellt. Im Rahmen der Schulung wurde den MitarbeiterInnen auch gezeigt, wie sie mögliche Datenverstöße erkennen und melden können
- Der Therefore™ Systemadministrator bei MIG hat den Therefore™ Audit Trail so konfiguriert, dass er protokolliert, wenn Dokumente aus dem System exportiert oder gesendet werden. Anschließend konfigurierte er einen Workflow, um daran zu erinnern, die Protokolle wöchentlich zu überprüfen, sie auf Therefore™ (zusammen mit anderen Compliance-Dokumenten) zu speichern und verdächtige Aktivitäten dem DPO zur weiteren Untersuchung zu melden

ÜBERPRÜFEN

- MIG hat einen Workflow für die Bearbeitung von Zugriffsanfragen eingerichtet. Dieses Verfahren wird gestartet, wenn ein Kunde ein auf seiner Website gehostetes Webformular ausfüllt, das automatisch einen Workflow in Therefore™ startet. Da MIG seine Kundeninformationen als Fälle, innerhalb von Therefore™ organisiert, ist es für die MitarbeiterInnen, die mit SARs umgehen, einfach, alle relevanten Informationen zu einem Kunden zu finden
- MIG führt regelmäßige Audits mit dem DPO durch, um sicherzustellen, dass der Umgang des Unternehmens mit den persönlichen Daten seiner Kunden weiterhin der EU-DSGVO entspricht

Schlussbemerkungen

Alle Organisationen, die personenbezogene Daten speichern und verarbeiten, sind verpflichtet zu wissen, dass die EU-DSGVO für sie gilt. Betroffene Organisationen sind ab dem 25. Mai 2018 somit dafür verantwortlich, über die Verordnung informiert zu sein und deren Bestimmungen einzuhalten.

Dieses Dokument dient nur zu Informationszwecken und ist keine umfassende Richtlinie zur Einhaltung der EU-DSGVO Vorschriften. Betroffene Organisationen müssen sich bei der Festlegung oder Überprüfung ihrer Prozesse auf die Einhaltung der in der Verordnung festgelegten rechtlichen Anforderungen oder sich daraus ergebenden spezifischen Fragen möglicherweise an unabhängige Rechtsberatungen wenden.

Weder der Autor dieses Dokuments noch die von ihm vertretene Organisation haften für die Verwendung dieses Dokuments in Vorbereitung auf die Einhaltung der EU-DSGVO oder für Schäden, die durch Nichtbeachtung entstehen.