PROSPER INTELLIGENCE

APILANi™ Your Enterprise Alliance

EU DSGVO – INTELLIGENT RISK MANAGEMENT

Das DSGVO – INTELLIGENT RISK MANAGEMENT (DSGVO – IRM) wird als Ergänzung zum DSGVO – IRA beauftragt und ist ein Service um die langfristige Konformität unseres Kunden sicherzustellen. Im DSGVO – IRM ist das standardisiertes Verfahren Audit Upon Procedure (AUP) inbegriffen und wird von unserem Kunden für die Dauer von 2 bis 4 Jahren beauftragt.

In diesem Verfahren werden zusätzliche Funktionen aus unserem Softwareprodukt ROBOTIC GRC|365 angewendet, um Verstöße im unsachgemäßen Umgang mit personenbezogenen Daten rechtzeitig aufzudecken bzw. präventiv dagegen vorzugehen. Das DSGVO – IRM überwacht hier Daten relevante Vorgänge im gesamten Verarbeitungsprozess beginnend vom PC Arbeitsplatz bis den Inhalten Ihrer Anwendungsdatenbanken sowie Datenverzeichnissen auf den Servern.

Das DSGVO – IRM stellt sich den drei großen Herausforderungen des DSGVO deren dauerhafte Umsetzung sehr hohen Zeit- und Personalaufwand für Unternehmen bedeuten. Da aber ihre Umsetzung verpflichtend ist, haben wir hierfür Funktionen entwickelt und machen diese zum Bestandteil unserer Dienstleistung. So lösen wir für Sie die drei teuersten und kompliziertesten Anforderungen des DSGVO:

I. Die Erfüllung der Auskunftspflicht nach Artikel 15

Nach einem durchgeführten DSGVO – CIA sowie dem DSGVO – IRA verfügen wir über eine Kartografie Ihrer IT Landschaft sowie eine holistische Sicht über Ihre unternehmensweite Datenverarbeitung. Unser Cross Database Select Feature ermöglicht uns über Kriterien betroffener Personen (z.B. über eine eindeutige Identifizierung durch eine Kundennummer, Kontonummer, Rechnungsnummer, etc …) quer über Ihre Applikationslandschaft hinaus Daten in einem Bericht zusammenzuführen. Ergänzend gibt es das Cross Workplace Select Feature, welches nach gleichen Kriterien sämtliche PC Arbeitsplätze nach Daten Betroffener durchsucht und einen Bericht über identifizierte Files erstellt. Beide hier beschriebenen Features sind sehr effizient und können eine hohe Zahl von Anfragen parallel abarbeiten und in Berichten zusammenstellen. Die Fristeneinhaltung sowie die Gesamtheit des Berichts an den Betroffen wird sichergestellt.

II. Das Recht auf Löschung nach Artikel 17

Nach verlangen Betroffener eine Löschung durchzuführen, können wir mit unserem Delete Due Relevance Feature, Daten abhängig von Erfüllung gesetzlicher Grundlagen von Ihren Systemen entfernen ohne die Integrität Ihrer Daten zu gefährden. Eine kurzzeitige Archivierung kann aktiviert werden. Diese wird systemseitig mit einem Ablaufdatum versehen und nach nochmaliger Sicherheitsüberprüfung durch unser Service zur restlosen Löschung freigegeben.

III. Meldung von Verletzungen des Schutzes personenbezogener Daten nach Artikel 33

Die Meldefrist von 72 Stunden ist im Falle einer Verletzung des Schutzes personenbezogener Daten stellt ein sehr enges Zeitfenster dar. Ein Prozess hierfür haben Unternehmen während der Vorbereitung bereits etabliert. Mit welchen Informationen sie die Meldepflicht tatsächlich versehen hängt vom Fall ab. Vor allem da diese gründlich mit einer Beschreibung der Art der Verletzung samt seinem Ausmaß, einer Beschreibung der zu erwartenden Folgen, einer Beschreibung der von dem Verantwortlichen ergriffenen Maßnahmen sowie Maßnahmen für eine Schadensabmilderung, zu erfolgen hat. Hier erweisen sich das DSGVO – CIA mit seinem eDiscovery sowie das DSGVO – IRM als Werkzeug um Verstöße rechtzeitig zu orten, den Auslöser festzustellen und den Schaden sofort beziffern zu können. Für unseren Kunden bedeutet dies eine rechtzeitige Schadensbegrenzung, die im Falle des Falles entscheidende Auswirkungen in der Zusammenarbeit mit der Datenschutzbehörde hat.

Die Zusammenarbeit mit den Behörden

Das gesamte Dienstleistungspaket inkludiert die Archivierung und Protokollierung sämtlicher Vorgänge in einem zentralen Datenraum. Dieser Datenraum steht dem Kunden jederzeit zur Verfügung. Sollte es einer Kontrolle durch die Datenschutzbehörde kommen wird die zentrale Rolle des Datenraumes aktiviert. Sie steht den Behörden als bestmögliche Informationsquelle zu Verfügung und signalisiert ihnen hohe Bereitschaft zur Zusammenarbeit.

Kontrolle der Prüfung nach dem Prinzip ‚Audit the Auditor'

Das AUP (Audit Upon Procedure) ist eine vom Kunden selbstinitiierte Auditierung mittels standardisiertem Verfahren und bietet die Sicherheit die bestmögliche Untersuchung durch einen externen Auditor durchzuführen. Das AUP findet zwangsläufig unangemeldet, nach einem CIG statt, unabhängig von seiner Bewertung. So funktioniert es:

1. Alle einbezogenen internen und externen Stellen werden von unserem Auditor besucht und die Richtigkeit des jährlichen CIG's wird direkt Vorort geprüft. Dabei werden Ergebnisse des DSGVO – Core Intelligence Assessment eingebunden um Grauzonen zu eliminieren, die durch einen asynchronen Betrieb zwischen IT und Business entstehen.

2. Teil des Audits sind Begehung der Betriebsstätten im In- und Ausland. Dabei werden auch alle DSGVO relevanten Dokumente gesichtet und eine detaillierte Überprüfung gemäß EU GDPR vorgenommen.

3. Erkannte Missstände werden den betroffenen Stellen unmittelbar kommuniziert, gefolgt von einer Aufforderung diese innerhalb einer gesetzten Frist zu beseitigen.

4. Bestandteil jedes AUP ist die Retrospektive über vorangegangen AUP's, der erkannten Missstände sowie durchgeführter Nachbesserungen.

Sichere Verwaltung der Dokumentation

Sämtliche Daten und Dokumente, die im Zusammenhang mit dem DSGVO gesammelt und geprüft wurden, werden zentral abgelegt und ermöglichen eine einfache Verknüpfung mit den dafür verantwortlichen Stellen und Organisationen im Unternehmen. Es entstehen folgende Vorteile:

1. Ein transparenter Überblick, welcher keine Lücken zulässt und dem Unternehmen garantiert flächendeckend Konformität erreicht zu haben.

2. Auf alle Informationen kann seitens des Datenschutzbeauftragten jederzeit zugegriffen werden.

3. Die zentrale Ablage erleichtert spätere Anpassungstätigkeiten und Nachbesserungen und dient dem Unternehmen als Collaboration-Room mit dem Zusatz eine gute Übersicht über Stärken und Schwächen zu bieten.

4. Unser Datenraum vermittelt Datenschutzbehörden einen ordentlichen Umgang mit der DSGVO da dieser über alle sachdienlichen Informationen verfügt und einen hohen Qualitätsanspruch signalisiert.

Optimierung im Umgang mit personenbezogenen Daten

Unsere Mandanten sind realistisch wenn sie davon ausgehen, dass nicht alle Stellen in ihrem Unternehmen mit der gleichsamen Sorgfalt und Qualität die DSGVO erfüllen. Hier kommt es zu großen Abweichungen unabhängig, ob die Verarbeitung intern oder extern passiert.
In internationalen Unternehmen können Kulturunterschiede zu großen Herausforderungen führen.
Hier bietet das DSGVO – IRM:
1. Eine hervorragende Möglichkeit die Performance aller Stellen zu vergleichen.
2. Bei vakanten Unterschieden kann eine Umschichtung in der Datenverarbeitung vorgenommen werden, um Optimierungen durchzuführen.
3. Wir unterstützen Sie mit der Erstellung von Anforderungen für Ausschreibungsunterlagen und bei der Auswahl in Betracht gezogener Anbieter.

Mit unserem Service Portfolio bieten wir den optimalen Schutz für Ihr Unternehmen.

Rufen Sie uns an und wir vereinbaren ein Gespräch

Mobile: +43 664 1033116
Mail: zjo@prosperintelligence.com
www.prosperintelligence.com
Breitenfurterstrasse 378/1/1
1230 Vienna, Austria