



SERVICE-METHODE GDPR ALLGEMEINER DATENSCHUTZ VERORDNUNG

EINFÜHRUNG IN GDPR

GDPR Für jeden Mitgliedsstaat der Europäischen Union gelten neue Anforderungen, mit dem Ziel, mehr zu schaffen konsequenter Schutz von Verbraucherdaten und personenbezogenen Daten EU-Staaten. Zu den wichtigsten Datenschutzanforderungen der GDPR gehören:

- Für die Datenverarbeitung ist die Einwilligung der Betroffenen erforderlich
- Anonymisieren Sie die gesammelten Daten, um die Privatsphäre zu schützen
- Bereitstellung von Benachrichtigungen über Datenschutzverletzungen
- Sichere Abwicklung des grenzüberschreitenden Datentransfers
- Bestimmte Unternehmen müssen einen Datenschutzbeauftragten zur Überwachung ernennen
GDPR Einhaltung

GDPR schreibt regulatorische Anforderungen für alle Unternehmen vor, die damit umgehen EU Bürgerdaten, um die Verarbeitung und Übertragung personenbezogener Daten der Bürger besser zu schützen.

BEGINNEN

Das Kickoff-Meeting ist ein wesentliches Instrument zur Kommunikation und Planung der Projektdurchführung mit minimaler Behinderung und um das Projekt innerhalb der geplanten Zeit und Kosten abzuschließen. Die Tagesordnung für das Kick-off-Meeting lautet:

- Diskussion des Projektplans: Dazu gehört auch die Diskussion über Verantwortlichkeit und Verantwortung von Stakeholder. Meilensteine und Ergebnisse im Projekt
- Leistungsumfang
- Gesetzliche und behördliche Anforderungen

BILDUNG DES KERNTREAMS

- Bestellung eines Datenschutzbeauftragten (DSB)
- Ernennung eines internen DSGVO-/GRC-Ausschusses (Governance Risk & Compliance)
(*Falls erforderlich)

GDPR Bewusstseinschulung

GDPR Für die Mitarbeiter Ihrer Organisation wird eine Sensibilisierungsschulung durchgeführt. Die Ausbildung Die Sitzung soll den Mitarbeitern helfen, sich Wissen anzueignen und die Konzepte zu verstehen GDPR, und Prozesse und Praktiken auf das Erreichen von und auszurichten Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Compliance-basierten Systems Arbeitsumfeld. Wenn die Mitarbeiter geschult sind, können sie denken, handeln und dazu beitragen die Ziele erreichen.

GDPR - PHASENWEISE UMSETZUNG

PHASE I - GAP ANALYSE

In dieser Phase führen wir eine Lückenanalyse durch, um zu überprüfen, wie groß Ihre aktuellen Praktiken sind entsprechend den Anforderungen. Ihre aktuellen Praktiken werden anhand der beiden folgenden überprüft Referenzkriterien,

- GDPR Anforderungen
- Gesetzliche, behördliche und gesetzliche Anforderungen

Die Ergebnisse dieser Analyse werden in Form eines Gap-Analyseberichts dargestellt. Dieser Bericht fungiert als Liste der Aktionselemente für die Erinnerung an das Projekt

PHASE II - BEWERTUNG DES INFORMATIONSFLUSSES

In dieser Phase helfen wir bei der Identifizierung von Informationsquellen und der Verarbeitung Infrastruktur, die Personal, Technologie und physische Infrastruktur in Bezug auf umfasst GDPR

PHASE III - Datenschutz-Folgenabschätzung (DPIA)

Eine Datenschutz-Folgenabschätzung (DPIA) ist ein Prozess, bei dem potenzielle Datenschutzprobleme & Risiken werden identifiziert und aus Sicht aller Stakeholder betrachtet. Dies ermöglicht die Die Organisation muss die wahrscheinlichen Auswirkungen neuer Initiativen antizipieren und gezielt angehen Maßnahmen zur Minimierung/Reduzierung der Risiken. DPIA sollen das Schadensrisiko minimieren kann durch die Nutzung/Missbrauch personenbezogener Daten verursacht werden, indem Sie sich mit dem Datenschutz befassen Datenschutzbedenken in der Entwurfs- und Entwicklungsphase eines Projekts

Wir helfen bei der Entwicklung eines DPIA-Verfahrens und eines DPIA-Registers, indem wir uns mit der Funktion abstimmen Kopf so, dass es der Organisation zugute kommt, indem es Risiken bewältigt und Schäden vermeidet Reputation, Gewährleistung der Einhaltung gesetzlicher Verpflichtungen und Verbesserung der Beziehungen zu Interessengruppen.

PHASE IV - SICHERE ÜBERTRAGUNGSANALYSE PERSÖNLICHER DATEN

Wir helfen bei der Analyse, welche personenbezogenen Daten außerhalb Ihres Unternehmens übertragen werden Darüber hinaus helfen wir auch bei der Gestaltung der notwendigen Sicherheitsmaßnahmen, um einen angemessenen Schutz zu gewährleisten personenbezogene Daten sowie personenbezogene Daten, die außerhalb des Unternehmens übermittelt werden

PHASE V - EINRICHTEN DES PROZESSES FÜR DATENVERLETZUNGSVORFÄLLE

Wir unterstützen Sie bei der Einrichtung von Prozessen zur Erkennung und Bewältigung von Verstößen gegen den Schutz personenbezogener Daten. (z. B. Daten (Verfahren zur Meldung von Verstößen) und helfen auch bei der Entwicklung von Verfahren zur Meldung von Vorfällen Mechanismus an die zuständige Aufsichtsbehörde weiterzuleiten

PHASE VI - Dokumentationsunterstützung

Wir unterstützen bei der Umsetzung notwendiger organisatorischer und technischer Maßnahmen zum Schutz der personenbezogener Daten der betroffenen Personen und helfen auch bei der Gestaltung relevanter Dokumentationen mit Kontrollrichtlinien und -verfahren, die sicherstellen, dass die GDPR gut in die GDPR eingebettet ist Organisationsprozesse

Datenschutzbeauftragter Interne Revisionsschulung



GDPR Für den DSB wird eine Schulung zum Internen Auditor (IA) angeboten. Dieses Training wird solche ausrüsten Personal, um den Bedarf an Folgenabschätzungen zu analysieren, Folgenabschätzungen zu planen und zu planen, Audit-Checklisten zu erstellen und durchzuführen eine Folgenabschätzung durchzuführen und ihre Beobachtungen zu dokumentieren und der obersten Leitung zu melden

GDPR INTERNE AUDIT



Unsere Experten überwachen die Durchführung der internen Revision durch Ihren Datenschutzbeauftragten. Dieses interne Audit wird Identifizieren Sie noch bestehende Lücken im System und demonstrieren Sie den Grad der Bereitschaft, diese zu bewältigen Compliance-Audit. Dieses Audit gibt der Organisation die Möglichkeit, alle nicht ordnungsgemäßen Anforderungen zu identifizieren und zu beheben. Konformitäten, bevor Sie mit dem Compliance-Audit fortfahren. Die oberste Leitung wird darüber informiert Feststellungen der internen Revision.

GDPR - URSACHENANALYSE (RCA) UND KORREKTURMASSNAHMEN



Alle Nichtkonformitäten, die während des internen Audits, der Kunden-oder Drittaudits oder von festgestellt wurden Risikoregister, DPIA-Register, Vorfalldokumente, Datensicherungsprotokolle, Benachrichtigungsberichte über Datenschutzverletzungen, Vulnerability Assessment & Penetration Test (VAPT), Datenaufbewahrungsprotokolle und alle anderen Quellen müssen aufgeführt werden. RCA wird mit Techniken wie Brainstorming und Fish-Bone-Methoden durchgeführt. Die optimalen Korrektur- und Korrekturmaßnahmen werden umgesetzt und die Wirksamkeit dieser wird überprüft Maßnahmen werden über einen GDPR Corrective Action Report (CAR) dokumentiert und überprüft.

Unsere Experten werden mit Ihrem Team anwesend sein, um Sie durch den Prozess zu begleiten.

GDPR Managementbewertung TREFFEN (MRM)

Das MRM bietet allen Beteiligten die Möglichkeit, sich in festgelegten Abständen zu treffen und zu besprechen und Maßnahmen zu den folgenden Tagesordnungspunkten planen,

- DPIA-Berichte
- Abweichungen zu Compliance-Aspekten
- Berichte über Aktivitäten nach der Lieferung
- Aktionsplan zur Lösung aller offenen Posten
- Verbesserungsmöglichkeiten und erforderliche Änderungen im System

GDPR COMPLIANCE-AUDIT

Wenn der Grad der Vorbereitung ein angemessenes Niveau erreicht hat, beginnt der Compliance-Prozess. Die Zertifizierung beginnt. Ein ernannter Auditor der Zertifizierungsstelle (CB) überprüft die Vorbereitung über ein externes Audit. Dazu gehört, dass der Prüfer die Richtlinien, Prozesse und SOPs kritisch überprüft Betriebsaufzeichnungen sowie IA- und MRM-Aufzeichnungen. Alle größeren Abweichungen von den Erwartungen der CB werden an dieser Stelle benachrichtigt, um die erforderlichen Korrekturen vorzunehmen. Dies verringert die Wahrscheinlichkeit von wesentlichen Abweichungen während des Zertifizierungsaudits. TOPCertifier wird mit allen zusammenarbeiten Stakeholder und überwachen den reibungslosen Abschluss des Audits.

FORTSETZUNG DER COMPLIANCE

TOPCertifier wird Teil der Compliance-Reise Ihres Unternehmens sein und Sie regelmäßig unterstützen Intervalle mit notwendigen Schulungen, Systembetreuung und Schulungen, internen und externen Audits und regelmäßige Erneuerung Ihrer Compliance-Zertifizierung.