



**ANTARES
NETLOGIX**

FACTSHEET

EU-Datenschutz-Grundverordnung

DATA PROTECTION

Die EU-Datenschutz-Grundverordnung wurde 2018 für alle Unternehmen, Behörden und öffentlichen Einrichtungen wirksam. Wir helfen Ihnen bei der Umsetzung komplexer Maßnahmen, um die rechtlichen Vorschriften in Ihrem Unternehmen einzuhalten. Im Fokus steht die Konvergenz von Recht, IT und Organisation.



DIE DATENSCHÜTZER

Wir begleiten Sie auf dem Weg.

Seit 2018 sind Unternehmen gefordert, der neuen DSGVO zu entsprechen. Zusätzlich gibt es auch nationale Gesetze, die zu beachten sind. In Kooperation mit Techsoft Datenverarbeitung und iQSol haben wir **DIE DATENSCHÜTZER** ins Leben gerufen.

DATENSCHUTZ IST KEIN IT-THEMA

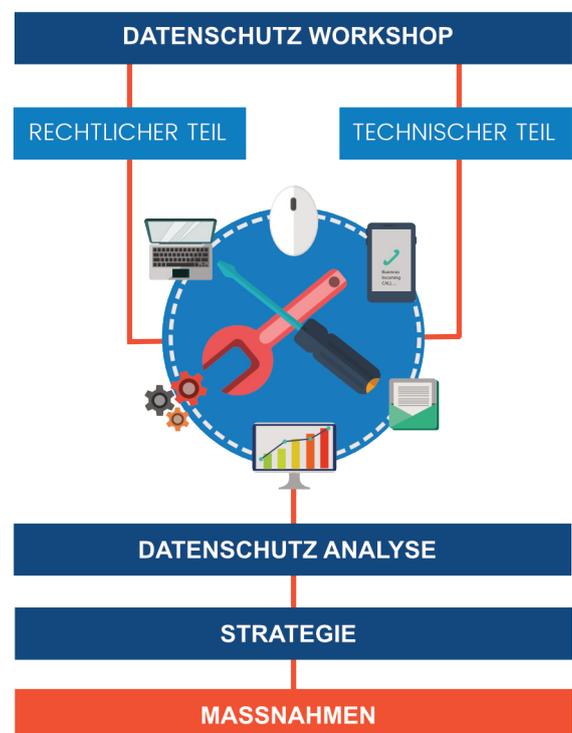
Da das Thema Datenschutz eigentlich kein Security-Thema ist, sollte auch die IT-Abteilung außen vor gehalten werden und lediglich als "Aufgaben-Erfüller & Informationszuträger" gesehen werden.

Starke Involvierung des Personalmanagements ist aber ebenso erforderlich, wie das prozessuale Vorgehen und Handeln der Stellen, die für Qualitätsmanagement/Zertifizierungen und ISO-Standards zuständig sind.

Hier ist im Idealfall auch der weisungsfreie Datenschutzbeauftragte angesiedelt.

SO FUNKTIONIERT'S

Schritt für Schritt zur DSGVO!



Besuchen Sie uns auf:

www.diedatenschuetzer.at



DIE DATENSCHÜTZER

rechtlicher und technischer Datenschutz

www.netlogix.at

ANLASS FÜR DATENSCHUTZMASSNAHMEN

Ihre Anforderungen

Es gibt viele Gründe, sich für mehr Sicherheit zu entscheiden. Aktuell gibt es fünf große Themen, die Unternehmen empfindlich treffen können. Jede dieser Bedrohungen ist mit hohen Kosten verbunden, bei manchen wird zusätzlich auch die Reputation des Unternehmens geschädigt.

! CYBER INSURANCE - PRÄMIENGESTALTUNG

Denken Sie über eine Cyber-Versicherung nach? Achtung, die Versicherer prüfen zuerst Ihre Infra-Struktur und erhöhen bei geringen Sicherheits-standards die Prämie.

Diese Module unterstützen Sie: Modul 1, Modul 2.2, 2.3, 2.4, Modul 3.1, 3.2, 3.3, 3.4, Modul 4, Modul 5.1, 5.2, 5.3, 5.5, Modul 6.1, 6.2, 6.3, Modul 8

! SCHADEN DURCH BETRUG

Phishing war gestern - heute werden große Fische gejagt. Mit "Whaling" werden ganz gezielt Mitarbeiter aus dem oberen Management geködert. Seien Sie wachsam!

Diese Module unterstützen Sie: Modul 1,1 Modul 2.1, 2.6, 2.7, 2.8, Modul 3.5, Modul 7

! SCHADEN DURCH DATENDIEBSTAHL

Ihre Daten sind wertvoll für Ihr Unternehmen - aber auch für den Wettbewerb. Mit unseren Modulen lassen Sie Datendieben keine Chance.

Diese Module unterstützen Sie: Modul 1, Modul 2.1, 2.3, 2.6, 2.7, 2.8, Modul 3.3, 3.4, Modul 7, Modul 8.3, 8.4

! SCHADEN DURCH IT-AUSFÄLLE

Ein Ausfall Ihrer IT-Systeme kann Ihren gesamten Betrieb lahmlegen. Gehen Sie kein Risiko ein und sichern Sie sich ab!

Diese Module unterstützen Sie: Modul 2.2, 2.3, 2.4, 2.5 Modul 3.1, 3.2, 3.3, 3.4, 3.6, 3.7 Modul 4, Modul 5, Modul 8.1, 8.3

! DSGVO-STRAFPRÄVENTION

Die Datenschutzbehörde kann Strafen bis zu 4 % vom Umsatz verhängen - gehen Sie auf Nummer sicher und stellen Sie Ihr Unternehmen DSGVO-konform auf.

Diese Module unterstützen Sie: Modul 1, Modul 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, Modul 3.1, 3.2, 3.3, 3.4, 3.6, 3.7 Modul 4, Modul 5.1, 5.2, 5.3, 5.5 Modul 6.1, 6.2, 6.3, 6.5, 6.6, Modul 8

TIPP VOM DATENSCHUTZBEAUFTRAGTEN

Der Start in die Welt des Datenschutzes ist für viele Unternehmen eine Reise ins Unbekannte. Beginnen Sie mit unseren beiden Workshops auf technischer und rechtlicher Ebene, um eine erste Struktur zu schaffen. In zwei Tagen wird der Ist-Stand Ihrer Infrastruktur und Organisation erfasst, und Sie erfahren alle wesentlichen Elemente der Datenschutz-Grundverordnung.

Mit den Ergebnissen dieser beiden Workshops sind Sie gut aufgestellt für die Zukunft. Sie bekommen einen konkreten Zeitplan und eine Liste mit Punkten, die empfohlen bzw. vorgeschrieben sind. Mit dieser Struktur können Sie die nächsten Schritte mit internen Res-sourcen oder auch mit bestehenden Partnern umsetzen.



DI (FH) Gerhard Kratschmar

Als zertifizierter Datenschutzbeauftragter bei Antares-NetlogiX und ehemaliger Berufspilot sowie Safety & Security Manager im weltweiten Einsatz, unterstützt Sie Gerhard Kratschmar bei der Umsetzung der DSGVO.

MODULÜBERSICHT

Schritt für Schritt zur EU-DSGVO!

Unsere Beratung und Unterstützung startet stets mit einem Datenschutz-Workshop und einer entsprechenden Analyse der aktuellen Situation. Danach stehen wir Ihnen bei der Ausarbeitung der Umsetzungsstrategie zur Seite und helfen Ihnen, die notwendigen Maßnahmen anhand unseres modularen Aufbaus Schritt für Schritt umzusetzen.

1 VERSCHLÜSSELUNG

- 1.1 E-Mail-Verschlüsselung
- 1.2 Datei-Verschlüsselung
- 1.3 Datenbank-Verschlüsselung
- 1.4 Cloud-Verschlüsselung

2 VERTRAULICHKEIT

- 2.1 Identitäts- & Berechtigungsmanagement
- 2.2 Datenschutzkonforme Protokollierung
- 2.3 System-Integritäts-Monitoring
- 2.4 Enterprise-Passwort-Management
- 2.5 Netztrennung/Zugangskontrolle
- 2.6 Privileged Access Management
- 2.7 Multifaktor-Authentifizierung
- 2.8 Schnittstellensicherheit

3 INTEGRITÄT

- 3.1 Wiederanlauf Rechenzentrum
- 3.2 Wiederanlauf Hub-Location
- 3.3 Datenarchivierung
- 3.4 Datenwiederherstellung
- 3.5 Advanced Threat Protection
- 3.6 Schwachstellen-Management
- 3.7 Patch-Management

4 VERFÜGBARKEIT

- 4.1 Co-Location
- 4.2 Geo Load Balancing
- 4.3 Failover-Architektur
- 4.4 Betriebshandbuch
- 4.5 Notfallhandbuch

5 QUALITÄTSSICHERUNG IM BETRIEB

- 5.1 Datenschutz-(Re-)Audit
- 5.2 Verfügbarkeits- und Infrastruktur-Audit
- 5.3 (regelmäßige) Risiko-Analyse
- 5.4 Forensische Analyse und Bewertung
- 5.5 (regelmäßige) Failover/Desaster-Test

6 COACHING & SCHULUNG

- 6.1 (externer) Datenschutzbeauftragter
- 6.2 Schulung Datenschutzbeauftragter
- 6.3 Erstellung von Datenschutzrichtlinien
- 6.4 Datenschutz Folgeabschätzungen
- 6.5 Verzeichnisse
- 6.6 Softwareentwicklung "privacy by design"

7 AWARENESS

- 7.1 Sicherheitsrichtlinien
- 7.2 Security-Awareness-Strategie
- 7.3 Security-Awareness-Training
- 7.4 Security-Awareness-Newsletter

8 CLOUD SERVICES & OUTSOURCING

- 8.1 Vertragsaudit bestehender Leistungen
- 8.2 Vertragsaudit DSGVO-Konformität
- 8.3 Technischer Infrastruktur-Audit
- 8.4 Technischer Security-Audit

EU-DSGVO: GESETZESANFORDERUNGEN

Mit unseren Modulen decken Sie folgende Gesetzesanforderungen ab:

EU-DATENSCHUTZ-GRUNDVERORDNUNG

MODULE

Artikel 25 – Datenschutzfreundliche Voreinstellungen	6.6 Softwareentwicklung "privacy by design"
Artikel 28 – Auftragsverarbeiter	8.1 Vertragsaudit bestehender Leistungen 8.2 Vertragsaudit DSGVO-Konformität 8.3 Technischer Infrastruktur-Audit 8.4 Technischer Security-Audit
Artikel 30 – Verarbeitungstätigkeiten	6.5 Erstellung Verfahrensverzeichnis
Artikel 32 (1) (a) Pseudonymisierung und Verschlüsselung	1.1 E-Mail-Verschlüsselung 1.2 Datei-Verschlüsselung 1.3 Datenbank-Verschlüsselung 1.4 Cloud-Verschlüsselung
Artikel 32 (1) (b) Vertraulichkeit sicherstellen	2.1 Identitäts- & Berechtigungsmanagement 2.2 Datenschutzkonforme Protokollierung 2.4 Enterprise Passwort Management 2.7 Multifaktor-Authentifizierung 2.8 Schnittstellensicherheit
Artikel 32 (1) (b) Integrität sicherstellen	2.3 System-Integritäts-Monitoring 2.6 Privileged Access Management 3.1 Wiederanlauf Rechenzentrum 3.2 Wiederanlauf Hub-Lokation 3.3 Daten-Archivierung 3.4 Daten-Wiederherstellung 3.5 Sandboxing 3.6 Schwachstellen-Management 3.7 Patch-Management
Artikel 32 (1) (b) Verfügbarkeit / Belastbarkeit der Systeme und Dienste	4.1 Co-Location 4.2 Geo Load Balancing 4.3 Failover-Architektur
Artikel 32 (1) (c) Wiederherstellung der Daten und des Zugriffs darauf bei technischem oder physischem Zwischenfall	4.4 Betriebshandbuch 4.5 Notfallhandbuch
Artikel 32 (1) (d) Regelmäßige Überprüfung der Maßnahmen	5.1 Datenschutz-(Re-)Audit 5.2 Verfügbarkeits- und Infrastruktur-Audit 5.5 Failover/Desaster-Test
Artikel 32 (2) Risikobewertung	5.3 Risikoanalyse
Artikel 32 (4) Sicherstellung, dass personenbezogene Daten nur auf Anweisung verarbeitet werden.	2.1 Identitäts- & Berechtigungsmanagement 2.2 Datenschutzkonforme Protokollierung 2.4 Enterprise-Passwort-Management 2.6 Privileged Access Management 6.3 Erstellung von Datenschutz-Richtlinien
Artikel 33 Meldungen von Verletzungen an die Aufsichtsbehörde	5.4 Forensische Analyse und Bewertung
Artikel 33 (5) Dokumentation der Verletzungen inkl. aller Fakten zur Überprüfung durch die Aufsichtsbehörde	2.2 Datenschutzkonforme Protokollierung 5.4 Forensische Analyse und Bewertung
Artikel 35 (1) Abschätzung für neue Verarbeitungsvorgänge	6.4 Datenschutz Folgeabschätzung
Artikel 37 – Datenschutzbeauftragter	6.1 Externer Datenschutzbeauftragter 6.2 Schulung Datenschutzbeauftragter
Artikel 47 – Verbindliche interne Datenschutzvorschriften	6.1 Externer Datenschutzbeauftragter 6.2 Schulung Datenschutzbeauftragter 6.3 Erstellung Datenschutzrichtlinien 6.4 Datenschutz Folgeabschätzung 7.1 Sicherheitsrichtlinien 7.2 Security-Awareness-Strategie 7.3 Security-Awareness-Training 7.4 Security-Awareness-Newsletter



Antares-Netlogix Netzwerkberatung GmbH

Feldstraße 13, A-3300 Amstetten

T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at