COMPACT

Kurz und knapp und schnell gelesen!

microPLAN SK.NET DATENSCHUTZ

Schutz vor missbräuchlicher Datenverarbeitung

microPLAN
SK.NET GmbH - Düsseldorf
Ihre IT - einfach gemacht

microPLAN SK.NET DATENSCHUTZ

Schutz vor unberechtigten Zugriffen

Beim Thema Datenschutz geht es nicht um den Schutz der Daten im klassischen Sinne. Der Datenschutz regelt sowohl die Voraussetzungen als auch die Folgen einer personenbezogenen Erhebung und Verwendung von Daten (Name, Alter, Geschlecht).

microPLAN SK.NET bietet Ihnen durch einen externen Datenschutzbeauftragten ein individuelles und rechtskonformes Datenschutz- und IT-Sicherheitskonzept, indem der externe Datenschutzbeauftragte für Sie die datenschutzrechtliche Umsetzung in Ihrem Unternehmen prüft und eine Bestandsaufnahme des Ist-Zustandes durchführt.

microPLAN
SK.NET GmbH - Düsseldorf
Ihre IT - einfach gemacht

EXTERNER DATENBEAUFTRAGTER

Die Aufgaben

Datenschutzbeauftragte betreuen und pflegen das Datenschutzmanagement und sichern die Kontrolle der Wirksamkeit sowie die Weiterentwicklung des Datenschutzes im Unternehmen. Dazu gehören auch die Schulung und Sensibilisierung der Mitarbeiter.

Sofern in Ihrem Unternehmen regelmäßig mindestens 20 Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten befasst sind, muss ein Datenschutzbeauftragter (DSB) schriftlich bestellt werden.

Mit allen personenbezogenen Daten muss in Ihrem Hause verantwortungsbewusst umgegangen werden, denn wird der Datenschutz verletzt, drohen nicht nur hohe Geldstrafen, weitreichender ist der Imageschaden für Ihr Unternehmen.

Die Einhaltung hoher Datenschutzstandards ist für Zertifizierungen zwingend nachzuweisen und wirkt sich häufiger positiv bei der Auftragsvergabe aus und ist als vertrauensbildende Maßnahme ein wichtiges Instrument zur Kundengewinnung.

UNSERE LÖSUNGSANGEBOTE

Sicher ist sicher

• Erstbriefing für Entscheider, kostenfreie, unverbindliche Bedarfsanalyse – Wir prüfen, ob Sie der Pflicht zur Bestellung eines Datenschutzbeauftragten unterliegen.

• Datenschutz First-Check – Ist-Aufnahme und Analyse zum Festpreis: Diese bestehen aus einer ca. einstündigen Befragung und Auswertung mit Handlungsempfehlungen.

• Externer unabhängiger Datenschutzbeauftragter – Auf Basis eines Geschäftsbesorgungsvertrages und einer schriftlichen Bestellung übernimmt der externe Datenschutzbeauftragte die gesetzlich vorgeschriebenen Aufgaben und Pflichten im Datenschutz für Ihr Unternehmen.

• Datenschutzberatung – Für den Fall, dass in Ihrem Unternehmen kein Datenschutzbeauftragter notwendig ist, stehen wir Ihnen dennoch gerne beratend für datenschutzrelevante Themen zur Verfügung.

• Datenschutzaudit – Im Rahmen eines Datenschutzaudits prüft der externe Datenschutzbeauftragte die Umsetzung der gesetzlich vorgeschriebenen Maßnahmen zum Bundesdatenschutzgesetz.

• Datenschutzprojekte – Wir unterstützen Sie als Projektleiter oder im Projektteam bei der Planung und Umsetzung gezielter Maßnahmen zur Verbesserung des Datenschutzniveaus in Ihrem Unternehmen.

• ISO-Zertifizierung – Die ISO 9001 legt die Mindestanforderungen an ein Qualitätsmanagementsystem fest, die von Unternehmen umzusetzen sind. Wir prüfen, worauf Sie in diesem Zusammenhang achten müssen.

• Mitarbeiterschulung – Neben der Betreuung und Pflege des Datenschutzmanagements übernimmt der externe Datenschutzbeauftragte auch die Schulung und Sensibilisierung der Mitarbeiter, die mit personenbezogenen Daten arbeiten.

DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG

Anwendungsbereiche und Pflichten

Seit Mai 2018 sind die Unternehmen der EU-Datenschutzgrundverordnung verpflichtet, die europaweit für viele neue Auflagen und Sanktionen verantwortlich ist. Unternehmen sind rechtlich verpflichtet, sich um die Aufstellung ihrer IT-Sicherheit und die Prozesse ihres Informationsmanagements zu kümmern und die gesetzlichen Regeln umzusetzen.

Die neuen Datenschutz-Regularien der 28 EU-Staaten sehen eine Modernisierung und Vereinheitlichung in Unternehmen vor. Unternehmen müssen dann beispielsweise Datendiebstahl innerhalb von 72 Stunden den Behörden melden. Außerdem können Datenschutzverstöße mit Bußgeldern von bis zu vier Prozent des Jahresumsatzes des Mutterunternehmens geahndet werden.

Die neue EU-Datenschutz-Grundverordnung sollte als Chance begriffen werden, den Umgang des Unternehmens mit geschäftskritischen Unternehmens- und Nutzerdaten auf den Prüfstand zu stellen. Damit schaffen Firmen ein Bewusstsein für den Wert und die Wichtigkeit der vorhandenen und genutzten Daten und können Wege entwickeln, die existierenden Daten anders zu nutzen, um Wettbewerbsvorteile zu generieren und gleichzeitig die gesetzlichen Vorschriften einzuhalten

DER microPLAN SK.NET FAHRPLAN
zur neuen Datenschutz-Grundverordnung

Mit nachstehendem Fahrplan unterstützen wir Sie dabei, Ihr Unternehmen für die neuen Regeln der Datenschutz-Grundverordnung fit zu machen.

1: Definieren Sie einen umfangreichen Rahmen und eine Strategie für digitale Sicherheit

Unternehmen sollten die Daten priorisieren, die sie sichern müssen, und somit die Informationssicherheit an die Geschäftsziele knüpfen.

2: Stellen Sie Ihre Daten in den Fokus – Registrierung, Klassifizierung, Verschlüsselung und Speicherung

Nur Unternehmen, die den Wert der Daten verstehen, können angemessene Schutzmaßnahmen ergreifen, um diese zu schützen. Versuchen Sie nicht, alles zu schützen, sondern konzentrieren Sie sich auf die kritischen Daten. Das reduziert nicht nur deutlich den Zeitaufwand für die Implementierung der richtigen Technologie und die Personalschulung, sondern ermöglicht außerdem eine zusätzliche Wertschöpfung.

3: Führen Sie ein komplettes Audit der gegenwärtigen und wahrscheinlichen Risiken durch

Unternehmen sollten zunächst identifizieren, welche Daten geschäftskritisch sind, wo diese liegen und wer darauf Zugriff hat. Die detaillierte Klassifizierung der Daten nach Typ, Inhalt und Nutzung bestimmt dann die passenden Technologien, Systeme und Prozesse, die für den wirkungsvollen Schutz und die Verwaltung der jeweiligen Daten angewendet werden müssen.

Wichtig ist, dass Unternehmen einen zentralen Regelsatz für Sicherheit, Compliance und Verhaltensregeln etablieren, der über den gesamten Lebenszyklus der Information hinweg angewendet wird. Zudem sollten Unternehmen dafür sorgen, dass Informationen regelmäßig durch ein Backup gesichert werden.

4: Bauen Sie Security von Beginn an in alle Prozesse ein (Security by Design)

Mitarbeiter sollten im Bereich Security und Datenschutz umfassend geschult werden, denn eines der größten Risiken für die Sicherheit der Daten geht von innen aus. Dabei handelt es sich meistens nicht um eine mutwillige Gefährdung oder Entwendung der Daten, sondern um fahrlässige Handlungsweisen, die die Unternehmenssicherheit in Gefahr bringen.

5: Bereiten Sie sich auf den unvermeidlichen Ernstfall vor

Auch wenn alle Sicherheitsmaßnahmen vorbildlich umgesetzt werden, empfiehlt es sich, den Ernstfall zu proben und sich auch gegebenenfalls auf behördliche Anweisungen vorzubereiten. Dazu gehören Maßnahmen zur

- **Reaktion** – um den Schaden einzudämmen
- **Kommunikation** – um Kunden und die Öffentlichkeit über Datenvorfälle zu informieren. Hier kommt es auf eine akkurate und schnelle Kommunikation an.
- **Wiederherstellung** – um verlorengegangene Daten wiederherzustellen, widerstandsfähig gegen Cyberattacken zu bleiben und während und nach dem Vorfall den Betrieb aufrechtzuerhalten.

IHR ANSPRECHPARTNER

- Benedikt Lohkemper
  b.lohkemper@microplan-sknet.de

DATEV SOLUTION PARTNER

EVault from Carbonite Preferred Partner

DataCore SOFTWARE

Microsoft CERTIFIED Partner

hp

vmware PROFESSIONAL SOLUTION PROVIDER

STARFACE EXCELLENCE PARTNER

veeam GOLD propartner

serviceconnect

microPLAN SK.NET GmbH

Wanheimer Str.68
40468 Düsseldorf

Fon (02 11) 369 75-0
Fax (02 11) 369 75-99

info@microplan-sknet.de
www.microplan-sknet.de