Die Treuhand im Westen

VdW

Assekuranzmakler
Betriebswirtschaft
Finanzmanagement

Auf der sicheren Seite

Informationen zur europäischen Datenschutz-Grundverordnung (DSGVO)

Ab dem 25. Mai 2018 gilt europaweit ein neues Datenschutzrecht: **die Datenschutz-Grundverordnung (DSGVO).** Im Zuge der neuen Gesetzgebung werden die nationalen Datenschutzvorschriften abgelöst – das bisher geltende Bundesdatenschutzgesetz (BDSG) bekommt zeitgleich mit der DSGVO eine ergänzende Neufassung für nationale Sonderregelungen und regelt teilweise Tatbestände anders und doppelt. Für Unternehmen hat die neue Gesetzeslage weitreichende Folgen. Sie stehen in der Pflicht, den gesamten bisherigen Datenschutzprozess im Hinblick auf die DSGVO zu überprüfen und anzupassen. Bei Verstößen gegen das neue Recht drohen empfindliche Strafen. Was Sie im Detail beachten müssen und wie Sie die neue Verordnung umsetzen, erfahren Sie auf den folgenden Seiten.

SCHRITT 1
DIE AUSGANGSLAGE

1. Der IST-Zustand

Der gesamte aktuelle Maßnahmenstand zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss unter Einbeziehung der unternehmensinternen Datenschutzorganisation eingehend analysiert und geprüft werden.

Das bedeutet unter anderem:

- Vollständige Analyse der bestehenden Unternehmens-Datenschutzprozesse
- Prüfung bestehender Dokumentationen wie Verfahrensverzeichnisse oder IT-Sicherheitskonzepte
- Prüfungen aller Dienstleistungsbeziehungen insbesondere im Hinblick auf Auftragsdatenverarbeitung
- Prüfung möglicher vorhandener Betriebsvereinbarungen

2. Der SOLL-Zustand

Um den SOLL-Zustand, also die Konformität mit der DSGVO zu gewährleisten, ergeben sich aus der Prüfung des IST-Zustands klare Handlungsaufträge in Form eines Maßnahmenkatalogs.

Folgende Aspekte spielen dabei eine wesentliche Rolle:

Rechtsgrundlage

Die Verarbeitung personenbezogener Daten benötigt zwingend eine Legitimationsgrundlage. Bei bestehenden Einwilligungen muss überprüft werden, ob diese den neuen Anforderungen an eine wirksame Einwilligung (Art. 7 DSGVO) entsprechen.

Betroffenenrechte

Personen, deren Daten verarbeitet werden, genießen umfangreiche Rechte. Dazu zählen z.B. Informationspflichten, Auskunftsrecht, Recht auf Berichtigung, Widerspruch und Löschung, Recht auf Datenübertragbarkeit.

Privacy by Design und Privacy by Default

Alle Anwendungen und Voreinstellungen müssen ausnahmslos datenschutzfreundlich gestaltet sein.

Dienstleistungsbeziehungen

Die Artikel 28 und 29 der DSGVO sehen spezielle Vorgaben für Dienstleistungsbeziehungen vor. Bestehende Verträge müssen daher auf die mögliche Klassifizierung als Auftragsverarbeitung überprüft werden.

Dokumentationspflichten

Die DSGVO sieht eine Rechenschaftspflicht zur rechtmäßigen Verarbeitung personenbezogener Daten vor. Das bedeutet, dass datenschutzrelevante Vorgänge oder Regelungen dokumentiert und nachgewiesen werden müssen. Dokumentationspflichten gibt es zusätzlich in vielen weiteren Bereichen – etwa für das Verarbeitungsverzeichnis (Art. 30), für die Dokumentation von Datenschutzvorfällen (Art. 33 Abs. 5) oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung (Art. 28 Abs. 3 lit.a).

Datenschutz-Folgenabschätzung

Die DSGVO sieht in Artikel 35 und 36 eine umfangreiche Dokumentation (bis hin zur Einbeziehung der Aufsichtsbehörde) über die Notwendigkeit und Durchführung einer Datenschutz-Folgenabschätzung (DSFA) vor.

Meldepflichten

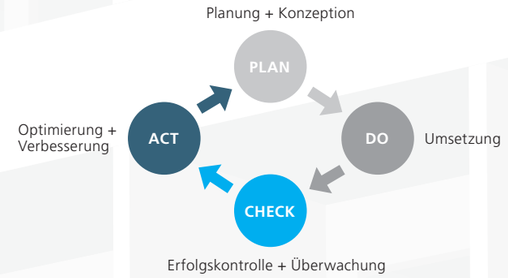
Entsprechend Artikel 37 Abs. 7 der DSGVO müssen die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde gemeldet werden. Eine Meldepflicht besteht darüber hinaus für die Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 1).

Datensicherheit

Um einen angemessenen Schutz bei der Datenverarbeitung zu gewährleisten, müssen Unternehmen gemäß DSGVO Artikel 24 und 32 Sicherungssysteme implementieren, die regelmäßig überprüft werden.

SCHRITT 2
DATENSCHUTZMANAGEMENT ETABLIEREN

Nach der Analyse und der Prüfung des IST-Zustands folgt die Umsetzung des neuen Datenschutzmanagements gemäß DSGVO. Am Effizientesten ist die Umsetzung, wenn sich alle definierten Maßnahmen am PDCA-Zyklus orientieren:



1. Datenschutzkonzept erstellen

Das Datenschutzkonzept enthält alle Prozesse, Verfahrensanweisungen, Richtlinien und verantwortliche Personen. Die Unternehmensführung muss sich zum Datenschutz und zur Gewährleistung der Vertraulichkeit, der Verfügbarkeit und der Authentizität von personenbezogenen Daten in der Informationsverarbeitung bekennen. Der Datenschutzbeauftragte, interne Dateschutzkoordinatoren, IT-Verantwortliche oder sonstige Verantwortliche müssen benannt werden.

2. Einführung eines Prozesses zur Melde- und Dokumentationspflicht bei Datenschutzverletzungen

Im Rahmen der DSGVO Melde- und Dokumentationspflicht muss die konkrete Vorgehensweise bei Datenschutzverletzungen festgelegt werden. Dies umfasst interne und externe Prozesse und ist idealerweise direkt im Datenschutzkonzept eingebunden.

3. Einführung eines Prozesses zur Beachtung der Betroffenenrechte

Jeder Mitarbeiter, der personenbezogene Daten erhebt, verarbeitet oder nutzt, muss über die Betroffenenrechte aufgeklärt und informiert werden. Dies umfasst auch Richtlinien zum korrekten Verhalten bei Anfragen.

4. Einführung eines Prozesses zur Datenschutz-Folgenabschätzung

Es gilt eine eindeutige Regelung zu definieren, wann eine Datenschutz-Folgenabschätzung durchgeführt werden muss, wer genau diese durchführt und wie die Durchführung dokumentiert wird.

5. Mitarbeiterschulung

Ein Großteil der Datenschutzverletzungen wird meistens unbewusst von den eigenen Mitarbeitern verursacht.
Alle Personen, die mit personenbezogenen Daten arbeiten, müssen zum Thema geschult und sensibilisiert werden.

6. Dokumentation der Datenflüsse (weltweit)

Um zuverlässige und sichere Datenübermittlungen zu garantieren, muss der gesamte Unternehmensdatenfluss transparent gemacht und dokumentiert werden. Die Dokumentation kann anschließend auch für das Verzeichnis von Verarbeitungstätigkeiten verwendet werden.

Die Treuhand im Westen

VdW

Assekuranzmakler
Betriebswirtschaft
Finanzmanagement

7. Verzeichnis von Verarbeitungstätigkeiten

Das DSGVO verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Das Verzeichnis umfasst alle automatisierten und nichtautomatisierten Datenverarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

8. Löschkonzept

Sobald der Zweck der Speicherung entfallen ist oder die gesetzliche Grundlage/Erfordernis müssen personenbezogene Daten gelöscht werden. Die Einrichtung und Umsetzung eines unternehmensweiten Löschkonzepts ist daher notwendig.

9. Technische und organisatorische Maßnahmen (ToM)

Die ToM-Anforderungen bleiben mit dem DSGVO nahezu unverändert. Einzig die Begrifflichkeiten haben sich verändert und müssen entsprechend angepasst werden. Ergänzt werden die ToMs jedoch durch den Aspekt der Risikoeinschätzung und -bewertung, die mit in der Verantwortung des Datenschutzbeauftragten liegen.

10. Auftragsverarbeitung

Die Regelungen für Auftragsdatenverarbeitungen werden mit der DSGVO wesentlich verschärft und Auftragnehmer sind zukünftig mitverantwortlich für die Datenverarbeitung. Auftragsverarbeiter haben somit zunehmende Dokumentationspflichten. Im Gegensatz zum bisherigen Bundesdatenschutzgesetz sind nun auch Auftragsverarbeiter verpflichtet, ein Verarbeitungstätigkeitsverzeichnis zu führen. Dies erfordert eine Überprüfung, Neubewertung und ggf. Neuverfassung aller bestehenden Verarbeitungsverträge.

11. Anpassung der Datenschutz- und IT-Richtlinien

Die DSGVO-konforme Umsetzung von Datenschutz und Informationssicherheit verlangt die Neueinführung bzw. Anpassung einer Vielzahl von Anweisungen und Richtlinien bezüglich Datensicherung, Hardwarenutzung, Nutzer- und Adminrechte u. v. m.

12. Anpassung weiterer Datenschutzdokumente: Mustereinwilligungen, Musterverträge usw.

Einwilligungserklärungen, Formulare zur Erfüllung der Transparenzpflicht und Datenschutzerklärungen sind nach Vorgaben der DSGVO zu überarbeiten bzw. einzuführen.

13. Anpassung bestehender Mitarbeiter- oder Betriebsvereinbarungen

Mit den veränderten Anforderungen der DSGVO verändern sich auch Mitarbeiter- oder Betriebsvereinbarungen. Das heißt, eine Überprüfung und Anpassung ist auch hier notwendig.

SCHRITT 3
DATENSCHUTZMANAGEMENT UMSETZEN

Zur Umsetzung des Datenschutzmanagements macht die DSGVO konkrete Vorgaben. Speziell Ihrem Datenschutzbeauftragten kommt eine besondere Bedeutung zu:

- Unterrichtung und Beratung der Verantwortlichen und der Mitarbeiter in allen Datenschutz-Fragen
- Permanente Überwachung und Sicherstellung der Einhaltung der Datenschutzvorschriften
- Mitarbeiterschulung und -sensibilisierung sowie Überprüfung der an Datenverarbeitungsvorgängen beteiligten Mitarbeiter
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und Überwachung der Umsetzung
- Ansprechpartner und Schnittstelle für die Aufsichtsbehörde

Frank Vohwinkel
VdW Treuhand GmbH, Kanzlerstr. 2, 40472 Düsseldorf
Tel.: 0211 9599-0, Fax: 0211 9599-211, Mobil: 0151 41 91 42 33
vohwinkel@vdw-treuhand.de