Mittelstand 4.0
Kompetenzzentrum
Cottbus

DATENSCHUTZGRUND-VERORDNUNG (DSGVO)

für kleine und mittelständische Unternehmen

www.kompetenzzentrum-cottbus.digital

Mittelstand-
Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IMPRESSUM

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o IHP GmbH - Innovations for High Performance Microelectronics/
Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
15236 Frankfurt (Oder)
info@kompetenzzentrum-cottbus.digital
Telefon: +49 355 695171

Handelsregister beim Amtsgericht: Frankfurt (Oder)
Registernummer: HRB1982

Umsatzsteuer-Identifikationsnummer gemäß §27 a
Umsatzsteuergesetz: DE 138996546

Vertretung: Geschäftsführer Prof. Dr. Bernd Tillack und Manfred Stöcker

Autor: Stephan Kornemann - IHP GmbH

Satz/Layout: maerkbar – Cottbus

Bildnachweis: Umschlag © pixabay/andibreit

In der Datenschutzgrundverordnung (DSGVO) geht es um den Schutz von Daten von EU-Bürgern. Die Umsetzung der DSGVO betrifft fast alle Unternehmen. Diese Broschüre bietet Ihnen die notwendigen Informationen, um entscheiden zu können, ob bzw. wie sie die DSGVO umsetzen müssen. Zunächst erläutern wir die in Art. 5 der DSGVO aufgeführten sieben Grundsätze.

DSGVO – GRUNDSÄTZE

Am Beispiel eines kleinen Heizungsbauunternehmens namens Heizungs-Muster-Bau GmbH (HMB GmbH) sollen die Grundsätze der DSGVO erläutert werden. Das Unternehmen betreibt neben den eigentlichen Aufbau- und Wartungsarbeiten zusätzlich einen Online-Shop für Heizungsteile.

1 Rechtmäßig, fair & transparent

Der erste Grundsatz fordert die rechtmäßige und nachvollziehbare Verarbeitung von personenbezogenen Daten. Des Weiteren muss eindeutig definiert sein wie und wo die personenbezogenen Daten gespeichert und an wen diese Daten evtl. weitergegeben werden.

> *Im Unternehmen HMB GmbH werden Personaldaten und Kundendaten verarbeitet. Für die Lohnabrechnung werden Daten wie z.B. Familienstand, Alter und Konfessionszugehörigkeit benötigt. Um Dienstleistungen zu erbringen, muss die Adresse der Kunden vorliegen.*

2 Zweckbindung

Der zweite Grundsatz beschäftigt sich mit der Zweckmäßigkeit der erhobenen personenbezogenen Daten. Diese dürfen ausschließlich für den vereinbarten Zweck genutzt werden.

> *Erhobene Kundendaten, die ausschließlich für den Zweck der Wartung gespeichert wurden, dürfen nicht für Werbezwecke des Online-Shops verwendet werden.*

3 Datenminimierung (Datensparsamkeit und Datenvermeidung)

Datenminimierung meint, dass ausschließlich die Daten gespeichert werden sollten, die für die Erfüllung des Zweckes benötigt werden.

Für den Newsletter des Online-Shops werden nur die E-Mail-Adressen der Interessierten benötigt. Sobald ergänzend der Name für eine persönliche Ansprache gespeichert wird, ist zusätzlich eine Einwilligung mit Begründung und der Angabe der Speicherdauer notwendig.

4 Richtigkeit und Aktualität

Der Grundsatz besagt, dass alle Daten sachlich richtig und – falls erforderlich – auf dem neuesten Stand sein müssen. Nicht mehr aktuelle oder unrichtige Daten erfordern eine unverzüglich Löschung oder Aktualisierung.

Es muss gewährleistet sein, dass z.B. bei der Lohnabrechnung alle personenbezogenen Daten korrekt sind und diese bei Unstimmigkeiten aktualisiert oder gelöscht werden.

5 Speicherbegrenzung

Die Speicherbegrenzung gibt die Zeitdauer an, wie lange personenbezogene Daten im System gespeichert bleiben. Die Daten dürfen nicht länger verarbeitet werden, als es für die bestimmten Zwecke notwendig ist. Ausnahmen gibt es bei öffentlichem Archiv-Interesse, bei wissenschaftlichen oder historischen Forschungszwecken.

Die gespeicherten personenbezogenen Daten für den Online-Shop-Newsletter müssen eine zeitliche Begrenzung haben. Diese kann z.B. auf ein Jahr gesetzt werden, somit muss eine Einwilligung jährlich erneuert werden.

6 Integrität und Vertraulichkeit

Der Grundsatz besagt: bei der Verarbeitung von personenbezogene Daten muss eine angemessene Sicherheit gewährleistet sein. Das heißt, die Daten müssen vor unbefugter Verarbeitung, unbeabsichtigter Zerstörung oder Schädigung geschützt werden. Wenn es zu einem Verlust/Datendiebstahl von sensiblen personenbezogenen Daten kommt, muss dieser innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde und bei den betroffenen Personen gemeldet werden.

Für die HMB GmbH bedeutet dies, dass z.B. nur die Personalabteilung Zugriff auf die Daten der Mitarbeiter haben darf. Einmal wöchentlich sollte ein komplettes sowie täglich inkrementelle Backups durchgeführt werden. So können die Daten z.B. bei Verlust durch Feuer wieder hergestellt werden.

UMSETZUNG DER DSGVO – SCHRITT FÜR SCHRITT

1 Zeit freimachen für den Weg zur DSGVO

Für die Durchführung der einzelnen Schritte muss genügend Zeit eingeplant werden, so dass eine gewissenhafte Bearbeitung der einzelnen Schritte gewährleistet werden kann. Aussagen über die voraussichtliche Dauer der Bearbeitung sind schwierig, da diese von der Komplexität oder Systematisierung der Arbeitsabläufe innerhalb des Unternehmens abhängt. Ein Unternehmen mit ca. 11 Mitarbeitern, das im Bereich „Social Media" arbeitet, hat ca. 2 Monate hierfür benötigt[1]. Bei diesem Unternehmen ist jedoch zu beachten, dass fast ausschließlich personenbezogene Daten verarbeitet werden.

2 Selbsteinschätzung durch Gap-Analyse

Die Gap-Analyse ist eine Methodik zur Identifizierung strategischer und operativer Lücken. Diese Methodik sollte Sie nicht abschrecken. Sie dient letztendlich dazu, die in Ihrem Unternehmen bestehenden Datenschutz-Strukturen in Bezug auf die Anforderungen der DSGVO zu untersuchen bzw. zu hinterfragen. Für die Analyse gibt es viele verschiedene Fragenbögen, welche unterschiedlich strukturiert sind. Am besten hat uns der interaktive Online-Fragebogen des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gefallen. Dieser ist auf der Webseite https://lda.bayern.de/tool/start.html zu finden. Es werden insgesamt 28 Fragen gestellt, welche durch das Auswählen von drei Möglichkeiten beantwortet werden. Sie sollten die Fragen sehr gewissenhaft beantworten, da sonst keine bzw. nur ungenügende Rückschlüsse auf Ihr Unternehmen gezogen werden können. Nach dem Beantworten aller Fragen erfolgt die Auswertung. Es werden insgesamt 100 Punkte vergeben, die sich in die Kategorien Datenschutzgrundsätze (12 Punkte), Betroffenenrechte (14 Punkte), Pflichten des Verantwortlichen (17 Punkte), Technischer Datenschutz (46 Punkte) und internationaler Datentransfer (11 Punkte) aufteilen. Die folgende Abbildung zeigt ein Ergebnis des Tests. Angezeigt werden die gewählten Antworten und die korrekten Antworten mit einer kurzen Erläuterung. So werden die notwendigen Schritte klarer. Punkt für Punkt sollten die Fragen und entsprechenden Antworten dann nochmal kritisch betrachtet und mit einem ausgewählten Gesprächspartner diskutiert werden. Gegebenenfalls ist eine Risikoanalyse durchzuführen.

[1] Florian Goldenstein, „Die EU-DSGVO: Was ist neu und was ist zu tun?", it-daily.net, eBook: „EU-DSGVO: Die Uhr tickt – alle Probleme gelöst?", 2018, Seite 17.

3 Bestellen eines Datenschutzbeauftragten (DSB)

Prinzipiell ist es sinnvoll einen DSB zu bestellen, auch wenn Ihr Unternehmen nicht dazu verpflichtet ist. So wird die Bedeutung der Einhaltung von Datenschutzrichtlinien deutlich und unterschiedliche Bereiche im Unternehmen können positiv verändert werden z.B. die Vermeidung nicht benötigter Daten. Aber es gibt klare Kriterien, die festlegen, ob Ihr Unternehmen einen DSB bestellen muss. Dies trifft zu, wenn Ihr Unternehmen eines oder mehrere der folgenden Kriterien erfüllt:

- Mehr als 9 Mitarbeiter nutzen und/oder erheben regelmäßig persönliche Daten mit Hilfe einer automatisierten Datenverarbeitung oder
- Mehr als 20 Personen sind beschäftigt.
- Neben der Anzahl der Mitarbeiter ist auch der Detailgrad der erhobenen personenbezogenen Daten zu betrachten. Wenn Daten Informationen über Rasse, ethnische Herkunft, politische Meinung, religiöse Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben verarbeitet werden, ist ebenfalls ein DSB notwendig.
- Die Bestellung ist ebenfalls notwendig, wenn die erhobenen Daten geschäftsmäßig genutzt werden.

Als DSB können Mitarbeiter oder fachkundige externe Dienstleister bestellt werden. Der DSB ist nicht selbst für die Durchführung der Datenschutzmaßnahmen verantwortlich, sondern darf Aufgaben delegieren. Er muss allerdings auf die Umsetzung und Einhaltung der Datenschutzmaßnahmen hinwirken. Der DSB kann sich u. U. strafbar machen, wenn er nicht in ausreichendem Umfang auf die Einhaltung der Datenschutzmaßnahmen im Unternehmen achtet. Deshalb sollte er seine Hinwirkungs- und Beaufsichtigungspflichten und –aktivitäten sorgfältig dokumentieren, um bei Verstößen sein korrektes Verhalten belegen zu können. Ein ausführliches Gutachten hinsichtlich der rechtlichen Stellung des DSB aus arbeits- und strafrechtlicher Sicht finden Sie unter:

www.bvdnet.de/wp-content/uploads/2017/11/DMP-BvD-e.V.-gutachterliche-Stellungnahme-31.07.2017.pdf

Wenn Sie einen DSB bestellt haben, stehen Sie in der Pflicht diesen bei der zuständigen Aufsichtsbehörde zu melden. Die Zuständigkeit richtet sich nach dem Sitz oder Hauptsitz des Unternehmens.

4 Verarbeitungsverzeichnis

Das Verarbeitungsverzeichnis dient zur Dokumentation aller Prozesse im Unternehmen im Zusammenhang mit der Verarbeitung personenbezogener Daten. Laut Art. 30 Abs. 5 DSGVO muss ein Verarbeitungsverzeichnis nicht geführt werden, wenn das Unternehmen weniger als 250 Mitarbeiter beschäftigt. Allerdings gibt es auch hier Ausnahmen. Unabhängig von der Anzahl der Mitarbeiter muss ein Verarbeitungsverzeichnis geführt werden, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Aber auch, wenn die Verarbeitung der personenbezogenen Daten regelmäßig bzw. eine Verarbeitung von besonderen Datenkategorien erfolgt.
Diese besonderen Kategorien beziehen sich auf:

- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Genetische sowie biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (z.B. Fingerabdruck eines Mitarbeiters)
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Das gilt auch für Daten, die kontinuierlich verarbeitet werden z.B. im Rahmen der Lohnabrechnung, Kundendatenverwaltung, usw.
Als Verarbeitung von Gesundheitsdaten gilt bereits die Speicherung/Archivierung von Krankmeldungen und Arbeitsunfähigkeitsbescheinigungen. Das heißt, für die Verarbeitung der Mitarbeiterdaten wird i. d. R. ein Verarbeitungsverzeichnis benötigt.
Die Erstellung und Führung eines Verarbeitungsverzeichnisses bedingt einen erheblichen Aufwand, aber es gibt auch Vorteile. Die Arbeit des Datenschutzbeauftragten wird erheblich erleichtert, da eine Übersicht über die zu verarbeitenden Daten vorhanden ist und Anfragen von Behörden schneller bearbeitet werden können.
Falls Sie sich für eine freiwillige Erstellung entschieden haben oder durch das Gesetz verpflichtet sind, können Sie folgenden Leitfaden nutzen.

www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html

Aber was gehört in das Verzeichnis? Zunächst muss man unterscheiden zwischen dem Verarbeitungsverzeichnis des Verantwortlichen und dem des Auftragsverarbeiters.

Der Verantwortliche ist eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Verarbeitung von personenbezogenen Daten entscheidet. Dagegen ist der Auftragsverarbeiter, eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen
In diesem Verzeichnis werden alle Tätigkeiten der Verarbeitung von personenbezogenen Daten dokumentiert. Dazu zählen unter anderen:

- die Namen und Kontaktdaten der Verantwortlichen,
- Zweck der Verarbeitung (z.B. allgemeine Kundenverwaltung oder Lohn- und Gehaltsabrechnung),
- Kategorien der betroffenen Personen sowie der personenbezogenen Daten (z.B. Abrechnungsdaten, Lohn- und Gehaltsdaten, Kontaktdaten)
- Kategorien von Empfängern der personenbezogenen Daten (z.B. Personalabteilung, Einkauf, Finanzamt)
- ggf. Übermittlung von personenbezogenen Daten an ein Drittland
- und vorgesehene Fristen für die Löschung der Datenkategorien
- sowie eine allgemeine Beschreibung technischer und organisatorischer Maßnahmen (TOM)

Eine kostenlose Vorlage, welche Sie für Ihr Unternehmen anpassen können, finden sie unter:

www.activemind.de/download/verzeichnis-verarbeitungstaetigkeiten/

Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters
Neben dem Verarbeitungsverzeichnis der Verantwortlichen, gibt es auch eine weniger detaillierte Dokumentation des Auftragsverarbeiters. Diese enthält:

- die Namen und Kontaktdaten der Auftragsverarbeiter und der Verantwortlichen
- Kategorien der Verarbeitungen
- ggf. Übermittlung von personenbezogenen Daten an ein Drittland
- sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM)

Auch hierfür gibt es kostenlose Vorlagen:

www.activemind.de/download/verzeichnis-verarbeitungstaetigkeiten-auftragsverarbeiter/

www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

5 Schutzbedarfsanalyse

Nachdem alle personenbezogenen Daten identifiziert und dokumentiert wurden, muss eine Schutzbedarfsanalyse durchgeführt werden. Mit dieser wird festgestellt, ob bei einem Verlust bzw. Veröffentlichung der Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 besteht. Das bestehende Risiko kann mit Hilfe des Schutzstufenkonzeptes der Landesbeauftragten für Datenschutz Niedersachsen (LfD Niedersachsen) bestimmt werden.

www.lfd.niedersachsen.de/download/52033/Schutzstufenkonzept_LfD_Niedersachsen_.pdf

In dem Konzept werden fünf Schutzstufen definiert. Die ersten beiden Stufen A und B definieren einen niedrigen Schutzbedarf. Beispiele hierfür sind frei zugängliche Daten wie Telefonbücher, Adressbücher sowie öffentliche personenbezogene Daten, die der Betroffene selbst veröffentlicht hat. Stufe C definiert einen mittleren Schutzbedarf. In diese Klasse fallen personenbezogene Daten, deren unsachgemäße Handhabung das Ansehen der Betroffenen beeinträchtigen könnte, wie z.B. Einkommen, Sozialleistungen, Grundsteuer oder Ordnungswidrigkeiten.

Bis zur Stufe C ist noch keine Datenschutz-Folgenabschätzung (DSFA) erforderlich. Allerdings gibt es auch Ausnahmen. Wenn biometrische Daten oder Daten von Kindern verarbeitet werden sowie die Überwachung von Mitarbeitern erfolgt, muss eine DSFA durchgeführt werden.
Daten mit hohem bzw. sehr hohem Schutzbedarf werden durch die Stufen D und E abgedeckt und erfordern ebenfalls eine DSFA. Unter Stufe D fallen personenbezogene Daten, welche den Betroffenen in seiner Existenz bedrohen können. Beispiele hierfür sind dienstliche Beurteilungen, Gesundheitsdaten, Schulden sowie Straffälligkeiten. Bei der Stufe E können unsachgemäße Handhabungen die Gesundheit, das Leben oder die Freiheit des Betroffenen beeinträchtigen. Dies sind zum Beispiel Informationen von V-Leuten.
Falls Sie festgestellt haben, dass einige Ihrer Daten einen hohen oder sehr hohen Schutzbedarf benötigten, können Sie folgenden Leitfaden verwenden um eine DSFA durchzuführen.

www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/Folgenabschätzung/

In vielen Fällen ist keine DSFA notwendig. Allerdings muss dieses in der Risikoeinschätzung gut begründet sein.

6 Umsetzung

Nach der Dokumentation der im Unternehmen verarbeiteten Daten und deren Schutzbedarfsanalyse folgt nun die Beschreibung und Umsetzung der technischen und organisatorischen Maßnahmen (TOM).
Je nach Eintrittswahrscheinlichkeit und Höhe des Risikos sollte eine einsprechende Umsetzung realisiert werden. Jüngste Ereignisse, wie z.B. der Erpresser-Trojaner Petya, haben gezeigt, dass diese Maßnahmen für jedes Unternehmen wichtig sind. Sie sollten mindestens Maßnahmen zur Integrität, Wiederherstellung und Vertraulichkeit umsetzen und diese regelmäßig überprüfen. Wie diese Maßnahmen beispielsweise umgesetzt werden können, sehen Sie in folgender Abbildung.

Integrität, Vertraulichkeit, Verfügbarkeit

- Firewall und Virenscanner sind auf allen Endgeräten installiert und werden regelmäßig aktualisiert
- Mitarbeiter erhalten klare Anweisungen zur Einhaltung der Datenschutzrichtlinien

Wiederherstellung

- Sensible Daten werden mit einer 3-2-1-Backup Strategie gesichert

Verschlüsselung

- Backup wird verschlüsselt

Vertraulichkeit

- Jeder Personalmitarbeiter hat eigene Zugangsdaten für seine Arbeitsrechner
- Büroräume werden nach Benutzung abgeschlossen

Pseudonymisierung

- Verwaltung von Kunden und Mitarbeitern erfolgt über IDs

Überprüfung

- Maßnahmen werden alle 2 Monate überprüft

Belastbarkeit

- Server wird mit USV vor Stromausfällen gesichert

Die Anzahl der Maßnahmen hält sich in Grenzen. Eine gute Dokumentation ist das A und O. Diese hilft Anfragen der Betroffenen oder der Datenschutzaufsichtsbehörden zu beantworten.
Für weitere Tipps können Ihnen folgende Links weiterhelfen:

www.datenschutz-praxis.de/fachartikel/technisch-organisatorische-massnahmen-das-aendert-sich/

dsgvo-vorlagen.de/tom-nach-dsgvo-richtig-dokumentieren

Viel Erfolg bei der Umsetzung.

WAS IST MITTELSTAND-DIGITAL?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.
Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit. Weitere Informationen finden Sie unter www.mittelstand-digital.de

Was ist das Mittelstand 4.0-Kompetenzzentrum Cottbus

Das Mittelstand 4.0-Kompetenzzentrum Cottbus setzt sich aus den fünf Partnern BTU Cottbus-Senftenberg (Projektleitung), Technische Hochschule Wildau, Hochschule für nachhaltige Entwicklung Eberswalde, IHP GmbH Leibniz-Institut für innovative Mikroelektronik Frankfurt (Oder) sowie IHK Cottbus als Vertreterin der Landesarbeitsgemeinschaft der Industrie- und Handelskammern in Brandenburg zusammen. Dabei stehen die Schwerpunkte Arbeit 4.0, Digitalisierung in Logistik und Produktion, IT-Sicherheit, Assistenzsysteme, Automatisierungstechnik, Robotik sowie Sozialpartnerschaften im Mittelpunkt. Das Zentrum gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

KONTAKT

Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o BTU Cottbus - Senftenberg
Siemens-Halske-Ring 14
03046 Cottbus
Tel.: +49 355 69 5171
info@kompetenzzentrum-cottbus.digital
www.kompetenzzentrum-cottbus.digital

Folgen Sie uns auf Twitter und XING.