DATENSCHUTZ
NEUE REGELUNGEN IN DER EU UND IN DEUTSCHLAND

Gültig ab 25. Mai 2018

SABU SCHUH & MARKETING GMBH®

VORWORT
VERSTÄNDLICH ERKLÄRT – WAS SIE IN PUNCTO DATENSCHUTZ KÜNFTIG BEACHTEN MÜSSEN

Datenschutz ist jetzt schon von großer Bedeutung und wird in Zukunft noch wichtiger. Jeden Tag werden neue Daten über uns gespeichert, z. B. unsere Einkäufe, Standorte oder Kommunikation. Auf diese Speicherwut hat die Politik nun reagiert.

Auch jetzt schon ist jedes Paar Schuhe ein Datensatz – und jeder Kunde ist es auch. Um den Schutz der personenbezogenen Daten weiter zu erhöhen, tritt nun am 25. Mai 2018 europaweit eine neue Verordnung in Kraft, die EU-Datenschutzgrundverordnung, abgekürzt EU-DSGVO. Sie hat auch ein paar Anpassungen des nationalen Rechts zur Folge, weshalb sich auch das Bundesdatenschutzgesetz an manchen Stellen ändert, zum BDSG-neu.

Was das nun für Sie als Fachhändler bedeutet – und wie Sie konkret handeln sollten – wollen wir Ihnen in dieser Broschüre darlegen, die Sie in die neue Gesetzeslage einführt und verständlich erklärt, was damit auf Sie zukommt.

Unterstützt hat uns dabei der Datenschutz-Experte Erich Zimmerman. Er ist unser geprüfter externer Datenschutzbeauftragter mit IHK-Zertifikat und Sprecher der Initiative „Sicherheit mit System". Zudem ist er mit der Firma ZiDa Datenschutz GmbH auf diese Materie spezialisiert und kann Sie in allen Datenschutzbelangen unterstützen – mit Antworten auf Ihre Fragen, mit einem Datenschutz-Check und als von Ihnen bestellter Datenschutzbeauftragter. Doch gehen wir es der Reihe nach an.

Herzlichst Ihr

Stephan Krug

Hinweis:
Diese Broschüre dient zur Information, sie kann keine Rechtsverbindlichkeit gewährleisten.

DATENSCHUTZ IM UNTERNEHMEN: DER PFLICHTENKATALOG

Ab dem 25. Mai gilt die neue EU-Datenschutzgrundverordnung (EU-DSGVO) sowie das neue Bundesdatenschutzgesetzes (BDSG-neu). Diese Regelungen sollen in erster Linie den Schutz personenbezogener Daten erhöhen. Sie betreffen gegebenenfalls die Bestellung eines Datenschutzbeauftragten und in jedem Fall erweiterte Dokumentationsvorschriften. Was diese Verordnungen für Sie als Fachhändler und für Ihr Unternehmen konkret bedeuten und was Sie als Geschäftsführer tun müssen, legen wir Ihnen in dieser Broschüre dar.

WAS IN JEDEM FALL ZU TUN IST:

SIE MÜSSEN PRÜFEN, OB SIE EINEN DATENSCHUTZBEAUFTRAGTEN BESTELLEN MÜSSEN.

Sie müssen dann einen Datenschutzbeauftragten (DSB) bestellen, wenn Ihr Unternehmen mehr als zehn Beschäftigte mit Zugriff auf automatisierte Datenverarbeitung hat – dazu gehört auch der Dienst an den Kassen und das Schreiben einer E-Mail.

Und bei den zehn Personen zählen die Geschäftsführung, Teilzeitkräfte und Aushilfen sowie Azubis voll mit. Also die komplette Belegschaft.

Der zweite Fall gilt unabhängig von der Zahl Ihrer Beschäftigten. Sie müssen auf jeden Fall einen Datenschutzbeauftragten bestellen, wenn Ihr Haus eine Videoüberwachung hat.

WAS HEISST: EINEN DATENSCHUTZBEAUFTRAGTEN „BESTELLEN"?

Das heißt erst mal: einfach haben. Sie können dafür einen Ihrer Mitarbeiter gewinnen oder einen externen Fachmann in einem befristeten Auftragsverhältnis beauftragen. Dieser ist bereits aktuell ausgebildet und hat fertige Vorlagen für Ihre Branche und er haftet umfänglich, gegebenenfalls auch für Bußgelder. Dafür will er natürlich bezahlt werden.

Aber auch ein eigener Mitarbeiter „kostet" sie etwas: Er muss für die Aufgabe ausgebildet werden, er hat einen erhöhten Kündigungsschutz, er unterliegt keinen Weisungen der Geschäftsführung, er muss ein eigenes Budget erhalten und seine Arbeit beansprucht Zeit, die ihm zur Verfügung gestellt werden muss und die er sich frei einteilen kann. Er haftet allerdings gemäß der neuen EU-DSGVO neben der Geschäftsführung persönlich mit.

Aus dem Gesagten folgt, was wir aber noch einmal ausdrücklich festhalten: Die Geschäftsführung selbst einschließlich der Familienangehörigen, aber auch – falls Sie eine solche Kraft beschäftigen – der IT-Beauftragte, dürfen, sofern andere Mitarbeiter vorhanden sind, nicht als Datenschutzbeauftragte fungieren, da sie laut Gesetz als befangen gelten.

WENN SIE EINEN DATENSCHUTZ-BEAUFTRAGTEN BRAUCHEN:

WELCHE FRISTEN SIND ZU BEACHTEN?

Ihr Datenschutzbeauftragter muss mit Inkrafttreten des Gesetzes, also am 25. Mai 2018, seinen Dienst aufnehmen.

Bis spätestens zum 24. Mai 2018 müssen die Kontaktdaten des ordnungsgemäß ausgebildeten Datenschutzbeauftragten über ein Onlineportal an die jeweilige Landesdatenschutzbehörde gemeldet werden. Wir helfen Ihnen dabei, die Adresse der für Sie zuständigen Datenschutzbehörde ausfindig zu machen.

Bei Verstoß gegen diese Vorschrift droht (nach EU-DSGVO, Art. 83, Absatz 4, Buchstabe a) die Verhängung eines Bußgelds bis zu 4 % des Jahresumsatzes.

DIES GILT WIEDER FÜR ALLE:

DIE NEUEN PFLICHTEN FÜR ALLE UNTERNEHMEN UND BETRIEBE

Alle Unternehmen und Betriebe sind zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten verpflichtet (vormals Verfahrensbeschreibung genannt).

Im Anhang ab Seite 8 finden Sie das Formular, auf welchem die entsprechenden Angaben gemacht werden können.
Die Angaben beinhalten auch Datenschutz-Folgeabschätzungen. So sollen die Maßnahmen beschrieben werden, welche die besonders sensiblen Daten bestimmter Personen ausreichend schützen – beispielsweise im Gesundheits- oder Finanzbereich. Die Dokumentation solcher technisch-organisatorischer Maßnahmen erfolgt nach DSGVO, Artikel 32, Absatz 1 (vormals BDSG § 9, Anlagen).

Alle Unternehmen und Betriebe sind ferner dazu verpflichtet, ihr Personal auf den korrekten Umgang und die Geheimhaltung von Daten zu verpflichten und dementsprechend zu schulen.

WAS SIND PERSONENBEZOGENE DATEN IM SINNE DER NEUEN EU-DSGVO?

BEISPIELE

- Name
- Adresse
- Geburtsdatum
- Telefonnummer
- E-Mailadresse
- IP-Adresse
- Bankverbindung
- Steuernummer
- Personalnummer
- Gesundheitszustand
- Bildaufnahmen
- Aussehen

Es sind alle Daten, durch die eine Einzelperson (natürliche Person) identifiziert werden kann – also Name, Anschrift, Telefon-, Personal-, Kunden-, Lieferanten- oder eine sonstige Nummer.

Auch sind alle Angaben über persönliche oder sachliche Verhältnisse der Betroffenen personenbezogene Daten, unabhängig davon, wie sensibel sie sind und woher sie stammen.

FORTSETZUNG DES PFLICHTENKATALOGS

Damit noch immer nicht genug der neuen Pflichten. Es wird zudem verlangt, dass Sie eine Richtlinie erlassen, die den Umgang mit Internet, sozialen Medien und E-Mail regelt, insbesondere über den Firmen-Account. Diese thematisiert beispielsweise das Verbot privater E-Mails und sträfliche Handlungen im Internet.

Auch alle externen Dienstleister, die Zugriff auf personenbezogene Daten haben, sind auf Geheimhaltung zu verpflichten – z. B. IT-Dienstleister, Webhoster, Katalogversender, Lohnbüros, Reinigungsunternehmen, Papierentsorger, Werbeagenturen. Die Informationssicherheit ist kontinuierlich zu überprüfen.

Sodann ist ein Verfahren festzulegen, wie Anfragen Betroffener behandelt werden – zum Beispiel, wenn Kunden eine Auskunft verlangen. Dieses Verfahren muss allen Mitarbeitern schriftlich mit Ablauf und Berichtsweg mitgeteilt werden.

Auf der rechten Seite drucken wir beispielhaft ein Schreiben ab, wie eine solche Betroffenenanfrage an Ihr Haus aussehen kann.

SO KÖNNTE DIE ANFRAGE EINES KUNDEN AN SIE FORMULIERT SEIN:

Sehr geehrte Damen und Herren,

unter Bezug auf die Datenschutzgesetze ersuche ich Sie, mir schriftlich, unverzüglich und kostenlos Auskunft über die zu meiner Person bei Ihnen gespeicherten Informationen zu erteilen:
Werden in Ihrem Unternehmen Daten über mich gespeichert?
Welche Daten zu meiner Person werden gespeichert?
Wer verarbeitet die Daten?
Von wem haben Sie Ihre Daten über meine Person erhalten (Quelle)?
Zu welchem Zweck werden die Daten verarbeitet?
An welche weiteren Empfänger wurden in der Vergangenheit meine persönlichen Daten weitergegeben?
Nennen Sie mir Ihren Datenschutzbeauftragten und dessen Kontaktdaten.

Mit freundlichen Grüßen
Max Mustermann

UM DEN ZWINGENDEN HANDLUNGSBEDARF ZU VERDEUTLICHEN, HIER NOCH EIN AUSZUG AUS DEM BUSSGELDKATALOG:

Mit Geldbußen bis zu 4 % vom Jahresumsatz bzw. 20 Mio. Euro (lt. EU-DSGVO) wird belegt, wer als verantwortliche Stelle der Meldepflicht nicht nachkommt, einen Beauftragten für den Datenschutz nicht ordnungsgemäß bestellt, Betroffene nicht ordnungsgemäß über Widerspruchsrechte informiert, Daten inkorrekt übermittelt oder nutzt, Gründe zur Datenübermittlung nicht aufzeichnet, Betroffene nicht ordnungsgemäß benachrichtigt, bestrittene Daten ohne Gegendarstellung übermittelt, Prüfungen der Aufsichtsbehörde behindert oder vollziehbare Anordnungen der Aufsichtsbehörde nicht beachtet.

HABEN SIE AN ALLES GEDACHT?

BEISPIELHAFT DER FRAGEBOGEN DER BAYERISCHEN DATENSCHUTZBEHÖRDE

Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch:

- Vorhandensein einer Datenschutzleitlinie
- Beschreibung der Datenschutzziele
- Regelung der Verantwortlichkeiten
- Bewusstsein der Datenschutzrisiken
- Ist ein Datenschutzbeauftragter vorhanden und ist er schon der Aufsichtsbehörde gem. Art.37 EU-DSGVO gemeldet?
- Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten?
- Wie stellen Sie sicher, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen berücksichtigt werden?
- Haben Sie externe Dienstleister zur Erledigung Ihrer Arbeiten eingebunden (Auftragsverarbeiter)?
- Haben Sie hierüber eine Übersicht?
- Haben Sie die erforderlichen Vereinbarungen zum Datenschutz/Geheimhaltung abgeschlossen?

Zur Transparenz, Informationspflicht und Sicherstellung der Betroffenenrechte:

- Wie lauten die Kontaktdaten Ihres Datenschutzbeauftragten?
- Wie berücksichtigen Sie die Rechte Betroffener auf Auskunft, Berichtigung, Löschung, Sperrung Ihrer Daten?
- Haben Sie ein Verfahren eingerichtet, um Anträge auf Auskunft zeitnah erfüllen zu können?
- Wissen Sie um das Widerrufsrecht bei Einwilligung (Werbung)?
- Gibt es zu den Verarbeitungstätigkeiten Angaben, mit denen die Rechtmäßigkeit nachgewiesen werden kann, z. B. Zweck, Kategorien, Empfänger, Löschfristen?
- Können Einwilligungen (Werbung) nachgewiesen werden?
- Haben Sie eine Risikobewertung mit Eintrittswahrscheinlichkeit und Schwere der Risiken mit regelmäßiger Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen eingerichtet?
- Ist ein Prozess zur Datenschutz-Folgenabschätzung (Risikomethode ähnlich ISO 27001-Informationssicherheit) etabliert?
- Haben Sie sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörden und die Betroffenen erfolgt?
- Ist festgelegt, wie diesbezüglich mit potentiellen Verletzungen intern umzugehen ist (Meldeverfahren, Informationsweg …)?

Hauptblatt

Verzeichnis der Verarbeitungstätigkeiten nach EU-DSGVO

Verantwortliche Stelle

Name der Firma

Straße

Telefon*

PLZ

E-Mail

Ort

Internet-Adresse (URL)*

Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter:
Bei verantwortlicher Stelle in Drittstaaten, d. h. mit Sitz außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Island, Norwegen und Lichtenstein), im Inland ansässiger Vertreter:

Anrede, Titel

Name, Vorname

Funktion

Anrede, Titel

Name, Vorname

Funktion

Anrede, Titel

Name, Vorname

Funktion

Mit der Leitung der Datenverarbeitung beauftragte Person:

Anrede, Titel

Name, Vorname

Funktion

Angaben zur Person der/des Datenschutzbeauftragten (extern mit Anschrift)*:

Anrede, Titel

Name, Vorname

Straße

PLZ, Ort

Telefon

E-Mail

* freiwillige Angaben

Verfahrensbeschreibung

Verzeichnis der Verarbeitungstätigkeiten nach EU-DSGVO

Verantwortliche Stelle | Name des Verantwortlichen | Telefon

Inhalt der Meldung	Beschreibung der automatisierten Verarbeitung
Name des Verfahrens/Programms/ der Anwendung	Angebotswesen und Kundenkontakt
Zweckbestimmung der Daten-erhebung, -verarbeitung und -nutzung	Die Zweckbestimmung der einzelnen Datenverarbeitung regelt u. a. die mit den Kunden getroffene anlehnende Vereinbarung hinsichtlich des anbahnenden Auftragsverhältnisses. Die ausschließlich zweckgebundenen Nutzungen der einzelnen Daten werden insbesondere zu folgenden Aufgabenerfüllungen verwendet (erhoben, verarbeitet, genutzt): Erstellung und Bearbeitung von Angeboten, Verwaltung von Kundenkontakten, Auftragsannahme und Auftragsabwicklung.
Beschreibung der betroffenen Personengruppen	☐ Bewerber/Mitarbeiter/Auszubildender ☒ Kunden ☒ Lieferanten ☐ Sonstige:
Beschreibung der diesbezüglichen Daten oder Datenkategorien	Angaben zu Geschäftsadresse, Tätigkeitsbereich, Transaktions- und Leistungsdaten, Bankverbindungsdaten, Kontaktinformationen, Mitarbeiterstatus
Regelfristen für die Löschung der Daten	Sofern Daten die für den unternehmerischen Ablauf nicht mehr relevant sind, können diese gelöscht werden. Eine automatisierte Löschung ist nicht vorgesehen.
Interne Empfänger von Daten (zugriffsberechtigte Personen und Personengruppen)	Abteilung / Personen: `Rechnungswesen, Geschäftsführung, MA im Aufgabenbereich, IT-Abteilung`
	Art der Daten: `Angaben zu Geschäftsadresse, Tätigkeitsbereich, Transaktions- und Leistungsdaten, Bankverbindungsdaten, Kontaktinformationen, Mitarbeiterstatus`
	Zweck des Transfers: `Erstellung und Bearbeitung von Angeboten, Verwaltung von Kundenkontakten, Auftragsannahme und Auftragsabwicklung`

Externe Empfänger von Daten	Rechnungswesen:
	`Distributor`
	`Hard/Software Partner`

	Art der Daten: `Transaktions- und Leistungsdaten, Bankverbindung, Angaben zur Geschäftsadresse, Distributor/Partner - Ansprechpartner, Kundennamen, Geschäftsadresse`

	Zweck der Übermittlung:
	`Erstellung von Rechnung`
	`Erstellung von Angeboten`

Fortsetzung auf der nächsten Seite

Inhalt der Meldung	Beschreibung der automatisierten Verarbeitung
Datenübermittlung ins Ausland	Welche Staaten:
	Welche vertraglichen Regelungen bestehen:
Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung	☒ Vertrag, vertragsähnliches Vertrauensverhältnis ☒ Einwilligung des Betroffenen ☐ Vorrangige Rechtsvorschrift ☒ Interessenabwägung ☐ Sonstiges:
Benachrichtigung	Nicht erforderlich, da: ☐ Kenntnis auf andere Weise ☐ Einwilligung vorliegt ☐ Öffentlich zugängliche Daten ☐ Sonstiges: Erfolgte durch:
Datenübermittlung	Im Rahmen einer komplexen Funktionsübertragung
Auftragsdatenverarbeitung liegt vor Vertragsbestandteile sind vorhanden	☐ Ja ☐ Gegenstand und die Dauer des Auftrags ☐ Umfang, Art und der Zweck der Verarbeitung ☐ Art der Daten und der Kreis der Betroffenen ☐ Technisch-organisatorische Maßnahmen ☐ Berichtigung, Löschung, Sperrung von Daten ☐ Pflichten des Auftragnehmers (Kontrollen) ☐ Berechtigung von Unterauftragsverhältnissen ☐ Kontrollrechte des Auftraggebers ☐ Mitteilungen über Datenschutzverstöße ☐ Weisungsbefugnisse des Auftraggebers ☐ Rückgabe / Löschung von Datenträgern / Daten Geprüft am:
Vorabkontrolle bzw. neu Folgenabschätzung	☐ Nicht erforderlich, weil ☐ Vertragsbestandteil ☐ Gesetzliche Vorschrift ☐ Sonstiges: ☐ Erforderlich ☐ Durchgeführt am: ☐ Mit Ergebnis: ☐ Wiedervorlage ☐ Nicht erforderlich ☐ Erforderlich am:

Verfahrensverantwortlicher | Datum | Unterschrift

Datensicherheitsbeschreibung nach rt. 32 Abs.1 DSGVO bzw. Anlage zu § 9 BDSG im Anhang

SABU-PARTNER FÜR DATENSCHUTZ

FÜR ALLE, DIE KEINEN EIGENEN MITARBEITER ALS DATENSCHUTZBEAUFTRAGTEN (DSB) QUALIFIZIEREN WOLLEN, BIETET SICH EINE EXTERNE LÖSUNG AN.

Die Vorteile sind:

- Flexibilität – der externe DSB unterliegt keinem besonderen Kündigungsschutz und der Dienstleistungsvertrag ist befristet.
- Professionalität – die Kernkompetenz des externen DSB ist Datenschutz und es entstehen keine zusätzlichen Kosten für Aus- und Weiterbildung eigener Mitarbeiter.
- Branchenspezifische Vorlagen vorhanden – daher geringer Aufwand für den Kunden bei der Datenschutz-Dokumentation.
- Minimierte Haftungsrisiken – bei internem DSB haften dieser und die Geschäftsführung persönlich für Fehler oder Versäumnisse im Datenschutz. Der externe Datenschutzbeauftragte haftet dagegen umfänglich auch für Bußgelder.

UNSER DATENSCHUTZ-EXPERTE STEHT IHNEN FÜR IHRE FRAGEN ZUR VERFÜGUNG.

Erich Zimmermann
Sprecher der Initiative „Sicherheit mit System“
Externer Datenschutzbeauftragter (IHK)

ZiDa-Datenschutz GmbH
Waldhofer Str. 102
69123 Heidelberg

Tel 0621 . 30696731
Mobil 0160 . 90248450
Fax 03212 . 3912345

e.zimmermann@zida-datenschutz.de
www.zida-datenschutz.de

DAS ANGEBOT UMFASST AUCH EINEN PROFESSIONELLEN DATENSCHUTZ-CHECK.

Nehmen Sie sich 30 Minuten Zeit und bearbeiten Sie mit uns telefonisch oder bei Ihnen und vertraulich Fragen zum Datenschutz-Status in Ihrem Unternehmen anhand einer „Datenschutz-Checkliste“.

Sie erhalten dann kostenlos Hinweise zu den für Ihr Haus zutreffenden Datenschutz- und Informationssicherheits-Erfordernissen und können Ihr persönliches Risiko besser einschätzen.

Bitte fordern Sie einen kostenlosen Datenschutz-Check bei der ZiDa-Datenschutz GmbH an.

VORBEHALT

Diese Broschüre gibt nach bestem Wissen und Gewissen die Inhalte der neuen EU-Datenschutzgrundverordnung (EU-DSGVO) sowie des neuen Bundesdatenschutzgesetzes (BDSG-neu), beide gültig ab 25. Mai 2018, wieder. Dennoch kann der SABU als Herausgeber dieser Broschüre keine Gewähr für die Richtigkeit übernehmen.

FÜR DEN FACHHANDEL ZUSAMMEN-
GESTELLT IN KOOPERATION MIT
ERICH ZIMMERMANN VON DER ZIDA
DATENSCHUTZ GMBH

SABU SCHUH & MARKETING GMBH®

WANNENÄCKERSTRASSE 50
74078 HEILBRONN
TEL 07131 . 97 370
FAX 07131 . 97 37 490

WWW.SABU-VERBUNDGRUPPE.DE
WWW.SABU.DE – DIE REGIONALE
SCHUHPLATTFORM FÜR SCHUHE