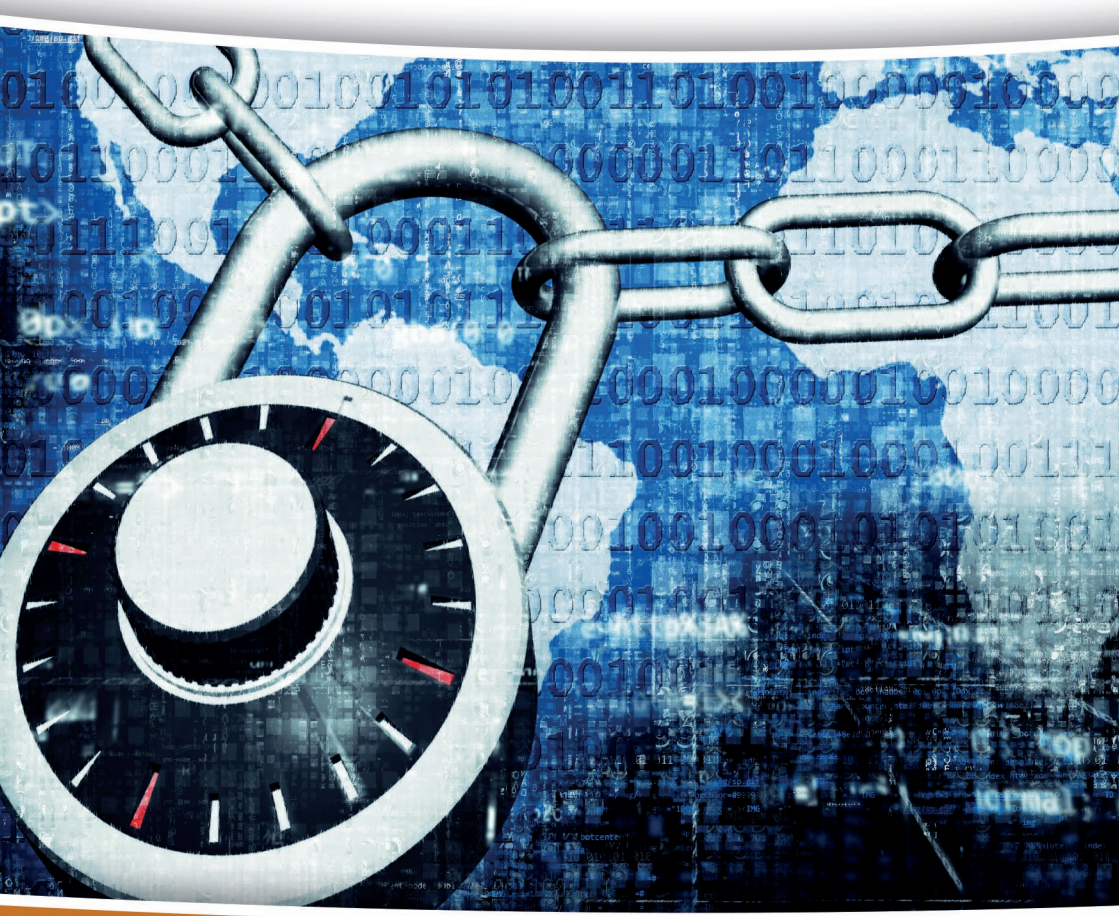
grabowski
UNTERNEHMENSBERATUNG & COACHING



RATGEBER DSGVO

Wichtige Informationen und Handlungsempfehlungen

Über mich

Ich bin Steffen Grabowski und Autor dieser kleinen Veröffentlichung. Seit 2005 beschäftige ich mich mit Unternehmen verschiedenster Branchen und bin als Unternehmensberater tätig.

Im Fokus meiner Arbeit als Unternehmensberater steht die systematische und professionelle Beratung kleiner und mittelständischer Unternehmen in allen erdenklichen Unternehmensphasen - von der Gründung bis zur Suche nach einer Unternehmensnachfolge.

Derzeit sind Hilfestellungen zur DSGVO sehr gefragt, weswegen ich mich entschloß, diesen Ratgeber zu verfassen und Ihnen damit eine wertvolle Hilfestellung zu bieten.

Gern bin ich auch darüber hinaus für Sie tätig, beantworte offene Fragen und helfe Ihnen bei der Einführung der DSGVO-Konformität in Ihrem Unternehmen.

Besuchen Sie auch meine Website:
www.grabowski-beratung.de

grabowski
UNTERNEHMENSBERATUNG & COACHING
Neubrandenburg • Johannesstr. 15b
Stavenhagen • Warener Str. 28
Telefon: (0395) 70 79 114

Inhaltsverzeichnis

Einführung ins das Thema 04

Betrifft mich die DSGVO überhaupt? 05

Was ist die DSGVO? 07

Was ist jetzt zu beachten? 11

Prüfung der Prozesse auf Zulässigkeit 11

Sicherheit der Daten 11

Datensparsamkeit und Privacy by Design & Default 12

Datenschutz- & Einwilligungserklärung 12

Auftragsdatenverarbeitung 13

Mitarbeiter sensibilisieren und zur Vertraulichkeit verpflichten . . . 14

Verarbeitungsverzeichnis 15

Datenschutzfolgenabschätzung 16

Datenschutzbeauftragter 17

Auskunftspflicht 18

Kontinuierliche Kontrolle der Prozesse
und Anpassung der Dokumentation 19

Meldepflicht 19

Sonderregelungen 20

Hilfen bei der Umsetzung 21

Beratung & Förderung 23

Disclaimer 23

Einführung in das Thema

Die Datenschutzgrundverordnung beschert vielen Unternehmen Sorgen und viel Arbeit. Seitens der Betroffenen herrscht häufig noch viel Unsicherheit und Angst vor den hohen Bußgeldern. Wiederum andere Unternehmen wissen noch gar nichts von der DSGVO. Dieser Beitrag soll Ihnen dabei helfen, einen Überblick über die Neuerungen und notwendigen Maßnahmen zu erhalten und Sie über meine Leistungen im Hinblick auf die Beratung zur DSGVO und den möglichen Handlungsempfehlungen informieren.

Betrifft mich die DSGVO überhaupt?

Nahezu jedes Unternehmen ist betroffen. Die nun folgenden Beispiele zeigen, wie Sie betroffen sein könnten:

Mitarbeiterdaten / Lohnabrechnung

Die Daten Ihrer Mitarbeiter, wie Name, Anschrift und Geburtsdatum sind personenbezogene Daten im Sinne der DSGVO. Hier gelten sogar besondere Regelungen für eine wirksame Einwilligung.

E-Mail-Account

Schreiben Sie regelmäßig E-Mails? Sind in ihnen beispielsweise Name und Anschrift Ihrer Kunden, zum Beispiel zu einer Reservierung, enthalten?

Website mit Kontaktformular, Besucheranalysen oder Onlineshop

Nutzen Sie ein Kontaktformular oder Shop, in dem Sie Daten von Ihren Besuchern erheben, so ist in der Regel eine Datenschutzerklärung sinnvoll / notwendig. Ebenso hat die Übertragung der Daten zu jener (Abhör-)Sicherheit nach aktuellem Stand der Technik verschlüsselt zu erfolgen (SSL-Zertifikat). Zudem ist dieser Vorgang in Ihrem Verarbeitungsverzeichnis zu dokumentieren und ggf. ein Löschdatum für die Daten zu definieren.

Auch eine kleine Website, ohne die Erfassung von Daten mittels Formular, sammelt in der Regel Daten von den Besuchern, die gegebenenfalls eine Identifizierung eben jener ermöglichen (zum Beispiel durch die IP-Adresse). Dies kann durch Serverstatistiken

oder Analysetools wie Google Analytics passieren, ohne dass Sie dies bisher bewusst wahrgenommen haben.

Newsletter per E-Mail, WhatsApp & Co.

Für Newsletter gilt das Prinzip von einem Double-Opt-In, dass heißt, der Benutzer muss die Eintragung in die Liste der Empfänger ein zweites Mal per Mail oder Link-Klick bestätigten. Auch hier ist eine informierte und verständliche Einwilligungserklärung und Verarbeitungsverzeichnis notwendig.

Kassensystem

Sie haben ein Kleidungsgeschäft in der Innenstadt und Fragen Ihre Kunden nach ihrem Namen und Anschrift, damit Sie ihnen einen Kundenaccount für Rabatte, vereinfachte Reklamationen und ggf. Mailings anlegen können? Auch hierbei handelt es sich um eine Verarbeitung von personenbezogenen Daten, welche u.a. eine dokumentierte und informierte Einwilligung und das Verarbeitungsverzeichnis notwendig macht.

Kundenverwaltung / Rechnungssoftware

Nutzen Sie eine Software, in der Sie die Daten Ihrer Kunden erfassen und aus der heraus Sie vielleicht Angebote und Rechnungen erstellen oder die Kommunikation dokumentieren? Werden diese Daten verschlüsselt? Haben Sie ein Verarbeitungsverzeichnis?

Was ist die DSGVO?

Stichtag zur vollen Wirkungsentfaltung der DSGVO ist der 25. Mai 2018. Es gibt für die Umsetzung notwendiger Maßnahmen keine weiterreichende Schon- oder Übergangsfrist. Ab dem 25. Mai drohen Unternehmen, die gegen die DSGVO verstoßen, Strafen in Höhe von bis zu 20 Millionen Euro oder 4% des Jahresumsatzes. Zusätzlich drohen Unternehmen kostenintensive Abmahnungen und Klagen von zum Beispiel Rechtsanwälten und Verbraucherschutzverbänden.

Betroffen von der DSGVO sind alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten. Hierzu genügt mitunter schon der E-Mailverkehr in Ihrem Postfach, wodurch nahezu jedes Unternehmen in der Region betroffen sein dürfte. Denn unter der Verarbeitung personenbezogener Daten ist die Erhebung, Speicherung, Offenlegung oder auch das Löschen eben jener zu verstehen. Dabei ist es egal, ob es sich um Daten von zum Beispiel Kunden oder Mitarbeitern handelt. Personenbezogen sind Daten immer dann, wenn sie sich auf eine identifizierbare Person beziehen. Wobei es unerheblich ist, ob die Identifizierung nur theoretisch möglich oder praktisch vorhanden ist.

Eine Verarbeitung personenbezogener Daten ist ab dem Stichtag nur noch erlaubt, wenn es eine gesetzliche Legalisierung oder eine wirksame(!) Einwilligung für sie gibt. Gesetzlich erlaubt ist die Verarbeitung im Rahmen der Beantwortung von Anfragen und zum Zweck der Vertragsabwicklung, Erfüllung anderer gesetzlichen Verpflichtungen (z.B. Steuerrecht) oder bei berechtigtem Interesse. Zur Wirksamkeit einer Einwilligung ist zu beachten, dass es notwendig

ist, dass die Einwilligung freiwillig, also mit einer Wahlmöglichkeit und informiert erfolgt. Ferner existieren ein Kopplungsverbot und das Unternehmen muss die Einwilligung nachweisen. Dies kann bei einem Online-Formular beispielsweise durch Protokollierung der Einwilligung samt Timestamp, Einwilligungstext und (verkürzter) IP-Adresse erfolgen.

Egal ob es eine gesetzliche Grundlage oder Einwilligung zur Erhebung der Daten gab, die DSGVO regelt auch die Löschung und Zweckbindung dieser Daten samt Dokumentationspflichten. Unternehmen sind verpflichtet, Verfahren in denen personenbezogene Daten verarbeitet werden, in einem Verarbeitungsverzeichnis zu dokumentieren und auf Verlangen entsprechenden Behörden bei einer Prüfung vorzulegen (Näheres hierzu in den folgenden Kapiteln). Außerdem haben Betroffene das Recht auf ein vergessen werden und Löschung der Daten. Ein „Hamstern" der Daten und Zweckentfremden der Datennutzung ist untersagt.

Die DSGVO regelt aber auch weitere Rechte der Betroffenen. So haben eben jene das Recht auf Auskunft. Entsprechende Anfragen müssen umgehend und vollständig beantwortet werden. Ferner können Betroffene die Löschung oder Korrektur der Daten verlangen.

Zusammenfassend kann man die Datenschutzprinzipien nunmehr wie folgt darstellen:

Rechtmäßigkeit

Man darf personenbezogene Daten nur dann verarbeiten, wenn es rechtlich zulässig ist.

Transparenz

Es muss eine Nachvollziehbarkeit in der Verarbeitung personenbezogener Daten gewährleistet sein, was zum Beispiel eine vollständige und verständliche Datenschutzerklärung notwendig macht.

Verbot der Verarbeitung mit Erlaubnisvorbehalt

Jegliche Verarbeitung personenbezogener Daten ist verboten, es sei denn sie wurde durch das Gesetz erlaubt.

Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden. Eine Zweckänderung ist nur dann zulässig, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar ist.

Datenminimierung

Eine Datenerhebung auf Vorrat ist verboten. Die Erhebung von personenbezogenen Daten muss sich auf das Maß beschränken, dass für den Verarbeitungszweck notwendig ist.

Integrität & Vertraulichkeit

Die Daten müssen vor unbefugter Verarbeitung, Löschung, Veränderung oder Zerstörung durch geeignete und zeitgemäße technische und organisatorischen Maßnahmen geschützt werden.

Privacy by Design

Datenschutzmaßnahmen müssen bereits bei der Konzeption von Produkten und Verfahren nach aktuellem Stand der Technik einbezogen werden.

Privacy by Default

Voreinstellungen in Geräten / Softwareprodukten sollen standardmäßig die höchste Datenschutzstufe haben.

Was ist jetzt zu beachten?

Die entscheidende Frage für jeden Unternehmer ist nunmehr, was konkret zu tun ist, um der DSGVO gerecht zu werden. Ich habe Ihnen einige Punkte hierzu zusammengestellt.

Prüfung der Prozesse auf Zulässigkeit

Alle Prozesse in Ihrem Unternehmen müssen analysiert werden und es muss festgestellt werden, ob in ihnen personenbezogene Daten verarbeitet werden. Dies muss akribisch erfolgen und dokumentiert werden. Wird festgestellt, dass in einem Prozess personenbezogene Daten verarbeitet werden, so ist nunmehr zu prüfen, ob diese Verarbeitung rechtmäßig ist. Hierbei kommen auch die Prinzipien Datensparsamkeit, Verbot der Zweckentfremdung etc. zur Anwendung. Ist etwas nicht zulässig, muss der Prozess neu strukturiert werden, sodass er mit der DSGVO konform ist. In jedem Fall ist er in dem Verarbeitungsverzeichnis aufzunehmen und zu dokumentieren.

Sicherheit der Daten

Die DSGVO sieht die Integrität und Vertraulichkeit der Daten vor. So müssen Daten durch geeignete technische Maßnahmen u.a. vor unbefugter Verarbeitung, Löschung und Zerstörung geschützt werden. Was bedeutet dies aber genau? Aus technischer Sicht ist die Hard- und Software in Ihrem Unternehmen so zu strukturieren, dass keine Datenpannen passieren können, beziehungsweise vermieden werden. Stichwörter hierzu sind die Verschlüsselung und der Passwortschutz der Daten, sowie der Schutz durch z.B. Firewalls. Ebenso sind regelmäßige Backups zum Schutz vor Zerstörung bindend. Ein weiterer Aspekt ist die Übertragung der Daten.

Füllt der Besucher Ihrer Website beispielsweise ein Kontaktformular aus und sendet mit ihm personenbezogene Daten an Sie, so muss, zum Beispiel durch eine SSL-Verschlüsselung des Formulars, eine Abhörsicherheit gegeben sein.

Datensparsamkeit und Privacy by Design & Default

Zu beachten ist auch die Datensparsamkeit. Stellen Sie sich die Frage, ob alle personenbezogenen Daten, die Sie verarbeiten auch wirklich notwendig sind. Für eine einfache und unverbindliche Reservierungsanfrage in einem Restaurant benötigen Sie beispielsweise nicht das Geburtsdatum des potentiellen Kunden. Ferner sind alle Produkte und Leistungen ihres Unternehmens so auszurichten, dass den hohen Sicherheits- und Datenschutzanforderungen gerecht geworden wird. Dies gilt nicht nur für bisher bestehende, sondern auch für künftige Projekte. Planen Sie entsprechende Mechanismen und Co. von Anfang an ein und vermeiden Sie damit kostspielige Anpassungen im Nachhinein.

Datenschutz- & Einwilligungserklärung

Betroffene Personen müssen über die Verarbeitung der eigenen personenbezogenen Daten informiert werden. Dies geschieht online in der Datenschutzerklärung. Diese muss präzise, transparent, verständlich und leicht zugänglich sein. Pflichtangaben hier sind unter anderem die Angaben zum Verantwortlichen, Kontaktdaten, Angaben zum Datenschutzbeauftragten, welche Arten von Daten zu welchem Zweck und auf welcher Grundlage sie verarbeitet werden, die Rechtsgrundlagen hierfür, Hinweise zum Zeitpunkt der Löschung, die Quelle der Datenerhebung und Hinweise auf die Rechte der Betroffenen (z.B. Auskunft, Löschung, Beschwerderecht & Widerrufsrecht).

In vielen Fällen, in denen die Verarbeitung von personenbezogenen Daten nicht durch das Gesetz legalisiert ist, können Sie dies durch eine Einwilligung des Betroffenen dennoch möglich machen. Wichtig ist hierfür eine Einwilligungserklärung. Diese Einwilligung muss jedoch von einer einwilligungsfähigen Person u.a. informiert und freiwillig erfolgen. Das bedeutet, dass die entsprechende Erklärung in einfacher und verständlicher Sprache erfolgen muss, der Betroffene von ihr Kenntnis hat und er auch wirklich eine echte Wahl hatte eben jene zu erteilen oder nicht. Es ist für die wirksame Erteilung der Einwilligung eine aktive Handlung des Betroffenen erforderlich, zum Beispiel durch das Auswählen einer Checkbox mit entsprechendem Hinweis. Auch die Möglichkeit eines Widerrufs der Einwilligung muss vorhanden und klar kommuniziert sein. In der Erklärung ist dem Betroffenen offenzulegen zu welchem Zweck, auf welche Art, in welchem Umfang die Daten genutzt werden, ob sie an Dritte weitergegeben werden und wann sie gelöscht werden. Ferner hat der Unternehmer die Pflicht, die Einwilligung nachzuweisen. Dies fällt bei einer schriftlichen Einwilligung relativ leicht, erfolgt die Einwilligung jedoch online, so ist deren Protokollierung ein wichtiges Instrument.

Ein weiterer wichtiger Punkt ist hier das Kopplungsverbot.
Die Erbringung einer Leistung darf nicht von der Einwilligung abhängig gemacht werden, wenn die Einwilligung nicht für die Leistungserbringung erforderlich ist.

Auftragsdatenverarbeitung

Wird ein Dritter mit der Verarbeitung personenbezogener Daten beauftragt, ist auch hier eine Einwilligung des Betroffenen denkbar. Da diese aber an hohe Hürden gebunden und schnell widerrufbar

ist, sollte dieser Weg die zweite Wahl sein. Wann immer es geht, sollte die Weitergabe auf gesetzliche Erlaubnisnormen gestützt werden.

Eine Weitergabe der Daten an einen Dritten kann zum Beispiel im Rahmen der Auftragserfüllung abgedeckt sein. Dies trifft regelmäßig dann zu, wenn ein Shopbetreiber die Adressdaten eines Kunden an einen Paketdienstleister weitergibt, damit dieser eine Bestellung zustellen kann.

Weitere Beispiele sind die Speicherung von Daten in einer Cloud, eine Weitergabe an den Newsletterversender oder die Weitergabe von Daten zur Websiteanalyse. Für diese Auftragsdatenverarbeitung sieht der Gesetzgeber den Abschluss und die Erfüllung eines speziellen Vertrages als ausreichende Risikominderung für die Betroffenen, einhergehend mit dem ggf. vorhandenen berechtigten Interesse des Unternehmens, als Erlaubnisgrundlage vor. Dies jedoch nur, wenn benannter Vertrag mit dem Auftragsdatenverarbeiter den gesetzlichen Vorgaben entspricht. Diese gilt es zu beachten, ebenso wie besondere Regelungen für den Fall, dass der Auftragsdatenverarbeiter und dessen IT nicht innerhalb der EU sitzt.

Mitarbeiter sensibilisieren und zur Vertraulichkeit verpflichten

Ein wichtiger Schritt ist ebenso, alle Mitarbeiter in Ihrem Unternehmen für das Thema Datenschutz zu sensibilisieren und im sorgsamen Umgang mit personenbezogenen Daten zu schulen. Zusätzlich sollte eine Vertraulichkeitsvereinbarung getroffen werden.

Verarbeitungsverzeichnis

Im Verarbeitungsverzeichnis sind Vorgänge, in denen personenbezogene Daten verarbeitet werden systematisch zu beschreiben und zu dokumentieren. Diese Pflicht entfällt nur dann bei kleinen Unternehmen, wenn die Verarbeitung nur gelegentlich erfolgt. Dank moderner Lohnsoftware, Websites, Kassensysteme, Kundensysteme und E-Mailpostfächer kann jedoch davon ausgegangen werden, dass nahezu jedes Unternehmen von der Erstellung und Pflege eines Verfahrensverzeichnisses betroffen ist.

Hierfür sieht die DSGVO Pflichtangaben vor, verzichtet jedoch darauf eine bestimmte Form zu definieren.

Zu den Pflichtangaben im Verarbeitungsverzeichnis zählen u.a.:

Angaben zum Unternehmen

Hier ist das Unternehmen samt Anschrift und Kontaktdaten zu benennen. Ebenso wie eben jene von der jeweils zuständigen Person.

Bestimmung der einzelnen Verarbeitungstätigkeiten

In diesem Teil werden die einzelnen Verarbeitungstätigkeiten von personenbezogenen Daten bestimmt und beschrieben. Dies könnten zum Beispiel Vorgänge aus dem Personalmanagement, Onlineshop und Marketingmanagement sein, aber auch die Verarbeitung durch Dritte gehört dazu.

Detaillierte Angaben zu den einzelnen Verarbeitungstätigkeiten

Hier geht es ins Detail. Jede einzelne Verarbeitungstätigkeit wird in diesem Teil genau beschrieben.

Dazu sind die folgenden Angaben notwendig:

- Datenkategorie (z.B. Beschäftigtenstammdaten, Kundenstammdaten, Nutzungsdaten, Bewerberdaten)
- Kategorie der Betroffenen (z.B. Mitarbeiter, Kunden, Bewerber, Lieferanten)
- Zweck der Verarbeitung
- rechtliche Grundlage hierfür (z.B. Auftragsabwicklung, Aufbewahrungsfrist, Einwilligung)
- Datenquelle
- Angaben zur Information der Betroffenen
- Empfänger der Daten (z.B. Versandabteilung oder Dritte)
- Angaben zum Löschdatum / Einschränkung der Verarbeitung
- Getroffene Schutzmaßnahmen

Technische und organisatorische Maßnahmen zum Schutz der Daten

In diesem Bereich muss beschrieben werden, welche technischen und organisatorischen Maßnahmen bezüglich der personenbezogenen Daten getroffen sind, um sie vor Kenntnisnahme durch Unbefugte, Missbrauch oder Zerstörung zu schützen.

Datenschutzfolgenabschätzung

Zusätzlich hierzu ist in einigen Fällen eine Datenschutz-Folgenabschätzung notwendig. Dies ist besonders der Fall, wenn eine Videoüberwachung eingesetzt wird, es sich bei dem Vorgang um ein Profiling handelt, das als Grundlage für schwerwiegende Entscheidungen eingesetzt wird oder im großen Umfang sensible Daten verarbeitet werden. Dies können zum Beispiel Daten zur Gesundheit, Sexualität, politischer Gesinnung oder Straftaten sein.

Trifft dies auf Ihr Unternehmen zu, so müssen Sie die jeweils betreffenden Verarbeitungen einem Stresstest unterziehen, mögliche Risiken auflisten und in einem Bericht deutlich machen, wie sie den Risiken begegnen und möglichen Schaden abwenden können. Betreffende Tätigkeiten müssen ständig erneut geprüft und deren Folgenabschätzung stets aktuell gehalten werden.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist für alle Unternehmen Pflicht, in denen in der Regel mehr als 9 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Bei der Ermittlung der Personenzahl ist es egal, ob es sich bei der Person um einen Angestellten, Inhaber, Auszubildenden oder Praktikanten handelt. Ebenso ist die wöchentliche Stundenzahl irrelevant – entscheidend ist die Zahl der Köpfe. Unabhängig von der Personenzahl ist ein Datenschutzbeauftragter zu bestellen, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, Markt- oder Meinungsforschung verarbeitet oder genutzt werden.

Die Bestellung des Datenschutzbeauftragten hat bei Aufnahme der verarbeitenden Tätigkeiten zu erfolgen und ein Schriftstück sollte die wesentlichen Rechte und Pflichten beider Parteien enthalten. Zum Datenschutzbeauftragten darf jedoch nur bestellt werden, der die dazu erforderliche Fachkunde und Zuverlässigkeit besitzt. Ebenso muss die bestellte Person unabhängig sein und die Lage objektiv betrachten können. Daher scheiden zum Beispiel die jeweiligen Inhaber des Unternehmens aus.

Die Kontaktdaten sind samt der Mitteilung über die Bestellung entsprechender Aufsichtsbehörde zu melden und zu veröffentlichen (Postanschrift, Telefon und E-Mail). Dies hat zum Beispiel auf der Website und in der Datenschutzerklärung zu erfolgen.

Eine sinnvolle Lösung für betroffene Unternehmen kann auch die Bestellung eines externen Datenschutzbeauftragten sein. Sind keine passenden Mitarbeiter im Unternehmen oder eine interne Besetzung nicht gewünscht, kann der externe Datenschutzbeauftragte mit seiner Fachkompetenz und Unabhängigkeit für das Unternehmen und im Sinne des Datenschutzes tätig werden.

Auskunftspflicht

Betroffene können Auskunft darüber verlangen, welche Daten zu welchem Zweck über sie verarbeitet werden und ob und welche Daten auf welcher Grundlage über sie weitergegeben werden. Ferner haben sie den Anspruch darauf eine Kopie der Daten zu erhalten. Eine Anfrage muss umgehend, innerhalb eines Monats, beantwortet werden. Entsprechend sinnvoll kann es jetzt schon sein, sich entsprechend darauf vorzubereiten und eine „1-Klick-Auskunft" in bestehende Systeme zu implementieren und/oder entsprechende Formulare vorzubereiten.

Die Personen können ebenso ihren Anspruch ihre Daten zu berichtigen oder zu ergänzen durchsetzen und einen Widerspruch gegen die Verarbeitung ihrer Daten einlegen. Diese Wünsche müssen dann umgehend umgesetzt werden. Es gibt nur wenige Fälle, in denen eine weitere Verarbeitung dann noch zulässig ist. Dies könnte zum Beispiel dann der Fall sein, wenn die Daten noch zur Geltendmachung eines Anspruches benötigt werden.

Kontinuierliche Kontrolle der Prozesse und Anpassung der Dokumentation

Nach der ganzen Arbeit freuen Sie sich sicherlich, dass Sie es endlich geschafft haben. Zu Recht! Doch leider muss ich Ihnen mitteilen, dass sie die implementierten Prozesse in regelmäßigen Abständen erneut auf den Prüfstand stellen müssen. Die Technik entwickelt sich fortwährend weiter und neue Mechanismen im Bereich der Sicherheit sollten auch bei Ihnen zum Datenschutz eingesetzt werden.

Ihr Unternehmen unterliegt zahlreichen Veränderungen, sobald davon auch die Verarbeitung von personenbezogenen Daten betroffen ist, müssen Sie die Auswirkungen der Veränderung auch hinsichtlich der DSGVO prüfen und zum Beispiel Ihr Verarbeitungsverzeichnis anpassen.

Das Verarbeitungsverzeichnis muss ohnehin, auch ohne eine Anpassung der Vorgänge, turnusmäßig aktualisiert werden. Dies soll mindestens einmal im Jahr erfolgen.

Meldepflicht

Unternehmen haben bei einem Datenschutzverstoß eine Meldepflicht gegenüber den Aufsichtsbehörden. Sie entfällt lediglich, wenn Sie in der Lage sind zu beweisen, dass der Verstoß nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führen wird. Die Prüfung dessen muss zu Nachweiszwecken dokumentiert werden.

Wenn ein Verstoß hochwahrscheinlich ist, hat die Meldung innerhalb von 72 Stunden zu erfolgen. Erfolgt die Meldung später, muss sie begründet werden. Es empfiehlt sich die Meldung vorab per E-Mail und gesondert per Einschreiben durchzuführen.

Aber auch die Betroffenen haben ein Recht auf Meldung des Vorfalls. Hier ist eine E-Mail ausreichend, welche jedoch viele Einzelheiten über den Vorfall enthalten muss, die vorher genau geprüft werden sollten.

Sonderregelungen

Neben diesen Basics der DSGVO gibt es eine nicht unbedeutende Zahl von verschärften Vorschriften. Diese betreffen unter anderem besonders sensible Daten, wie zum Beispiel Gesundheitsdaten und Daten zur sexuellen Gesinnung.

Auch Minderjährige und Angestellte des Unternehmens sind besonders geschützt und für eine wirksame Einwilligung in der Verarbeitung von personenbezogenen Daten sind höhere Hürden gesetzt, aber jene Einwilligung sollte ohnehin die zweite Wahl sein. Besser ist es ohnehin die Verarbeitung durch eine gesetzliche Grundlage legal umzusetzen.

Hilfen bei der Umsetzung

Datenschutz ist Chefsache! Doch neben dem Tagesgeschäft bleibt oft wenig Zeit für eine konforme Umsetzung der Vorschriften. Hilfe können Unternehmensberater, Datenschutzbeauftragte, IT-Spezialisten und Rechtsanwälte bieten.

Unternehmensberater

Unternehmensberater, wie ich, sind kompetente Unterstützer bei der Schaffung einer DSGVO-Konformität. Wir sind es gewohnt Prozesse zu analysieren und Lösungswege zu suchen, zu entwickeln und umzusetzen. Mit fachlichem Know-How, zahlreichen Vorlagen und individuellen Umsetzungen können wir Sie ideal begleiten und Ihnen die Umsetzung der DSGVO deutlich vereinfachen. Auch Schulungen rund um das Thema Datenschutz sind möglich. Unter Umständen kann die Beratung zur DSGVO auch gefördert werden. Weitere Informationen zu den Fördermöglichkeiten finden Sie in dem nachfolgenden Kapitel.

Externer Datenschutzbeauftragter

Wenn Sie ohnehin einen Datenschutzbeauftragten benötigen, bietet es sich an einen externen Datenschutzbeauftragten in Ihr Unternehmen zu holen. Dieser ist mit seinem Fachwissen gut dafür geeignet und begleitet Sie, auch nachdem der Unternehmensberater mit Ihnen alle notwendigen Maßnahmen umgesetzt hat, fortlaufend.

Rechtsanwalt

Auch ein Anwalt ist ein geeigneter Partner, der Ihnen zum Beispiel eine Datenschutzerklärung, Einwilligungserklärung und notwendige Formulare, vollkommen auf Sie zugeschnitten, erstellt. Zudem kann er prüfen, ob eine Verarbeitung rechtskonform ist.

IT-Dienstleister

Zur Umsetzung verschiedener Sicherheitsstandards in Ihrem Unternehmen stehen Ihnen IT-Dienstleister zur Seite. Insbesondere die Absicherung Ihres Netzwerkes und Datenbanken sowie effiziente Backuplösungen stehen dabei im Fokus.

Beratung & Förderung

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle fördert mit dem Programm „Förderung unternehmerischen Know-hows“ die Beratung von Unternehmen. Hierfür muss der Berater, wie ich, bei dem Bundesamt gelistet sein. Das Programm sieht eine Förderung von 80% der Beratungskosten vor, wenn das Unternehmen seinen Sitz in Mecklenburg-Vorpommern hat.

Weiterführende Informationen erhalten Sie gern auf Anfrage.

Disclaimer

Diese Ausarbeitung erhebt aufgrund der Komplexität der Thematik keinen Anspruch auf Vollständigkeit. Sie soll Ihnen vielmehr einen ersten Eindruck von den Regelungen der DSGVO bieten und kann eine professionelle Beratung zu dem Thema nicht ersetzen. Durch rechtliche Neuerungen können sich Änderungen ergeben.
Stand: Februar 2018

grabowski
UNTERNEHMENSBERATUNG & COACHING

Im Fokus meiner Tätigkeit als Unternehmensberater steht die systematische und professionelle Beratung kleiner und mittelständischer Unternehmen in allen erdenklichen Unternehmensphasen - von der Gründung bis zur Suche nach einer Unternehmensnachfolge.

Aktuelle Themen in der Beratung:

- Einhaltung der neuen DSGVO
- Fachkräftemangel & Onboarding
- Start-Up-Beratung & Businessplan
- Marketingberatung
- Strategieberatung uvm.

- gelisteter Berater beim Bundesamt für Wirtschaft und Ausfuhrkontrolle
- gelistet bei der Beraterbörse der KfW
- bis zu 90% Förderung möglich

grabowski
UNTERNEHMENSBERATUNG & COACHING

INH. STEFFEN GRABOWSKI

Johannesstraße 15b
17034 Neubrandenburg
Tel. (0395) 70 79 114
info@grabowski-beratung.de

Warener Straße 28
17153 Stavenhagen
Mobil (0151) 588 10 474
www.grabowski-beratung.de