GEWERBE · HANDWERK
STEIERMARK

DIE DATENSCHUTZGRUNDVERORDNUNG - SCHNELLANLEITUNG FÜR DIE UMSETZUNG IN IHREM BETRIEB

Ausgangslage

Die Datenschutz-Grundverordnung (DSGVO) tritt am 25.5.2018 in Kraft. Bestimmte Daten sollen dadurch besser geschützt werden – daraus ergibt sich eine Reihe an Verpflichtungen für UnternehmerInnen.

BIN ICH BETROFFEN?

Jedes Unternehmen, das Daten von Personen verarbeitet, ist betroffen.

Kaltstart für Eilige:

- Erstellen Sie ein Verarbeitungsverzeichnis – welche Daten verarbeiten Sie im Unternehmen? Eventuell haben Sie schon einmal eine Meldung an das Datenverarbeitungsregister (DVR) gemacht. Diese können Sie als Basis heranziehen.
- Zum Muster: wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.DOCX
- Sorgen Sie dafür, dass Kunden auf deren Anfrage hin eine Auskunft erhalten, welche Daten Sie von ihnen verarbeiten (binnen eines Monats) – und dass diese Daten berichtigt und gelöscht werden können.
- Ein Gedanke zur Löschung der Daten: Oft muss das auch mit dem Anbieter der Software geklärt werden, die Sie verwenden. Denn manche Datenbanken sind gar nicht auf Löschung ausgelegt.
- Geben Sie Daten an externe Dienstleister weiter? Etwa an Ihren Steuerberater? Oder speichern Sie Kundendaten online in Clouds? – Dann sichern Sie sich vertraglich ab, dass dieser Dienstleister die Daten mit ausreichenden Sicherheitsmaßnahmen behandelt. Informieren Sie die Kunden außerdem darüber, etwa mit einem Merkblatt https://dsgvo-informationsverpflichtungen.wkoratgeber.at/
  Dieses Merkblatt können Sie gleich zur Erfüllung der Informationspflichten bei Erhebung von Kundendaten heranziehen.
- Datensparsamkeit: Erheben Sie (ab jetzt) nur die Daten von Kunden, die Sie wirklich brauchen.
- Haben Sie die Zustimmung des Kunden zur Datenverarbeitung, und zwar schriftlich? Falls nicht, misten Sie Ihren Datenbestand aus und lassen Sie nur Daten über, wo nachweislich eine Zustimmung des Kunden gegeben ist. Bei Vertragsverhältnissen reicht da übrigens der Vertrag an sich aus. Denn für die Ausführung eines Vertrags, ist die Erhebung der nötigen Daten einfach erforderlich. Das heißt aber: Fällt der Vertrag weg, müssen Sie die Daten löschen. (Ausnahme: gesetzliche Fristen wie etwa sieben Jahre in der Buchhaltung)

WIE HOCH IST MEIN AUFWAND?

Der Aufwand ist eher hoch und betrifft vor allem Unternehmen, die sich bisher nicht um Datenschutz gekümmert haben.

WAS ÄNDERT SICH?

Zum Beispiel muss ein Verarbeitungsverzeichnis für die Daten erstellt werden und die Rechte Betroffener werden ausgeweitet (Recht auf Löschung, Recht auf Auskunft). Auch das Bußgeld bei Verstößen wird deutlich erhöht. Die für die Verhängung von Bußgeldern verantwortliche Datenschutzbehörde hat allerdings klar gestellt, dass der Grundsatz „Beraten statt Strafen" im Vordergrund steht.

GEWERBE · HANDWERK
STEIERMARK

DIE DATENSCHUTZGRUNDVERORDNUNG - SCHNELLANLEITUNG FÜR DIE UMSETZUNG IN IHREM BETRIEB

FÜR WELCHE DATEN GILT DIE VERORDNUNG?

Als erstes gilt es, den Begriff der „Daten", die betroffen sind, zu klären.

Die DSGVO regelt alles rund um personenbezogene Daten – also alles, was eine bestimmte Person erkennbar machen kann. Das können IP Adressen sein, aber auch ein Foto oder eine Adresse mit Namen.

Anonyme Daten wie z.B. Statistiken sind nicht betroffen.

Diese Daten werden geschützt, egal ob sie von Ihnen erhoben, gespeichert oder übermittelt werden.

Sensible Daten müssen noch besser geschützt werden – etwa Gesundheitsdaten. Diese sollten Sie nur verarbeiten, wenn eine ausdrückliche Zustimmung Betroffener oder ein gesetzlicher Auftrag vorliegen!

WANN DARF ICH JETZT DIESE PERSONENBEZOGENEN DATEN VERARBEITEN?

- Sie dürfen die Daten verarbeiten, wenn die betroffene Person eingewilligt hat. Von einer Einwilligung kann man auch ausgehen, wenn die Person Ihnen freiwillig Daten gibt, z.B. sich für einen Newsletter auf Ihrer Homepage einträgt oder ein Datenblatt genau ausfüllt.
- Sie haben einen Vertrag zu erfüllen. Ein Beispiel: Wenn eine Person sich von Ihnen fotografieren lässt ist davon auszugehen, dass Sie dieses Bild aufnehmen dürfen. Möchten Sie das Bild aber auf Ihre eigene Homepage stellen, etwa zu Werbezwecken, benötigen Sie eine zusätzliche Einwilligung.
- Gesetzliche Pflichten. Für die Buchhaltung müssen Belege sieben Jahre aufbewahrt werden. Das ist ein typisches Beispiel für die gesetzliche Aufbewahrungspflicht. Weitere Aufbewahrungspflichten finden Sie hier: wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html
- Ihre berechtigten Interessen. Diese Interessen betreffen Ihr Unternehmen und umfassen auch wirtschaftliche Interessen! Da geht es zum Beispiel um Verarbeitung von Daten zur Gewinnsteigerung und um die Optimierung des Kundenservice. Vor allem im Marketing wird diese Bestimmung eine große Rolle spielen, etwa wird das Verwenden von Werkzeugen wie Google Analytics dadurch möglich gemacht.

  Alle Verarbeitungen, die vernünftigerweise für den Betroffenen „erwartbar" sind, werden so möglich gemacht.

  Direktwerbung an Bestandskunden für ähnliche Produkte bleibt damit erlaubt.

SPEZIALREGELN FÜR BESONDERS SENSIBLE DATEN

Alles, wo es um heikle Themen wie Sexualität, Gesundheit, Ethnie, Biometrie, Genetik, Religion oder Politik geht, muss besonders beachtet werden.

Hier braucht man auf jeden Fall eine ausdrückliche Einwilligung der Betroffenen und muss fallweise auch einen Datenschutzbeauftragten bestellen (siehe nächste Frage).

Wenn Sie im großen Umfang sensible Daten verarbeiten, ist auch eine Folgeabschätzung durchzuführen. Das ist Aufgabe Ihres Datenschutzbeauftragten.

WER BRAUCHT EINEN DATENSCHUTZBEAUFTRAGTEN?

Zwingend ist der nur für Unternehmen, deren Kerntätigkeit regelmäßige umfangreiche Überwachung ist (etwa Detektive) oder die als Kerntätigkeit besondere Datenkategorien wie etwa Gesundheitsdaten verarbeiten. Der Datenschutzbeauftragte kann ein eigener Mitarbeiter sein, man kann aber auch einen externen Datenschutzbeauftragten nominieren, etwa einen Anwalt oder einen dafür zertifizierten Anbieter.

GEWERBE · HANDWERK
STEIERMARK

DIE DATENSCHUTZGRUNDVERORDNUNG - SCHNELLANLEITUNG FÜR DIE UMSETZUNG IN IHREM BETRIEB

MUSS ICH EIN VERARBEITUNGSVERZEICHNIS ERSTELLEN?

Sofern Sie nicht nur gelegentlich Daten verarbeiten, ja. Die Datenschutzbehörde rät jedem Unternehmen, pro forma ein Verzeichnis zu erstellen. Darin sind alle Anwendungen enthalten, mit denen Sie Daten verarbeiten und auch, welche Daten das sind.

Tipp: Differenzieren Sie zuerst nach Abteilungen wie etwa „Schauraum, Montage, Werkstatt,....", und erst danach nach den Daten. In der Werkstatt kann es zum Beispiel Feed Back Bögen für Kunden geben, die man im Verzeichnis dann als eine Verarbeitungsart einträgt. Hier finden Sie ein Musterverzeichnis: wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.DOCX

Hier finden Sie diese Vorlage ausgefüllt mit Beispieldaten: wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-bsp-verarbeitungsverzeichnis-verantwortlicher.pdf

DATENSCHUTZERKLÄRUNG - INFORMATIONSPFLICHTEN

Sie nehmen Daten Ihrer Kunden auf, zum Beispiel weil Sie beim Schneidern von Kundenbekleidungen Maß nehmen. Dann müssen Sie nach der neuen Gesetzeslage ab 25.5.2018, streng genommen die Betroffenen, über bestimmte Details dazu informieren.

Die Zustimmung der Betroffenen benötigen Sie nicht – aber Sie haben eine Informationspflicht.

Wie Sie informieren müssen, sagt uns der Gesetzgeber aber nicht. Am einfachsten ist, Sie hängen einen Aushang gut sichtbar in Ihr Geschäft oder stellen eine Datenschutzerklärung auf Ihren Internetauftritt.

Hier finden Sie ein Informationsblatt mit den nötigen Daten zu Ihrer Verwendung: https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

Speziell für Ihre Homepage eignet sich dieses Muster: wko.at/service/wirtschaftsrecht-gewerberecht/muster-informationspflichten-website-datenschutzerklaerung.html

ICH VERSENDE NEWSLETTER AN MEINE KUNDEN

Der Versand von Newslettern wird rechtlich im Wesentlichen wie bisher gehandhabt. Man darf bestehenden Kunden weiterhin Newsletter schicken. Die Details dazu können Sie hier nachlesen: wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html

Etwa muss der Kunde die Möglichkeit haben, die Zusendung künftig abzubestellen.

ICH STELLE FOTOS MEINER MITARBEITERINNEN AUF MEINE HOMEPAGE

Dazu benötigen Sie die Einwilligung Ihrer Mitarbeiter.

ICH FILME UND FOTOGRAFIERE AUF MEINEN VERANSTALTUNGEN MIT

Auch dafür brauchen Sie eine Zustimmung der Veranstaltungsteilnehmer. Daher ist die beste Vorgangsweise, dem Anmeldeformular für die Veranstaltung eine kurze Information und Einwilligung beizulegen, die die Gäste mit unterschreiben.

WAS MACHE ICH MIT BEWERBUNGSUNTERLAGEN?

Im Gleichbehandlungsgesetz gibt es eine Bestimmung, dass Unterlagen sechs Monate für den Fall eines Prozesses aufbewahrt werden müssen. Diese Frist kann daher als Maßstab herangezogen werden. Nach Ablauf dieser sechs Monate sollten die Bewerbungsunterlagen vernichtet werden. Will man die Unterlagen länger aufheben, zum Beispiel für den Aufbau eines Pools, empfiehlt es sich, schon vorab eine Zustimmung der Bewerber einzuholen.

Achtung: Sozialversicherungsnummern oder die Konfession, die Bewerber angeben, sind sensible Daten. Dafür braucht man eine eigene Einwilligung! Im besten Falle frägt man diese Daten von den Bewerbern, etwa auf Online Formularen, einfach nicht mit ab. Gibt ein Bewerber die Daten von sich aus an, gilt die Einwilligung auf jeden Fall als erteilt.

GEWERBE · HANDWERK
STEIERMARK

DIE DATENSCHUTZGRUNDVERORDNUNG - SCHNELLANLEITUNG FÜR DIE UMSETZUNG IN IHREM BETRIEB

BRAUCHE ICH FÜR DATEN, DIE ICH SCHON VOR DER NEUEN DSGVO VERARBEITET HABE, EINE NEUE EINWILLIGUNG?

Wenn Sie irgendwann die Zustimmung des Betroffenen eingeholt haben, ist davon auszugehen, dass diese noch immer gilt. Gleiches gilt, wenn die Daten für die Vertragserfüllung nötig sind. Auch wenn Sie ein berechtigtes Interesse haben, ist von der Rechtmäßigkeit auszugehen.

Ansonsten empfiehlt sich, die DSGVO zum Anlass zu nehmen, alte und ungenutzte Daten auszumisten und zu vernichten.

DIE PERSONENBEZOGENEN DATEN WERDEN AN MEINEN STEUERBERATER, EVENTAGENTUR ODER ANDERE DIENSTLEISTER WEITERGEGEBEN.

Dann sichern Sie sich vertraglich ab, dass dieser Dienstleister die Daten mit ausreichenden Sicherheitsmaßnahmen behandelt.

Eine Vorlage für so eine Dienstleistervereinbarung finden Sie hier: wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Auftragsverarbeite.docx

Außerdem sind Sie verpflichtet, die Betroffenen (z.B. bereits bei Vertragsabschluss oder Anmeldung zur Veranstaltung) von dieser Weitergabe zu informieren.

Ein zugeschnittenes Merkblatt für die Betroffenen können Sie hier erstellen: https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

PRAKTISCHE BEISPIELE – WELCHE GEWOHNHEITEN KÖNNTEN EINE DATENSCHUTZVERLETZUNG SEIN?

Bei einem Newsletter den Verteiler für alle Empfänger sichtbar verschicken, geht – und ging auch vor der DSGVO – gar nicht. E-Mail Adressen Ihrer Kunden sind schützenswerte personenbezogene Daten!

Auch das Sammeln von Kundendaten auf Zetteln im Geschäft, wo sich andere Kunden bereits eingetragen haben, ist nach derselben Logik zu vermeiden.

WIE PACK ICHS JETZT AN?

- Klicken Sie sich zu allererst durch den Online Ratgeber, um Ihren momentanen Status abzufragen https://dsgvo.wkoratgeber.at/
- Entscheiden Sie, ob Sie einen Datenschutzbeauftragten brauchen; Zwingend ist der nur für Unternehmen, deren Kerntätigkeit regelmäßige umfangreiche Überwachung ist oder die als Kerntätigkeit besondere Datenkategorien wie etwa Gesundheitsdaten (sensible Daten) verarbeiten.
- Bestimmen Sie die zuständigen Mitarbeiter. Sie erstellen ein Verarbeitungsverzeichnis und sehen so, wo im Unternehmen die Verarbeitung von personenbezogenen Daten stattfindet.
- Prüfen Sie Ihre Verträge mit Unternehmen, denen Sie Daten weitergeben (z.B. Steuerberater). Aktualisieren Sie die Verträge gegebenenfalls und lassen Sie sich schriftlich versichern, dass mit den Daten DSGVO-konform umgegangen wird.
- Richten Sie einen Prozess ein, der Betroffenen die Auskunft über gespeicherte Daten – auf deren Anfrage – garantiert. Beachten Sie dabei die Frist von einem Monat, die nur im Ausnahmefall auf drei Monate verlängert werden darf.
- Sorgen Sie dafür, dass Daten, nachdem diese nicht mehr benötigt werden, gelöscht werden. Ebenso müssen die Daten auf Anfrage der betroffenen Person gelöscht oder berichtigt werden können.
- Aktualisieren Sie Ihre Datenschutzerklärungen für Betroffene (Kunden, Lieferanten etc.)
- Schulen Sie Beschäftigte und verpflichten Sie diese auf Verschwiegenheit.

Wir möchten darauf hinweisen, dass aus Gründen der leichteren Lesbarkeit auf diesen Seiten die männliche Sprachform verwendet wird. Sämtliche Ausführungen gelten natürlich in gleicher Weise für die weibliche.