Juni 2018

TAXtuell

Sonderausgabe zur DSGVO

„Erste-Hilfe-Paket“
zur DSGVO-Umsetzung

Häufige Fragen
zur DSGVO

Webseite DSGVO-fit
Was ist zu beachten

GSTÖTTNER & PARTNER
Steuerberatung

Dr. Klaus Gstöttner, StB

Thomas Hackl, BiBu

Mag. Rainer Moosbauer, StB

Vorwort

Die sog. Datenschutz-Grundverordnung (DSGVO) sowie deren verbindliche Umsetzung mit 25.5.2018 sind momentan in aller Munde. Aus diesem Anlass haben wir für Sie eine Sonderausgabe unseres Klientenmagazins TAXtuell mit dem Thema „DSGVO" gestaltet.

Im ersten Teil soll Ihrem Unternehmen ein „Erste-Hilfe-Paket" zur DSGVO-Umsetzung mitgegeben werden. Die Schritte 1-7 sind von allen Unternehmen, die Maßnahmen 8-10 nur von Unternehmen, die Mitarbeiter beschäftigen, durchzuführen. Für die Umsetzung vieler dieser Maßnahmen (z.B. Abklärung ob ein Datenschutzbeauftragter notwendig ist, Durchführung einer Risikoanalyse, Check der betrieblichen Sicherheitsmaßnahmen, Datenschutzerklärung gegenüber den Mitarbeitern und Datenschutz-Verpflichtungserklärung des Mitarbeiters) können Sie auf standardisierte Vorlagen zurückgreifen (die Sie auf unserer Homepage www.gstoettner-partner.at unter „AKTUELLES" zum Download finden). Andere Maßnahmen (Verarbeitungsverzeichnis, Datenschutzerklärung gegenüber den Kunden, Löschungskonzept,...) sind sehr branchenspezifisch und müssen demnach in Ihrem Unternehmen eigenständig erarbeitet werden.

Neben diesem „Ersten-Hilfe-Paket" haben wir betreffend die häufigsten (in unserer Kanzlei) aufgetretenen Fragen zur DSGVO eine FAQ-Seite gestaltet, die Ihnen ebenso die Umsetzung der DSGVO erleichtern soll.

Des Weiteren finden Sie in dieser Ausgabe eine Expertenmeinung, wie Ihre Webseite DSGVO-fit gemacht werden kann.

In den letzten Tagen haben Sie zudem unsere interne Datenschutzerklärung gegenüber Ihnen als Kunde und unsere um die DSGVO adaptierten neuen Allgemeinen Auftragsbedingungen erhalten (auch diese stehen Ihnen auf unserer Homepage als Download zur Verfügung). Sollten Fragen zu diesen Dokumenten bzw. allgemein zur Umsetzung der DSGVO in Ihrem Betrieb auftreten, stehen wir dafür gerne und jederzeit persönlich bzw. unter der E-Mail-Adresse datenschutz@gstoettner-partner.at zu Ihrer Verfügung.

Ihr,
Klaus Gstöttner

Downloads

Mit diesem QR-Code gelangen Sie direkt zu den im „Erste-Hilfe-Paket" erwähnten Vorlagen auf unserer Webseite.

Anleitung QR-Code: Kamera-App am Mobiltelefon öffnen; Code anvisieren; Webseite öffnet sich

„ERSTE-HILFE-PAKET“

zur DSGVO-Umsetzung

Schritt 1 - Abklärung, ob in Ihrem Unternehmen ein Datenschutzbeauftragter bestellt werden muss:
Ein Datenschutzbeauftragter ist nicht generell, sondern nur in bestimmten Fällen verpflichtend zu bestellen. Auf unserer Homepage steht Ihnen eine Checkliste zur Verfügung, die bei der Beurteilung helfen soll, ob für Ihr Unternehmen ein Datenschutzbeauftragter notwendig ist.

Schritt 2 - Erstellung eines Verarbeitungsverzeichnisses:
Eine der wohl zeitaufwändigsten Unternehmerpflichten ist die Erstellung eines unternehmensinternen Verarbeitungsverzeichnisses. Die **Pflicht** ein Verarbeitungsverzeichnis zu führen, **trifft de facto alle Unternehmer** (auch EPUs und KMUs). Zunächst ist die Erstellung einer „Dateninventur“ sinnvoll (= eine Auflistung, wo überall im Unternehmen personenbezogene Daten verarbeitet werden). Das Verarbeitungsverzeichnis ist das **„Herzstück“ des betrieblichen Datenschutzes**, weil es als allgemeine Informationsgrundlage für zahlreiche weitere datenschutzrechtliche Vorgänge dient (z.B. Erfüllung von Informations-, Auskunfts- und Löschpflichten gegenüber Geschäftspartnern und Mitarbeiter).
Das Verarbeitungsverzeichnis ist schriftlich oder in elektronischer Form zu führen. Es soll einen guten Überblick über die Datenverarbeitungen (insbesondere die Datenkategorien) bieten und ist ein bloß unternehmensinternes Dokument.
Das Verarbeitungsverzeichnis muss folgende Informationen enthalten:

- Namen und Kontaktdaten des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- Zwecke der Verarbeitung (z.B. Personalverwaltung)
- Kategorien der betroffenen Personen (z.B. Bewerber, Mitarbeiter) und Kategorien der personenbezogenen Daten (z.B. Name, SV-Nummer, Adresse, etc.)
- Kategorien von Auftragsverarbeitern und sonstigen Empfängern (z.B. IT-Dienstleister, etc.)
- wenn möglich: Die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich: Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherung der Datenverarbeitung (z.B. Zugangskontrolle zum Betrieb, versperrt gelagerte Daten, Passwortschutz der Datenträger etc.)

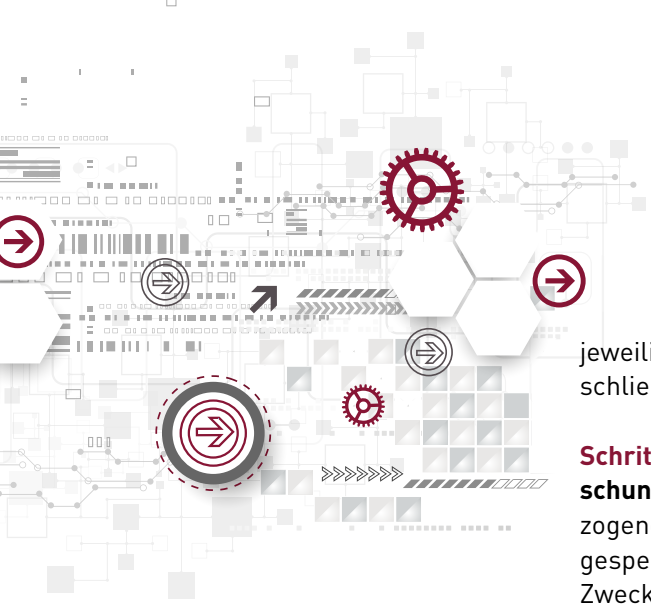
Bei der praktischen Erstellung eines Verarbeitungsverzeichnisses müssen immer die Verhältnisse der Branche und die Eigenheiten des Unternehmens berücksichtigt werden, weshalb es diesbezüglich keine allgemein verwendbare Vorlage gibt.

Schritt 3 - Informationspflicht gegenüber Kunden (sog. Datenschutzerklärung gegenüber Kunden):
Ihr Unternehmen muss Geschäftspartner (Kunden, Lieferanten etc.) in verständlicher und leicht zugänglicher Form (schriftlich oder elektronisch) darüber informieren, welche Daten in welcher Weise über diese verarbeitet werden. Die Datenschutzerklärung gegenüber Geschäftspartner kann in der Regel auch Online auf der Webseite des Unternehmens erfolgen, sofern dadurch eine leicht zugängliche Information gewährleistet ist. Die Datenschutzerklärung unserer Kanzlei gegenüber Ihrem Unternehmen müssten Sie in den letzten Tagen postalisch erhalten haben – zusätzlich steht diese auf unserer Homepage zum Download zur Verfügung.

Schritt 4 – Durchführung einer Risikoanalyse:
Anstelle der bisherigen DVR-Meldungen muss das datenverarbeitende Unternehmen nunmehr das Risiko der Datenverarbeitungen eigenverantwortlich beurteilen. Dabei sind zwei Schritte zu unterscheiden:

- **Allgemeine Risikoanalyse:** Jedes Unternehmen hat eine allgemeine Risikoanalyse durchzuführen, um festzustellen, ob die jeweilige Datenverarbeitung ein hohes Risiko für Rechte anderer Personen in sich birgt oder nicht. Auf unserer Homepage finden Sie eine Vorlage zur allgemeinen Risikoanalyse.
- **Datenschutz-Folgenabschätzung:** Nur wenn aufgrund der allgemeinen Risikoanalyse ein hohes Risiko erkennbar ist, ist eine Datenschutz-Folgenabschätzung vorzunehmen. Vor allem bei kleineren Unternehmen wird dies eher selten der Fall sein. Wenn sich aufgrund der allgemeinen Risikoanalyse hingegen die Notwendigkeit einer Datenschutz-Folgenabschätzung ergibt, sollte für deren Durchführung – aufgrund der Komplexität und des hohen Aufwands – ein erfahrener Datenschutzexperte zur Unterstützung beigezogen werden.

Schritt 5 – Check der betrieblichen Datensicherheitsmaßnahmen:
Jedes Unternehmen hat unter Berücksichtigung des Stands der Technik, der Kosten und der Schwere der Datenrisiken geeignete technische und organisatorische



Maßnahmen zu treffen, um ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten. Art und Umfang der in Betracht kommenden Sicherheitsmaßnahmen sind sehr vielschichtig. Den möglichen Datenschutzrisiken (z.B. infolge von technischen Problemen, organisatorischen Schwierigkeiten, Bedienungsfehlern, Computermissbrauch, Datendiebstahl, Schadsoftware, Pishing etc.) sollte mit einem ausgewogenen „Mix" aus verschiedenen Maßnahmen begegnet werden.
Eine Checkliste auf unserer Homepage soll zur Bestandsaufnahme über den aktuellen Sicherheitsstand (Status Quo) und gleichzeitig als Hilfe bei der Planung und Umsetzung betrieblicher Sicherheitsmaßnahmen dienen.

Schritt 6 – Abschluss von Auftragsverarbeitungsverträgen mit externen Auftragsverarbeitern: Beinahe jedes Unternehmen nimmt für die Erledigung seiner unternehmerischen Aufgaben auch externe Dienstleister in Anspruch (z.B. wird die betriebliche EDV von einem IT-Unternehmen betreut). Ein Unternehmen, das seinen Kooperationspartnern zwecks Ausführung vereinbarter Dienstleistungen Zugriff auf personenbezogene Mitarbeiter-, Kunden- oder sonstige Daten gewährt, muss sich vergewissern, dass diese Kooperationspartner über ein ausreichendes Datenschutzniveau verfügen. Dazu muss das Unternehmen einen Auftragsverarbeitungsvertrag in schriftlicher oder elektronischer Form mit dem jeweiligen Datenempfänger abschließen.

Schritt 7 - Erstellung eines Löschungskonzeptes: Personenbezogene Daten dürfen nur solange gespeichert werden, wie es für Zwecke der Verarbeitung erforderlich ist (Grundsatz der Speicherbegrenzung). Daher hat eine Löschung zu erfolgen, wenn die personenbezogenen Daten für die Verarbeitungszwecke nicht mehr gebraucht werden. Eine Ausnahme von der Löschpflicht gilt allerdings, solange die Daten zur Erfüllung gesetzlicher Aufbewahrungspflichten oder zur Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich sind. Es sollte ein Löschkonzept erarbeitet werden, das als Grundlage für die Durchführung der Löschungen dient. Im Falle einer Kontrolle durch die Datenschutzschutzbehörde ist es wichtig, dass die Existenz eines betrieblichen Schemas für die Verarbeitungsdauer (Fristen) und ein realistisches Prozedere für die Umsetzung dieser Fristen (Löschung der jeweiligen Daten) nachgewiesen werden kann.

Zusätzliche Maßnahmen für Unternehmen mit Mitarbeiter:

Nachfolgende Schritte hat Ihr Unternehmen nur dann durchzuführen, wenn von Ihnen Mitarbeiter beschäftigt werden.

Schritt 8 - Erfüllung der Informationspflicht gegenüber Mitarbeiter (sog. Datenschutzerklärung gegenüber Mitarbeiter): Der Arbeitgeber hat jeden seiner Mitarbeiter in präziser, verständlicher und leicht zugänglicher Form (schriftlich oder elektronisch) darüber zu informieren, welche Daten in welcher Weise über diesen verarbeitet werden. Diese Datenschutzerklärung gegenüber Mitarbeiter hat ehestmöglich, somit i.d.R. bei Eintritt des Mitarbeiters ins Unternehmen, zu erfolgen (z.B. durch Aushändigung oder Übermittlung des vorbereiteten Infodokuments an den Mitarbeiter). Auf unserer Homepage findet sich die Vorlage einer Datenschutzerklärung zum Download.

Schritt 9 - Abschluss von Geheimhaltungsvereinbarungen mit den Mitarbeitern (sog. Datenschutz-Verpflichtungserklärung des Mitarbeiters): Jeder Mitarbeiter hat personenbezogene Daten aus Datenverarbeitungen, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung zugänglich werden, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der Daten besteht. Der Arbeitgeber hat seine Mitarbeiter vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Dienstverhältnisses einzuhalten. Eine Vorlage dieser Datenschutz-Verpflichtungserklärung der Mitarbeiter finden Sie ebenfalls auf unserer Homepage.

Schritt 10 – Erstellung einer betrieblichen Datenschutzrichtlinie (Umgang mit Daten, Datenschutzanfragen, ...): Jedes Unternehmen hat unter Berücksichtigung des Stands der Technik, der Kosten und der Schwere der Datenrisiken geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten. Die Erstellung einer betrieblichen Datenschutzrichtlinie, die den Mitarbeitern nachweislich zur Kenntnis gebracht wird, ist daher zu empfehlen. Die tatsächliche Einhaltung dieser Richtlinie durch die Mitarbeiter ist im Betriebsalltag natürlich regelmäßig zu überprüfen.

Häufige Fragen

zur DSGVO

Sind wir als Steuerberater für Ihr Unternehmen Auftragsverarbeiter?
Diese Frage ist nicht unumstritten. Während uns die Wirtschaftskammer als Auftragsverarbeiter qualifiziert, sind wir nach Ansicht unserer Kammer (= Kammer für Steuerberater und Wirtschaftsprüfer, KSW) als Steuerberater aufgrund unserer berufsrechtlichen Unabhängigkeit und Eigenverantwortlichkeit in der Regel als Verantwortlicher im Sinne der DSGVO tätig, und demnach nicht als Auftragsverarbeiter zu qualifizieren. Die dazu von der KSW in Auftrag gegebene umfangreiche Stellungnahme ist ebenfalls auf unserer Homepage abrufbar. Bis zu einer endgültigen Klärung dieser Fragestellung vertreten wir die Ansicht der KSW, sodass Sie mit unserer Kanzlei keinen Auftragsverarbeitungsvertrag abschließen müssen.

Dürfen Sie Newsletter ausschließlich mit der Zustimmung Ihrer Kunden versenden?
Nein, wenn folgende fünf Voraussetzungen kumulativ gegeben sind, dürfen Sie Newsletter auch ohne explizite Kundenzustimmung versenden: 1.) die E-Mail-Adresse des Kunden wird beim Verkauf einer Ware/Dienstleistung erhoben, 2.) der Kunde erhält bei Erhebung der E-Mail-Adresse die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen, 3.) der Kunde erhält bei jeder Zusendung die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen, 4.) die Zusendung erfolgt zur Direktwerbung für eigene, ähnliche Produkte und 5.) der Kunde ist nicht in die sog „ECG-Liste“ eingetragen. Wenn eine dieser Voraussetzungen nicht vorliegt, brauchen Sie die Zustimmung des Kunden für den Newsletterversand.

Kann ich auf Rechnungen weiterhin Name und Anschrift des Kunden anführen?
Um weiterhin ordnungsgemäße Rechnungen gegenüber Ihren Kunden ausstellen zu können, können Name und Anschrift natürlich weiterhin auf den Rechnungen angeführt werden.

Wie ist mit Daten von Bewerbern, die nicht eingestellt wurden, umzugehen?
Die „Speicherbegrenzung“ bedeutet, dass Daten nur solange gespeichert werden dürfen, wie dies erforderlich ist. Wird ein Bewerber abgelehnt, kann eine Aufbewahrung jedenfalls noch 6 Monate argumentiert werden (Frist zur Geltendmachung von Ansprüchen nach dem Gleichbehandlungsgesetz). Möchte man Bewerberdaten darüber hinaus speichern, ist dazu die Zustimmung des Bewerbers einzuholen.

Welche Strafen drohen, wenn die DSGVO nicht korrekt umgesetzt wird?
Grundsätzlich sind die in der DSGVO verankerten Geldstrafen (Geldbußen bis maximal € 20 Millionen bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes), welche von der Datenschutzbehörde verhängt werden können, sehr hoch. Am 20.4.2018 hat der Nationalrat allerdings das Datenschutz-Deregulierungsgesetz beschlossen, in welchem (sofern europarechtlich zulässig) der Grundsatz der Verhältnismäßigkeit bei der Verhängung von Strafen und „Beraten statt Strafen“ explizit verankert wurden. Das heißt: Bei Erstverstößen werden Unternehmen grundsätzlich mit einer Abmahnung davonkommen, erst im Wiederholungsfalle wird es Geldbußen geben.

Zudem hat jede Person (Kunde, Mitarbeiter,...), der wegen eines Verstoßes nach der DSGVO ein materieller oder immaterieller Schaden entstanden ist, das Recht gegen den Verantwortlichen bzw. Auftraggeber Schadenersatz geltend zu machen.

Kann ich für Verstöße vor 25.5.2018 bestraft werden?
Unternehmen müssen sich um allfällige vor 25.5.2018 begangene Verstöße keine Gedanken im Sinne der DSGVO machen, da diese auch nach dem In-Kraft-Treten der DSGVO nach den alten Bestimmungen beurteilt werden.

Für individuelle Fragen zur DSGVO
stehen wir Ihnen gerne zur Verfügung.

Wie mache ich meine Webseite DSGVO-fit?

Die Aufnahme des Ist-Zustandes zur Identifizierung der einzelnen TO-DOs ist essentiell, um zu prüfen, ob Ihre Webseite DSGVO-fit ist. Für jede Seite und Unterseite muss klar ersichtlich sein, welche Funktionen und Tools personenbezogene Daten erfassen, speichern und verarbeiten. Zudem sollte jeder Webseitenbetreiber wissen, auf welchen Seiten welche Daten anfallen, die an externe Unternehmen weitergeleitet werden.

Sobald personenbezogene Daten an Dritte weitergegeben werden, ist ein Vertrag zur Auftragsdatenverarbeitung abzuschließen. Typische Vertragspartner sind beispielsweise der Hosting-Provider, der externe EDV-Anbieter oder Google Analytics.

Ebenso sollte man kritisch prüfen, ob die Zustimmungstexte in allen Formularen den Anforderungen der DSGVO entsprechen und ob die Nutzer hinreichend auf ihre Rechte hingewiesen werden.

Einige Punkte, die nunmehr explizit in der DSGVO verankert sind, werden in der Regel im Rahmen einer Webseitenerstellung bereits standardmäßig umgesetzt, andere Anforderungen kommen neu hinzu. Beispiele für derartige umzusetzende Anforderungen sind:

OFFENE PUNKTE	TO-DO
Die Webseite ist nicht verschlüsselt	SSL-Verschlüsselung aktivieren
Die Datenschutzerklärung ist nicht konform oder unvollständig	Formulierung der Datenschutzerklärung überarbeiten bzw. ergänzen
Es gibt keine Einwilligungserklärung für die Datennutzung	Einwilligungserklärung einbinden
Die Datenschutzerklärung ist nicht offensichtlich auffindbar	Datenschutzerklärung als eigene Unterseite anlegen und im Hauptmenü oder im unteren Bereich verlinken
Cookie-Hinweis existiert nicht	Cookie Hinweis auf der Webseite einbinden
Analysetools zeichnen alle Daten auf	Die Einbindung des Analysetools kontrollieren und die IP anonymisieren

Abschließend sei darauf hingewiesen, dass jede Webseite unterschiedlich aufgebaut ist und auf verschiedenen Technologien basieren kann. Wenn Unklarheiten bestehen, sollte man sich individuell beraten lassen.

Diesbezüglich können wir Ihnen folgende Experten empfehlen:

ecreation e.U.
Inhaber: Christoph Zeller, MSc
Wagnergasse 5
4210 Unterweitersdorf
www.ecreation.at
TelNr.: 0699/17077912

Webonia e.U.
Inhaber: DI Alexander Hennerbichler
Technologiepark 17
4320 Perg
www.webonia.at
TelNr.: 07262/21810

Impressum
Herausgeber: Gstöttner & Partner Steuerberatung GmbH & Co. KG, Linzer Straße 10, 4320 Perg
Redaktion: Dr. Klaus Gstöttner, Mag. Rainer Moosbauer Gestaltung: Consolution GmbH, Bildnachweis: istock.com, projects4.com