Umfassende, professionelle Beratung

Steuerplanung ♦ Steueroptimierung
Umstrukturierungen ♦ Transaktionen
Jahresabschuss ♦ Steuererklärungen
Buchhaltung ♦ Personalverrechnung
Controlling ♦ Wirtschaftsberatung

PECUNIA
Steuerberatung

Ihr Erfolg und Ihre Zufriedenheit sind unser Ziel!
Kompetenz ♦ Kreativität ♦ Verlässlichkeit

A-3500 Krems/Donau, Austraße 13/1/3
Tel. +43-2732-712 39
Fax. +43-2732-712 39-30
E-mail: office@pecunia-wt.at
www.pecunia-wt.at
WT-Code 804276
UID-Nr.: ATU62397427

Krems/Donau, im Mai 2018

PECUNIA NEWS – Steuerrecht und Wirtschaft

Sind Sie schon DSGVO-fit?
Eine Kurzdarstellung und Checkliste

Die Datenschutz-Grundverordnung (DSGVO) ist immer dann zu beachten, wenn **personenbezogene Daten** (zB Name, Adresse, Geburtsdatum, IP-Adresse) von **natürlichen Personen** erhoben, gespeichert, verändert, verwendet oder übermittelt werden. Wir gehen davon aus, dass fast jedes Unternehmen betroffen ist (zB durch Erstellung einer Kundendatei, Mitarbeiterdatenbank etc.). Datenschutz ist über den 25.05.2018 hinaus ein permanenter Prozess, da sich die Beurteilung eines gesetzeskonformen Datenschutzes am jeweiligen Stand der Technik orientiert.

- Analysieren Sie, welche **personenbezogenen Daten** erhoben und verarbeitet werden

  - Verarbeiten Sie neben „normalen“ (nicht-sensiblen) personenbezogenen Daten auch **sensible Daten**? (zB Daten über rassische, ethnische Herkunft, politische Meinungen, religiöse, weltanschauliche Überzeugungen, genetische, biometrische Daten, Gesundheit, Sexualleben). Für diese sensiblen Daten bestehen ein höheres Datenschutzniveau und umfangreichere Vorgaben.
  - Nicht betroffen von der DSGVO sind lediglich rein private oder familiäre Datenverarbeitungen (zB Sammlung von Urlaubsfotos). Manuelle Datensammlungen (zB händisches Telefonverzeichnis) unterliegen nur dann nicht dem Datenschutz, wenn sie nicht strukturiert und durchsuchbar sind.

- Prüfen Sie, ob Sie als **Verantwortlicher oder Auftragsverarbeiter** Daten verarbeiten

  - **Verantwortlicher**: entscheidet darüber, welche personenbezogenen Daten für welchen Zweck verarbeitet werden. Der Verantwortliche ist für die Einhaltung sämtlicher datenschutzrechtlichen Vorgaben verantwortlich und haftbar.
  - **Auftragsverarbeiter**: verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Der Auftragsverarbeiter entscheidet also nicht selbst, sondern hat den Weisungen des Verantwortlichen zu folgen. Er haftet der von der Datenverarbeitung betroffenen Person nur für Schäden im Rahmen seiner vertraglichen Pflichten.

▪ Beachten Sie die **datenschutzrechtlichen Grundsätze** bei jeder Datenverarbeitung

- **Rechtmäßigkeit:** Werden die Daten rechtmäßig erhoben? Jede Verarbeitung muss auf einer Rechtsgrundlage beruhen.
- Grundsatz von **Treu und Glauben**: Jede Verarbeitung muss sich im Rahmen der vernünftigen Erwartungen der von der Datenerhebung betroffenen Person bewegen.
- **Transparenz:** Ihre Datenverarbeitung muss für die betroffene Person transparent (nachvollziehbar) sein. Alle Informationen und Mitteilungen müssen leicht zugänglich und verständlich sein.
- **Zweckbindung:** Jede Datenverarbeitung darf nur zu einem im vorhinein festgelegten legitimen Zweck erfolgen. Eine Weiterverarbeitung zu einem anderen Zweck ist nicht bzw. nur eingeschränkt möglich. Die Daten sind bei Zweckerreichung grundsätzlich zu löschen.
- **Datenminimierung**: Jede Verarbeitung ist auf das unbedingt erforderliche Maß zu beschränken.
- **Richtigkeit**: Nur sachlich richtige Daten dürfen verarbeitet werden. Unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen.
- **Speicherbegrenzung**: Die Daten dürfen nicht länger gespeichert werden, als für die Zweckerreichung nötig ist.
- **Integrität und Vertraulichkeit**: Die Daten sind vor unbefugter Verarbeitung und vor unbeabsichtigtem Verlust/Zerstörung zu schützen.

Der Verantwortliche hat Maßnahmen zu treffen, damit er die Einhaltung dieser Grundsätze nachweisen kann (Dokumentations-/Rechenschaftspflicht).

▪ Werden die Daten **rechtmäßig** erhoben und verarbeitet?

Die Verarbeitung von personenbezogenen Daten ist nur dann zulässig, wenn sie ausdrücklich gesetzlich erlaubt ist. Folgende **Rechtsgrundlagen** sind bei (normalen) nicht-sensiblen Daten möglich:

- Einwilligung der betroffenen Person. Eine Einwilligung kann jederzeit widerrufen werden!
- Vertragsanbahnung und Vertragserfüllung
- Erfüllung einer rechtlichen Verpflichtung: zB Daten für Anmeldung eines Arbeitnehmers
- Schutz lebenswichtiger Interessen und öffentlicher Interessen
- Berechtigtes Interesse: Eine Datenverarbeitung zum Zweck der Direktwerbung könnte ein berechtigtes Interesse darstellen.

▪ Welche **Pflichten** haben Sie als **Verantwortlicher** zu erfüllen?

- Führung eines **Verarbeitungsverzeichnisses**
  Ist für Unternehmen mit weniger als 250 Mitarbeitern nur dann nicht verpflichtend, wenn die Datenverarbeitung

  a) nur gelegentlich erfolgt
  b) voraussichtlich kein Risiko für die betroffene Person darstellt
  c) keine sensiblen Daten erfasst.

Jedes Unternehmen, das eine monatliche Lohnverrechnung zu erstellen hat, verarbeitet regelmäßig Daten und hat daher ein Verarbeitungsverzeichnis zu führen. Ein Muster eines Verarbeitungsverzeichnisses ist von der Homepage der WKO downloadbar.

- **Datenschutz-Folgenabschätzung**
  Ist verpflichtend durchzuführen, wenn aus der Datenverarbeitung voraussichtlich ein sehr hohes Risiko für die Rechte und Freiheiten der betroffenen Personen entsteht und ist daher insbesondere bei Profiling und der Verarbeitung von sensiblen Daten notwendig.

- **Konsultationspflicht**
  Ergibt die **Datenschutz-Folgenabschätzung** tatsächlich ein hohes Risiko, das durch unternehmensinterne Maßnahmen nicht eingedämmt werden kann, ist vor der Datenverarbeitung die Datenschutzbehörde zu konsultieren.

- **Datenschutzbeauftragter**
  Eine Pflicht zur Bestellung besteht **unabhängig von der Unternehmensgröße** immer dann, wenn die **Kerntätigkeit** des Unternehmens

  a) eine regelmäßige und systematische Überwachung der betroffenen Personen erforderlich macht (zB Banken)
  b) in der umfangreichen Verarbeitung sensibler Daten besteht (zB Krankenhäuser)

  Der Datenschutzbeauftragte kann ein Mitarbeiter des Unternehmens oder ein externer Berater sein.

▪ Welche **Rechte der betroffenen Personen** haben Sie als Verantwortlicher zu beachten?

- **Informationsrecht (Datenschutzerklärung)**
  Sie müssen der von der Datenverarbeitung betroffenen Person **unaufgefordert** im Zeitpunkt der Datenerfassung folgende Informationen erteilen: Kontaktdaten des Verantwortlichen, Verarbeitungszweck, Rechtsgrundlage, Kategorie von Empfängern, Aufklärung über Betroffenenrechte (zB Auskunft, Berichtigung, Löschung, Widerruf, Beschwerde), Dauer der Datenspeicherung.
  Werden die Daten nicht bei der betroffenen Person selbst erhoben (sondern zB von dritter Seite erhalten), sind zusätzlich die Datenquelle und die Kategorie der personenbezogenen Daten binnen maximal eines Monats anzugeben.

- **Auskunftsrecht**
  Über Anfrage der betroffenen Person sind dieselben Informationen zu erteilen wie im Rahmen der Informationspflicht.

- **Berichtigungrecht hinsichtlich falscher Daten**

- **Löschungsrecht**
  Über Anfrage des Betroffenen sind die Daten zu löschen, wenn die Daten für den Verarbeitungszweck nicht mehr notwendig sind, die Einwilligung widerrufen wird oder Widerspruch erhoben wird. Keine Löschungspflicht besteht, wenn

  a) eine Verpflichtung zur weiteren Verarbeitung besteht (zB für gesetzliche Aufbewahrungsfristen)

b) die Daten für die Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich sind.

- **Einschränkung der Datenverarbeitung**
  Bei Aufforderung durch den Betroffenen, wenn ein Streit über die Berechtigung der Datenverarbeitung besteht

- **Recht auf Datenportabilität**

- **Widerspruchsrecht**
  Die betroffene Person kann Widerspruch erheben, wenn die Daten insbesondere aufgrund eines berechtigten Interesses des Verantwortlichen verarbeitet werden. Die Datenverarbeitung muss eingestellt werden, wenn der Verantwortliche nicht nachweisen kann, dass seine Interessen überwiegen oder die Daten zur Geltendmachung seiner Rechte erforderlich sind.

▪ Haben Sie bereits Verträge mit **Auftragsverarbeiter** abgeschlossen?

Ein Unternehmer kann sich für eine Datenverarbeitung eines Auftragverarbeiters bedienen. Zwischen dem Verantwortlichen und dem Auftragsverarbeiter ist aus datenschutzrechtlicher Sicht ein schriftlicher Vertrag abzuschließen, der insbesondere den Gegenstand, den Zweck und Dauer, die Art der Daten, die Weisungsgebundenheit usw. festzuhalten hat. Ein Muster für eine derartige vertragliche Vereinbarung ist von der Homepage der WKO downloadbar.

Hinweis: Auftragnehmer, die **eigenverantwortlich** tätig sind (zB Rechtsanwälte, Notare, Steuerberater) sind nicht als Auftragsverarbeiter, sondern als **Verantwortliche** zu sehen.

▪ Setzen Sie Maßnahmen zur **Datensicherheit** und zum **Datenschutz**

Folgende Maßnahmen sind zur Erhöhung der Datensicherheit und des Datenschutzes denkbar:

- **Authentifizierung und Zugriffskontrolle**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung. Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know“-Prinzip.
- **Passwortsicherheit** zur Authentifizierung
- **Verschlüsselung** von personenbezogenen Daten auf dem Übertragungsweg
- **Verschlüsselung mobiler Geräte**
- **Netzwerksicherheit** durch Einsatz einer Firewall und Anti-Viren Software
- **Installation von Sicherheitsupdates**
- **Scans nach Schadsoftware**
- **Verschwiegenheitspflicht der Dienstnehmer**
- **Schulungen** zu Fragen der Datensicherheit bzw. des Datenschutzes
- **Keine unnötige Verwendung administrativer Accounts**
- **Auswahl der Dienstleister**: Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, darf nur nach Abschluss einer Auftragsverarbeitervereinbarung erfolgen.
- **Sichere Datenentsorgung**
- **physische Zugangskontrolle**
- **Einbruchssicherheit**

- **Besonderer Schutz von Servern:** Der Zugang zu Räumlichkeiten, in denen sich Server befinden, sollte durch besondere Maßnahmen gesichert werden.
- **Schlüsselverwaltung**
- **Automatische und manuelle Prüfung von Logfiles**
- **Erkennung von Sicherheitsverletzungen durch Dienstnehmer**
- **Audits**
- **Datensicherung**: Es werden regelmäßig Datensicherungen erstellt und sicher an einem anderen Ort aufbewahrt.
- **Datenwiederherstellungskonzept** zur raschen Wiederherstellung von Daten
- **Meldepflicht für Dienstnehmer** im Falle von Sicherheitsverletzungen
- **Prozess für die Reaktion auf Sicherheitsverletzungen**: (z.B. Notfall-Telefonnummer für den IT-Support).

Weitere Informationen zum Thema Datensicherheit und Datenschutz finden Sie unter https://www.wko.at/site/it-safe/sicherheitshandbuch.html bzw. https://www.wko.at/site/it-safe/mitarbeiter-handbuch.html.

Hinweis:
Abschließend möchten wir darauf hinweisen, dass die in den PECUNIA-NEWS behandelten Themen aufgrund der Komplexität des Steuer- bzw. Wirtschaftsrechts vereinfacht und insbesondere nicht in allen Einzelfällen dargestellt sind bzw. sein können. Trotz sorgfältiger Bearbeitung kann keine Haftung für Richtigkeit und Vollständigkeit übernommen werden.

Für nähere Auskünfte zu diesen oder anderen Themen stehen wir Ihnen natürlich gerne zur Verfügung. Vereinbaren Sie bitte einen Termin mit uns: Tel. 02732/712 39, E-Mail: office@pecunia-wt.at

Es ist unser ständiges Bemühen, unsere Klienten bestmöglich zu betreuen und nutzenbringende Informationen zur Verfügung zu stellen. Wir hoffen, auch mit dieser Ausgabe der PECUNIA NEWS Ihre Erwartungen erfüllt zu haben und würden uns freuen, wenn Sie diese an Ihre **Geschäftsfreunde weiterleiten** (bitte beachten Sie dabei die Bestimmungen des TKG).

Hinweis nach TKG: Wenn Sie keine weiteren Fach-Newsletter von uns erhalten möchten, senden Sie bitte dieses E-Mail mit dem Hinweis „keine Newsletter erwünscht“ an uns retour. Sie werden daraufhin vom Verteiler gelöscht.

Firma und Sitz des Medieninhabers/Herausgebers:
PECUNIA Steuerberatung GmbH
Austraße 13/1/3, 3500 Krems/Donau
Tel.: +43 2732 712 39,
Fax: +43 2732 712 39-30
E-Mail: office@pecunia-wt.at
www.pecunia-wt.at
Landesgericht Krems, FN 274548y
Mitglied der Kammer der Wirtschaftstreuhänder
Auf unsere Tätigkeit ist das Wirtschaftstreuhandberufsgesetz (WTBG) anwendbar.
Unternehmensgegenstand des Medieninhabers:
Steuerberatung und Beratung in Wirtschaftsangelegenheiten
Geschäftsführer (GF) und Gesellschafter (GS) des Medieninhabers:
Mag. Martin Kirchwegerer (GF, 70% GS), Elfriede Leuthner (GF, 30% GS)
Grundlegende Richtung des Mediums:
Allgemeine Informationen auf dem Gebiet der Steuerberatung, des Wirtschaftsrechts und der Wirtschaftsberatung