Leitfaden für Steuerberater

Die europäische Datenschutz-grundverordnung

Ein Überblick

Autor: Nicolas Nagel, Senior Consultant für Datenschutz & CIS zertifizierter Datenschutzbeauftragter

Jänner 2018

Im Auftrag des Instituts Österreichischer Steuerberater

Die europäische Datenschutzgrundverordnung

Ein Überblick

Leitfaden für Steuerberater

herausgegeben vom
INSTITUT ÖSTERREICHISCHER STEUERBERATER

Der Leitfaden ist auf Grundlage der unsicheren und noch nicht in Geltung stehenden Rechtslage zur Datenschutz-Grundverordnung und zum Datenschutz-Anpassungsgesetz 2018 erstellt worden. Sämtliche Inhalte des Leitfadens sind völlig unverbindlich und erfolgen ohne Gewähr. Es handelt sich um keine abschließende Information. Diese unverbindliche Information kann eine Beratung durch Spezialisten nicht ersetzen, diese wird ausdrücklich empfohlen. Eine Haftung der Autoren und des INSTITUTS ÖSTERREICHISCHER STEUERBERATER sowie deren Organe wird ausgeschlossen.

1. Auflage 2018

Inhalt

Vorwort der Präsidentin des IÖS

Als neues Regelwerk für die gesamte Europäische Union wird die Datenschutzgrundverordnung (DSGVO) ab dem 25. Mai 2018 nach einer zweijährigen nationalen Umsetzungsphase nun auch in Österreich unmittelbar gelten. Bis zu diesem Zeitpunkt müssen alle Datenanwendungen und Geschäftsprozesse an die neue Rechtslage angepasst werden. Auch auf unseren Berufsstand kommen damit gravierende Änderungen zu.

Die Nichtbeachtung bzw. Verletzung der Bestimmungen der DSGVO ist mit empfindlichen Sanktionen und Geldbußen bedroht. Nachdem die Aufsichtsbehörden bereits angekündigt haben, die Einhaltung der DSGVO verstärkt prüfen zu wollen, ist es Gebot der Stunde, sich mit den Neuerungen zu befassen und diese rechtzeitig umzusetzen. Auch müssen die Mitarbeiter umfassend geschult werden.

Der Vorstand des Instituts Österreichischer Steuerberater hat sich daher entschlossen, den Steuerberatungskanzleien einen Leitfaden zur Verfügung zu stellen, der die Umsetzung der teilweise komplizierten und unklaren Bestimmungen ermöglichen und erleichtern soll. Weiters soll er bei der der Implementierung eines Datenschutzmanagementsystems unterstützen.

Da die Rechtslage derzeit noch unklar ist, bleiben zum Zeitpunkt der Herausgabe dieser Auflage noch ausstehende Aussagen, Empfehlungen und Arbeitsbehelfe der berufsrechtlichen Vertretung (KSW) abzuwarten. Dies betrifft insbesondere die Frage, ob bzw. unter welchen Voraussetzungen ein Datenschutzbeauftragter zu bestellen ist, eine Datenschutzfolgenabschätzung erforderlich ist und welche konkreten Daten in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen sind. Auch wird die Frage der Qualifikation des Steuerberaters als Verantwortlicher oder als Auftragsverarbeiter noch weiter zu würdigen sein.

Es freut mich sehr, Herrn Nicolas Nagel als Autor für diesen Leitfaden gewonnen zu haben. Er ist als zertifizierter Datenschutzbeauftragter beim TÜV Austria und als Lektor und Vortragender im Bereich Datenschutz tätig und somit ausgewiesener Fachmann im Bereich DSGVO. Ihm gilt mein besonderer Dank, ebenso wie meinem IÖS-Vorstandskollegen Mag. Christian Rauter für seine wertvolle Unterstützung.

Vordringliches Anliegen des Instituts Österreichischer Steuerberater ist es, den hohen Qualitätsstandard des Berufsstandes auch weiterhin sicherzustellen. Die Herausgabe des vorliegenden Leitfadens sehen wir als integralen Bestandteil der Qualitätssicherung an. Wir werden die Umsetzung der DSGVO auch weiterhin in Form von Vorträgen und Seminaren thematisieren und Sie auch über allfällige neue Rechtsansichten und Verwaltungsübungen und damit einhergehenden Anpassungsbedarf informieren.

Wien, im Jänner 2018

Dr. Christa Farmer, StB

Präsidentin des Instituts Österreichischer Steuerberater

Vorwort des Autors

LIEBE STEUERBERATERINNEN, LIEBE STEUERBERATER;

LIEBE LESERINNEN, LIEBE LESER,

die europäische Datenschutzgrundverordnung (DSGVO) gehört zu der bedeutendsten Gesetzesentwicklung der Europäischen Union in den letzten Jahren. Mit Stichtag 25. Mai 2018 wird sie das österreichische Datenschutzgesetz ablösen und muss dann auch in Österreich unmittelbar angewendet werden.

Aber was wird sich damit für Steuerberater ändern?
Wie wird sich die Datenschutzgrundverordnung auf die vielen alltäglichen Datenverarbeitungen und Unternehmensabläufe im Steuerberatungsbereich konkret auswirken – und zwar europaweit, von Brüssel über Wien und Lissabon bis nach Warschau?

Wie immer bei gesetzlichen Neuerungen ist anfangs vieles unklar und es gibt viele offene Fragen – dieser Leitfaden liefert dazu erste Antworten und Analysen, wie Datenverarbeitungen und Prozesse in diesem Bereich künftig vonstattengehen werden/müssen/sollten.

Mein Dank geht an den Vorstand des Instituts Österreichischer Steuerberater, mit dem dieser Leitfaden gemeinsam entstanden ist.

Sie, liebe Leserinnen, liebe Leser, finden hier konkrete Tipps und Hilfestellungen, wie Sie künftig personenbezogene Daten von Klienten, deren Mitarbeitern und Kunden sowie Ihren eigenen Mitarbeitern verarbeiten können.

Abschließend sei angemerkt, dass es sich dabei um Empfehlungen und meine konkrete und persönliche Sichtweise und um keine abschließenden Anweisungen handelt. Dieser Leitfaden soll letztendlich praktisches Hilfsmittel sein, damit Sie rasch und unkompliziert die neuen gesetzlichen Regelungen anwenden können.

Da der Bereich Datenschutz ein schnelllebiger und sich rasch verändernder Bereich ist und der stetigen Weiterentwicklung sowie Judikatsentscheidungen unterliegt, ist es ratsam sich weiterhin intensiv und kontinuierlich mit der Datenschutz-Grundverordnung zu beschäftigen und wo notwendig professionelle Unterstützung zu Rate zu ziehen.

Nicolas Nagel
CDPO, CIPM, CIPP
Senior Consultant für Datenschutz & zertifizierter Datenschutzbeauftragter

Wien, im Jänner 2018

1 Allgemeiner Überblick

Rahmen-bedingungen

Die Verarbeitung personenbezogener Daten einer Person unterliegt verschiedensten rechtlichen Regelungen. Die bedeutsamsten sind dabei insbesondere:

- Die EU-Datenschutzgrundverordnung (DSGVO)
- Das österreichische Datenschutzgesetz 2000 (DSG 2000)
- Das Datenschutzanpassungsgesetz 2018 (DSG 2018)

1.1 Die EU-Datenschutzgrundverordnung[1]

Harmonisierung des Datenschutz-rechts in Europa

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden.

Die Verordnung ersetzt ab 25. Mai 2018 die aus dem Jahr 1995 stammende Richtlinie 95/46/EG[2] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr sowie das österreichische Datenschutzgesetz (DSG 2000).

Im Gegensatz zur Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018.

Vorrang von EU-Recht

Die DSGVO regelt unter anderem die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen. Die bereits geltenden Betroffenenrechte werden erweitert und um neue Rechte ergänzt (z.B. um das Recht auf Datenübertragbarkeit oder das Recht auf Einschränkung).

[1] Vgl. http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1486463316887&uri=CELEX%3A32016R0679.
[2] Vgl. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046

Steuerberater sind in Ausübung mancher ihrer Dienstleistungen Auftragsverarbeiter im Sinne der DSGVO und für die „eigene" Datenverarbeitung (zB von Mitarbeiterdaten) sowie Bereiche der eigenverantwortlichen Dienstleistungserbringung, wie etwa die Steuerberatung und Prüfung, Verantwortliche i.S.d DSGVO – dieser Leitfaden zeigt daher auf, welche Neuerungen sich daraus für die Branche ergeben und worauf die Unternehmen unbedingt zu achten haben.

Verstärkte Kontrollen der Behörde

Das Datenschutzniveau wird mit der DSGVO nicht abgesenkt, sondern an einigen Stellen sogar weiter verschärft. Insbesondere bringt die DSGVO neue Transparenz- und Dokumentationsanforderungen für Verantwortliche der Datenverarbeitung und Auftragsverarbeiter mit sich.

Die Aufsichtsbehörden haben bereits jetzt angekündigt, die Einhaltung der Datenschutzgrundverordnung verstärkt prüfen zu wollen – umso wichtiger ist es daher, sich schon jetzt mit den geplanten Neuerungen zu befassen und diese rechtzeitig umzusetzen. Zumal die Eingriffsrechte der Aufsichtsbehörden und die Sanktionen, die gegen die Unternehmen verhängt werden können, wesentlich verschärft werden.

1.2 Das österreichische Datenschutzgesetz 2000[3]

DSG 2000 wird aufgehoben

Das Datenschutzgesetz 2000 ist ein österreichisches Gesetz, welches auf Basis der Datenschutz Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, etabliert wurde. Dieses gilt als Rechtsgrundlage, für die Verarbeitung personenbezogener Daten, bis zum 25. Mai 2018 in Österreich.

Aufgrund der Aufhebung des DSG 2000 mit gleichzeitigem Inkrafttreten der Datenschutzgrundverordnung am 25. Mai 2018 wird im Folgenden nicht mehr auf die Besonderheiten und Vorgaben des DSG 2000 näher eingegangen, sondern alle Ausführungen zu diesem Thema mit Bezug auf die DSGVO erläutert.

[3] Vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

1.3 Das österreichische Datenschutzanpassungsgesetz[4]

Das österreichische Datenschutzanpassungsgesetz 2018 („DSG 2018“) tritt ab 25. Mai 2018 gleichzeitig mit der DSGVO in Kraft.

Das DSG 2018 regelt insbesondere jene Bereiche des Datenschutzrechts, welche durch die DSGVO den europäischen Staaten zur näheren Regelung überlassen wurden bzw. einen Spielraum zur Ausgestaltung bieten oder ergänzende Regelungen vorschreiben.

Dieser Leitfaden geht in den nachstehenden Ausführungen und relevanten Bereichen auf die Spezifika des DSG 2018 entsprechend ein.

Das österreichische Ergänzungs- und Anpassungsgesetz zur DSGVO tritt gleichzeitig mit dieser in Kraft

2 Mythen rund um die Datenschutzgrundverordnung (DSGVO)

2.1 „Die DSGVO trifft mich als kleines Unternehmen doch nicht!“

Falsch!

Die Datenschutzgrundverordnung gilt für jede Person, jedes Ein-Mann Unternehmen, jeden klein- und mittelständischen Betrieb und jeden Konzern, der personenbezogene Daten verarbeitet. Dabei ist es unerheblich, ob die Daten elektronisch oder nicht-automatisiert verarbeitet werden.

Anwendbar auf alle Unternehmen

Ausnahmen bestehen nur im persönlichen oder familiären Tätigkeitsbereich (zB das private Adressbuch von Freunden) oder im staatlichen Bereich der nationalen Sicherheit.

Die DSGVO gilt daher gleichermaßen für:

- Einzelpersonen
- Unternehmen
- Vereine
- Parteien
- Behörden
- Öffentliche Stellen
- Stiftungen
- Bund, Länder, Gemeinden

[4] Vgl. https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.html

2.2 „Es hat bis jetzt niemanden interessiert – dies wird weiterhin so sein!“

Falsch!

Die Datenschutzgrundverordnung hat im Gegensatz zum bis dato geltenden DSG 2000 einen Strafrahmen von bis zu 20 Millionen Euro oder 4% des weltweit erzielten Jahresumsatzes eines Unternehmens! Das DSG 2000 hatte einen Strafrahmen von 25.000 Euro.

Strafen bis zu 20 Millionen Euro oder 4% des Jahresumsatzes

Weiters sind im Rahmen der DSGVO Verbandsklagen möglich, welche nun von Datenschutz-NGOs oder sonstigen Vereinigungen wahrgenommen werden können.

2.3 „Die Aufsichtsbehörde kontrolliert doch niemanden!“

Falsch!

Die österreichische Datenschutzbehörde hat zwar durchaus keine üppige personelle Ausstattung, jedoch soll sich dies mit Wirkung der DSGVO erheblich ändern und die Personalressourcen aufgestockt werden. Somit rücken flächendeckende Kontrollen deutlich näher.

Weiters muss sich die Behörde zur Prüfung in einem ersten Schritt nicht aktiv vor Ort in die Unternehmen begeben, sondern kann sich aufgrund der Rechenschaftspflicht der Unternehmen die Einhaltung der DSGVO nachweisen lassen.

Zusätzlich können betroffene Personen mittels Beschwerde bei der Behörde vorstellig werden und auf Missstände hinweisen. Dazu reicht oftmals ein Screenshot von unzulässigen Vertragsformulierungen, Missachtung von detaillierten Informationspflichten oder unrechtmäßig ausgestalteten Einwilligungserklärungen.

Beschwerderechte von betroffenen Personen

Dazu zählen insbesondere unzufriedene Kunden, Lieferanten, Mitarbeiter oder aber Wettbewerber!

Die Behörde geht jeder Beschwerde von betroffenen Personen nach. Somit führt jede Beschwerde zu einer konkreten Untersuchung gegen das Unternehmen. Das Unternehmen muss dann nachweisen, dass entgegen der Beschwerde die Datenverarbeitung im Rahmen der DSGVO erfolgt ist.

2.4 „Die DSGVO ändert ja nichts!“

Falsch!

Die Datenschutzgrundverordnung behält zwar viele Grundsätze des bestehenden Datenschutzrechts, führt allerdings auch zahlreiche Neuerungen für Unternehmen ein.

Dazu zählen insbesondere die zahlreichen Dokumentationspflichten, Verzeichnisse und Register neben den neu einzuführenden Unternehmensprozessen sowie Richtlinien und der Sicherstellung von Betroffenenrechten.

Unternehmen haben zukünftig durch eine geeignete Organisation die Einhaltung des Datenschutzes fortlaufend zu kontrollieren, zu adaptieren und proaktiv nachzuweisen.

Auch muss an die Datenschutzbehörde ein etwaiger Datenschutzbeauftragter gemeldet werden. Eine Behörde kann dabei relativ einfach mit Unternehmens- und Branchenregistern feststellen, ob gegen eine Bestellpflicht verstoßen wurde.

Neue Dokumentations- und Nachweispflichten für Unternehmen

2.5 „Schön und gut, aber wir verarbeiten ja gar keine Daten!“

Falsch!

Diese Meinung resultiert oftmals von einer falschen Vorstellung, was unter „personenbezogenen Daten“ oder „verarbeiten“ verstanden wird.

Personenbezogene Daten sind alle Informationen, welche man einer natürlichen Person zuordnen kann. Dazu zählen sowohl Mitarbeiter als auch Kunden, Lieferanten, Ansprechpartner in Unternehmen sowie Mitarbeiter und Kunden von Kunden.

Vielfältige personen-bezogene Daten

Beispiele sind etwa Name, E-Mail-Adresse, Telefonnummer, Gehalt, Foto, erfasste Meinungen, Vermerke zu einer Person, ein Vertrag oder eine Rechnung mit einem Namen etc…

In der Praxis sind nahezu alle Daten auch personenbezogene Daten!

Hinter dem Begriff „verarbeiten“ verbirgt sich nicht mehr und nicht weniger als ein Hilfsbegriff des Datenschutzrechts.

Weiter Begriff der Datenverarbeitung

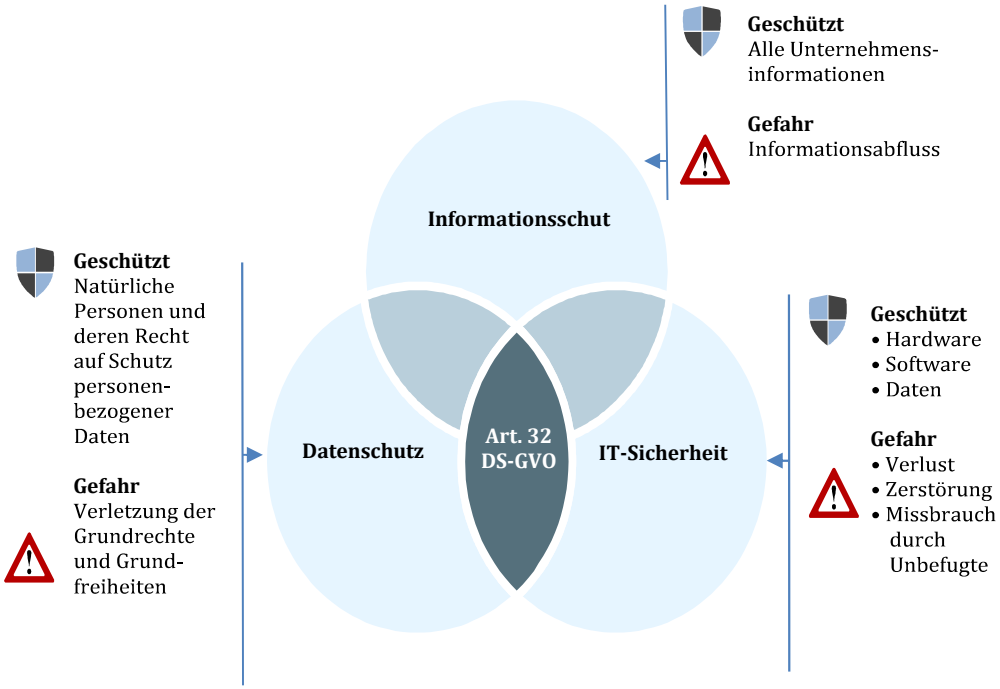
Denn unter einem Verarbeiten von Daten wird erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen,

verwenden, offenlegen, übermitteln, verbreiten, abgleichen oder verknüpfen, einschränken, löschen oder vernichten verstanden.

Im Endergebnis alles, was man mit Daten anstellen kann.

3 „Datenschutz“ – Worum geht es?

3.1 Datenschutz & Datensicherheit



Gemeinhin kommt es oftmals zu unterschiedlichen Ansichten, worum es beim Datenschutz tatsächlich geht und was dieser in der konkreten Anwendung bedeutet.

Datenschutz und Datensicherheit sind dabei entsprechend zu differenzieren.

Der Datenschutz hat zum Ziel, den Menschen und dessen personenbezogene Daten (besser: Informationen) zu schützen. Man spricht auch vom höchstpersönlichen Recht auf **informationelle Selbstbestimmung**.

*Beim **Datenschutz** geht es um personenbezogene Daten und dem **Schutz des dahinterstehenden Menschen** vor Missbrauch während Erhebung, Verarbeitung und Nutzung dieser Daten.*

Unterschied Datenschutz und Datensicherheit

Grundrecht auf Datenschutz mit dem Ziel den Menschen zu schützen

Die Datensicherheit hingegen hat zum Ziel, die Daten selbst – unabhängig davon, ob diese einer Person oder einem Unternehmen zugeordnet werden können oder gänzlich ohne diesen Bezug verarbeitet werden – zu schützen. Die Datensicherheit wird dabei als Teilaspekt des Datenschutzes verstanden, bei dem technische und organisatorische Aspekte im Vordergrund stehen.

Hierzu zählen insbesondere Aspekte wie:

- Die physische Sicherheit
- Der Schutz vor internen wie externen Fremdzugriffen
- Die Datensicherung
- Die Verschlüsselung der Kommunikation
- Relevante Updates und Patches von Software

3.2 Datenschutz – Etwas gänzlich Neues?

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 1978 Ausgegeben am 28. November 1978 193. Stück

565. Bundesgesetz: Datenschutzgesetz – DSG
(NR: GP XIV RV 72 AB 1024 S. 104. BR: 1893 AB 1895 S. 380.)

565. Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG)

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von

Bei der auftauchenden Frage, ob „Datenschutz“ etwas völlig Neues sei und vor allem, ob rechtliche Regelungen dazu nun aus heiterem Himmel kommen, muss man doch recht deutlich sagen: Nein!

In Österreich gab es bereits seit dem Jahr 1978 ein Datenschutzgesetz, welches den Schutz personenbezogener Daten zum Ziel hatte[5]. Nach der EU-Richtlinie 1995 zum Datenschutz kam es dann zu einer Modernisierung des Datenschutzes und im Jahr 2000 trat das Datenschutzgesetz 2000 in Kraft.

Dieses galt in Österreich seit 18 Jahren und noch bis zum 25. Mai 2018 und wird sodann von der DSGVO entsprechend abgelöst.

Datenschutzgesetze stellen somit keine Neuerungen in der österreichischen Rechtsordnung dar, sondern sind bereits jetzt fester Bestandteil der anzuwendenden Rechtsnormen für Unternehmen.

[5] Vgl. https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.html

4 Geldbußen & weitere Maßnahmen

Neben den erheblichen Geldbußen bestehen jedoch noch zusätzliche Sanktionsmöglichkeiten im Strafrecht oder Spezialvorschriften. Ebenso stehen der Aufsichtsbehörde noch weitere Abhilfemaßnahen zur Verfügung.

4.1 Strafrecht

Strafrecht neben Datenschutzrecht

Das Strafrecht wird weiterhin von den einzelnen EU-Mitgliedstaaten geregelt, dh. jeder Staat bestimmt seine Straftatbestände und daraus folgende Sanktionen selbst.

Verwaltungsstraftatbestände hingegen ergeben sich zum einen direkt aus der DSGVO und finden sich in den Art. 83 und Art. 84.

Daneben gelten aber auch noch einschlägige nationale Sanktionsvorschriften, insbesondere für besonders geregelte Bereiche.

Auf die Verletzung von Berufsgeheimnissen und branchenbedingten Verschwiegenheitspflichten ist hier entsprechend hinzuweisen, da diese für Steuerberater von außerordentlicher Bedeutung sind.

4.2 Geldbußen

Strafrahmen bis 20 Millionen Euro oder 4% des weltweit erzielten Jahresumsatzes

War bis dato der Strafrahmen für Datenschutzverletzungen im DSG 2000 noch verhältnismäßig „niedrig“ angesetzt, konkret bis 25.000 Euro, so wurde der Strafrahmen für Verstöße gegen die DSGVO deutlich angehoben. Um nicht zu sagen **drastisch angehoben**.

Bereits im Gesetzgebungsverfahren zur DSGVO wurde verstärkt darauf hingewiesen, dass die Geldbuße im Verletzungsfall verhältnismäßig ausfallen, aber dennoch abschreckend, d. h. für das Unternehmen deutlich spürbar, sein soll.

Wie man im Folgenden sehen kann, können die Bußgelder tatsächlich schmerzhaft sein:

Je nachdem, gegen welche Vorschrift der DSGVO verstoßen wurde, beträgt die maximale Geldbuße entweder ***10 bzw. 20 Millionen Euro oder 2% bzw. 4% des vom Unternehmen weltweit erwirtschafteten Jahresumsatzes*** *im vorherigen Geschäftsjahr.*

Dabei ist der jeweils höhere Wert von beiden Optionen ausschlaggebend! Erschwerend kommt hinzu, dass für die Berechnung der Konzernumsatz maßgebend ist.
Um nicht ungerechtfertigt unterschiedliche Strafen in Kauf nehmen zu müssen, sind verschiedenste Faktoren für die Bemessung der Strafe ausschlaggebend.

Dazu zählen zB Art, Schwere und Dauer des Verstoßes, die Zahl der betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens oder aber ob der Verstoß vorsätzlich oder fahrlässig erfolgt ist und frühere Vergehen.

4.3 Abhilfemaßnahmen

Weitere Abhilfemaßnahmen

Der jeweiligen nationalen Aufsichtsbehörde stehen neben der Verhängung von Geldbußen noch zahlreiche weitere Abhilfemaßnahmenmöglichkeiten zur Verfügung.

Dazu zählen insbesondere:

- Warnungen, dass bestimmte Datenverarbeitungen gegen die DSGVO verstoßen
- Verwarnungen auszusprechen
- Weisungen auszusprechen
- Verarbeitungsvorgänge einzustellen oder einzuschränken
- Weisungen, die betroffene Person von Verletzungen zu unterrichten
- vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung anzuordnen
- eine Zertifizierung zu widerrufen
- die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland anzuordnen

4.4 Schadenersatz

Materieller und immaterieller Schadenersatz

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Interessant erscheint in diesem Zusammenhang der stetig voranschreitende Grundsatz des Einzugs eines immateriellen Schadenersatzkonzepts, das bis dato in der österreichischen Rechtsordnung noch eher selten vertreten war.

Betroffene können somit auf zivilrechtlichem Weg sowohl tatsächlich entstandene, bezifferbare Schäden geltend machen, aber auch entstandene Unannehmlichkeiten, Bloßstellungen oder Ruf- und Imageschäden.

4.5 Haftung

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurde.

Haftung für Verantwortliche und Auftragsverarbeiter

Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Für Steuerberater ist daher einerseits von erheblicher Bedeutung, welche Pflichten ihnen seitens deren Klienten im Dienstleistervertrag auferlegt wurden, andererseits aber auch die Einhaltung der DSGVO im Bereich der eigenen Datenverarbeitung (zB Mitarbeiter oder Kundendaten für eigene Zwecke) oder allgemeiner Pflichten aus der DSGVO (wie etwa ein Verfahrensverzeichnis zu führen).

4.6 Entdecken von Verstößen

Verstöße gegen die DSGVO können auf vielfältigste Weise ans Tageslicht rücken und als Folge die oben angeführten Konsequenzen nach sich ziehen:

Zahlreiche Einfallstore

- Anzeige durch die betroffene Person selbst
- Überprüfung durch die Aufsichtsbehörde
- Beschwerden eines ehemaligen Mitarbeiters
- Selbstanzeige des Unternehmens
- Journalistische Tätigkeiten
- Datenschutz NGOs
- Unzufriedene Kunden
- Wettbewerb

4.7 Präventionsmaßnahmen

Welche Maßnahmen sollten nun präventiv zur Vermeidung von Datenschutzverstößen ergriffen werden?

Ein vollständiges Datenschutzmanagementsystem, laufende professionelle Beratung und die regelmäßige Überprüfung der Einhaltung der DSGVO sind unverzichtbare Kernbestandteile bei der Vorbeugung von Verstößen und die empfindlichen Geldbußen, die Unternehmen drohen.

Dabei sollte auf eine durchgehende und lückenlose Dokumentation von Datenquellen und -verarbeitungen geachtet werden, um dem DSGVO Erfordernis des jederzeitigen Nachweises der Compliance liefern zu können.

Stellen Sie daher folgendes für Ihr Unternehmen bis 25. Mai 2018 sicher:

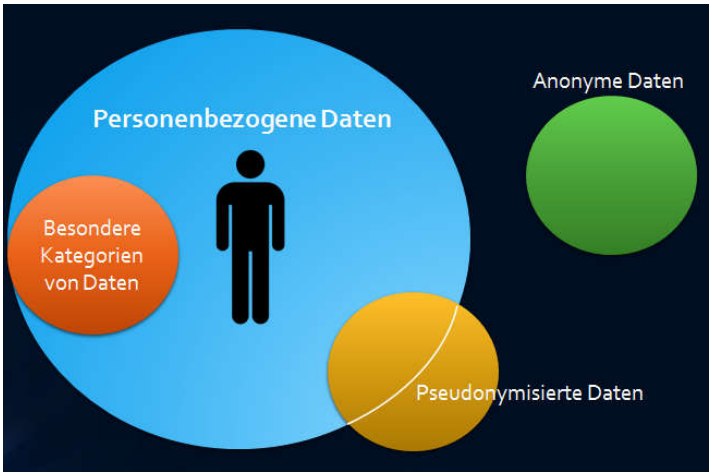
to do's bis 25.05.2018

- ❖ Durchgeführtes DSGVO Implementierungsprojekt inkl. GAP Analyse und konkreter Maßnahmenumsetzung
- ❖ Etabliertes Datenschutzmanagementsystem im Unternehmen
- ❖ Verfügbarer Datenschutzexperte im Unternehmen oder externe Unterstützung
- ❖ Regelmäßige Kontrolle und Audits der Einhaltung aller DSGVO Vorschriften
- ❖ Lückenlose Dokumentation der Datenschutz Compliance (siehe insbesondere auch die Folgekapitel dieses Leitfadens)

5 Definitionen und Begriffe

Die DSGVO umfasst zahlreiche Definitionen und Begriffe, welche nachstehend im Detail anhand konkreter Beispiele erläutert werden.

5.1 Verschiedenste Datenarten



– Personenbezogene Daten

Personenbezogen – was bedeutet das?

Sind alle Daten und Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene Person) beziehen.

Explizit ist nun auch die Online-Kennung (z. B. IP-Adressen oder Cookie-Kennung) erfasst. Auch pseudonymisierte Daten fallen unter die Anwendbarkeit der DSGVO. Um personenbezogene Daten handelt es sich immer dann, wenn eine Zuordnung zu einer natürlichen Person möglich ist.

Der Begriff umfasst alle Daten lebender natürlicher Personen, d. h. auch z. B. von Einzelunternehmen und Dritten jeglicher Art wie: Mitarbeiter, Dienstleister, Rechtsanwälte, Arbeitgeber, Bevollmächtigte.

Beispiele:

Der Name, die Adresse, das Gehalt, die Kontaktdaten, die Bewertung, eine Meinung, ein Foto, eine Stimmaufzeichnung, ein zugeordneter Vertrag, eine Telefonnummer, …

– Besondere Kategorien von Daten

Sensible Daten = besondere Kategorien von personen-bezogenen Daten

Die taxative Aufzählung umfasst insbesondere:

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung

– Anonyme Daten

Anonymität als Faktum

Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Anonymität ist ein Faktum!

Niemandem ist es mehr möglich, die dahinterstehende Person zu identifizieren.

Übersicht zum „Verwenden" von Daten

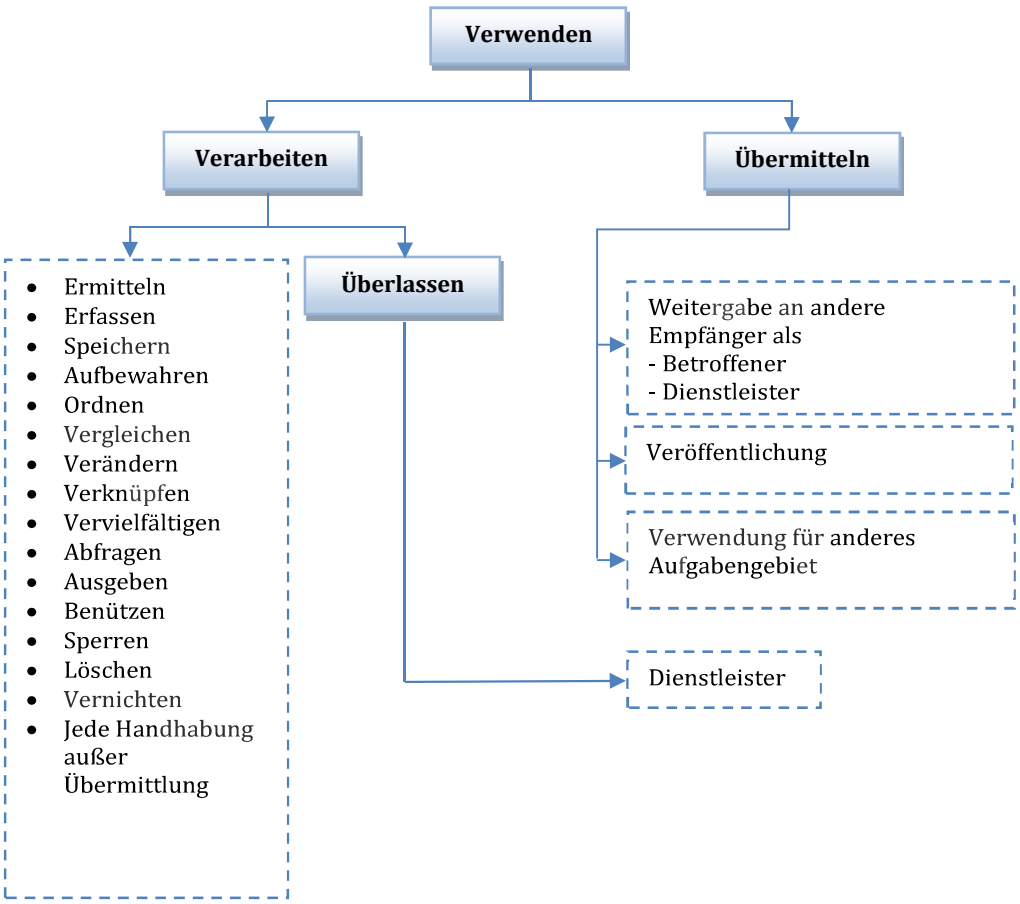
5.2 Verarbeitungsbegriffe

– Verarbeiten von Daten

Verarbeiten von Daten = nahezu alles

Bedeutet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Kurz: *Alles(!), was man mit personenbezogenen Daten machen kann!*



– **Pseudonymisierung**

Neue Kategorie: pseudonyme Daten

Verarbeitung personenbezogener Daten dergestalt, dass ohne Hinzuziehung zusätzlicher Informationen die Daten nicht mehr einer bestimmten betroffenen Person zugeordnet werden können. Voraussetzung ist aber, dass diese gesondert aufbewahrt und somit geschützt sind.

Die vorschriftsgemäße Pseudonymisierung ermöglicht das Nutzen von Daten innerhalb eines Unternehmens. Es sind technisch-organisatorische Maßnahmen zu ergreifen, die sicherstellen, dass keine Zuordnung / Identifizierung erfolgen kann.

5.3 Dateisystem

Dateisystem = Datenanwendung = Datenverarbeitung

Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (auch „Datenanwendung“).

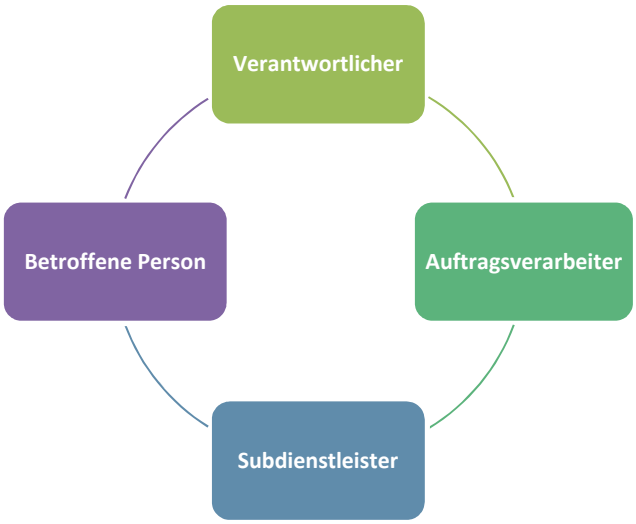
Beispiele:

- *Personalverrechnung*
- *Bewerbermanagement*
- *Buchhaltung*
- *Geburtstags - Excel Liste*
- *Karriereplanung*
- *Urlaubsplanung*
- *Zeiterfassung*
- *Umfragen*
- *Videoüberwachung*
- *Fotoablagen*
- *Internet / Intranet*
- *Spesenkostenabrechnung*
- *Kundendatenbank*
- *Interessentenmanagement*
- *Zutrittskontrollsysteme*
- *Skype for Business*
- *CRM Datenbank*
- *Vertragsmanagement*
- *Adresslisten*
- *Archivsysteme*
- *Controlling Tools*
- *Vertriebssysteme*
- *Newsletter System*
- *Rechnungsablagen*

Beispiele für „Dateisysteme“

5.4 „Spieler“ im Datenschutz

Die „Spieler“ des Datenschutzrechts



– Verantwortlicher

Ehemals Auftraggeber = Verantwortlicher

Natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

*Verantwortliche sind insbesondere als **„Herrscher über die Daten“** anzusehen (zB für die Personalverrechnung ist man immer Verantwortlicher, auch wenn man sich eines Dienstleisters (=Auftragsverarbeiter) bedient)..*

– Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde oder Einrichtung, die im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.

*Auftragsverarbeiter führen immer Datenverarbeitungen **im Auftrag** eines Verantwortlichen durch!*

Ehemals Dienstleister = Auftrags-verarbeiter

– Betroffene Person

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.

Dessen Daten verarbeitet werden = betroffene Person

– Empfänger

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden – egal, ob es sich um einen Dritten handelt oder nicht.

Beispiele:

Finanzamt oder Sozialversicherung im Rahmen der Personalverrechnung; Gerichte bei Klagen; Strafverfolgungsbehörden bei Anzeigen; oder aber auch Subdienstleister

– Aufsichtsbehörde

Eine von einem Mitgliedstaat eingerichtete unabhängige staatliche Stelle. In Österreich: die „österreichische Datenschutzbehörde“ (https://www.dsb.gv.at)

6 Tätigkeit als Steuerberater

Das Wirtschaftstreuhandberufsgesetz (WTBG)[6] regelt welche Tätigkeiten ein Steuerberater im Rahmen seines Berufes ausüben darf bzw. welche Tätigkeiten Steuerberatern vorbehalten sind. Dies umfasst insbesondere folgende Tätigkeiten:

Weites Tätigkeitsfeld als Steuerberater

- Führung der Buchhaltung und Lohnverrechnung
- Erstellung von Jahresabschlüssen
- Erstellung von Steuererklärungen
- Vertretung in Abgaben- und Abgabenstrafverfahren vor Abgabenbehörden
- Sonstige Vertretung insbesondere vor Sozialversicherungen
- Beratungsleistungen
    - betriebswirtschaftliche Beratung
    - Steuerberatung
    - Beratungsleistungen im Zusammenhang mit dem betrieblichen Rechnungswesen und der Beratung betreffend der Organisation und Einrichtung des internen Kontrollsystems
    - Sanierungsberatung, Erstellung von Sanierungsgutachten etc.
    - Beratung in Rechtsangelegenheiten, soweit diese mit wirtschaftstreuhändischen Tätigkeiten unmittelbar in Zusammenhang stehen
- Treuhandaufgaben
- Prüfungsaufgaben
- Sachverständigengutachten

Neben der „klassischen“ Tätigkeit des Steuerberaters – der steuerlichen Beratung und Vertretung, Führung der Buchhaltung und Lohnverrechnung und der Erstellung von Jahresabschlüssen und von Abgabenerklärungen – tritt die betriebswirtschaftliche Beratung der Klienten in letzter Zeit immer mehr in den Vordergrund.

Bei allen Tätigkeiten werden üblicherweise Daten verarbeitet, weshalb es für den Steuerberater unabdingbar ist, sich mit der DSGVO eingehend auseinanderzusetzen.

[6] Vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009983

7 Rechtsgrundlagen der Datenverarbeitung

Das Datenschutzgesetz ist als Verbotsgesetz konstruiert!

Jede Datenverarbeitung ist grundsätzlich verboten!

Ausnahme: Es ist eine entsprechende Rechtsgrundlage vorhanden!

Datenschutz-gesetz = Verbotsgesetz mit Erlaubnis-vorbehalt

Verschiedene Rechtsgrundlagen zur Daten-verarbeitung

7.1 Einwilligung

Die Einwilligung als Rechtsgrundlage für Datenverarbeitungen durch Steuerberatungskanzleien als Verantwortlichen bildet eher die Ausnahme. Relevanz erlangt sie aber beispielsweise in Bereichen wie etwa dem Direktmarketing bei Klienten oder bestimmten Fällen der Datenweitergabe.

Strenge Einwilligungsregeln

– Definition

Die Datenschutz-Grundverordnung (DSGVO) definiert die Einwilligung folgendermaßen:

Definition

> „Einwilligung der betroffenen Person bezeichnet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."

– Bedingungen einer rechtmäßigen Einwilligung

- **Klare und einfache Sprache**

Die „klare und einfache Sprache“ bedingt, dass selbst Nutzer mit einer niedrigen Lesefähigkeit aufgrund eines geringen Bildungsniveaus oder fehlender Sprachkenntnisse den Text verstehen können sollten. Juristische Termini, Fremdwörter und Fachausdrücke sind zu vermeiden.

Text muss eine klare und einfache Sprache darstellen

- **Umfang der Information**

Die Einwilligungserklärung sollte insbesondere folgenden Inhalt umfassen, um das Kriterium der „informierten Weise“ zu erfüllen:

Umfangreiche Inhaltsangaben notwendig

  - Die konkreten Datenarten/Datenkategorien, welche verarbeitet werden (zB Name, Adresse, Telefonnummer, E-Mail-Adresse, Interessen, Kontaktwünsche, usw.)
  - Die konkreten Zwecke, wofür die Daten verwendet werden (werden verschiedene Zwecke verfolgt so sind diese separiert anzuführen)
  - Den Verantwortlichen der Datenverarbeitung
  - Etwaige Empfänger der Daten und der dazugehörige Übermittlungszweck

Insbesondere „Globaleinwilligungen“ sind als unzulässig anzusehen.

- **Hinweis auf das Widerrufsrecht**

Widerrufsrecht der betroffenen Person

Einwilligungen können jederzeit ohne Angaben von Gründen widerrufen werden. Die Einwilligungserklärung muss einen entsprechenden Widerrufshinweis samt Widerrufsadresse hierfür beinhalten.

Der Widerruf muss ebenso leicht wahrgenommen werden können wie die ursprüngliche Einwilligung, zB über das gleiche Medium (E-Mail, Website, …)

- **Eindeutige bestätigende Handlung**

Untersagt sind insbesondere folgende Varianten:

Opt-In statt Opt-Out

  - Bereits angekreuzte Kästchen oder vorausgefüllte Felder
  - Schweigen oder Untätigkeit der betroffenen Person
  - Jedwede Opt-Out Lösungen

In der Praxis bietet sich auch das s.g. **„Double-Opt-In-Verfahren“** an, bei dem nach Eingabe der Daten zur Datenverarbeitung der betroffenen Person eine E-Mail an die angegebene Adresse zur Bestätigung des Verarbeitungswunsches übermittelt wird.

- **Freiwilligkeit**

Freiwilligkeit wird nur als gegeben betrachtet, wenn die betroffene Person eine freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Freiwilligkeit als Vorrang

> ***Achtung!***
> *Ohne Freiwilligkeit ist die Einwilligung jedenfalls unwirksam!*

- **Unterscheidbarkeit**

Kein Verstecken von Einwilligungen

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft (zB Bestellung von Produkten oder AGB), so muss das Ersuchen um Einwilligung so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

- **Kopplungsverbot**

Eine „Kopplung" liegt insbesondere vor, wenn

Neu: Verbot der Koppelung

- ein Vertragsabschluss oder
- die Erbringung einer Leistung

davon abhängig gemacht wird, dass der Betroffene in eine weitergehende Erhebung oder Verarbeitung seiner personenbezogenen Daten einwilligt, welche nicht zu Abwicklung des Geschäfts erforderlich sind.

Beispiel:

Die Teilnahme an einem Gewinnspiel ist an die Weiterverwendung der Daten einer betroffenen Person durch den Verantwortlichen zu Werbezwecken gekoppelt. (= unzulässig!)

– Organisatorische Erfordernisse

- **Nachweispflicht**

Jederzeitiger Nachweis muss möglich sein

Der Nachweis der erteilten Einwilligung muss jederzeit erbracht werden können. Dies bedeutet, dass unternehmensintern die Dokumentation bzw. Protokollierung der erteilten Einwilligung sicherzustellen ist.

- **Anlaufstelle für den Widerruf**

Anlaufstelle für Widerruf

Intern ist eine entsprechende Anlaufstelle für die Wahrnehmung des Widerrufsrechts durch die betroffene Person sicherzustellen.

– Sonderregelung zu „elektronischer Post“

Auch Anrufe und elektronische Postsendungen (wie E-Mails oder SMS Nachrichten), als Massensendung (über 50 Empfänger) oder zu Werbezwecken, benötigen grundsätzlich die vorherige Zustimmung.

Tele-kommunikations-gesetz beachten!

Dieser Grundsatz der vorherigen Zustimmung (Opt-In) wird allerdings für elektronische Post bei Vorliegen bestimmter Voraussetzungen, durchbrochen:

- wenn die Kontaktinformation im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung erhalten wurde und
- die Nachricht erfolgt zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen und
- der Kunde hat die Möglichkeit erhalten, den Empfang solcher Nachrichten bei der Erhebung und bei jeder Übertragung kostenfrei und problemlos abzulehnen und
- der Kunde hat die Zusendung nicht im Vorhinein abgelehnt (zB. ECG Liste).

Achtung!
Bereits das Einholen der Zustimmung per Telefon, Fax oder elektronischer Post für nachfolgende Kontaktaufnahmen ist unzulässig.

– Beispiel

Beispieltext

Ich erkläre mich damit einverstanden, dass meine personenbezogenen Daten … (hier sollten diese Daten so genau und umfassend wie möglich beschrieben werden) zum Zwecke … (hier sollte der entsprechende Zweck bzw. die Zwecke, sofern mehrere verfolgt werden, angegeben werden) von … (hier den Namen des Verantwortlichen und seine Anschrift angeben) verarbeitet werden.

Bitte beachten Sie, dass Sie Ihre nachfolgende Zustimmung jederzeit mittels Nachricht an … (hier sollte die Widerrufsadresse postalisch/elektronisch angegeben sein) widerrufen können. Ihr Widerruf entfaltet rechtliche Wirkung nur für die Zukunft ab Widerruf.

7.2 Vertragserfüllung / Vorvertragliche Maßnahmen

Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist.

Vertragserfüllung und Geschäfts-anbahnung als Rechtfertigung

Somit kann eine weitere Rechtsgrundlage zur Datenverarbeitung:

- die Vertragserfüllung selbst oder
- die Verarbeitung im Rahmen der Geschäftsanbahnung sein.

Ein überwiegender Teil der Tätigkeit als Steuerberater erfolgt im Rahmen der Vertragserfüllung bzw. Geschäftsanbahnung. Insbesondere die Beauftragung eines Steuerberaters durch seinen Klienten zur Steuerberatung, Personalverrechnung oder Buchhaltung sind typische Anwendungsbeispiele.

Achtung!

Zu beachten ist hier jedoch zwingend der Zweckbindungsgrundsatz des Datenschutzrechts. Eine Datenverarbeitung in Umfang oder Zweck, welche über die Vertragserfüllung hinausgeht, muss auf eine eigene Rechtsgrundlage gestützt werden.

7.3 Erfüllung einer rechtlichen Verpflichtung

Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist.

Gesetzliche Pflicht oder Ermächtigung zur Datenverarbeitung

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt sein.

7.4 Lebenswichtige Interessen

Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Ausnahme im Tagesalltag: Lebenswichtige Interessen

Da dieser Anwendungsbereich für Steuerberater im Alltag als äußerst unwahrscheinlich erscheint, wird an dieser Stelle nicht näher auf diese Bestimmung eingegangen.

7.5 Aufgabe im öffentlichen Interesse

Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Öffentliches Interesse

Da dieser Anwendungsbereich für Steuerberater im Alltag als eher unwahrscheinlich erscheint, wird an dieser Stelle nicht näher auf diese Bestimmung eingegangen.

7.6 Berechtigtes Interesse

Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Auffangtatbestand „Berechtigtes Interesse“

Hierbei handelt es sich insbesondere um einen Auffangtatbestand der DSGVO.

Die Rechtsgrundlage „berechtigtes Interesse“ hat immer eine Interessensabwägung zwischen den Interessen des Betroffenen und des Unternehmens zu beinhalten:

Interessens-abwägung durchzuführen

Was sind exemplarisch „berechtigte Interessen“?

Beispiele

- Direktwerbung (etwa der Newsletter Versand an bestehende Kunden – Achtung Sonderregeln zu elektronischer Post beachten – Kapitel 7.1)
- Betrugsbekämpfung
- Weitergabe innerhalb der Unternehmensgruppe für interne Verwaltungszwecke
- Verarbeitung von personenbezogenen Daten durch Computer-Notdienste
- Verarbeitung von personenbezogenen Daten durch Anbieter von Sicherheitstechnologien und -diensten, soweit dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist

Achtung:
Bei Berufung auf berechtigte Interessen ist dies bei den ***Informationspflichten*** *gegenüber betroffenen Personen zu beachten und entsprechend anzuführen!*

7.7 Checkliste

Prüffragen	Ja / Nein
Allgemein	
Wurde für alle Datenverarbeitungen festgestellt, auf welche Rechtsgrundlagen sich gestützt wird?	
Einwilligung	
Wurde für jene Fälle der Einwilligung überprüft, ob nicht eine andere Rechtsgrundlage zu Anwendung gelangen kann?	
Wurde eine Einwilligung vor Erhebung oder Verarbeitung der personenbezogenen Daten eingeholt?	
Ist der Nachweis der eingeholten Einwilligungen samt Zeitangabe und Textinhalt möglich?	
Erfüllt die konkrete Einwilligung das Erfordernis der verständlichen und leicht zugänglichen Form?	
Erfüllt die konkrete Einwilligung das Erfordernis der klaren und einfachen Sprache?	
Beinhaltet die Einwilligung den geforderten Inhalt gemäß DSGVO?	
Wurde das Kopplungsverbot beachtet?	
Wurden die Informationspflichten berücksichtigt und ausreichende Informationen bereitgestellt?	
Erfolgt die Bestätigung der betroffenen Person mittels eindeutig bestätigender Handlung?	
Wurde das Gebot der „Freiwilligkeit“ berücksichtigt?	
Ist sichergestellt, dass die Einwilligung gesondert unterzeichnet wird und nicht in anderen Dokumenten „versteckt“ ist?	
Ist ein Widerrufshinweis samt den daraus resultierenden Folgen in der Einwilligung angeführt?	
Sind die Zwecke hinreichend spezifisch angegeben?	
Wird ein Double Opt In Verfahren zur Einholung der Einwilligung angewandt?	
Wurden alle bestehenden Einwilligungen dahingehend überprüft ob diese den Anforderungen der DSGVO genügen?	
Vertragserfüllung bzw. Geschäftsanbahnung	
Wurde überprüft, ob die verarbeiteten Daten ausschließlich für die Vertragserfüllung oder Geschäftsanbahnung verwendet werden?	
Werden die im Rahmen der Vertragserfüllung erlangten Daten noch für andere Zwecke verarbeitet?	
Ist für diese weiteren Zwecke eine Rechtsgrundlage gegeben?	

Rechtliche Grundlage	
Ist im Falle der Stützung auf einer rechtlichen Grundlage die entsprechende Verpflichtung oder Ermächtigung konkretisiert?	
Umfasst die rechtliche Grundlage die gesamte Datenverarbeitung samt der verfolgten Zwecke und die damit verbundenen Datenkategorien?	
Werden die Daten noch für andere Zwecke verwendet?	
Ist für diese weiteren Zwecke eine Rechtsgrundlage gegeben?	
Berechtigtes Interesse	
Wurden bei Heranziehen von berechtigten Interessen diese konkreten Interessen erfasst?	
Wurde in diesem Rahmen eine Interessensabwägung zwischen Unternehmensinteressen und jenen der betroffenen Person auf Geheimhaltung vorgenommen?	
Wurden diese bei der Bereitstellung der Informationen nach Art. 13 und 14 DSGVO berücksichtigt?	
Wissen alle Mitarbeiter, wie mit einem wahrgenommenen Widerspruchsrecht der betroffenen Person umzugehen ist?	
Ist sichergestellt, dass die berechtigten Interessen im Zuge der Beauskunftung an betroffene Personen berücksichtigt werden?	

8 Datenschutzgrundsätze

Die Datenschutz-Grundsätze sind immer zu berücksichtigen!

Die Datenschutzgrundsätze, oder auch Prinzipien genannt, müssen jedenfalls zu jedem Zeitpunkt der Datenverarbeitung eingehalten werden. Der Steuerberater trägt dabei die Beweislast dafür, dass er die gesetzlichen Vorgaben einhält. Alle Geschäftsprozesse und technisch-organisatorischen Maßnahmen müssen daher dokumentiert werden.

Jede Steuerberatungskanzlei muss somit bis spätestens Mai 2018, wenn die DSGVO unmittelbar geltendes Recht sein wird, schriftliche Dokumentationen erstellen. Die nationalen Datenschutzaufsichtsbehörden haben bereits angekündigt, dass genau hier der Fokus ihrer Unternehmensüberprüfungen liegen wird.

8.1 Rechtmäßigkeit

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Datenverarbeitung nur mit Rechtsgrundlage

Die Verarbeitung personenbezogener Daten ist dabei nur aufgrund einer expliziten Rechtsgrundlage erlaubt.

Zweckbindung zentrales Element

Betroffene müssen weiters informiert sein, welche ihrer Daten zu welchen Zwecken verarbeitet werden, wo diese gespeichert werden und wer Zugriff darauf hat.

> Die Steuerberatungs-, Personalverrechnungs- oder Buchhaltungstätigkeit eines Steuerberaters, aber auch die Verrechnung gegenüber dem Klienten, sind durch die Rechtsgrundlage „Vertragserfüllung“ gedeckt.

8.2 Zweckbindung

– Allgemein

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Verarbeitung für andere Zwecke als die ursprünglichen

Schon vor der Datenerhebung muss jedenfalls feststehen bzw. muss der Verantwortliche festlegen, welche Daten für welche Zwecke verarbeitet werden sollen. Jeder Zweck muss dabei eindeutig und legitim sein.

Insbesondere die „Speicherung auf Vorrat" mit dem Motto „Schauen wir einfach später, was wir mit den Daten anstellen" ist mit dem Grundsatz der Zweckbindung unvereinbar.

Konkrete Zweckangaben

Der Zweck der Verarbeitung von Daten durch den Steuerberater muss daher entweder der ursprünglichen Absicht entsprechen, die mit bzw. vom Klienten festgelegt worden ist, oder/und dieser darf nicht in Widerspruch zum ursprünglichen Zweck stehen und muss mit diesem nach den Bestimmungen der „Weiterverarbeitung" vereinbar sein.

– Zweckspezifizierung

Steuerberater müssen, wie andere Verantwortliche auch, ihre Datenverarbeitungen spezifischen Zwecken zuordnen. Dies erfolgt insbesondere im Rahmen der Erfassung aller Datenverarbeitungen im Verzeichnis für Verarbeitungstätigkeiten.

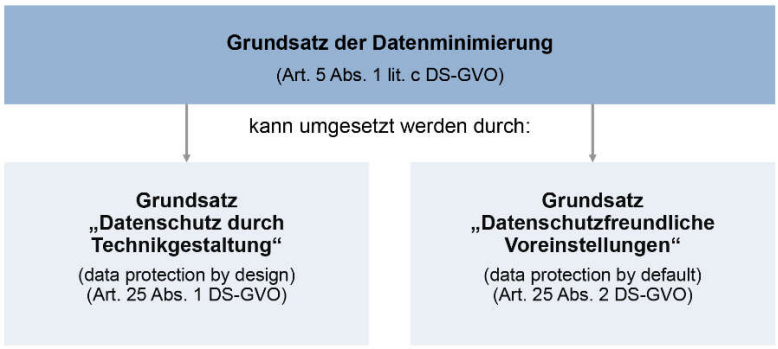
Dabei wird unterschieden zwischen Datenverarbeitungen für eigene Zwecke, wie etwa die eigene Personalverrechnung, Urlaubs- und Zeitmanagement oder Kundenbeziehungsmanagement, und Datenverarbeitungen im Rahmen einer Dienstleistung als Auftragsverarbeiter, wie etwa der Steuerberatungstätigkeit oder Buchhaltung und Lohnverrechnung für Klienten.

8.3 Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

So wenig wie möglich – so viel wie nötig

Dieser Grundsatz der Datenminimierung findet insbesondere in den neuen Schlagworten und Grundsätzen „Privacy by Design" (Datenschutz durch Technikgestaltung) und „Privacy by Default" (datenschutzfreundliche Voreinstellungen) ihren Niederschlag.



Aufgrund der engen Verknüpfung des Datenminimierungsgrundsatzes mit den zusätzlichen, allgemeinen Grundsätzen des „Datenschutzes durch Technikgestaltung“ und „datenschutzfreundlichen Voreinstellungen“ erfolgen aufgrund Verständnisüberlegungen die näheren Ausführungen zu diesen beiden Grundsätzen an dieser Stelle des Leitfadens.

– Privacy by Design / Datenschutz durch Technikgestaltung

Privacy by Design als neuer Grundsatz

Hinter dem medial wirksamen Begriff des „Privacy by Design“ verbirgt sich der im Deutschen durchaus schlicht wirkende Grundsatz des „Datenschutzes durch Technikgestaltung“.

Was versteht man nun darunter?

Die DSGVO verlangt dabei von jedem Verantwortlichen, dass er

- unter Berücksichtigung des Stands der Technik,
- der Implementierungskosten,
- der Art,
- des Umfangs,
- der Umstände,
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen
    - sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung
    - als auch zum Zeitpunkt der eigentlichen Verarbeitung

⇨ **geeignete technische und organisatorische Maßnahmen trifft**

- die dafür ausgelegt sind, die Datenschutzgrundsätze umzusetzen und
- die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und
- die Rechte der betroffenen Personen zu schützen

Konkrete Überlegungen notwendig

Dies bedeutet, dass sich insbesondere jeder Verantwortliche für alle seine Datenverarbeitungen überlegen muss, wie er die DSGVO durch technische Ausgestaltung und organisatorische Maßnahme bestmöglich umsetzen kann und Datenschutzverletzungen vermieden werden können.

Konkrete Maßnahmen

Dazu können etwa folgende **Maßnahmen** zählen:

- Mitarbeiteranweisungen
- Prozessdokumente
- Ablaufbeschreibungen
- Beschaffungsvorgaben zu Software
- Unternehmensrichtlinien
- Verschlüsselungen
- Pseudonymisierung
- IT-Security Konzepte und Vorgaben

– Privacy by Default / Datenschutzfreundliche Voreinstellungen

Datenschutz-freundlichkeit als Basis

„Privacy by Default" bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen" und impliziert, dass die Werks- und Grundeinstellungen datenschutzfreundlich auszugestalten sind.

Der Verantwortliche hat daher geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Diese Verpflichtung gilt für die *Menge* der erhobenen personenbezogenen Daten, den *Umfang* ihrer Verarbeitung, ihre *Speicherfrist* und ihre *Zugänglichkeit*.

– Praktische Relevanz und Anwendung der Grundsätze

Keine Standardantwort möglich

Bei den Regelungen rund um Privacy by Design, Privacy by Default und Datenminimierung handelt es sich um äußerst praxisrelevante Anforderungen, die jedoch aufgrund des jeweiligen, einzelfallspezifischen Falles keine standardisierte Antwort erlauben.

Da insbesondere die Technikgestaltung in einem frühen Entwicklungsstadium zu berücksichtigen ist und entsprechende Auswirkungen auf das gesamte datenverarbeitende System hat, sind die Verantwortlichen angehalten, sich mit diesen Anforderungen frühzeitig zu befassen. An dieser Stelle bietet es sich an, einen Blick auf andere Standards, wie etwa die deutschen IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnologie (BSI), zu werfen.

Daten müssen stets richtig sein

8.4 Richtigkeit

Personenbezogene Daten müssen stets sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

Es sind dabei alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Klären Sie im Rahmen der Analyse Ihrer Datenanwendungen, ob sie für alle verarbeiteten Datenarten

- deren Ursprung kennen;
- deren Erfassungszeitpunkt feststellen können;
- verifizieren können, ob die Daten richtig sind;
- verifizieren können, ob die Daten vollständig sind.

Aufbewahrungs-pflichten vs. Löschpflicht

8.5 Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Grundsätzlich wären personenbezogene Daten, die im Rahmen einer Dienstleistungserbringung eines Steuerberaters verarbeitet wurden, nach Zweckerreichung (dh nach der Steuerberatung, Buchhaltung, Lohnverrechnung, …) entsprechend zu löschen. Allerdings greifen hier die spezialgesetzlichen Aufbewahrungsfristen als Grundlage für eine darüberhinausgehende Speicherung der personenbezogenen Daten.

Achtung: *Verwenden Sie aktuelle technische Standards, welche ein sicheres Löschverfahren oder eine Anonymisierung garantieren!*

Beispiele für gesetzliche Aufbewahrungspflichten:

- 7-jährige Aufbewahrungsfrist im Unternehmensrecht nach §212 UGB
- 7-jährige Aufbewahrungsfrist im Steuerrecht nach §132 BAO
- 22-jährige Aufbewahrungsfrist über Aufzeichnungen und Unterlagen über Grundstücksgeschäfte nach UStG
- 10-jährige Aufbewahrungsfrist nach §13 PHG
- 30-jährige Aufbewahrungsfrist nach §1489 ABGB aufgrund der absoluten Verjährungsfrist

8.6 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Im gesamten oftmals als Datensicherheit bezeichnet, kann insbesondere unter diesem Begriff eine Kombination der beiden folgenden Fachbereiche verstanden werden:

- IT-Sicherheit
- Informationssicherheit

Grundsätzlich stellt die DSGVO die sehr simpel formulierte Anforderung an Unternehmen, geeignete Sicherheitsmaßnahmen zu ergreifen, um personenbezogene Daten angemessen zu schützen. Im Rahmen dieses Leitfadens, welcher die DSGVO und den Datenschutz im Fokus hat, kann insbesondere nicht auf die Details eines umfassenden Informationssicherheitsmanagements und IT-Sicherheitskonzepts eingegangen werden.

An dieser Stelle sei daher auf folgende Quellen zur vertiefenden Analyse für Ihr Unternehmen verwiesen:

- IT Sicherheitshandbuch für KMU der Wirtschaftskammer Österreich[7]
- BSI IT-Grundschutz[8]

[7] https://www.wko.at/service/innovation-technologie-digitalisierung/IT-Sicherheit_fuer_KMU_und_EPU.html#heading_IT_Sicherheitshandbuch_fuer_KMU
[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

8.7 Checkliste

Grundsätzlich empfiehlt es sich für alle Datenverarbeitungen folgende Vorüberlegungen und Vorfragen anzustellen:

Prüffragen	Ja / Nein
Datenschutzgrundsätze	
Habe ich evaluiert, welche personenbezogenen Daten im Rahmen der Datenanwendung verarbeitet werden?	
Stellen diese personenbezogenen Daten das Minimum dar, um meinen verfolgten Zweck zu erreichen?	
Kann ich meinen Zweck womöglich mit anonymen Daten oder pseudonymisierten Daten erreichen?	
Besteht eine Korrelation zwischen den für die Datenverarbeitung geplanten Datenarten und der Zweckerreichung?	
Gibt es für jede Datenverarbeitung ein Zugriffsmanagement, um sicherzustellen, dass nur Personen mit ausreichendem Interesse Zugriff zu den Daten erhalten?	
Habe ich geklärt, welche personenbezogenen Daten ich im Rahmen der Datenverarbeitung benötige?	
Wissen alle meine Mitarbeiter entsprechend ihrer Aufgaben und Rollen Bescheid?	
Ist sichergestellt, dass Werkseinstellungen datenschutzfreundlich und möglichst wenig invasiv für die betroffenen Personen eingestellt sind?	
Sind Maßnahmen ergriffen, welche die Richtigkeit der Daten sicherstellen?	
Wurde für alle Datenkategorien einer Datenanwendung eine Speicher- und/oder Löschfrist festgelegt?	
Technische und organisatorische Maßnahmen	
Gibt es eine Beschaffungsrichtlinie für neu geplante Software?	
Gibt es eine Datenschutzrichtlinie?	
Gibt es eine IT-Security Richtlinie?	
Sind die technischen Schutzmaßnahmen am aktuellen Stand der Technik oder sollte nachgebessert werden?	
Sind die Grundsätze der Informationssicherheit umgesetzt?	
Sind Prozesse nach gängigen „Good Practice“ Ansätzen umgesetzt?	
Sind alle Mitarbeiter betreffend Datenschutz und Datensicherheit zumindest grundgeschult?	
Ist eine ausreichende Dokumentation sichergestellt?	
Gibt es Backups und Datensicherungsverfahren im Unternehmen?	
Ist eine angemessene Netzwerksicherheit gegeben?	
Werden personenbezogene Daten bei E-Mail Versand angemessen geschützt (zB Verschlüsselung)?	
Gibt es ein Zutritts- und Zugriffskontrollsystem?	

Achtung!
Hinsichtlich einer Erstüberprüfung des Compliancegrads aus Datenschutz- und Datensicherheitssicht wird dringend empfohlen, eine professionelle Beratung in Anspruch zu nehmen, die sowohl technische, organisatorische, prozessuale als auch infrastrukturelle Maßnahmen überprüft!

8.8 Rechenschaftspflicht

Gemäß Artikel 5 Abs. 2 ist der Verantwortliche für die Einhaltung aller Datenschutzgrundsätze verantwortlich und muss dessen Einhaltung nachweisen können.

Aus dieser allgemeinen Verpflichtung ergeben sich die unterschiedlichsten Prüfungs- und Dokumentationspflichten eines datenverarbeitenden Unternehmens.

Nachweis der Einhaltung der DSGVO

Die Nachweispflicht hat insbesondere konkrete Bedeutung im Hinblick auf Überprüfungen durch die Aufsichtsbehörden, die auch die Möglichkeit und Befugnis haben, den Verantwortlichen zur Lieferung von Informationen anzuweisen.
Kann der Verantwortliche die Einhaltung der Datenschutzgrundsätze nicht nachweisen, dann geht dies jedenfalls als Verletzung der Nachweispflicht zu seinen Lasten und er kann sich dann auch nicht von seiner Haftung befreien.

Ein Unternehmen muss im Ergebnis ein Sammelsurium an Maßnahmen (risikobasiert) definieren, umsetzen, dokumentieren und kontrollieren. Angesichts der Fülle von Anforderungen einerseits und der Rechenschafts- und Nachweispflicht aus der DSGVO andererseits wird er dabei um ein geordnetes System, wie ein **Datenschutzmanagementsystem (DSMS)**, wohl nicht herumkommen.

Datenschutz-Managementsystem

9 Informationspflichten

9.1 Allgemein

Verantwortliche müssen künftig umfassender und detailreicher informieren, wenn sie personenbezogene Daten von natürlichen Personen verarbeiten.

Neu: Umfassende Informations-pflichten

Zur Wahrung der informationellen Selbstbestimmung enthält die DSGVO daher besondere Informationspflichten, die auch Steuerberater einhalten müssen und deren Umsetzung organisatorisch sicherstellen sollten.

Die detaillierten und umfangreichen Informationen sind der betroffenen Person im Regelfall bei Erhebung der Daten bzw. unverzüglich danach zugänglich zu machen, egal ob die betroffene Person ein Interesse an diesen Informationen bekundet hat oder nicht.

Unternehmen laufen Gefahr, Bußgelder in beachtlicher Höhe zu zahlen, wenn sie diesen komplexen Informationspflichten nicht nachkommen. Neben dem Risiko einer Geldbuße durch die Aufsichtsbehörde droht zudem die zivilrechtliche Verfolgung durch Verbraucherschützer, Mitbewerber oder Datenschutz-NGO´s.

Im Gegensatz zur bestehenden Rechtslage sind die Informationspflichten hinsichtlich der Betroffenenrechte nun an Formvorschriften gebunden. Zum jetzigen Stand ist davon auszugehen, dass die Informationen und Auskünfte schriftlich oder in elektronischer Form zu erteilen sind.

Keine mündlichen Auskünfte erteilen

Um dem Grundsatz der Transparenz, Rechtmäßigkeit und seinen eigenen Dokumentationspflichten als Verantwortlicher nachzukommen,empfiehlt es sich **dringend(!)** Informationen und Auskünfte nicht mündlich und schon gar nicht am Telefon zu erteilen. Dies birgt vor allem wieder die Gefahr der Verletzung von Datengeheimnissen.

Egal ob es sich um Informationen, Auskünfte oder Mitteilungen handelt:
Es ist stets auf leicht zu verstehende, aber präzise Formulierungen zu achten.

9.2 Datenerhebung bei der betroffenen Person

– Inhalt

Exakt vorgegebener Inhalt

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- Identität des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszweck(e) und Rechtsgrundlage(n)
- Berechtigte Interessen
- Empfänger der personenbezogenen Daten
- Drittstaaten
- Speicherdauer
- Aufklärung über Betroffenenrechte

- Aufklärung über Widerrufsrecht
- Aufklärung über Beschwerderecht
- Aufklärung über Bereitstellung der Daten
- Bestehen einer automatisierten Einzelentscheidung oder Profiling

Achtung!

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für **einen anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so hat er der betroffenen Person **vor** dieser Weiterverarbeitung Informationen über diesen anderen Zweck zur Verfügung zu stellen.

Neuer Zweck = neue Information

– Ausnahme von der Informationsverpflichtung

Ausnahmen

Der Verantwortliche kann die Bereitstellung der Informationen unterlassen, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Diese Regelung greift allerdings nur, wenn die betroffene Person über die konkret mitzuteilenden Informationen verfügt. Der Informationsstand der betroffenen Person muss daher in Umfang, Detailgrad und Klarheit den Informationen entsprechen, die der Verantwortliche der betroffenen Person zur Verfügung stellen müsste.
Dies wird in den meisten Fällen wohl nicht der Fall sein!

9.3 Datenerhebung bei einem Dritten

Datenerhebung über Umwege

– Inhalt

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so hat der Verantwortliche der betroffenen Person grundsätzlich die Informationen gemäß Punkt 9.2 mitzuteilen. Es entfällt allerdings die Aufklärung über die Bereitstellung der Daten. Zusätzlich sind die Kategorien personenbezogener Daten, die verarbeitet werden und die Quelle der personenbezogenen Daten mitzuteilen.

– Zeitpunkt und Fristen

Genaue Fristvorgaben

Werden die Informationen aus dritter Quelle gewonnen, muss das Unternehmen seiner Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung der Daten innerhalb einer

angemessenen Frist nach Erlangung der Daten, längstens jedoch innerhalb eines Monats, nachkommen. Werden die Daten zur Kommunikation mit der betroffenen Person verwendet, entsteht die Informationspflicht spätestens zum Zeitpunkt der ersten Mitteilung. Werden Daten an einen anderen Empfänger weitergegeben, muss der Verantwortliche die betroffene Person darüber spätestens zum Zeitpunkt der Weitergabe in Kenntnis setzen.

Ausnahmen

– Ausnahme von der Informationsverpflichtung

Wenn und soweit

- die betroffene Person bereits über die Informationen verfügt,
- die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde oder soweit dies die Verwirklichung der Ziele unmöglich macht,
- die Erlangung oder Offenlegung durch Rechtsvorschriften, denen der Verantwortliche unterliegt ausdrücklich geregelt ist oder
- die personenbezogenen Daten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Berufsgeheimnis

Dieser spezielle Ausschlusstatbestand dient insbesondere dem Schutz von Berufsgeheimnissen und ist von erheblicher Relevanz für Steuerberater. Die Norm verweist neben dem Unionsrecht auch auf das mitgliedstaatliche Recht, um zu bestimmen, welche Berufe einem Berufsgeheimnis unterliegen.

Einschränkung

> ***Achtung!***
> *Diese Norm kann nicht herangezogen werden, um Informationspflichten des Berufsgeheimnisträgers gegenüber dem Begünstigten des Berufsgeheimnisses auszuschließen!*

Der Ausschlusstatbestand greift wohl, wenn ein Steuerberater von seinem Klienten relevante personenbezogene Daten über dessen Kunden erhält. Der Steuerberater ist dabei zB gegenüber diesen Personen von den Informationspflichten ausgenommen.

Die Reichweite und der Umfang des Ausschlusstatbestands richten sich nach der Reichweite und dem Umfang des Berufsgeheimnisses. Dabei ist zu beachten, dass die Informationspflichten nicht die erhobenen Daten selbst umfassen, sondern sich auf die Datenkategorien sowie weitere Metainformationen der Datenerhebung beschränken.

9.4 Beispiel „Information nach Art. 13/14 DSGVO“

Sehr geehrte(r) Herr/Frau Muster,

wir informieren Sie nachstehend gemäß Art. 13/14 DSGVO über die Verarbeitung Ihrer Daten.

Identität des Verantwortlichen:
Muster Steuerberatung GmbH, Musterstr. 1, 1111 Musterstadt, Österreich

Kontaktdaten des Datenschutzbeauftragten:
Sie erreichen unseren zuständigen Datenschutzbeauftragten unter: Datenschutzbeauftragter der Muster Steuerberatung GmbH, Musterstr. 1, 1111 Musterstadt, oder datenschutzbeauftragter@muster.at

Verarbeitungszwecke und Rechtsgrundlage:
Die Datenverarbeitung erfolgt zum Zweck (konkreten Verarbeitungszweck einfügen). Weiterer von uns verfolgter Zweck der Datenverarbeitung ist (weitere verfolgte Zwecke einfügen).
Die Verarbeitung Ihrer Daten basiert auf Art. 6 Abs. 1 Buchstabe (konkreten Buchstaben der Bestimmung einfügen) DSGVO.
Darüber hinaus ist die Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe f DSGVO zur Wahrung unserer berechtigten Interessen oder der eines Dritten erforderlich. Unsere berechtigten Interessen sind (berechtigtes Interesse einfügen).

Datenkategorien und Datenherkunft:
Wir verarbeiten nachfolgende Kategorien von Daten: Basisdaten, Kommunikationsdaten (E-Mail, Adresse, Tel.Nr.), Vertragsdaten, Zahlungsinformationen, Rechnungen, Gehaltsdaten

Die Daten aus den genannten Datenkategorien wurden uns von … (Name des Übermittlers) übermittelt.

Empfänger:
Im Rahmen der Steuerberatung werden wir Ihre Daten an (Name konkreter Empfänger) und ggf. folgende Kategorien von Empfängern übermitteln, sofern dies im Rahmen der Vertragserfüllung erforderlich ist: Abtretungsempfänger, Auskunfteien, Dienstleister, Drittschuldner, Gerichte, Finanzämter, Rechtsanwälte, Sozialversicherungen

Rechte der betroffenen Person:
Ihnen stehen bei Vorliegen der gesetzlichen Voraussetzungen folgende Rechte nach Art. 15 bis 22 DS-GVO zu: Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und auf Datenübertragbarkeit.

Außerdem steht Ihnen nach Art. 14 Abs. 2 Buchstabe c in Verbindung mit Art. 21 DSGVO ein Widerspruchsrecht gegen die Verarbeitung zu, die auf Art. 6 Abs. 1 Buchstabe f DSGVO beruht.
Dauer der Speicherung:
Nach Erreichung (Zweck einfügen) prüfen wir nach Ablauf von (konkrete Frist einfügen), ob wir Ihre Daten noch benötigen und einer Löschung gesetzliche Aufbewahrungspflichten entgegenstehen.

Beschwerderecht bei der Aufsichtsbehörde
Sie haben gemäß Art. 77 DSGVO das Recht, sich bei der Aufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Die Anschrift der für unser Unternehmen zuständigen Aufsichtsbehörde lautet: … (Name und Anschrift der zuständigen Aufsichtsbehörde).
Drittstaaten
Im Rahmen der Datenverarbeitung werden Auftragsverarbeiter in Drittstaaten eingesetzt, welche in Indien ansässig sind und für uns das Hosting unserer Datenbank übernehmen. Indien ist ein Drittstaat ohne angemessenes Schutzniveau. Dieses angemessene Schutzniveau haben wir insbesondere durch Abschluss von Standardvertragsklauseln sichergestellt. Diese sind abrufbar unter (Link einfügen).

9.5 Anwendungsbeispiele Steuerberater

Steuerberater müssen stets analysieren, für welche Datenverarbeitungen diese als Verantwortliche und für welche diese als Auftragsverarbeiter zu qualifizieren sind. Wie auch die anderen Betroffenenrechte sind diese grundsätzlich vom Verantwortlichen zu erfüllen, und der Auftragsverarbeiter muss den Verantwortlichen entsprechend unterstützen.

Konkrete Beurteilung der einzelnen Verarbeitungen

Im Tätigkeitsfeld der Personalverrechnung agiert ein Steuerberater wohl oftmals als Auftragsverarbeiter, im Bereich der Steuerberatungsleistung wohl in der Regel als Verantwortlicher. Agiert ein Steuerberater nun als Verantwortlicher, so hat er seinen Klienten entsprechend zu informieren (zB den Einzelunternehmer als betroffene Person). Agiert ein Steuerberater als Auftragsverarbeiter, trifft die Informationspflicht den Verantwortlichen (zB das Klientenunternehmen) und er muss dabei lediglich unterstützend tätig werden.

Gegenüber den eigenen Mitarbeitern agiert ein Steuerberater wie auch jedes andere Unternehmen als Verantwortlicher und hat den Informationspflichten entsprechend nachzukommen.

9.6 Checkliste „Informationspflichten“

Prüffragen	Ja / Nein
Wurden im Unternehmen alle Bereiche identifiziert, in denen eine Information bereitgestellt werden muss?	
Wissen alle Mitarbeiter über die Bereitstellungspflicht der Informationen Bescheid?	
Werden alle Mitarbeiter ausreichend bestimmt informiert?	
Werden alle Kunden ausreichend bestimmt informiert?	
Sind geeignete Verfahren im Unternehmen etabliert?	
Ist eine standardisierte Vorlage im Unternehmen verfügbar?	

10 Betroffenenrechte

Um die zeitgerechte und umfassende Behandlung von Betroffenenrechten im Unternehmen sicherzustellen, ist es notwendig, die bestehenden Unternehmensabläufe und Prozesse entsprechend zu evaluieren und wo notwendig zu adaptieren.

Zahlreiche Rechte von betroffenen Personen

Stellen Sie sich für jede Ihrer Datenanwendungen immer die folgende Frage:

Kann ich allen Betroffenenrechten rasch und unkompliziert nachkommen?

10.1 Recht auf Auskunft

Überblicksmäßig hat eine Person folgende Auskunftsrechte gegenüber einem Verantwortlichen in Hinblick auf ihre personenbezogenen Daten gegenüber dem Verantwortlichen:

Recht zu wissen ob und welche Daten verarbeitet werden

- Bestätigung zu erhalten, ob ihre Daten vom Verantwortlichen verarbeitet werden
- Auskunft betreffend dieser Daten und
- Eine Kopie der verarbeiteten Daten zu erhalten

– Inhalt der Auskunft

Der Auskunftsinhalt hat folgendes zu enthalten:

Detaillierte Inhalte der Beauskunftung

- **die Verarbeitungszwecke**
- **die Kategorien personenbezogener Daten**, die verarbeitet werden
- **die Empfänger oder Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- falls möglich die **geplante Dauer**, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die **Kriterien für die Festlegung dieser Dauer**
- das **Bestehen eines Rechts auf Berichtigung oder Löschung** der sie betreffenden personenbezogenen Daten oder auf **Einschränkung** der Verarbeitung durch den Verantwortlichen oder eines **Widerspruchsrechts** gegen diese Verarbeitung
- das **Bestehen eines Beschwerderechts** bei einer Aufsichtsbehörde

- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die **Herkunft** der Daten

- das Bestehen einer **automatisierten Entscheidungsfindung einschließlich Profiling** und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

- ggf. ein **Drittland** oder die internationale Organisation, an die Daten übermittelt werden, und die **geeigneten Garantien**

– Ablauf, Form, Frist und Sonstiges

Hinsichtlich des Gegenstands des Anspruchs wird stets auf den Zeitpunkt des Auskunftsansuchens abgestellt. Die Daten sind dabei so bereitzustellen, wie sie konkret vorliegen. Der Verantwortliche darf auch die Daten nicht durch eine Aufbereitung abändern, da er hierdurch den Informationsgehalt der Daten verändern könnte.

Immer Auskunft erteilen!

Auch Negativauskünfte sind zu erteilen

Grundsätzlich muss der Verantwortliche der betroffenen Person in allen Fällen mitteilen, ob er sie betreffende personenbezogene Daten verarbeitet. Auch wenn keine personenbezogenen Daten verarbeitet werden, muss eine Negativauskunft erteilt werden.

Form

Die Auskunft hat in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.

Identitätsfeststellung

Immer zuerst die Identität feststellen

Vor Auskunftserteilung hat sich der Verantwortliche insbesondere von der Identität der auskunftssuchenden Person in geeigneter Art und Weise zu überzeugen. Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Bereitstellung

Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt,

kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt. Um die Anforderungen des Auskunftsrechts zu erfüllen, sollte der Verantwortliche nach Möglichkeit den Fernzugang zu einem sicheren System bereitstellen. Er soll der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen.

Eine probate Lösung könnte das Einrichten eines geschützten Bereichs auf der jeweiligen Unternehmenswebseite sein, zu der die betroffene Person nach hinreichender, eindeutiger Identifizierung Zugang erhält. Eine andere Möglichkeit wäre wohl bei einem bestehenden Account einen Bereich bezüglich der Beauskunftung bereitzustellen.

Frist

Monatsfrist beachten

Der Verantwortliche stellt der betroffenen Person die angesuchten Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung.

Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche hat die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung zu unterrichten, zusammen mit den Gründen für die Verzögerung.

Kosten

kostenlos

Die Auskunft und Bereitstellung einer Kopie hat unentgeltlich zu erfolgen.

Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat allerdings den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen!

Stellen Sie für alle Verarbeitungen sicher, wo Sie Verantwortlicher und wo Sie Auftragsverarbeiter sind! Der Verantwortliche ist zur Wahrung der Betroffenenrechte verpflichtet. Der Auftragsverarbeiter muss diesen jedoch unterstützen.
Sind Sie etwa Personalverrechner und als Auftragsverarbeiter zu qualifizieren, wäre der Klient für die Beauskunftung an seine Mitarbeiter verantwortlich.
Für Steuerberatungstätigkeiten, bei der Sie als Verantwortlicher gelten, bedingt dies eine Auskunftspflicht durch Sie.

10.2 Recht auf Richtigstellung

Korrektur unrichtiger oder unvollständiger Daten

– Allgemein

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person auch das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Auch die Berichtigung von Daten hat unentgeltlich zu erfolgen.

Mitteilungspflicht an andere Empfänger

– Mitteilungspflicht

Im Zusammenhang mit dem Richtigstellungsrecht ist auch die allgemeine Mitteilungspflicht des Verantwortlichen näher zu beleuchten. Diese gilt ebenso für das Recht auf Löschung und das Recht auf Einschränkung.

Der Verantwortliche hat allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mitzuteilen!

Eine Ausnahme wäre, wenn sich dies als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

10.3 Recht auf Löschung

Pflicht zur Löschung bedingt auch das Recht auf Löschung

Das Recht auf Löschung wurde auch bekannt unter dem medienwirksamen Schlagwort „Recht auf Vergessenwerden“. Neben dem Löschungsanspruch der betroffenen Person bestehen auch von der Geltendmachung des Anspruchs unabhängige Löschungspflichten des Verantwortlichen.

– Wann besteht nun das Recht auf Löschung und die Pflicht zur Löschung?

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

Insbesondere im Bereich des Zivilrechts stellt sich oftmals die Frage, inwieweit das Laufen einer Verjährungsfrist die weitere Speicherung von Daten zur Geltendmachung oder Abwehr von Ansprüchen notwendig macht. Hier ist jedenfalls eine Interessensabwägung vorzunehmen. Dabei kommt es auf die Wahrscheinlichkeit der Geltendmachung von Ansprüchen sowie auf das mögliche Gewicht dieser Ansprüche und auf das Ausmaß der Beeinträchtigung der Belange der betroffenen Person durch eine weitere Speicherung an.
Eine pauschale Aussage in dem Sinne, dass eine weitere Speicherung bis zum Ablauf der Verjährungsfrist in jedem Fall zulässig sei, lässt sich nicht argumentieren. Bei umfangreichen Datenbeständen empfiehlt sich die Implementierung eines (automatisierten) Löschkonzepts mit Löschfristen für bestimmte Arten von Daten. Weiters sollte der Verantwortliche die Notwendigkeit der weiteren Datenspeicherung regelmäßig überprüfen.

- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor (Stützung auf „berechtigte Interessen“), oder die betroffene Person legt Widerspruch gegen die Verarbeitung ein (Direktmarketing).

- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben und die betroffene Person verlangt die Löschung.

Achtung!
Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so hat er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen zu ergreifen, auch technischer Art, um andere Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien dieser personenbezogenen Daten verlangt hat.

– Inhalt des Löschungsanspruchs bzw. der Pflicht zur Löschung

In der DSGVO selbst gibt es keine Definition des Begriffs "Löschens".

Wie ist zu löschen?

Das Löschen kann auf unterschiedliche Weise erfolgen. Entscheidend ist vorrangig das Endergebnis der Löschungshandlung, nämlich die faktische Unmöglichkeit, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen. Nach dem Löschvorgang darf es niemandem mehr ohne unverhältnismäßigen Aufwand möglich sein, die betreffenden Informationen zu eruieren.

Achtung!

Keine ausreichende Löschungshandlung sind rein organisatorische Maßnahmen, die die Wahrnehmung der personenbezogenen Daten verhindern sollen (wie zB das Verbot des Einsehens oder Abrufens).

Auch das bloße Entsorgen des Datenträgers als allgemeiner Müll ist kein Löschen, solange die Zugriffnahme zu den Informationen durch andere Personen (die den Datenträger etwa zufällig finden und an sich nehmen) noch möglich ist. Die Zuhilfenahme spezieller Entsorgungsfirmen ist hingegen eine Möglichkeit der „sicheren“ Entsorgung.

Wenn der Verantwortliche über Backups der zu löschenden Daten verfügt, sind auch die Backups zu löschen, es sei denn die Datenbestände sind mit anderen Datenarten derart „verwoben“ und verknüpft, so dass eine Löschung technisch nicht möglich ist. Dann besteht die entsprechende Möglichkeit die Daten aus den Backups „herauswachsen“ zu lassen.

Auch die Löschung hat grundsätzlich unentgeltlich zu erfolgen. Hinsichtlich der Mitteilungspflicht im Zusammenhang mit der Löschung sei an dieser Stelle auf das Kapitel „Recht auf Richtigstellung“ verwiesen. Es gelten dabei die dort angeführten Ausführungen.

Es ist von immenser Bedeutung, ein geeignetes Löschkonzept zu entwickeln um dem Recht auf (sowie der Pflicht zur) Löschung nachkommen zu können. Gesetzliche Aufbewahrungspflichten wie etwa 7 Jahre bei Belegdaten gem. BAO oder 30 Jahre für dienstzeugnisrelevante Daten sind in geeigneter Form umzusetzen.
Konkrete Empfehlungen der Kammer der Steuerberater und Wirtschaftsprüfer sind hier abzuwarten und auch die technische Umsetzung der Softwarehersteller.

10.4 Recht auf Einschränkung

Neu: das Einschränken von Daten

Das Recht auf Einschränkung gilt als Ergänzungsrecht zum Recht auf Löschung. Aber was bedeutet nun „Einschränken von Daten“?

Wie wir bei der Löschung bereits erfahren haben, ist das Merkmal des Löschens, dass personenbezogene Daten und Informationen nicht mehr abrufbar sind – für niemanden.

Beim Einschränken von Daten werden hingegen die Daten nicht gelöscht, allerdings derart „eingeschränkt“ und gesperrt, dass diese nicht mehr verarbeitet werden können. Um diese konkrete Zweckbegrenzung zu erreichen, sind die betroffenen personenbezogenen Daten entsprechend zu markieren.

Allgemeiner Zweck dieses Rechts ist die Beweissicherung und um verfrühtes Löschen von Datenbeständen in unklaren Rechtssituationen zu vermeiden.

– Wann besteht das Recht auf Einschränkung?

Wann ist dieses anzuwenden?

Die betroffene Person hat insbesondere das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn:

- die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen, oder

- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt, oder

- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

- die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

– **Was nun?**

Wurde die Verarbeitung eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur

Umsetzung des „Einschränkens“

- mit Einwilligung der betroffenen Person oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden

Stellen Sie dabei jedoch sicher, dass niemand mehr im Unternehmen die Daten der betroffenen Person verarbeitet! Der Verantwortliche hat die betroffene Person zudem zu unterrichten, sofern er vorhat, die Einschränkung aufzuheben.

10.5 Recht auf Widerspruch

Widerspruch gegen die Verarbeitung von Daten

Ein Widerspruchsrecht gegen die Datenverarbeitung besteht für betroffene Personen insbesondere in drei Fallkonstellationen:

– **Direktmarketing (absolutes Recht)**

– **Verarbeitung aufgrund „berechtigter Interessen“**

Der Verantwortliche darf die personenbezogenen Daten dann nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Achtung!
Der Verantwortliche hat die Darlegungs- und Beweislast der überwiegenden Interessen, ansonsten hat er die Verarbeitung einzustellen.

– **Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder zu statistischen Zwecken**

10.6 Recht auf Datenübertragbarkeit

Was ist damit gemeint?

Das Recht auf Datenübertragbarkeit ist ein neues Recht, welches betroffenen Personen mit der DSGVO zukommt, denn in der „alten" Rechtslage gab es dazu keine vergleichbare Regelung.

Neu: Recht auf Datenübertragung

In den Grundüberlegungen zu diesem Betroffenenrecht steht die Erleichterung eines typischen „Anbieterwechsels" oder „Profilumzugs" im Vordergrund. Dabei ist zB an Dienstanbieter im Internet wie soziale Netzwerke, aber auch E-Mail Provider zu denken. Der betroffenen Person sollen insbesondere keine „Steine in den Weg gelegt" werden bei der Absicht, den Anbieter zu wechseln.

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

- die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und
- die Verarbeitung mithilfe automatisierter Verfahren erfolgt

Bei der Ausübung ihres Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Das Recht auf Datenportabilität darf dabei die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Wie auch bereits bei den anderen Betroffenenrechten haben die Maßnahmen durch den Verantwortlichen unentgeltlich zu erfolgen und dem Recht ist unverzüglich, spätestens aber binnen eines Monats nachzukommen.

Relevanz für Steuerberater

Der praktische Anwendungsfall für Steuerberater ist für Tätigkeiten, bei denen diese als Auftragsverarbeiter für ihre Klienten auftreten und nicht als direkte Anbieter wie soziale Netzwerke oder Email-Provider agieren oder auch Banken, ausgeschlossen, da dieses Recht gegenüber Verantwortlichen wahr genommen werden muss.

Einzelfall-evaluierung notwendig

Für jene Bereiche, in denen Steuerberater jedoch als Verantwortliche agieren (hier wäre an „die Steuerberatung" selbst zu denken), wäre es jedoch durchaus denkbar, dass das Recht auf Datenübertragung von Klienten wahrgenommen werden kann, insofern diese als betroffene Personen i.S.d. DSGVO qualifiziert werden können, etwa weil diese Einzelunternehmer sind. Auch hier bleiben die Ansichten der KSW abzuwarten.

Beispiel:

Datenübertragung vom Alt-Steuerberater an Neu-Steuerberater, wenn es sich beim Klienten um eine natürliche Person handelt. Ist der Klient allerdings eine juristische Person, greift das Recht auf Datenübertragbarkeit nicht.

10.7 Checkliste

Checkliste

Prüffragen	Ja / Nein
Wurde für alle Datenverarbeitungen evaluiert, ob jeweils alle Betroffenenrechte erfüllt werden können?	
Wurden standardisierte Abläufe zur Erfüllung von Betroffenenrechte im Unternehmen eingeführt?	
Sind, wo technisch möglich, automatisierte Verfahren eingesetzt?	
Ist sichergestellt, dass die erforderlichen Inhalte der Betroffenenrechte erfüllt werden können?	
Sind die Mitarbeiter ausreichend geschult, um zu wissen wie bei Anfragen vorzugehen ist?	
Ist die Dokumentation der einzelfallspezifischen Erfüllung sichergestellt?	
Wird die Identität der anfragenden betroffenen Person adäquat überprüft?	

11 Profiling und automatisierte Entscheidungen

11.1 Allgemein

Was versteht man unter „Profiling“ oder „automatisierter Verarbeitung“?

Verbot von automatisierten Einzel-entscheidungen

- jede Art der automatisierten Verarbeitung personenbezogener Daten,
- die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, insbesondere *Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel*
- die sich auf eine natürliche Person beziehen, zu bewerten, analysieren oder vorherzusagen

Wenn automatisierte Einzelentscheidungen, basierend auf automatisierter Verarbeitung oder Profiling, rechtliche Wirkungen oder erhebliche Beeinträchtigungen auf eine betroffene Person haben können, hat die betroffene Person das Recht, eben nicht einer solchen Entscheidung unterworfen zu werden. Eine konkret resultierende Maßnahme ist einer Entscheidung gleichzusetzen.

Beispiele:

Die automatische Ablehnung eines Online-Kreditantrags oder eines Online-Einstellungsverfahrens ohne jegliches menschliches Eingreifen.

11.2 Ausnahmen

Ausnahmen vom Verbot

Eine auf einer derartigen Verarbeitung, einschließlich des Profilings, beruhende Entscheidungsfindung ist allerdings erlaubt, wenn

- dies aufgrund von Rechtsvorschriften, denen der Verantwortliche unterliegt, ausdrücklich zulässig ist oder
- dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder
- die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat.

Profiling und automatisierte Entscheidungen sind insbesondere Anwendungsfälle einer durchzuführenden und dokumentierten Datenschutzfolgenabschätzung!

11.3 Anwendbarkeit auf Steuerberater

Steuerberater werden im Tagesalltag und in Durchführung ihrer Dienstleistungen wohl nur selten Profiling betreiben und noch seltener daran automatisierte Einzelentscheidungen knüpfen.

Denkbar wäre jedoch als Anwendungsbereich eine auf einer automatisierten Verarbeitung, einschließlich des Profilings, beruhende Entscheidungsfindung, um im Einklang mit den Vorschriften, Standards und Empfehlungen der Europäischen Union oder den nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern sowie die Sicherheit und Zuverlässigkeit eines bereitgestellten Dienstes zu gewährleisten.

12 Verzeichnis von Verarbeitungstätigkeiten (VVV)

12.1 Allgemein

Neu: Verzeichnis von Verarbeitungs-tätigkeiten

Mit der Datenschutz-Grundverordnung muss ein Unternehmen nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies ist nur eine von mehreren, neuen Vorgaben zur Dokumentationspflicht.

Bei der Einhaltung aller gesetzlichen Vorgaben wird das Verzeichnis aber eine tragende Rolle spielen. Denn es enthält eine Dokumentation und Übersicht über alle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden.

12.2 Pflicht zum Führen eines Verzeichnisses

In der Regel müssen alle Verantwortlichen ein Verzeichnis von Verarbeitungstätigkeiten führen. Auftragsverarbeiter müssen explizit ein Verzeichnis im Hinblick auf ihre Dienstleistungen führen (VVV-AV). Dies entbindet allerdings nicht von der Verpflichtung zu einem originären VVV für die eigenen Geschäftsprozesse.

Selbst-verantwortung

In der Praxis erscheint es sinnvoll, gesonderte Vorlagen für die allgemeinen Verarbeitungen des Unternehmens sowie für den Bereich der Auftragsverarbeitung zu haben (jeweils mit eigenem Aufbau und als gesonderte Formulare).

12.3 Form

Das Verzeichnis von Verarbeitungstätigkeiten darf in einem elektronischen Format geführt werden. Wegen der Vorlagepflicht gegenüber der Aufsichtsbehörde muss es in elektronischer oder gedruckter Form exportierbar sein.

Elektronisches Format

Da das VVV mit der Weitergabe an die Aufsichtsbehörde das Unternehmen verlässt, sollte es keine schutzbedürftigen, internen Informationen im Zusammenhang mit den IT-Sicherheitsmaßnahmen enthalten.

Die Handhabung über ein standardisiertes Excel Dokument mit mehreren Tabellenblättern für die Stammdaten des Unternehmens sowie die Einzeleinträge und allgemeine Maßnahmen stellt sicherlich eine einfache Methode der Handhabung dar.

Der Einsatz spezieller Software zur Verwaltung des Verzeichnisses von Verarbeitungstätigkeiten ist eine entsprechende Alternative.

12.4 Inhalte

Das VVV ist nicht als Auflistung einzelner Datenverarbeitungen, sondern als prozessorientierte Übersicht der Datenverarbeitungen zu verstehen. Entscheidend ist, dass über das VVV der einzelne Verarbeitungsprozess, dh die konkrete Datenanwendung, zu identifizieren ist.

Prozesse vor Einzelfällen

Es muss daher nicht jedes Mal ein wiederkehrender Prozessschritt in das Verzeichnis von Verarbeitungsvorgängen eingetragen werden, sondern der Verarbeitungsprozess „als Ganzes“.

Die „Personalverrechnung“ oder der „Newsletterversand“ kann dabei einmal erfasst werden, so wie er im Unternehmen in der Regel durchgeführt wird, mitsamt der Listung aller verarbeiteten Datenarten, Speicherdauer, etc.

– VVV Vorlage

STAMMDATENBLATT (Angaben zum Verantwortlichen)

	Bezeichnung	Erklärung	Angabe
1	**Verantwortlicher** (= Unternehmen) *Name/Ladungsfähige Anschrift*	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet	
2	**Gesetzlicher Vertreter** *Name/Kontaktdaten*	Vorstände, Geschäftsführer oder sonstige gesetzliche oder berufene Leitungsfunktionen	
3	**Vertreter in der EU** *Name / Ladungsfähige Anschrift*	Bei Unternehmen ohne eigene Niederlassung in der EU ist der benannte Vertreter des Verantwortlichen anzugeben	
4	**Datenschutzbeauftragter** *Name/Kontaktdaten*	Der vom Verantwortlichen bestellte Datenschutzbeauftragte	
5	**Zuständige Aufsichtsbehörde** *Name*	Die zuständige nationale Aufsichtsbehörde	
6	**Angaben zur Datensicherheit** *Verweis auf übergreifende IT-Sicherheitskonzepte*	Hinweis auf unternehmensweite Regelungen, die alle Datenverarbeitungen betreffen. Achtung: Der Verweis entbindet nicht von der Dokumentation in den einzelnen Verarbeitungstätigkeiten	
7	**Angaben zur Datenlöschung** *Verweis auf übergreifende Löschkonzepte*	Hinweis auf Löschkonzepte, die füralle Datenverarbeitungen gelten	
8	**Generelle Angaben zu Drittstaatenübermittlungen** *Verweis auf übergreifende Punkte wie Binding Corporate Rules*	Hinweis auf Regelungen zur Drittstaatenübermittlung sind sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR	

Verarbeitungstätigkeit Nr. ____

	Bezeichnung	Erklärung	Angabe
1	**Verarbeitungsname** *Name und Kurzbezeichnung*	Bezeichnung anhand des konkreten Unternehmensprozesses, der bekannt ist (zB CRM, Spesenkostenabrechnung, Urlaubsmanagement, …)	
2	**Zweck der Verarbeitung** *Konkrete Kurzbeschreibung*	Beschreibung der Verarbeitungstätigkeit samt Teilprozessen. Es können auch mehrere Zwecke verfolgt werden.	
3	**Verantwortliche Person IT** *Wer ist technisch zuständig*	Die verantwortliche Funktion/Person, die die betreffende Verarbeitungstätigkeit betreut bzw. technische Fragen beantworten kann	
4	**Verantwortliche Person Fachbereich** *Wer ist fachlich zuständig*	Die für die betreffende Verarbeitungstätigkeit verantwortliche Fachbereichsfunktion oder Leitungsfunktion	
5	**Datum der letzten Prüfung** *Letztes Evaluierungsdatum*	Das Datum der letzten Überprüfung auf Vollständigkeit und Richtigkeit der Angaben des Eintrags	
6	**Rechtsgrundlage** *Konkrete Angabe der zutreffenden Art. 6 DSGVO Bestimmung*	Wird die Datenverarbeitung auf Einwilligung, Vertragserfüllung, Geschäftsanbahnung, rechtliche Verpflichtung oder Ermächtigung oder berechtigtes Interesse gestützt	
7	**Kategorien der betroffenen Personen** *Welche Personengruppen sind betroffen*	Welche Personengruppen sind von der Verarbeitung umfasst (Mitarbeiter, Kunden, Lieferanten, Pensionisten, …)	
8	**Kategorien der personenbezogenen Daten** *Welche Datenarten werden verarbeitet*	Welche Datenarten und/oder Kategorien von personenbezogenen Daten sind von der Verarbeitung umfasst	
9	**Kategorien vom Empfängern** *Interne und externe Datenweitergabe (auch Zugriffe)*	Empfänger sind alle an der Verarbeitungstätigkeit beteiligte Stellen (wie andere Konzerngesellschaften, Dienstleister, Subdienstleister, Behörden, …)	
10	**Involvierte Drittländer** *Staaten außerhalb der EU/EWR*	Angabe, welche Empfänger in Drittländern personenbezogene Daten erhalten oder Zugriff darauf nehmen können	
11	**Fristen für die Löschung der verarbeiteten Datenkategorien** *Konkrete Zeitangaben*	Die konkreten Aufbewahrungs-, Speicher- und Löschfristen für die jeweiligen Datenarten und Verarbeitungsschritte	
12	**Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** *(Sicherheitskonzepte)*	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, der technischen Infrastruktur oder prozessualer Vorgaben	
13	**Gemeinsame Verantwortliche** *Name und Anschrift*	Angabe der an der Verarbeitungstätigkeit beteiligten „Gemeinsamen Verantwortlichen“ (zB konzerninterne Bonitätsdatenbank)	

– Verzeichnis von Auftragsverarbeitungen

Das Verzeichnis von Verarbeitungstätigkeiten, das ein Auftragsverarbeiter zu erstellen hat, dient primär dazu, eine erste Übersicht darüber zu erhalten, welche Leistungen für welchen Verantwortlichen erbracht werden.

Verzeichnis auch für Dienstleistungen

Die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten sollte sich grundsätzlich an den Anforderungen des Auftragsverarbeiters (Dienstleisters) und damit an seinen Dienstleistungen und Produkten orientieren. Hieraus lassen sich die „Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden" ableiten.

Bei der Bestimmung der Leistung, insbesondere bei der vertraglichen Gestaltung, sollte darauf geachtet werden, was in den Verantwortungsbereich des Auftragsverarbeiters bzw. des Verantwortlichen fällt. So ist zum Beispiel die Weitergabe personenbezogener Daten an einen vom Auftragsverarbeiter eingesetzten Unterauftragnehmer im Drittland (zB Hosting) Bestandteil der vom Auftragsverarbeiter angebotenen Leistungskette. Insoweit fällt diese Weitergabe in die Sphäre des Auftragsverarbeiters und ist von ihm in seinem VVV zu dokumentieren. Dagegen fällt eine vom Verantwortlichen angewiesene Weitergabe seiner Daten an eine Stelle im Drittland in die Sphäre des Verantwortlichen.

Die Inhalte des VVV für Auftragsverarbeiter ergeben sich wie folgt:

Was muss alles drinnen stehen?

- den Namen und die Kontaktdaten:
- des Auftragsverarbeiters oder der Auftragsverarbeiter;
- jedes Verantwortlichen, in dessen Auftrag der AV tätig ist;
- gegebenenfalls des Vertreters des Verantwortlichen;
- gegebenenfalls des Vertreters des Auftragsverarbeiters;
- eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation;
    - einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation;
    - die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO

13 Datenschutzbeauftragter (DSB)

13.1 Bestellungspflicht nach der DSGVO

Wann muss ich einen Datenschutz-Beauftragten haben?

Mit der Datenschutzgrundverordnung hält nun europaweit der Datenschutzbeauftragte Einzug in die Unternehmen. Eine der wesentlichen Pflichten von Verantwortlichen oder Auftragsverarbeitern ist die ex lege-Bestellpflicht eines Datenschutzbeauftragten für bestimmte Datenverarbeitungskonstellationen.

Eine Verpflichtung zur Bestellung eines DSB besteht für

- Behörden und öffentliche Stellen[9] und
- nichtöffentliche Stellen, wenn die Kerntätigkeit des Unternehmens
    - in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund von Art, Umfang und/oder Zweck eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
    - in der umfangreichen Verarbeitung von besonderen Kategorien von Daten besteht. Dazu gehören insbesondere Rasse, ethnische Herkunft, politische, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, Daten zur Sexualität, strafrechtliche Verurteilungen oder Straftaten.

Stellen Sie daher sicher, eine ausreichende Evaluierung der Bestellpflicht eines Datenschutzbeauftragten dokumentationssicher nachweisen zu können!

Ebenso ist eine freiwillige Bestellung möglich und in vielen Situationen durchaus sinnvoll, auf fachkundigen, datenschutzrechtlichen Rat bei der Umsetzung der DSGVO zurückgreifen zu können.

Achtung!
Auch wenn offiziell kein Datenschutzbeauftragter bestellt werden muss, so hat sich jemand im Unternehmen des Datenschutzes anzunehmen und die Einhaltung der DSGVO sicherzustellen.

[9] mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln

13.2 Fakultative Benennung eines Datenschutzbeauftragten

Unabhängig von der Feststellung eines Negativergebnisses zur Bestellpflicht ist es ratsam, dass Verantwortliche oder Auftragsverarbeiter einen DSB bestellen,

- wenn die Kerntätigkeit in der Verarbeitung von personenbezogenen Daten besteht, insbesondere wenn besondere Kategorien personenbezogener Daten verarbeitet werden;
- wenn ein hoher Automatisierungsgrad in der Organisation gegeben ist;
- wenn der Verantwortliche oder der Auftragsverarbeiter in einem regulierten Bereich tätig ist.

Benennt eine Organisation freiwillig einen Datenschutzbeauftragten, so ist diese Rolle so auszugestalten, als wäre ein DSB ex lege zu bestellen.[10]

Freiwillige Benennung unter Umständen sinnvoll

13.3 Aufgaben und Anforderungen

Die Aufgaben eines Datenschutzbeauftragten gemäß DSGVO sind:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten
- Überwachung der Einhaltung der DSGVO sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten
- Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation im Rahmen der Datenschutzfolgenabschätzung

Was hat ein Datenschutz-Beauftragter zu tun?

Der mitzubringende Grad des Fachwissens richtet sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die vom Verantwortlichen oder vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten.

[10] Vgl. WP 243, 20.

Der Datenschutzbeauftragte sollte umfassende Kenntnisse und praktische Erfahrung im Datenschutzrecht aufweisen.

Der Datenschutzbeauftragte kann grundsätzlich auch andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter hat jedoch sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Ein solcher Interessenkonflikt ist insbesondere bei Ausübung der Datenschutzbeauftragtenrolle durch folgende Funktionen anzunehmen:

Interessens-konflikte

- Geschäftsführung
- Leitung IT
- Leitung HR
- Betriebsrat
- Leitung Recht

13.4 Externe Bestellung

Unternehmen dürfen sowohl einen gemeinsamen Datenschutzbeauftragten für eine Unternehmensgruppe benennen als auch einen externen Datenschutzbeauftragten bestellen.

Externe Bestellung mit Vorteilen

Der Vorteil für Unternehmen besteht oftmals darin, dass nicht nur ein Datenschutzbeauftragter gestellt wird, sondern eine gesamte Datenschutzorganisation im Hintergrund verfügbar ist.

Die externe Bestellung bietet insbesondere folgende Vorteile:

- Vertretung im Krankheits- und Urlaubsfall
- Kein Ersatzproblem beim Ausscheiden eines Mitarbeiters
- Zurverfügungstellung von unterschiedlichsten Expertisen (technisch, juristisch, organisatorisch)
- Oftmals integrierter Ansatz mit Informationssicherheit
- Ein externer Datenschutzbeauftragter ist auch kurzfristig und anlassbezogen verfügbar.
- Interessenskonflikte werden vermieden.
- Die intern ausgeübten Haupttätigkeiten der Mitarbeiter werden durch die Zusatzbelastung, die die Bestellung zum behördlichen Datenschutzbeauftragten zwangsläufig mit sich bringt, nicht beeinträchtigt.

- Externe Datenschutzbeauftragte verfügen infolge ihrer Neutralität über besondere Vermittlungsfähigkeiten, so etwa bei Konflikten zwischen Vorgesetzten und Mitarbeitern.
- Die Kosten eines externen behördlichen Datenschutzbeauftragten sind für die verantwortliche Stelle kalkulierbar und oftmals günstiger als eine interne Lösung.
- Es entstehen keine fortlaufenden Nebenkosten für die Ausbildung/Fortbildung von Mitarbeitern in Zeiten stetig wachsender rechtlicher Anforderungen.

13.5 Beurteilung für Steuerberater

Was nun bei Steuerberatern?

Die Haupttätigkeit eines Steuerberaters erstreckt sich, je nach individueller Unternehmensausrichtung, von der Beratung über die Personalverrechnung, die Buchhaltung und die Erstellung von Jahresabschlüssen bis hin zu Sachverständigentätigkeiten sowie die Erbringung von Prüfungsleistungen.

Diese Tätigkeiten werden dabei als Dienstleister ausgeführt, denn die jeweiligen personenbezogenen Daten der Mitarbeiter, Kunden oder Lieferanten des Klienten werden insbesondere im Auftrag des Klienten für dessen Zwecke verarbeitet.

Werfen wir einen Blick auf die einzelnen Tatbestandsmerkmale:

Kerntätigkeit

Die zugrundeliegende Datenverarbeitung von vom Klienten bereitgestellten Daten ist dabei eindeutig mit der Kerntätigkeit des Steuerberaters verbunden. Die unternehmerische Tätigkeit ist dabei von der besonderen personenbezogenen Datenverarbeitung abhängig, dh ohne diese Datenverarbeitung kann insbesondere die unternehmerische Tätigkeit nicht ausgeübt werden. Aus dem Zweck der unternehmerischen Tätigkeit ist daher abzuleiten, dass die Kerntätigkeit eine bestellungsrelevante Datenverarbeitung umfasst.

Regelmäßige und systematische Überwachung

Die Verarbeitungstätigkeit ist ebenso als regelmäßige und systematische Überwachung (Beobachten) von betroffenen Personen zu qualifizieren. Denn ohne die wiederkehrende Datenverarbeitung mittels Systemen und Software und/oder Datenbanken ist wohl keine Ausübung des Steuerberaterunternehmertums möglich.

Umfangreich

Wie weit reicht der Begriff „umfangreich“?

Entscheidend ist im Endergebnis, in welchem Umfang ein Steuerberater seiner Tätigkeit nachgeht und vor allem, in welchem Umfang personenbezogene Daten von wie vielen betroffenen Personen verarbeitet werden. Der Begriff „umfangreich“ ist vom Gesetzgeber sehr vage gewählt. Jedoch lässt sich über Umwege durchaus eruieren, was wohl darunter zu verstehen ist.

Wenn ein einzelner Steuerberater seiner unternehmerischen Tätigkeit nachgeht, wird dieser in aller Regel von einer Bestellpflicht auszunehmen sein.[11]

Eine große Steuerberatungskanzlei hingegen mit beispielsweise über 100 Mitarbeitern, zahlreichen großen Klienten (darunter womöglich Konzernunternehmen) und hunderttausenden oder Millionen Datensätzen von Mitarbeitern, Kunden und Lieferanten der Klienten wird wohl einer „umfangreichen“ Verarbeitung nachgehen und dadurch einer Bestellpflicht unterliegen.

Grauzone

Was aber ist mit Steuerberatungskanzleien mit fünf, zehn, 25 oder 50 Mitarbeitern?

Genau an dieser Stelle muss unseres Erachtens eine konkrete Einzelfallbetrachtung und Evaluierung der Bestellpflicht erfolgen. Dabei sind insbesondere die Zahl der betroffenen Personen (also Mitarbeiter, Kunden und/oder Lieferanten des Klienten), das Datenvolumen, die Dauer/Permanenz der Datenverarbeitung (zB nur jährlich wie bei der Bilanzierung oder aber monatlich wie in der Personalverrechnung und Buchhaltung) und die Ausdehnung der Tätigkeit (zB regional, österreichweit oder europaweit) zu berücksichtigen.

Dokumentation der Beurteilung

Wenn Sie nicht einem der beiden Extremfälle zuordenbar sind, führen Sie eine entsprechende, detaillierte Beurteilung und Abwägung durch und dokumentieren Sie diese im Unternehmen. Dabei sollten im Vorfeld die einzelnen Parameter evaluiert und berücksichtigt werden.

Insbesondere bleibt hier abzuwarten, welche Rechtsmeinung die KSW vertreten wird, wobei die derzeitige Tendenz wohl in die Richtung geht, dass Steuerberater in der Regel keinen Datenschutzbeauftragten bestellen müssen.

[11] Vgl. ErwGr 91 DSGVO

14 Auftragsverarbeiter

14.1 Allgemein

Dienstleister heißen nun Auftrags-verarbeiter

Die DSGVO definiert einen „Auftragsverarbeiter“ als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Aus dieser Definition geht hervor, dass der Auftragsverarbeiter bloß im Auftrag handelt und personenbezogene Daten auch nur in dem Rahmen, dem ihm der Verantwortliche vorgibt, verarbeitet. „Im Auftrag“ eines Verantwortlichen zu handeln bedeutet, in dessen Interesse zu handeln. Der Verantwortliche ist am Ende des Tages der „Herrscher über die Daten“. Er entscheidet, welcher Zweck verfolgt wird, was mit den Daten geschieht, wie diese verarbeitet werden und vor allem, wer was machen darf. Der Auftragsverarbeiter führt dies entsprechend aus.

Die konkrete Klassifizierung als Auftragsverarbeiter oder Verantwortlicher muss stets aufgrund der durchgeführten Tätigkeit erfolgen. Ein Unternehmen kann daher in manchen Bereichen Verantwortlicher und in anderen Bereichen Auftragsverarbeiter sein.
Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

Beispiele

Einige exemplarische Beispiele:

- Internetdienstanbieter (zB Hosting)
- Auslagerung von Postdienstleistungen
- E-Mail Plattformen
- Cloud Anbieter
- Outsourcing von Marketingaktivitäten
- Personalverrechner

14.2 Auswahl eines Auftragsverarbeiters (AV)

Erhöhte Anforderungen an die Auswahl

Deutliches Augenmerk sollte in Zukunft auf die Auswahl eines Auftragsverarbeiters gelegt werden. Die DSGVO verlangt von einem Verantwortlichen nämlich Auftragsverarbeiter auszusuchen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen ergriffen worden sind, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Verantwortliche müssen daher die beabsichtigte Beauftragung von Auftragsverarbeitern vorab genau prüfen!

14.3 Auftragsverarbeitervertrag

Vertrag abschließen!

– Abschluss eines Vertrags

Die Verarbeitung durch einen Auftragsverarbeiter darf nur auf der Grundlage eines Vertrags erfolgen, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. Der Vertrag ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Grundsätzlich hat der Verantwortliche die Pflicht, einen solchen Vertrag abzuschließen.

Der Mindestinhalt eines solchen Auftragsverarbeitervertrags ist in der DSGVO genau geregelt. Allerdings sollten Sie, um sich bestmöglich abzusichern, stets eine umfassende Variante verwenden, welche zusätzliche Verpflichtungen des Auftragsverarbeiters beinhaltet.

Inkludieren Sie ebenso detaillierte Vorgaben zu technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zu ergreifen hat. Zusätzlich können entsprechende Vertragsstrafen in solche Verträge mitaufgenommen werden.

Es bleibt abzuwarten, inwieweit die KSW eine für Steuerberater passende Vorlage zu Verfügung stellen wird.

– Sub-Auftragsverarbeiter

Weitere Auftrags-verarbeiter

Oftmals werden im Tagesalltag seitens des Auftragsverarbeiters noch weitere Auftragsverarbeiter eingesetzt. Diese Sub-Auftragsverarbeiter dürfen jedoch nicht ohne weiteres eingesetzt werden. Ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen ist die Unterbeauftragung untersagt.

Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, so ist mit diesem ein Vertrag abzuschließen („Spiegelvertrag"). Dabei sind dem Sub-Auftragsverarbeiter dieselben Datenschutzpflichten aufzuerlegen, die in dem ursprünglichen Vertrag zwischen Verantwortlichen und dem Auftragsverarbeiter vereinbart worden sind.

Achtung!

Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

14.4 Anwendbarkeit auf Steuerberater

Steuerberaterkanzleien gehören sicherlich zu jenen datenverarbeitenden Unternehmen, die im Tagesalltag, je nach durchgeführter Tätigkeit, sowohl als Verantwortlicher als auch als Auftragsverarbeiter bzw. auch als Sub-Auftragsverarbeiter zu qualifizieren sind.

Insbesondere ist an die Einordnung als Verantwortlicher zu denken, wenn Steuerberater – oftmals für Einzelunternehmer oder Kleinbetriebe – ihre Dienstleistungen auf der Grundlage einer sehr allgemeinen Weisung erbringen. Bei Aussagen eines Klienten wie „Erstellen Sie meine Steuererklärung." handeln Steuerberater oftmals, wie beispielsweise Rechtsanwälte und Notare, als Verantwortliche.

Wird ein Steuerberater jedoch für ein Unternehmen tätig, um etwa die Personalverrechnung oder Buchhaltung für dieses Unternehmen durchzuführen, und dabei detaillierten Weisungen des Klienten unterliegt, dann ist er aufgrund der klaren Weisungen und des doch eingeschränkten Handlungsspielraums unter Umständen als Auftragsverarbeiter einzustufen.

Beschäftigt der Steuerberater Personen im Werkvertrag (zB ausgelagerte Auftragsabwicklung durch eine andere STB-Kanzlei, Beschäftigung eines Berufsberechtigten im Werkvertrag, etc.), so liegt ein Sub-

Auftragsverarbeitungsverhältnis mit allen Folgen vor, sollte der beauftragte Steuerberater den Weisungen des beauftragenden Steuerberaters unterliegen, ansonsten ist der im Werkvertrag beschäftigte Berufsberechtigte ebenfalls Verantwortlicher.

Typische EDV-Dienstleister, die etwa das Hosting der IT-Infrastruktur des Unternehmens übernehmen oder Programmierdienstleistungen bereitstellen und/oder die Wartung von Systemen übernehmen und dabei Zugang zu personenbezogenen Daten erhalten, sind in der Regel als Auftragsverarbeiter zu qualifizieren. Ausgeschlossen wäre dies hingegen dann, wenn durch technische Sicherheitsmaßnahmen ein Zugang oder Zugriff seitens des Dienstleisters auf personenbezogene Daten ausgeschlossen werden kann (zB durch sichere Verschlüsselung).

Beispiele:

Agiert eine Steuerberatungskanzlei als Verantwortlicher, so steht es ihr grundsätzlich frei, auch weitere Dienstleister zu beschäftigen. Diese sind in den Informationspflichten gegenüber natürlichen Personen anzuführen. Gegenüber juristischen Personen sind die Informationspflichten nicht anwendbar.

Agiert eine Steuerberatungskanzlei als Auftragsverarbeiter, so dürfen weitere Dienstleister nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen in Anspruch genommen werden.

14.5 Checkliste

Prüffragen	Ja / Nein
Wurden im Unternehmen alle Tätigkeiten auf ihren Charakter als „Verantwortlichentätigkeit“ oder „Auftragsverarbeitung“ hin überprüft?	
Wurden mit allen eingesetzten Auftragsverarbeitern entsprechende datenschutzrechtliche Verträge abgeschlossen?	
Ist im Unternehmen eine Vertragsvorlage verfügbar?	
Beinhaltet die Auftragsverarbeitervertragsvorlage alle relevanten Inhalte der DSGVO?	
Wurde evaluiert, ob eingesetzte Auftragsverarbeiter wiederum Sub-Auftragsverarbeiter einsetzen? • Werden Sub-Auftragsverarbeiter eingesetzt, ist sichergestellt, dass diese die die selbst auferlegten Datenschutzpflichten erfüllen? • Wurde ein Vertrag mit diesen abgeschlossen? • Gibt es das Einverständnis des Verantwortlichen dazu?	

Wurden alle Dienstleister im Verzeichnis von Verarbeitungstätigkeiten erfasst?	
Ist im Unternehmen eine dokumentationssichere Vertragsdatenbank etabliert?	

15 Internationaler Datenverkehr

15.1 Allgemein

Was versteht man denn überhaupt unter einem „Datentransfer“ oder einer „Datenübermittlung“?

Im Allgemeinen herrscht hier bereits die erste Unklarheit, was unter einem „Datentransfer“ oder einer „Datenübermittlung“ verstanden wird. Die beiden Begriffe suggerieren grundsätzlich, dass man Daten aktiv zu einem konkreten Empfänger „hinschickt“. Dies ist jedoch für die Erfüllung einer Datenübermittlung nicht notwendig.

Es genügt bereits das Bestehen eines Zugriffsrechts zu einem bestimmten Dateisystem. Auch würde das „Zeigen“ von Dokumentenordnern und deren Inhalt dem Übermittlungsbegriff genügen. Im Endergebnis ist der Begriff daher nicht an einen physischen Transfer gebunden.

15.2 Datenübermittlung in ein „Drittland“?

Was tun bei Datenverkehr ins Ausland?

Innerhalb der Europäischen Union ist der Datenverkehr und Datenaustausch grundsätzlich erlaubt und darf ohne zusätzliche Mechanismen und Auflagen durchgeführt werden. Hier herrscht aus Sicht der DSGVO ein angemessenes Datenschutzniveau.

Voraussetzung dafür ist jedoch immer, dass es eine Rechtsgrundlage für die Datenverarbeitung gibt, die Datenschutzgrundätze eingehalten werden und die Bedingungen der restlichen DSGVO beachtet werden.

Werden Daten jedoch in ein sog. Drittland übermittelt, ist dies nur möglich, wenn ein angemessenes Datenschutzniveau besteht oder dieses mittels verschiedenster Angemessenheitsmechanismen hergestellt wird. Dabei können insbesondere dem Verantwortlichen einige Aufgaben zukommen.

Was ist nun ein „Drittland“?

Drittland – was fällt darunter?

Nach der DSGVO Bestimmungen sind alle Nicht-EU Länder als Drittländer zu qualifizieren.

15.3 Anwendungsbeispiele

Beispiele:

- Eine Konzerngesellschaft in Österreich übermittelt Gehaltsdaten an die Muttergesellschaft in China.
  = Datenübermittlung in ein Drittland!
- Die österreichische Personalabteilung betreibt ihre Anwendungen auf einem Server in Indien.
  = Datenübermittlung in ein Drittland!
- Der weltweite Vertriebschef in Brasilien kann auf das österreichische Verrechnungssystem zugreifen.
  = Datenübermittlung in ein Drittland!
- Die Mitarbeiter des Unternehmens verwenden eine Cloud Lösung, deren Serverstandort in den USA ist.
  = Datenübermittlung in ein Drittland!
- Die österreichische Marketingabteilung lässt ihre Newsletter über einen Anbieter in Südafrika versenden.
  = Datenübermittlung in ein Drittland!

15.4 Konsequenzen bei Datenübermittlungen in Drittländer

Werden personenbezogene Daten an ein Drittland übermittelt, hat der Verantwortliche bzw. Auftragsverarbeiter sicherzustellen, dass bei seinem Gegenüber (zB Dienstleister) ein angemessenes Datenschutzniveau vorherrscht. Dies kann in etwa durch ein bereits festgestelltes angemessenes Datenschutzniveau seitens der EU-Kommission gegeben sein, aber auch durch vertragliche Vereinbarungen, konzerninterne Richtlinien oder nationale, anerkannte Zertifizierungsverfahren sichergestellt werden.

Achtung!
Ist kein angemessenes Datenschutzniveau sichergestellt, ist eine Datenübermittlung verboten!

Die Angemessenheit des Datenschutzniveaus kann sich auf unterschiedlichste Art und Weise ergeben oder sicherstellen lassen.

– Angemessenheitsbeschluss der EU-Kommission

Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

Die EWR Länder Liechtenstein, Norwegen und Island[12] werden grundsätzlich den Ländern der Europäischen Union gleichgestellt. Ob diese offiziell mit den EU Staaten gleichzusetzen sind oder unter die Rubrik „angemessenes Niveau" fallen, ist zum jetzigen Zeitpunkt unklar, jedoch für das Endergebnis nicht erheblich.

Länder mit angemessenem Datenschutz-Niveau

Folgenden Ländern wurde seitens der EU-Kommission ein angemessenes Datenschutzniveau attestiert[13]:

- Andorra
- Argentinien
- Färöer
- Guernsey
- Insel Man
- Israel
- Jersey
- Kanada
- Neuseeland
- Schweiz
- Uruguay

– Privacy Shield Framework

EU < > USA

Für die USA gibt es einen speziellen Mechanismus zur Herstellung eines angemessenen Datenschutzniveaus. Dies ist das Privacy Shield (PS) Framework zwischen der Europäischen Union und den USA.

Privacy Shield stellt insbesondere nicht die gesamte USA datenschutzrechtlich gleich, sondern ermöglicht vielmehr U.S.-amerikanischen Unternehmen, sich datenschutzrechtlichen Regelungen zu unterwerfen und dadurch freiwillig zu zertifizieren.

Öffentliche Liste der zertifizierten Unternehmen

Die Zertifizierung nach Privacy Shield ist für jedermann öffentlich abruf- und einsehbar unter: https://www.privacyshield.gov/list

[12] Vgl. http://www.europarl.europa.eu/atyourservice/de/displayFtu.html?ftuId=FTU_5.5.3.html
[13] Vgl. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Insgesamt herrscht derzeit bei Unternehmen, welche sich auf das Privacy Shield Framework stützen, erhebliche Rechtsunsicherheit über das Fortbestehen dieser Vereinbarung und die Möglichkeit der Herstellung eines angemessenen Datenschutzes mittels dieses Angemessenheitsmechanismus.

Unternehmen ist daher in der derzeitigen Phase dazu zu raten, sich zusätzlich auf andere Mechanismen zu stützen, wie etwa Standardvertragsklauseln.

Vorteil der Verwendung: Wenig bis kein Aufwand seitens des Verantwortlichen

Nachteil der Verwendung: Rechtsunsicherheit

– Binding Corporate Rules (BCR)

Verbindliche Unternehmens-Richtlinien

Für (Konzern-)Unternehmen bietet sich im Speziellen die Möglichkeit, sog. verbindliche, unternehmensinterne Richtlinien (im Englischen „Binding Corporate Rules“) zu verwenden.

Diese internen Richtlinien müssen dabei insbesondere für alle Mitglieder der Unternehmensgruppe rechtlich bindend sein und betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten bieten.

Das Erstellen, aber auch das Genehmigungsverfahren bei der Aufsichtsbehörde entsprechender unternehmensinterner Richtlinien gehört sicherlich zu den aufwendigeren Szenarien einer Unternehmensgruppe.

Der große Vorteil einer solchen „Einmal-Genehmigung“ liegt insbesondere darin, dass alle Datenübermittlungen, welche von den unternehmensinternen Richtlinien umfasst sind, ohne weiteres Verfahren stattfinden dürfen.

Vorteil der Verwendung: Einheitlich angemessenes Datenschutzniveau im gesamten Konzernunternehmen

Nachteil der Verwendung: Hoher Aufwand der Implementierung seitens des Verantwortlichen

– Standardvertragsklauseln (Standarddatenschutzklauseln)

Vertragsvorlagen der EU

Eine weitere Möglichkeit der Herstellung eines angemessenen Datenschutzniveaus stellen sog. Standardvertragsklauseln (im Englischen: EU

Model Clauses) dar[14], welche seitens der EU-Kommission als Standardvertragswerke zur Verfügung gestellt werden.

Entscheidend bei der Verwendung der Standardvertragsklauseln ist, dass die Klauseln selbst nicht abgeändert werden dürfen. Sie sind unverändert zu übernehmen und als Ergänzung zu dem eigentlichen Vertrag über Auftragsverarbeitung hinzuzufügen.

Aufbau

Der Standardvertrag für das Verhältnis „Verantwortlicher <=> Auftragsverarbeiter" („Controller to Processor") besteht stets aus drei Teilen:

- Den eigentlichen Standardvertragsklauseln
- Anhang 1 mit Angaben zur konkreten Datenverarbeitung
- Anhang 2 mit einer Beschreibung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters

Die Unterschrift der beiden beteiligten Verantwortlichen genügt dabei für den Abschluss des Vertragswerks.

Vorteil der Verwendung: Schnelle Abwicklung zwischen den Vertragspartnern

Nachteil der Verwendung: Muss mit jedem einzelnen Vertragspartner separat abgeschlossen werden

15.5 Anwendbarkeit für Steuerberater

Praktische Umsetzung für Steuerberater

Für Steuerberatungsunternehmen werden sich aus dem Alltag heraus und dem typischen Unternehmensaufbau wohl nur die Anwendungsfälle der Standardvertragsklauseln oder des Privacy Shield ergeben.

Eine weitere Möglichkeit stellt allerdings unabhängig von den Angemessenheitsverfahren die Einwilligung einer betroffenen Person dar, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde.

Achtung!
Die Einwilligung muss immer von der betroffenen Person selbst stammen und kann nicht etwa durch eine Einwilligung des Klienten ersetzt werden.

[14] Vgl. http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

15.6 Checkliste

Prüffragen	Ja / Nein
Wurden alle Datenübermittlungen, Speicherorte und Transfers von Daten in Hinblick auf involvierte Drittländer überprüft?	
Wurde sichergestellt, dass für alle Datenübermittlungen in Drittländer ein angemessenes Datenschutzniveau sichergestellt ist?	
Ist der Nachweis eines angemessenen Datenschutzniveaus für alle einzelnen Datenübermittlungen möglich?	
Wissen alle Mitarbeiter im Unternehmen Bescheid, wie im Fall einer Datenübermittlung in Drittländer vorzugehen ist?	
Sind im Unternehmen Vertragsvorlagen iZm Standardvertragsklauseln verfügbar?	
Wurde evaluiert, ob unternehmensinterne verbindliche Richtlinien genutzt werden sollen?	
Wurde für den Bereich als Auftragsverarbeiter mit Speicherung in einem Drittstaat die Einwilligung des Kunden eingeholt?	

16 Datenschutzfolgenabschätzung (DFA)

Risikobeurteilung

16.1 Allgemein

Die „Datenschutzfolgenabschätzung“ (Privacy Impact Assessment) ist ein neues Konzept der DSGVO, welches als Verfahren im Sinne der Rechenschaftspflicht konstruiert wurde.

Ziel der Datenschutzfolgenabschätzung ist es, die Risiken, die durch die Verarbeitung von personenbezogenen Daten gegenüber der betroffenen Person entstehen, zu evaluieren, zu bewerten und entsprechende Abhilfemaßnahmen zu ergreifen.

Erstschritt

16.2 Erstbeurteilung

Ob die Durchführung einer solchen Abschätzung erforderlich ist oder nicht, hat der Verantwortliche selbst zu erheben und zu bewerten. Dieser erste Schritt der Beurteilung ist entsprechend zu dokumentieren.

Der Dokumentationsnachweis dieses ersten Prüfschritts kann insbesondere im Verzeichnis von Verarbeitungstätigkeiten erfolgen.

Hat eine Form der Verarbeitung, insbesondere

- bei Verwendung neuer Technologien,
- aufgrund der Art,
- des Umfangs,
- der Umstände und
- der Zwecke der Verarbeitung

voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Definitive Anwendungsfälle

Eine Datenschutzfolgenabschätzung ist, jedoch nicht abschließend, insbesondere in folgenden Fällen erforderlich:

(1) Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen

(2) Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

(3) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen (zB Videoüberwachung)

(4) Umfangreiche Verarbeitungsvorgänge, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und, aufgrund ihrer Sensibilität, wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird.

An dieser Stelle sei insbesondere auf die vorhergehenden Ausführungen zum Begriff „umfangreich“ verwiesen, wenn die Verarbeitung personenbezogener Daten von Patienten, Mandanten und Klienten durch einen einzelnen Arzt, Rechtsanwalt, Steuerberater oder anderen freien Beruf erfolgt. In diesen Fällen sollte eine Datenschutzfolgenabschätzung nicht zwingend vorgeschrieben sein.

(5) Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren.

Zusätzlich kann die Aufsichtsbehörde Listen jener Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die eine, oder eben auch keine, Datenschutzfolgenabschätzung erforderlich ist!

16.3 Inhalt einer Datenschutzfolgenabschätzung

Die Datenschutzfolgenabschätzung enthält zumindest Folgendes:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen

Stellt der Verantwortliche fest, dass das Risiko nicht eingedämmt werden kann, so ist die Aufsichtsbehörde zu konsultieren.

16.4 Auswirkungen auf Steuerberater

Aufgrund der hohen Komplexität einer durchzuführenden Datenschutzfolgenabschätzung und der Verschränkung mit anderen Themenfeldern wie Risikomanagement oder IT-Sicherheit, kann diese oftmals nicht von jedem Verantwortlichen, insbesondere von kleinen und mittelständischen Unternehmen, ohne Unterstützung durch Datenschutzexperten vollständig erfasst und dokumentationssicher durchgeführt werden.

Inwiefern Steuerberater von dem Erfordernis einer Datenschutzfolgenabschätzung für ihre Datenverarbeitungen betroffen sind,

sollte nach den konkret durchgeführten Tätigkeiten, unter Berücksichtigung der erwarteten Aussagen der KSW, beurteilt werden.

Das Tätigkeitsfeld von Steuerberatern reicht von der Beratung über die Personalverrechnung, Buchhaltung und Bilanzierung bis hin zu gutachterlichen und prüfenden Tätigkeiten. Aus den o.a. Konstellationen erscheint die Erwähnung von Verarbeitungsvorgängen, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, relevant, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren.
Dies ist etwa bei einer hohen Komplexität und dadurch für die betroffenen Personen resultierenden Intransparenz der Datenverarbeitung, einer Vielzahl von beteiligten Verantwortlichen oder geheimen und anlasslosen Datenverarbeitungen der Fall. Ersteres wäre unter Umständen und der Kombination aus den verschiedenen Tätigkeiten durchaus denkbar.

Dokumentation notwendig

Als mögliche Risiken einer unrechtmäßigen Datenverarbeitung kommt dabei zB Identitätsdiebstahl (bei Abhandenkommen von Ausweisdokumenten, Unterschriften oder Fotos) in Betracht, aber auch Informationslecks, welche brisante Daten von Klienten oder deren Mitarbeitern, Kunden und Lieferanten beinhalten können.
Auch an den Missbrauch von Zahlungsinformationen oder eine Informationsspionage ist dabei zu denken.

Gerade für Steuerberater gilt es daher die durchgeführten Datenverarbeitungen genauestens zu analysieren und auf etwaige Risiken für betroffene Personen hin zu bewerten. Dabei sollte ein ebenso großes Augenmerk auf die implementierten, technischen und organisatorischen Maßnahmen im Unternehmen gelegt werden.

Checkliste

Achtung!
Dokumentieren Sie daher Ihre Überlegungen im Zuge der Datenschutz-folgenabschätzungen nachweislich – auch wenn Sie zur Überzeugung gelangen keine Datenschutzfolgenabschätzung durchführen zu müssen!

16.5 Checkliste

Prüffragen	Ja / Nein
Wurde für alle Datenverarbeitungen evaluiert, ob eine Datenschutzfolgenabschätzung durchzuführen ist?	
Kann der Nachweis der Erstbeurteilung, etwa im Verzeichnis von Verarbeitungstätigkeiten, erbracht werden?	
Ist sichergestellt, dass etwaige Black & White Lists der Aufsichtsbehörde regelmäßig überprüft werden?	
Ist ein standardisierter Ablauf einer Datenschutzfolgenabschätzung sichergestellt?	
Beinhaltet der Prozess zur Datenschutzfolgenabschätzung Vorgaben zur Risikobeurteilung?	
Beinhaltet der Prozess zur Datenschutzfolgenabschätzung kategorisierte Risiken und Eintrittswahrscheinlichkeiten?	
Ist die zentrale Dokumentation der durchgeführten Datenschutzfolgenabschätzungen möglich?	
Gibt es einen Revalidierungsprozess im Unternehmen?	
Ist sichergestellt, dass ein Datenschutzbeauftragter zu Rate gezogen wird?	
Ist sichergestellt, dass die betroffenen Personen oder deren Vertreter bei Bedarf befragt werden?	
Wissen alle Mitarbeiter über das Konzept der Datenschutzfolgenabschätzung Bescheid?	

17 Behörden, europäische Stellen & Rechtsbehelfe von Betroffenen

Was können Betroffene unternehmen?

17.1 Rechtsbehelfe von Betroffenen

Wie kommen nun betroffene Personen zu ihrem Recht?

Die DSGVO bietet verschiedenste Rechtsbehelfe für betroffene Personen, welche sich gegen einen Verantwortlichen oder Auftragsverarbeiter richten können und auch gegen Aufsichtsbehörden, etwa bei Untätigkeit der jeweiligen Behörde.

Dazu zählen insbesondere:

- Das Recht auf Beschwerde bei einer Aufsichtsbehörde
- Das Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde
- Das Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche und Auftragsverarbeiter

Beschwerde auch direkt an Dienstleister

Ist eine betroffene Person der Ansicht, dass ein Verantwortlicher oder Auftragsverarbeiter gegen Regelungen der DSGVO verstößt, so kann er bei einer Aufsichtsbehörde Beschwerde einlegen.

Achtung!
Eine betroffene Person kann sich daher auch über den Auftragsverarbeiter direkt beschweren.

Datenschutz NGO

Betroffene Personen können auch entsprechende Klagen bei den Zivilgerichten einbringen, welche auf Schadenersatz, Feststellung oder Unterlassung gerichtet sein können.

Rechtsbehelfe kann die betroffene Person grundsätzlich selbst erheben. Weiters können aber ebenso Einrichtungen, Organisationen oder Vereinigungen mit der Durchsetzung ihres Anspruchs beauftragen. So können beispielsweise auch Datenschutz NGOs[15] oder Verbraucherverbände die Rechte der betroffenen Person durchsetzen.

Ende 2017 wurde bereits die erste Datenschutz NGO in Österreich gegründet!

Aufsichtsbehörde

17.2 Nationale Aufsichtsbehörden

Die in Österreich etablierte Aufsichtsbehörde ist die „Datenschutzbehörde“[16], vormals Datenschutzkommission, und ist für die Einhaltung des Datenschutzes in Österreich zuständig. Im Gegensatz zu Deutschland gibt es in Österreich nur eine bundesweit zuständige Behörde und nicht mehrere Behörden in unterschiedlichen Bundesländern.

Die für in Österreich ansässige Steuerberater zuständige Aufsichtsbehörde ist daher die österreichische Datenschutzbehörde. Diese ist „federführend“. Wird

[15] Vgl. https://noyb.eu/?lang=de
[16] Vgl. https://www.dsb.gv.at/

bei einer anderen europäischen Behörde eine Beschwerde eingebracht worden, so ist diese zwar auch zuständig jedoch ist die nationale Behörde als federführende Behörde einzubinden.

Die Befugnisse der Aufsichtsbehörde reichen von Weisungen und Hinweise über Verwarnungen, Auflagen oder Verbote bis hin zur Verhängung von Geldbußen.

17.3 Europäischer Datenschutzausschuss

Art. 29 Datenschutz-gruppe = Europäischer Datenschutz-ausschuss

Eine altbekannte Gruppe mit neuem Namen.

Bis dato kannte man diese unter dem Namen „Artikel 29 Datenschutzgruppe". Nunmehr lautet der Name für diese Vereinigung „Europäischer Datenschutzausschuss" (EDA), welcher über den nationalen Aufsichtsbehörden steht.

Dieser Ausschuss setzt sich aus jeweils einem Vertreter der nationalen Datenschutzaufsichtsbehörden sowie einem Vertreter des Europäischen Datenschutzbeauftragten zusammen.

Zu den Aufgaben des Ausschusses zählt die Harmonisierung der Anwendung der DSGVO in den einzelnen Mitgliedstaaten. Es ist daher damit zu rechnen, dass sich die Behörden in ihren bereitgestellten Richtlinien, Auslegungen und Meinungen abstimmen und vereinheitlicht auftreten werden.

Der Europäische Datenschutzausschuss berät auch die EU Kommission, stellt Meinungen, Empfehlungen und auch Richtlinien und bewährte Verfahren bereit und fördert die Zusammenarbeit zwischen den einzelnen Behörden.

Einige der bis dato ergangenen Richt- und Leitlinien sind in diesem Zusammenhang zu den Themen „Datenschutzbeauftragte", „Datenschutzfolgenabschätzung" oder „Profiling" erfolgt.

17.4 Exkurs – Meldepflichten

Meldepflicht bei Datenschutz-verletzungen

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt

die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. Der Verantwortliche hat alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und den ergriffenen Abhilfemaßnahmen zu dokumentieren. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der DSGVO ermöglichen.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Beispiel:

Wird die Geburtstagsliste der Mitarbeiter versehentlich veröffentlicht, wird in aller Regel kein (hohes) Risiko für die betroffene Person ableitbar sein.

Werden hingegen heikle Informationen, wie jene eines Steuerakts, an unberechtigte Personen gesendet oder betroffene Server gehackt, so ist wohl zumindest von einem Risiko für die Rechte und Freiheiten der betroffenen Person auszugehen.

DSGVO-Text in 24 Sprachen

18 Übersicht DSGVO Artikel inkl. Erwägungsgründe

Nachfolgend finden Sie einen Link zum Verordnungstext der DSGVO in den 24 Sprachfassungen der Europäischen Union:

http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&qid=1512933519199&from=EN

Erwägungsgründe zugeordnet

Neben dem offiziellen Verordnungstext haben Sie auch Einblick in die einleitenden Erwägungsgründe (ErwGr) für die DSGVO.

Erwägungsgründe sind die ausführlicheren, jeweiligen Formulierungen zu den Zielen, welche mit einem bestimmten Artikel verfolgt wurden. Erwägungsgründe sind keine Rechtsnormen, allerdings sind diese äußerst

hilfreich für die Auslegung der Rechtsnormen.

Thema	Artikel	ErwGr
Allgemeine Bedingungen für die Verhängung von Geldbußen	83	148,150,151
Aufgaben Aufsichtsbehörde	57	123, 132
Aufgaben Datenschutzbeauftragter	39	-
Aufsichtsbehörde	51	117 – 119
Auftragsverarbeiter	28	81
Automatisierte Einzelentscheidungen einschließlich Profiling	22	71,72
Auskunftsrecht	15	63, 64
Befugnisse der Aufsichtsbehörde	58	129
Begriffsbestimmungen	4	26-37
Benachrichtigung von betroffenen Personen bei Datenschutzverletzungen	34	85-88
Benennung eines Datenschutzbeauftragten	37	97
Beschränkungen	23	-
Beschwerderecht	77	141
Besondere Kategorien von Daten	9	51-56
Datenschutzfolgenabschätzung	35	84,89-93
Datenübermittlung in Drittländer	44,45,46	6,101,107,108, 110-113,115
Datenübertragbarkeitsrecht	20	68
Einschränkungsrecht	18	67,85,156
Einwilligungen	7, 8	
Gemeinsam für die Verarbeitung Verantwortliche	26	-
Grundsätze für die Verarbeitung von personenbezogenen Daten	5	39
Haftung und Schadenersatz	82	146,147
Informationspflichten bei Direkterhebung	13	60-62
Informationspflichten bei indirekter Erhebung	14	60-62
Löschungsrecht	17	65,66
Meldepflichten bei Datenschutzverletzungen	33	85-88
Mitteilungspflicht	19	-
Privacy by Design & by Default	25	78
Räumlicher Anwendungsbereich	3	22-25
Rechtsbehelf gegen Aufsichtsbehörden	78	143
Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	79	145
Rechtsgrundlagen der Verarbeitung	6	40,41,44-50
Richtigstellungsrecht	16	65,66
Sachlicher Anwendungsbereich	2	-
Sanktionen	84	149,152

Sicherheit der Verarbeitung	32	83
Stellung des Datenschutzbeauftragten	38	97
Strafrechtliche Verurteilungen und Straftaten	10	75,80,91,97,149, 152
Transparenz, Kommunikation und Modalitäten für die Betroffenenrechte	12	58,59
Verantwortung des Verantwortlichen	24	74-77
Verbindliche interne Rechtsvorschriften	47	
Vertretung von betroffenen Personen	80	142
Verzeichnis von Verarbeitungstätigkeiten	30	82
Widerspruchsrecht	21	69,70
Zertifizierung	42	77,81,100,166, 168

Über den Autor

EU-Datenschutzgrundverordnung

„Chance oder Stolperstein? – Auf die Umsetzung kommt es an!"

Der aus der Juristerei stammende und technikaffine Autor Nicolas Nagel ist bereits seit vielen Jahren als Berater von Unternehmen in Datenschutzangelegenheiten tätig und als eine feste Größe in der Datenschutzszene Österreichs verankert.

Er versteift sich dabei nicht auf theoretische oder akademische Diskussionen, sondern legt seinen Fokus auf die praktische Umsetzung und praktikable Lösungen sowie der Anwendbarkeit der jeweiligen Vorgaben aus dem Datenschutzrecht.

Nicolas Nagel war jahrelang selbst in der Rolle als Konzern-Datenschutzbeauftragter eines international agierenden Unternehmens tätig, leitete zahlreiche Implementierungsprojekte und weiß daher nur zu gut, worauf es in der tatsächlichen Umsetzung im Unternehmen ankommt.

Datenschutz soll am Ende des Tages nicht zur Blockade des unternehmerischen Tuns führen, sondern einen Mehrwert für das Unternehmen, seine Mitarbeiter und deren Kunden bieten.

Nicolas Nagel ist zudem zertifizierter Datenschutzbeauftragter und als Lektor an der Donauuniversität Krems sowie der Akademie für Recht, Steuern und Wirtschaft sowie als Vortragender auf verschiedenen nationalen wie internationalen Fachtagungen und Konferenzen tätig.

„Mir persönlich ist es insbesondere ein Anliegen, dass Datenschutz nicht als bloßes Hemmnis und bürokratische Hürde verstanden wird, sondern als Chance und positive Grundrechtsentwicklung für uns alle betrachtet wird!

Die Umsetzung der datenschutzrechtlichen Anforderungen sollte dabei jedoch so praktikabel wie möglich sein und mit Rücksicht auf den Alltag der Unternehmen erfolgen."