IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

EU DSGVO in der Praxis

Datenschutzgrundverordnung gültig ab 25.05.2018

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Peter Lohmüller

Vertrieb und

Organisationsberatung

Certified ITIL Service Level Manager

Certified Network Manager

Certified Project Manager

Tel.: +49 221 952681-190

Fax: +49 221 952681-114

peter.lohmueller@it-audit.com

Was ist eigentlich Datenschutz

… Datenschutz?

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Er beinhaltet technische und organisatorische Maßnahmen gegen den Missbrauch von Daten durch Organisationen.

Datenschutz-Grundrecht

- Recht auf informationelle Selbstbestimmung, Art. 1, Art. 2 GG („Datenschutz-Grundrecht“)
  = *Das Recht des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.*

Personenbezogene Daten

- „alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physichen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen identität dieser person sind“

Personenbezogene Daten sind bspw.

Daten aus denen sich unmittelbar der Personenbezug ergibt oder mittelbar hergestellt werden kann:

- Name
- Adresse
- Telefonnummer
- Geburtsdatum
- Bankverbindung / Kontonummern
- Sozialversicherungsnummern
- IP-Adresse / Web-Cookies

Wer haftet eigentlich?

Geschäftsführer, Vorstände und Inhaber von Unternehmen sind im Rahmen ihrer Sorgfaltspflichten angehalten, Missbrauch von den ihnen anvertrauten Daten zu verhindern.

Info zur EU Datenschutz Grundverordnung

- Die EU-DSGVO ist ein europaweit einheitliches, unmittelbar geltendes Regelwerk zum Datenschutz.
- Sie löste das deutsche Bundesdatenschutzgesetz (BDSG) am 25.05.2018 ab und gilt für alle Unternehmen und Behörden.
- Zielsetzung ist die Stärkung der Rechte von Betroffenen sowie ein europaweit einheitliches Datenschutzrecht und die Förderung des freien Datenverkehrs.
- Dort, wo die EU-DSGVO nicht greift oder es Öffnungsklauseln gibt, wird es weiterhin eine nationale Datenschutzgesetzgebung geben. Z. B. in einem neuen Bundesdatenschutzgesetz (BDSG neu) oder den Landesdatenschutzgesetzen (LDSG).

Wesentliche Änderungen 1/2

- Deutlich erweiterte Rechenschafts- und Dokumentationspflichten.
- Erhöhter Bußgeldrahmen
- Umfassende Betroffenenrechte (Auskunft, Berichtigung, Löschung)
- Recht auf Datenübertragbarkeit
- Datenschutzfolgenabschätzung
- Gesamtschuldnerische Haftung von Auftragsverarbeitern und Verantwortlichen (disponibel)

Wesentliche Änderungen 2/2

- Technikneutraler, risikobasierter Ansatz
- Besonderheiten Art. 88 DSGVO: Möglichkeit Datenschutzbestimmungen in Kollegtivvereinbarungen zu Regeln (rglm. In Betriebsbvereinbarungen)
- Erhöhte Anforderungen an den Datenschutzbeauftragten

Benennung eines fachkundigen Datenschutzbeauftragten

Unternehmen müssen einen Datenschutzbeauftragten benennen, wenn …

… sie mindestens 10 Personen beschäftigen, die automatisiert Daten verarbeiten.

… ihre Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien **personenbezogener Daten** besteht.

… sie Datenschutz-Folgenabschätzungen vornehmen.

Seine Kontaktdaten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen!

Meldung des Datenschutzbeauftragten

- 

www.ldi.nrw.de
Stand: 12.04.2018

Umsetzungserfordernisse

Grundsätzlich gilt:
Wer unter dem alten BDSG gut aufgestellt war, wird es auch nach neuem Recht sein.

Trotzdem gibt es Handlungsbedarf!

- Erfüllung der Nachweispflicht
- Überarbeitung der Dokumentationen
- Einführung neuer Prozesse
- Bewertung von Schutzmaßnahmen
- Überarbeitung von Vorlagen

- Einhaltung der Rechte Betroffener

Die Umsetzung

1. Benennung eines fachkundigen Datenschutzbeauftragten
2. Bestandsaufnahme durchführen
3. Verzeichnis der Verarbeitungstätigkeiten erstellen

Die Umsetzung

4. Festlegung des Dokumentationsumfangs zur Erfüllung der Rechenschaftspflichten

5. Rechtsgrundlagen der Verarbeitung überprüfen

6. Datenschutz-Management-System aufbauen

Die Umsetzung

7. Umsetzung der Informationspflichten

8. Auftragsverarbeitung überprüfen

9. Überprüfung der technisch-organisatorischen Maßnahmen

10. Mitarbeiter nach dem neuen Recht und seiner Umsetzung schulen

Notwendige Workflows

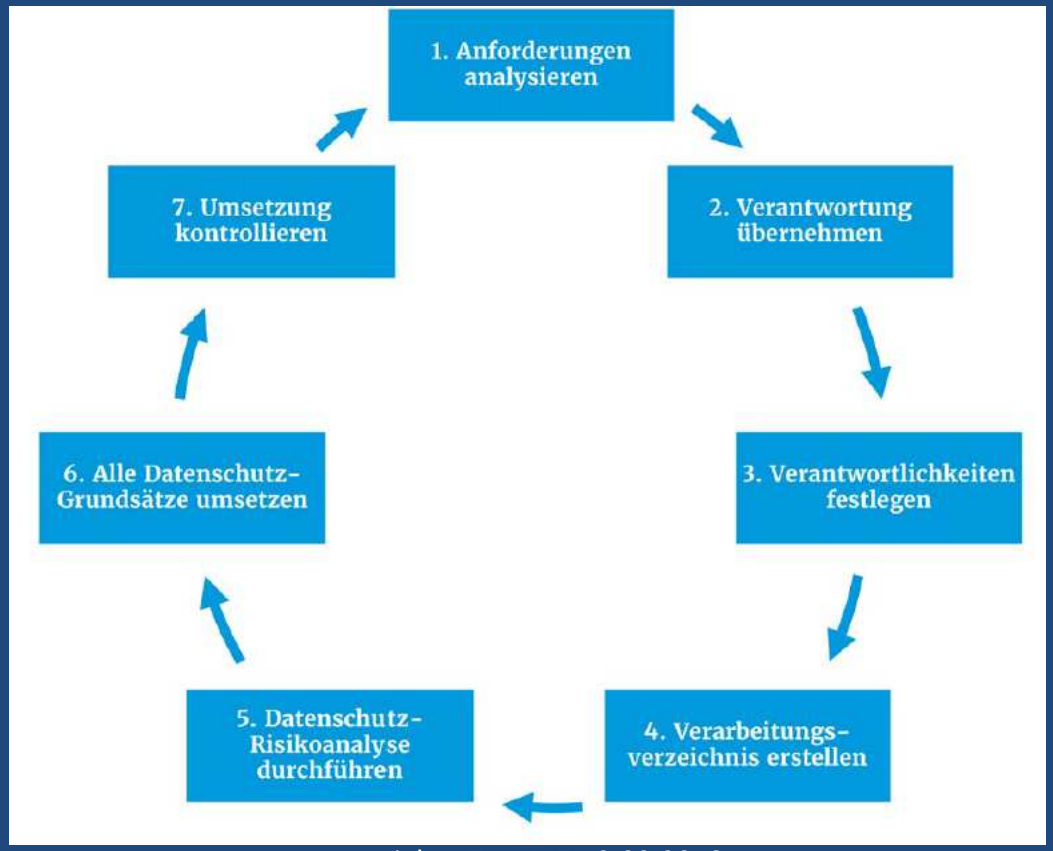
- Meldung Datenpanne an Aufsichtsbehörde (Frist 72 Std.!) (Datenpannen unbedingt vermeiden, da die Aufsichtsbehörde Meldefälle zum Anlass nehmen könnte genauer hinzuschauen)

- Beantwortung eines Auskunftsverlangens (Frist 1 Monat)

Notwendige Templates (Dokumentvorlagen)

- Beantwortung Auskunftsverlangen
- Standardberichte aus IT-Systemen
- Anschreiben Aufsichtsbehörde, Betroffene etc.
- (Rahmen-) Betriebsvereinbarungen / MA-Vereinbarungen
- Verpflichtung auf Vertraulichkeit
- Verzeichnis der Verarbeitungstätigkeiten
- AV-Vereinbarungen (Auftragsdatenverarbeitungen)
  Bsp: DATEV / KANZLEI oder Unternehmen mit Dienstleistern

Schritt für Schritt Empfehlung :



1. Anforderungen analysieren

Die Anforderungen in der Kanzlei sind die Anforderungen der Datenschutz-Grundverordnung 25.05.2018, des Datenschutz-Anpassungsgesetzes sowie der ePrivacy-Richtlinie (voraussichtlich 2019).

Es können noch weitere Anforderungen hinzukommen, wie z. B. vertragliche Anforderungen von Mandanten (z. B. dass gewisse Mitarbeiter gewisse Mandantendaten nicht einsehen dürfen, weil es Familienmitglieder sind). Dies hat dann wiederum auch Auswirkungen darauf, wie die Informationssicherheit, also das Rollen- und Rechtekonzept, ausgestalten werden muß.

2. Verantwortung übernehmen

Die Kanzlei-Leitung muss aktiv die Verantwortung für die Umsetzung übernehmen, also sagen „Jawohl, wir wollen dieses Projekt umsetzen!“ und entsprechend ein Team aus Mitarbeitern zusammenstellen.

3. Verantwortlichkeiten festlegen

Dieses Mitarbeiter-Team arbeitet gemeinsam die Anforderungen ab. D. h. man überlegt z. B., ob ein Datenschutzbeauftragter zu bestellen ist. Sollte dies der Fall sein, dann bestellt man diesen, damit er auch den Umsetzungsprozess unterstützen kann. Die anderen Mitglieder des Umsetzungsteams helfen z. B. beim Erstellen des Verfahrensverzeichnisses oder bei den Auftragsverarbeitungsverträgen.

4. Verarbeitungsverzeichnis erstellen

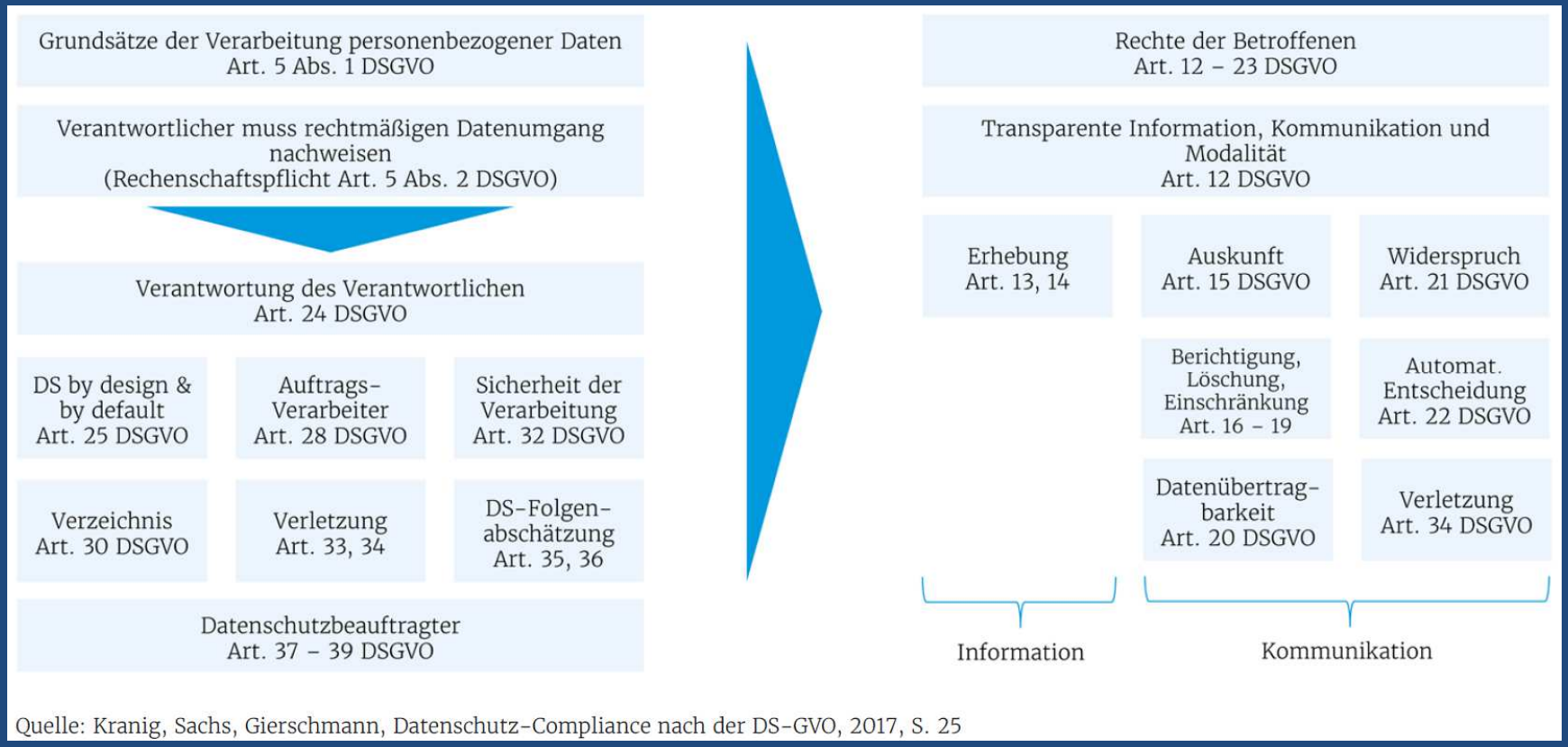
- Der erste Schritt des wirklichen „Doings“ ist dann das Erstellen des Verarbeitungsverzeichnisses.
- Dieses Verarbeitungsverzeichnis stellt nicht irgendein Katalog dar, der einfach statisch ins Regal gestellt wird, sondern damit muss zukünftig gearbeitet werden.

4.1 Was ist eine Verarbeitungstätigkeit?

Strategie-Prozesse	Bearbeitungs-Prozesse allgemein	Leistungs-Prozesse Steuerberatung	Leistungs-Prozesse betriebsw. Beratung sonst.	Leistungs-Prozesse sonst.V.Tätig	Unterstützungs-Prozesse	Überwachungs-Prozesse
Kanzleiziele festlegen	Sachverhalt sorgfältig ermitteln	Lohnbuch-haltung	Unternehmens-nachfolge	Testamentsvoll-streckung, Nachlass-pflegschaft	Aufbau- und Ablauforgani-sation festlegen	Kontrollen
Dienstleistungs-politik festlegen	Mandats-/ Auftrags-annahme	Finanzbuch-haltung	Vorweg-genommene Erbfolge	Krisenberatung	Personal-management organisieren	Nachschau (interne Audits)
Mandatspolitik festlegen	Auftrag planen und steuern	Jahresabschluss	Mergers and Acquisitions	Finanzierungs-beratung	Sachmittelaus-stattung bereitstellen	Zertifizierung/ Konformitäts-erklärung

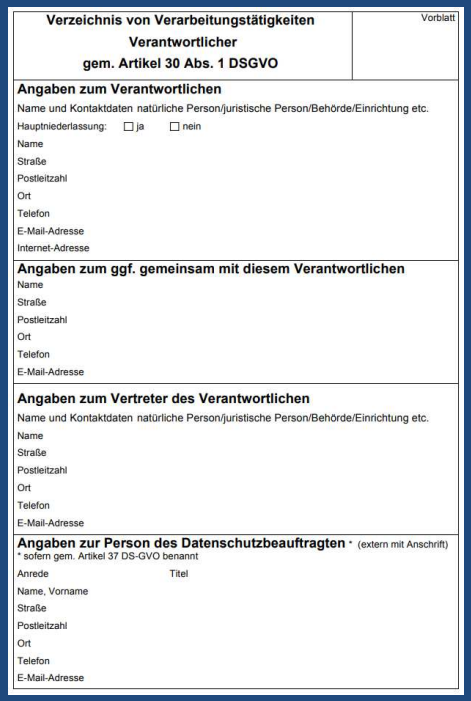
Quelle: BStBK, DStV, DATEV: Handbuch Qualitätssicherung und Qualitätsmanagement in der Steuerberatung

4.2 Zulässigkeit einer Verarbeitungstätigkeit?



Quelle: Kranig, Sachs, Gierschmann, Datenschutz-Compliance nach der DS-GVO, 2017, S. 25

Formular *„Verantwortlicher“*
„Verzeichnis von Verarbeitungstätigkeiten“



Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Hauptniederlassung: ☐ ja ☐ nein

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

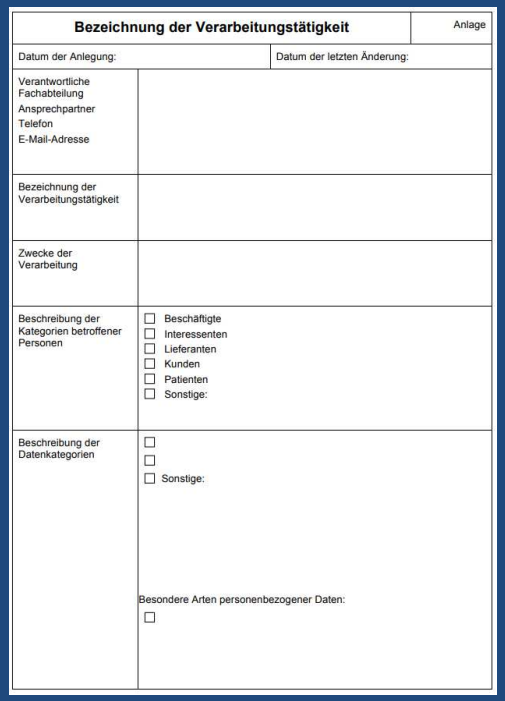
Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)
* sofern gem. Artikel 37 DS-GVO benannt

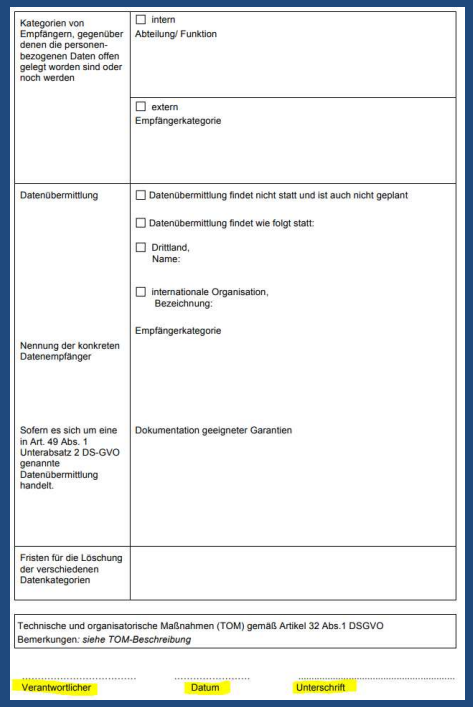
Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse



Bezeichnung der Verarbeitungstätigkeit

Anlage

Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ ☐ ☐ Sonstige: Besondere Arten personenbezogener Daten: ☐

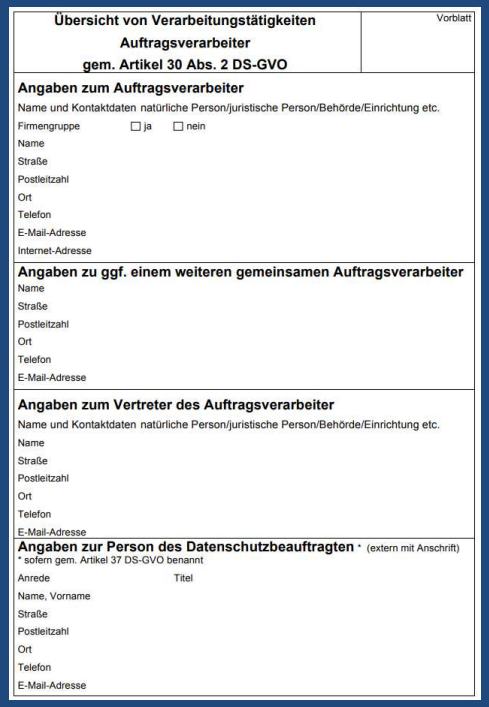


Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	☐ intern Abteilung/ Funktion ☐ extern Empfängerkategorie
Datenübermittlung Nennung der konkreten Datenempfänger	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland, Name: ☐ internationale Organisation, Bezeichnung: Empfängerkategorie
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO
Bemerkungen: *siehe TOM-Beschreibung*

Verantwortlicher Datum Unterschrift

Formular *„Auftragsverarbeiter“*
Übersicht von Verarbeitungstätigkeiten



Übersicht von Verarbeitungstätigkeiten
Auftragsverarbeiter
gem. Artikel 30 Abs. 2 DS-GVO

Vorblatt

Angaben zum Auftragsverarbeiter

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Firmengruppe ☐ ja ☐ nein
Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zu ggf. einem weiteren gemeinsamen Auftragsverarbeiter

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

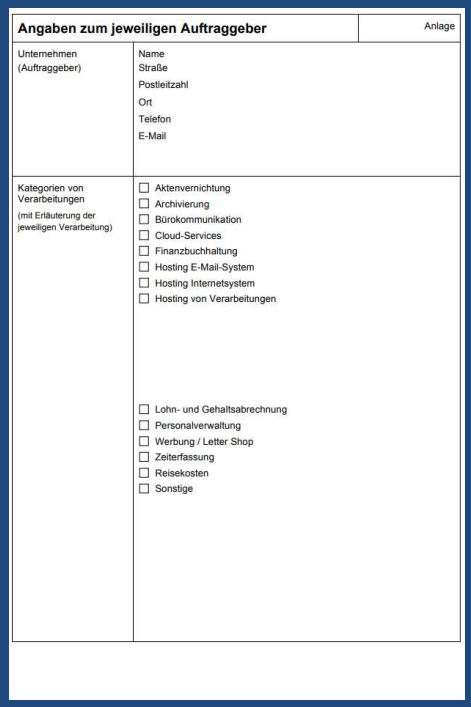
Angaben zum Vertreter des Auftragsverarbeiter

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)
* sofern gem. Artikel 37 DS-GVO benannt

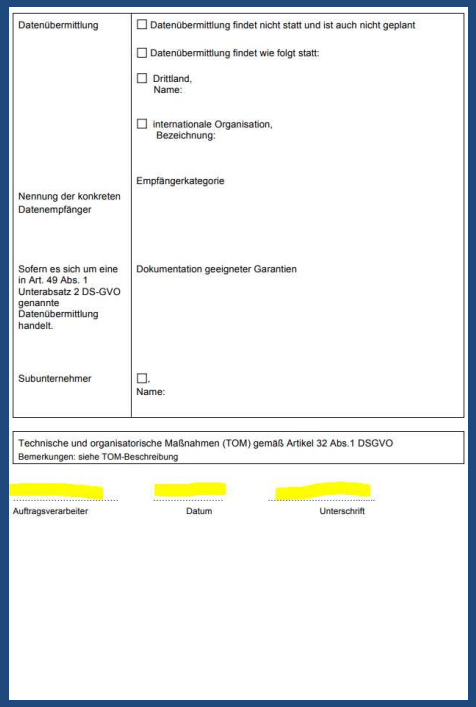
Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse



Angaben zum jeweiligen Auftraggeber

Anlage

Unternehmen (Auftraggeber)	Name Straße Postleitzahl Ort Telefon E-Mail
Kategorien von Verarbeitungen (mit Erläuterung der jeweiligen Verarbeitung)	☐ Aktenvernichtung ☐ Archivierung ☐ Bürokommunikation ☐ Cloud-Services ☐ Finanzbuchhaltung ☐ Hosting E-Mail-System ☐ Hosting Internetsystem ☐ Hosting von Verarbeitungen ☐ Lohn- und Gehaltsabrechnung ☐ Personalverwaltung ☐ Werbung / Letter Shop ☐ Zeiterfassung ☐ Reisekosten ☐ Sonstige



Datenübermittlung	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland, Name: ☐ internationale Organisation, Bezeichnung:
Nennung der konkreten Datenempfänger	Empfängerkategorie
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Subunternehmer	☐. Name:

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO
Bemerkungen: siehe TOM-Beschreibung

Auftragsverarbeiter Datum Unterschrift

5. Datenschutz-Risikoanalyse durchführen

- Alle Analysen, die gesetzlich gefordert sind, müssen in diesem Schritt umgesetzt werden.

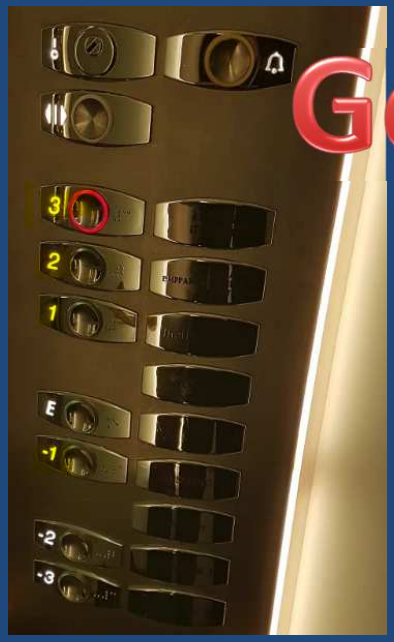
6. Alle Datenschutzgrundsätze umsetzen

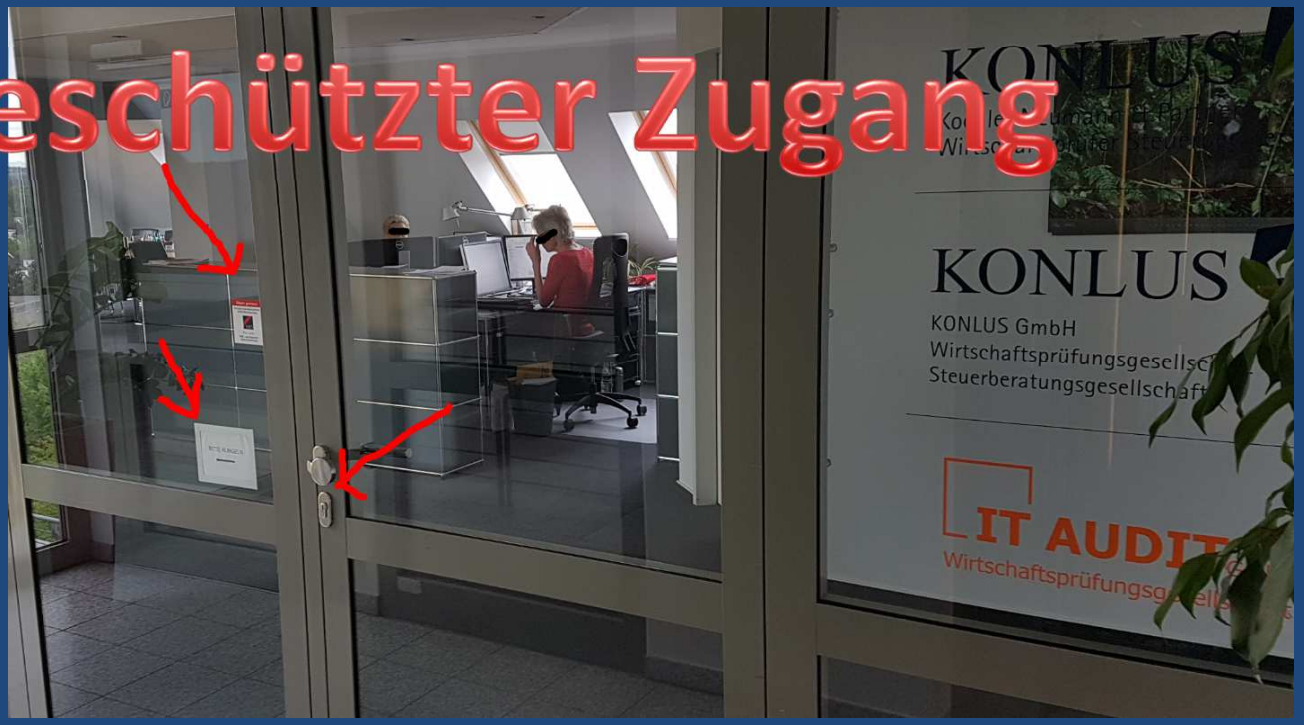
Diese Datenschutzgrundsätze sind die absolute Grundlage der Datenschutz-Grundverordnung und müssen deshalb strikt eingehalten werden. Die Art. 5 – 50 DSGVO lassen sich unter diese Datenschutzgrundsätze subsumieren. Dazu gehören z. B. Rechtmäßigkeit, Datenminimierung, Speicherbegrenzung, Zweckbindung. D. h. diese Artikel sind in der Praxis anzuwenden. Danach kommen in der DSGVO Regelungen zum Kohärenzverfahren (Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung), zur Aufsichtsbehörde usw., was in der praktischen Umsetzung nicht wichtig ist.

7. Umsetzung der * *TOM* kontrollieren

Abschließend muss kontrolliert werden, ob diese Datenschutzgrundsätze richtig umgesetzt worden sind. Diese Audits sind gesetzlich vorgeschrieben (im Bereich der * *technisch-organisatorischen Maßnahmen* Art. 32 DSGVO). Ansonsten benötigen man diese internen Audits, um einer Aufsichtsbehörde nachweisen zu können, dass man gemäß der Datenschutz-Grundverordnung gearbeitet hat. Daher haben die Audit-Dokumente eine sehr hohe Relevanz in der Praxis.

7.1.1 *TOM* / Zugang zur Kanzlei





7.1.2 *TOM* / Zugang zur Kanzlei

7.1.2 *TOM* / Besucheranmeldung Kanzlei

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Anmeldung: Wer für wen

Ggf. Datenschutzformular

7.1.3 *TOM / Kanzleibesucher:*

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

· Zugangsregelungen innerhalb unserer Kanzlei:

- Kein Zutritt zu unseren Arbeitsräumen!
  (Vermeidung von Unterlageneinsicht)
- Besucher werden in Besprechungsräumen empfangen!
- Betriebsprüfer und andere externe Personen werden generell aufgefordert unsere Verschwiegenheitserklärung zu unterschreiben.

7.1.4 *TOM* / Kanzlei-Besucher

7.1.5 *TOM* / Kanzlei-Technik Besprechung

Kein Kanzlei-Netzwerk

7.1.6 *TOM* / Kanzlei-Unterlagen Besprechung

.

7.1.7 *TOM* / Büroräume

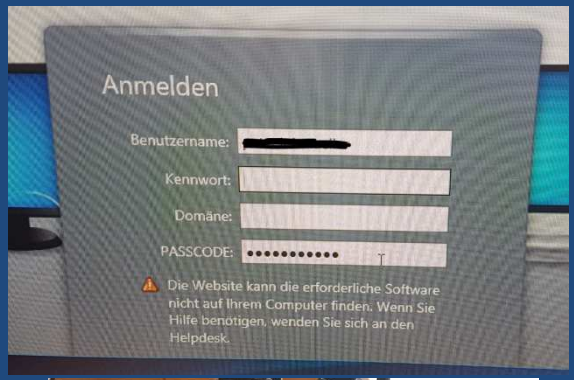
IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Kein Zugang zu den Arbeitsräumen und Büros!

7.1.8 *TOM* / Systemschutz/Bildschirmschoner

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Kein Zugang oder Einblick in Arbeitsplatz-systeme



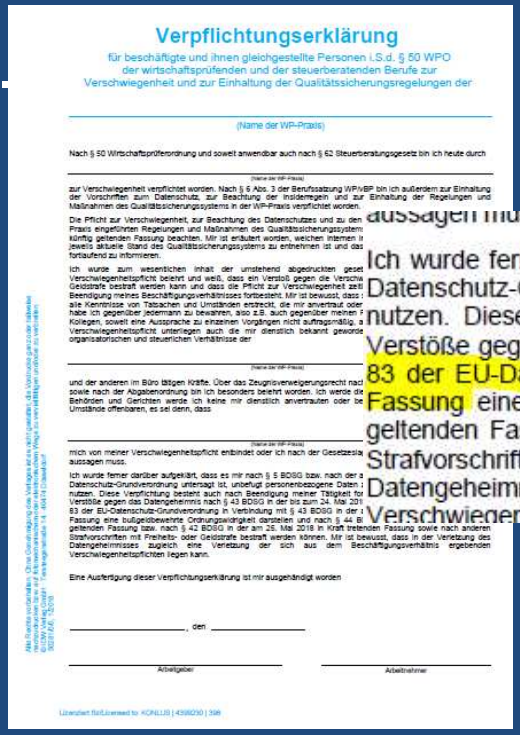
IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Kanzleileitung & Kanzleiteam Informationsveranstaltung

Kanzleimitarbeiterinnen und Mitarbeiter

- Alle sollten ab dem 25.05.2018 über die kanzleirelevanten Neuerungen der EU DSGVO informiert werden und anschließend die aktualisierte Fassung des IDW 50281/0/0, 1/2018 *„Verpflichtungserklärung für beschäftigte und ihnen gleichgestellten Personen i,S.d. § 50 WPO der Wirtschaftsprüfenden und der steuerberatenden Berufe zur Verschwiegenheit und zur Einhaltung der Qualitätssicherungsregelungen der Kanzlei, Wirtschaftsprüfungsgesellschaft und (oder) Steuerberatungsgesellschaft“* Unterschreiben.

Verpflichtungserklärung Mitarbeiter (IDW)



Verpflichtungserklärung

für beschäftigte und ihnen gleichgestellte Personen i.S.d. § 50 WPO der wirtschaftsprüfenden und der steuerberatenden Berufe zur Verschwiegenheit und zur Einhaltung der Qualitätssicherungsregelungen der

(Name der WP-Praxis)

Nach § 50 Wirtschaftsprüferordnung und soweit anwendbar auch nach § 62 Steuerberatungsgesetz bin ich heute durch

(Name der WP-Praxis)

zur Verschwiegenheit verpflichtet worden. Nach § 6 Abs. 3 der Berufssatzung WP/vBP bin ich außerdem zur Einhaltung der Vorschriften zum Datenschutz, zur Beachtung der Insidergesetze und zur Einhaltung der Regelungen und Maßnahmen des Qualitätssicherungssystems in der WP-Praxis verpflichtet worden.

Die Pflicht zur Verschwiegenheit, zur Beachtung des Datenschutzes und zu den in der Praxis eingeführten Regelungen und Maßnahmen des Qualitätssicherungssystems in der künftig geltenden Fassung beachten. Mir ist erläutert worden, welchen internen Informationsquellen ich mich zu bedienen habe, um den jeweils aktuellen Stand des Qualitätssicherungssystems zu entnehmen ist und das mir fortlaufend zu informieren.

Ich wurde zum wesentlichen Inhalt der umstehend abgedruckten gesetzlichen Vorschriften über die Verschwiegenheitspflicht belehrt und weiß, dass ein Verstoß gegen die Verschwiegenheitspflicht mit Geldstrafe bestraft werden kann und dass die Pflicht zur Verschwiegenheit auch nach Beendigung meines Beschäftigungsverhältnisses fortbesteht. Mir ist bewusst, dass die Verschwiegenheitspflicht alle Kenntnisse von Tatsachen und Umständen erstreckt, die mir anvertraut oder bekannt geworden sind. Ich habe ich gegenüber jedermann zu bewahren, also z.B. auch gegenüber meinen Angehörigen, meinen Kolleginnen und Kollegen, soweit eine Aussprache zu einzelnen Vorgängen nicht auftragsmäßig, also im Rahmen der Verschwiegenheitspflicht unterliegen auch die mir dienstlich bekannt gewordenen wirtschaftlichen, organisatorischen und steuerlichen Verhältnisse der

(Name der WP-Praxis)

und der anderen im Büro tätigen Kräfte. Über das Zeugnisverweigerungsrecht nach der Strafprozessordnung sowie nach der Abgabenordnung bin ich besonders belehrt worden. Ich werde die Vorschriften der Behörden und Gerichten werde ich keine mir dienstlich anvertrauten oder bekannt gewordenen Umstände offenbaren, es sei denn, dass

(Name der WP-Praxis)

mich von meiner Verschwiegenheitspflicht entbindet oder ich nach der Gesetzeslage zur Aussage aussagen muss.

Ich wurde ferner darüber aufgeklärt, dass es mir nach § 5 BDSG bzw. nach der ab dem 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung untersagt ist, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Diese Verpflichtung besteht auch nach Beendigung meiner Tätigkeit fort. Ich wurde darüber belehrt, dass Verstöße gegen das Datengeheimnis nach § 43 BDSG in der bis zum 24. Mai 2018 geltenden Fassung bzw. nach Art. 83 der EU-Datenschutz-Grundverordnung in Verbindung mit § 43 BDSG in der am 25. Mai 2018 in Kraft tretenden Fassung eine bußgeldbewehrte Ordnungswidrigkeit darstellen und nach § 44 BDSG in der bis zum 24. Mai 2018 geltenden Fassung bzw. nach § 42 BDSG in der am 25. Mai 2018 in Kraft tretenden Fassung sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe bestraft werden können. Mir ist bewusst, dass in der Verletzung des Datengeheimnisses zugleich eine Verletzung der sich aus dem Beschäftigungsverhältnis ergebenden Verschwiegenheitspflichten liegen kann.

Eine Ausfertigung dieser Verpflichtungserklärung ist mir ausgehändigt worden

_____, den _____

Arbeitgeber | Arbeitnehmer

aussagen muss.

Ich wurde ferner darüber aufgeklärt, dass es mir nach § 5 BDSG bzw. nach der ab dem 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung untersagt ist, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Diese Verpflichtung besteht auch nach Beendigung meiner Tätigkeit fort. Ich wurde darüber belehrt, dass Verstöße gegen das Datengeheimnis nach § 43 BDSG in der bis zum 24. Mai 2018 geltenden Fassung bzw. nach Art. 83 der EU-Datenschutz-Grundverordnung in Verbindung mit § 43 BDSG in der am 25. Mai 2018 in Kraft tretenden Fassung eine bußgeldbewehrte Ordnungswidrigkeit darstellen und nach § 44 BDSG in der bis zum 24. Mai 2018 geltenden Fassung bzw. nach § 42 BDSG in der am 25. Mai 2018 in Kraft tretenden Fassung sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe bestraft werden können. Mir ist bewusst, dass in der Verletzung des Datengeheimnisses zugleich eine Verletzung der sich aus dem Beschäftigungsverhältnis ergebenden Verschwiegenheitspflichten liegen kann.

To do Kanzleiintern und extern

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

· Organisatorische Maßnahmen:

- Regelmäßige Mitarbeiter-Information / Schulung
- Auskünfte und einheitliche Sprachregelung zur EU DSGVO gegenüber Mandanten (evtl. Text Flyer)

Kanzleiinterne / Kanzleiexterne Information

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

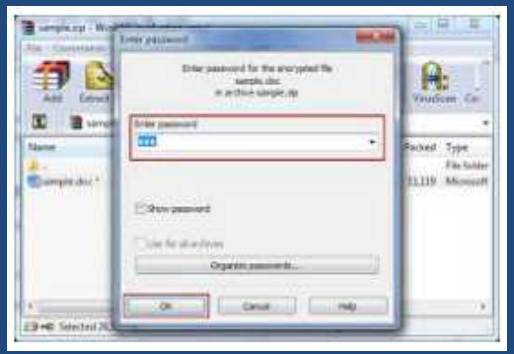
· Organisatorische Maßnahmen:

- Regelmäßige Mitarbeiter-Informationen / Schulungen
- Kanzleidatenschutzrichtlinie:
  - Sicherer Umgang mit Mandanten-Daten
  - Sicherer Datenaustausch mit Mandanten (Verschlüsselt)
  - Sicherer Umgang mit Mandanten-Daten
  - „Sparsame“ / nur notwendige Daten erfassen

Empfehlung:

Verschlüsselter Datenaustausch mit Mandanten

Passwortschutz PDF, Zip, oder zum Bsp.: WebAkte mit zweifacher Authentifizierung (TAN) etc.

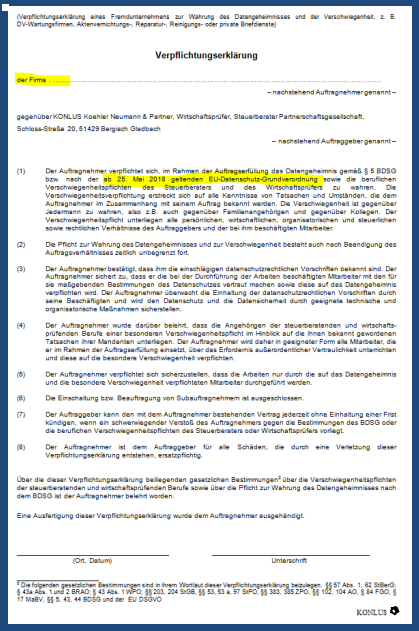


Mandantensensibilisierung

Warum Passwortschutz / Verschlüsselung

Kanzleisicht	Mandantensicht
Datenschutz / Sorgfaltspflicht / Qualitätssicherung /	Schutz von personenbezogener Daten: Bsp.: Löhne, Steuererklärungen
Haftung / Berufsrechtliche Verschwiegenheit	Schutz vor Falschübermittlung (Falscher Empfänger etc.)

Verpflichtungserklärung für externe Besucher



(Verpflichtungserklärung eines Fremdunternehmens zur Wahrung des Datengeheimnisses und der Verschwiegenheit, z. B. DV-Wartungsfirmen, Aktenvernichtungs-, Reparatur-, Reinigungs- oder private Briefdienste)

Verpflichtungserklärung

der Firma .....

– nachstehend Auftragnehmer genannt –

gegenüber KONLUS Koehler Neumann & Partner, Wirtschaftsprüfer, Steuerberater Partnerschaftsgesellschaft,
Schloss-Straße 20, 51429 Bergisch Gladbach

– nachstehend Auftraggeber genannt –

(1) Der Auftragnehmer verpflichtet sich, im Rahmen der Auftragserfüllung das Datengeheimnis gemäß § 5 BDSG bzw. nach der ab 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung sowie die beruflichen Verschwiegenheitspflichten des Steuerberaters und des Wirtschaftsprüfers zu wahren. Die Verschwiegenheitsverpflichtung erstreckt sich auf alle Kenntnisse von Tatsachen und Umständen, die dem Auftragnehmer im Zusammenhang mit seinem Auftrag bekannt werden. Die Verschwiegenheit ist gegenüber Jedermann zu wahren, also z.B. auch gegenüber Familienangehörigen und gegenüber Kollegen. Der Verschwiegenheitspflicht unterliegen alle persönlichen, wirtschaftlichen, organisatorischen und steuerlichen sowie rechtlichen Verhältnisse des Auftraggebers und der bei ihm beschäftigten Mitarbeiter.

(2) Die Pflicht zur Wahrung des Datengeheimnisses und zur Verschwiegenheit besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbegrenzt fort.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut machen sowie diese auf das Datengeheimnis verpflichten wird. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften durch seine Beschäftigten und wird den Datenschutz und die Datensicherheit durch geeignete technische und organisatorische Maßnahmen sicherstellen.

(4) Der Auftragnehmer wurde darüber belehrt, dass die Angehörigen der steuerberatenden und wirtschaftsprüfenden Berufe einer besonderen Verschwiegenheitspflicht im Hinblick auf die ihnen bekannt gewordenen Tatsachen ihrer Mandanten unterliegen. Der Auftragnehmer wird daher in geeigneter Form alle Mitarbeiter, die er im Rahmen der Auftragserfüllung einsetzt, über das Erfordernis außerordentlicher Vertraulichkeit unterrichten und diese auf die besondere Verschwiegenheit verpflichten.

(5) Der Auftragnehmer verpflichtet sich sicherzustellen, dass die Arbeiten nur durch die auf das Datengeheimnis und die besondere Verschwiegenheit verpflichteten Mitarbeiter durchgeführt werden.

(6) Die Einschaltung bzw. Beauftragung von Subauftragnehmern ist ausgeschlossen.

(7) Der Auftraggeber kann den mit dem Auftragnehmer bestehenden Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des BDSG oder die beruflichen Verschwiegenheitspflichten des Steuerberaters oder Wirtschaftsprüfers vorliegt.

(8) Der Auftragnehmer ist dem Auftraggeber für alle Schäden, die durch eine Verletzung dieser Verpflichtungserklärung entstehen, ersatzpflichtig.

Über die dieser Verpflichtungserklärung beiliegenden gesetzlichen Bestimmungen[1] über die Verschwiegenheitspflichten der steuerberatenden und wirtschaftsprüfenden Berufe sowie über die Pflicht zur Wahrung des Datengeheimnisses nach dem BDSG ist der Auftragnehmer belehrt worden.

Eine Ausfertigung dieser Verpflichtungserklärung wurde dem Auftragnehmer ausgehändigt.

(Ort, Datum) Unterschrift

[1] Die folgenden gesetzlichen Bestimmungen sind in ihrem Wortlaut dieser Verpflichtungserklärung beigelegen: §§ 57 Abs. 1, 62 StBerG; § 43a Abs. 1 und 2 BRAO; § 43 Abs. 1 WPO; §§ 203, 204 StGB; §§ 93, 93 a, 97 StPO; §§ 383, 386 ZPO; §§ 102, 104 AO; § 84 FGO; § 17 MaBV; §§ 5, 43, 44 BDSG und der EU DSGVO

KONLUS

(Verpflichtungserklärung eines Fremdunternehmens zur Wahrung des Datengeheimnisses und der Verschwiegenheit, z. B. DV-Wartungsfirmen, Aktenvernichtungs-, Reparatur-, Reinigungs- oder private Briefdienste)

Verpflichtungserklärung

der Firma . . . . . .

– nachstehend Auftragnehmer genannt –

gegenüber KONLUS Koehler Neumann & Partner, Wirtschaftsprüfer, Steuerberater Partnerschaftsgesellschaft,

Schloss-Straße 20, 51429 Bergisch Gladbach

– nachstehend Auftraggeber genannt –

r Auftragnehmer verpflichtet sich, im Rahmen der Auftragserfüllung das Datengeheimnis gemäß § 5 BDSG nach der ab 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung sowie die beruflichen wiegenheitspflichten des Steuerberaters und des Wirtschaftsprüfers zu wahren. Die haltsverpflichtung erstreckt sich auf alle Kenntnisse von Tatsachen und Umständen

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

EU DSGVO

Kanzlei - Internetseite

Kanzlei - Internetseite

- Datenschutzerklärung

  Besucher müssen auf den Einsatz von Cookies hingewiesen werden
  „welche Daten werden gespeichert“
  (Einsatz von Google Analytics)

Opt in:
Hier ist die Zustimmung für die Speicherung der Nutzerdaten beim Aufruf der Seite zu erfragen

Opt out:

Gibt den Besuchern erst im Nachhinein die Chance die Speicherung Ihrer Nutzer-Daten ablehnen

Lösung: Datenschutzgenerator (Textgenerator für EU DSGVO / Webseiten)

Kanzlei - Internetseite / Verschlüsselung

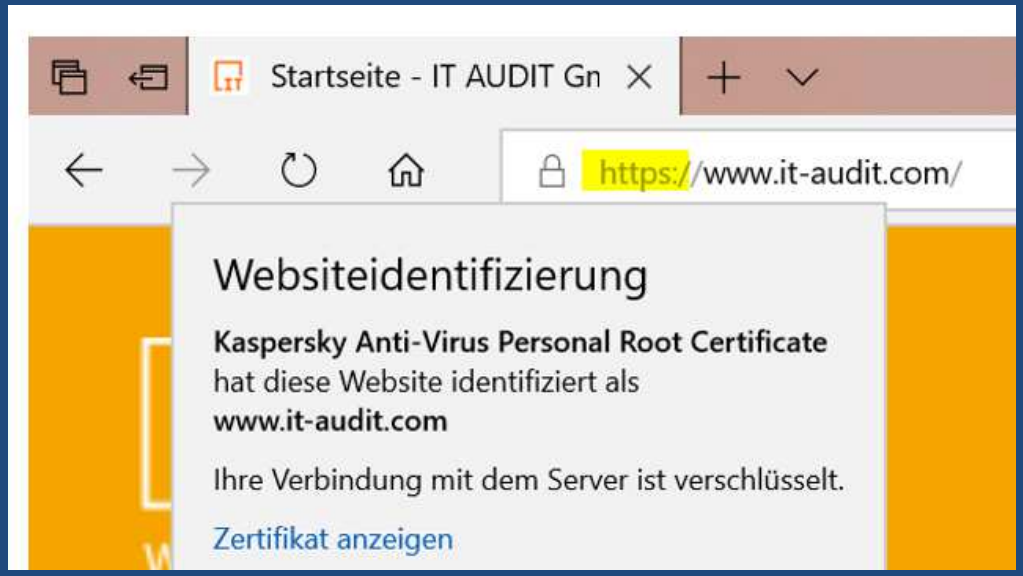
Wenn Seitenbesucher Daten bspw. über ein Kontaktformular übermitteln ist es dringend empfehlenswert das diese Informationen verschlüsselt durch das Internet gesendet werden.

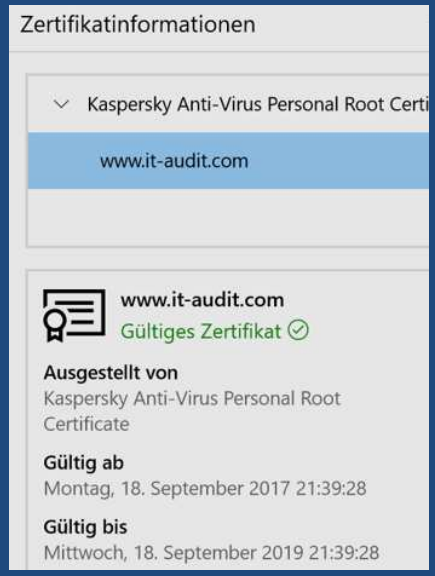
SSL-Zertifikat:

SSL steht für „Security Sockets Layer“ und beschreibt ein Verschlüsselungs- und Kommunikationsprotokoll.

Ein SSL-Zertifikat ist ein digitales Zertifikat, welches durch eine CA (Certificate Authority, Zertifizierungsstelle) ausgestellt wird. Es sorgt dafür, dass zwischen Webserver und Webbrowser eine SSL-Verbindung hergestellt werden kann und somit die Kommunikation zwischen den beiden verschlüsselt wird. So können sensible Daten nicht von Dritten ausgelesen werden.

Kanzlei - Internetseite / SSL-Zertifikat:





Kanzlei - Internetseite / Info zu HTTPS:

HTTP und HTTPS: Wo ist der Unterschied?

Das Das Hypertext Transfer Protocol, kurz HTTP, wird genutzt, um Websites vom Server in Ihren Webbrowser zu laden.
Das Hypertext Transfer Protocol **Secure**, kurz HTTPS, hat die gleiche Aufgabe, tut dies jedoch verschlüsselt und kann somit eine abhörsichere Verbindung zwischen dem Betreiber der Website und Ihrem Browser herstellen.

Kanzlei - Internetseite / HTTPS aktivieren:

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Woher bekommt man ein Zertifikat für die eigene Seite?

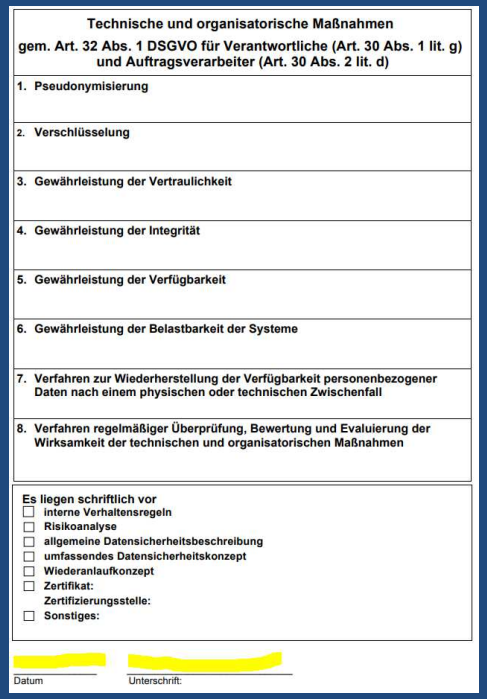
Man kann bei fast allen Providern ein SSL-Zertifikat innerhalb des aktuellen Vertrages aktivieren oder ein Zertifikat für jeweils ein Kalenderjahr erwerben. Dies kostet ca. EUR 70,-- per Anno und kann optional regelmäßig automatisch gegen Bezahlung verlängert werden.

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

EU DSGVO

Kanzlei - Dienstleister

Formular „*Verantw.- und Auftragsverarbeiter*“ Technische und organisatorische Maßnahmen



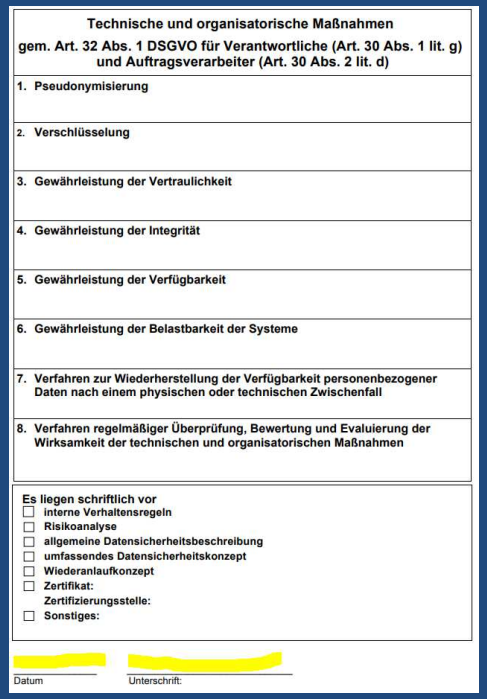
Technische und organisatorische Maßnahmen
gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung
2. Verschlüsselung
3. Gewährleistung der Vertraulichkeit
4. Gewährleistung der Integrität
5. Gewährleistung der Verfügbarkeit
6. Gewährleistung der Belastbarkeit der Systeme
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor
- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle:
- ☐ Sonstiges:

Datum Unterschrift:

Formular „*Verantw.- und Auftragsverarbeiter*“ Technische und organisatorische Maßnahmen



Technische und organisatorische Maßnahmen
gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung
2. Verschlüsselung
3. Gewährleistung der Vertraulichkeit
4. Gewährleistung der Integrität
5. Gewährleistung der Verfügbarkeit
6. Gewährleistung der Belastbarkeit der Systeme
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor
- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle:
- ☐ Sonstiges:

Datum Unterschrift:

Situation Kanzlei < > Mandant:

Unsere Tätigkeit unterliegt dem Begriff der **Funktionsübertragung**, welche über unsere geltenden Mandatsverträge mit unseren Mandanten geregelt sind.
Also keine Auftragsdatenverarbeitung

„Klassische“ Steuerberatungstätigkeit ist keine Auftragsdatenverarbeitung

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Soweit der Steuerberater „klassische“ Steuerberatungstätigkeiten erbringt (Erstellung Jahresabschluss, Steuerberatung etc.) handelt er ausweislich:

§ 32 Abs. 2 Steuerberatungsgesetz („StBerG“) i.V.m. den tätigkeitsbeschreibenden Normen im StBerG eigenver-antwortlich und damit aufgrund gesetzlicher Vorgaben weisungsfrei.
Aus dieser Weisungsfreiheit ergibt sich bereits, dass ein Steuerberater hinsichtlich dieser Tätigkeiten nicht den Vorgaben der Auftragsdatenverarbeitung nach § 11 BDSG bzw. der ab 25.05.2018 geltenden EU DS-GVO und damit der Weisungs-gebundenheit des Auftraggebers unterworfen werden kann.

„Klassische“ Steuerberatungstätigkeit ist keine Auftragsdatenverarbeitung

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

Situation Kanzlei < > DATEV

Die Kanzlei selbst, **hat** beispielsweise **eine** Vereinbarung über die **Auftragsdatenverarbeitung** mit der DATEV, da diese Genossenschaft ein Dienstleistungsunternehmen ist.

FAZIT:

Dienstleistungsunternehmen benötigen Vereinbarungen über Auftragsdatenverarbeitung

Steuerberater benötigen Mandantenverträge (Funktionsübertragung)

Fazit / Schlußwort:

- **„Alle Anstrengungen dokumentieren“**

  Man sollte alle Anstrengungen dokumentieren: Zu welchem Seminar ist der Datenschutzbeauftragte gegangen? Welche Firewall wurde wann installiert? Welche Verträge wurden mit Dienstleistern geschlossen? Denn selbst bei Datenlecks oder Verstößen wie Fehlern in der Datenschutz-Erklärung besteht bei guter Dokumentation die Chance, ohne Bußgeld davonzukommen. Dafür muss man aber die Unterlagen auf Anfrage umgehend vorlegen können.

ENDE

IT AUDIT GmbH
Wirtschaftsprüfungsgesellschaft

„Vielen Dank für Ihre Aufmerksamkeit“