WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

# Pflichten für IT-Dienstleister

## 1. Allgemeines

Mit der EU-Datenschutz-Grundverordnung (DSGVO) und dem österreichischen Datenschutz-Anpassungsgesetz 2018 (DSG) kommen einige betriebliche und organisatorische Änderungen auf österreichische Unternehmen zu. Diese gelten ab dem 25. Mai 2018 für jeglichen betrieblichen Umgang mit personenbezogenen Daten, das sind alle Informationen, welche direkt oder indirekt einen Bezug zu einer Person herstellen können (z.B. Name, Adresse, Geburtsdatum, genetische Daten, Gesundheitsdaten).

Auch Begriffsbestimmungen werden sich ändern, u.a. wird der Begriff des datenschutzrechtlichen Dienstleisters auf „Auftragsverarbeiter“ geändert.
Sie sind als externer IT-Dienstleister „Auftragsverarbeiter“ gemäß Art 4 Z 8 der DSGVO, da Sie personenbezogene Daten im Auftrag Ihrer Auftraggeberin und Ihres Auftraggebers (Verantwortliche und Verantwortlicher gemäß Art 4 Z 7) bearbeiten.

**Beispiele:** Sie erhalten und verarbeiten Kundendaten von Ihrem Auftraggeber. Im Rahmen Ihrer Supporttätigkeit (Software as a Service) haben Sie umfassenden Zugriff auf die Unternehmensdaten wie Bilanzahlen, Mitarbeiterdaten, etc. Sie sind datenschutzrechtliche Auftragsverarbeiter.

Als IT-Dienstleister können Sie von Ihrem Kunden auch als externer Datenschutzbeauftragter beauftragt werden, wobei hier aber bzgl. Beratungsleistungen aus anderen Bereichen als der Technik die Grenzen des § 32 Abs. 1a GewO idgF zu beachten sind. Mehr zu Datenschutzbeauftragter IT-Dienstleister

## 2. Datensicherheit

Als Auftragsverarbeiter müssen Sie für geeignete technische und organisatorische Maßnahmen (TOMs) garantieren, die eine Verarbeitung im Einklang mit den Anforderungen dieser Verordnung sicherstellen und den Schutz der Rechte der betroffenen Person gewährleisten. Sie sind daher als Auftragsverarbeiter verpflichtet, Datensicherheitsmaßnahmen zu implementieren, wobei eine Kostenberücksichtigung im Verhältnis zum bestehenden Risiko besteht. Folgende Maßnahmen in der DSGVO selbst ausgewiesen:

- die **Pseudonymisierung und Verschlüsselung personenbezogener Daten** (z.B. Passwortsicherungen von Dateien): „Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

- die **Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen** (z.B. Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen). Dazu gehört auch, dass unterstellte natürliche Personen, die Zugang zu

personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten („Auftragsprinzip“);

- die **Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen** (z.B. Backup-Programme);

- ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung** (z.B. Selbstevaluierungsprozesse).

**Beispiel:** Bei Lizenz-Bestandsverträgen gemäß OGH gibt es sehr wohl die Verpflichtung zu einer gewissen Instandhaltung, jedoch keine Verpflichtung für die Zurverfügungstellung von „Komfortfunktionen“ in einer Software.

**VORSICHT:** Wenn das Produkt zB privacy by design & by default (datenschutzfreundlich Technik und Voreinstellungen) gemäß DSGVO widerspricht, dann muss es sehr wohl angepasst werden (brauchbares Produkt).

Mehr zu Datensicherheitsmaßnahmen.

### 2.1. Beurteilung des angemessenen Schutzniveaus

Sie müssen die Risiken berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere bei unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten („risikobasierter Ansatz“).

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

### 2.2. Privacy by design / privacy by default

Zum Schutz der personenbezogenen Daten haben Sie ua auch die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.

- **Datenschutz durch Technik:** Sowohl bei der Planung als auch bei der Datenverarbeitung selbst haben Sie und Ihre Auftraggeberin und Ihr Auftraggeber geeignete technische und organisatorische Maßnahmen zu berücksichtigen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen (z.B. Pseudonymisierung).

- **Datenschutzfreundliche Voreinstellungen:** Ihr Auftraggeber hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

- Die Einhaltung eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

**Tipp:** Welche Datensicherheitsmaßnahmen konkret im Betrieb sinnvoll / empfehlenswert sind, finden Sie unter www.it-safe.at. Hier sind insbesondere der Onlineratgeber und die Handbücher (KMU und Mitarbeiter) empfehlenswert.

## 3. Weniger Meldeverpflichtungen – mehr Selbstverantwortung im Betrieb

### 3.1. Verarbeitungsverzeichnis

Aufgrund der DSGVO muss keine Meldung mehr an das Datenverarbeitungsregister (DVR) erstattet werden und auch die DVR-Nummer gehört der Vergangenheit an. Stattdessen müssen Sie und Ihr Auftraggeber Verzeichnisse über die Verarbeitung von Daten führen. Diese Verzeichnisse sind schriftlich zu führen, wobei dies auch in einem elektronischen Format erfolgen kann. Im Verarbeitungsverzeichnis sind unter anderem die Kategorien von Empfängern (Auftragsverarbeiter, andere Verantwortliche, sonstige Empfänger) anzugeben.

**Achtung**: Dieses Verzeichnis müssen Sie einmal für sich selbst (= für die eigenen datenschutzrelevanten Vorgänge im Betrieb) und jeweils für Ihre Kunden führen!

Der Umfang der Dokumentationspflicht ist für Sie als Auftragsverarbeiter aber immerhin geringer als für die Verantwortliche und den Verantwortlichen, siehe Muster:

- Musterverzeichnis Autragsverarbeiter
- EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Auftragsverarbeiter
- Anwendungsbeispiel für Auftragsverarbeiter

Muster für Verantwortliche:

- EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher
- Anwendungsbeispiel für Verantwortlichen

**Tipp:** Wenn schon Datenanwendungen im DVR registriert sind, können diese als Anhaltspunkt für die Dokumentation dienen. Die bisherigen Meldungen wurden mittlerweile bereits exportierbar zur Verfügung gestellt (vgl.: https://www.dsb.gv.at/dvr-online).

Sie sind verpflichtet, bei der Erfüllung Ihrer Aufgaben mit der Aufsichtsbehörde zusammenzuarbeiten. Auf Anfrage sind die Verzeichnisse der Behörde vorzulegen. Anhand dieser Verzeichnisse ist es für die Aufsichtsbehörde möglich, die betreffenden Verarbeitungsvorgänge zu kontrollieren.

**Achtung**: Das Verarbeitungsverzeichnis ist ein Kernpunkt der DSGVO! Dieses muss unter allen Umständen vorgelegt bzw eingesehen werden können!

### 3.2. Risikoanalyse & Datenschutzfolgenabschätzung

Sie müssen Risikoanalysen der Datenanwendungen durchführen und den Verantwortlichen bei Erfüllung ihrer und seiner Pflichten nach der DSGVO unterstützen. Eine genaue Anleitung dieser Analysen finden Sie unter: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html.

Wenn ein hohes Risiko für die Rechte und Freiheiten der Personen durch die Verarbeitung der Daten besteht (insbesondere bei Verwendung neuer Technologien), so muss Ihr Unternehmen eine Datenschutz- Folgenabschätzung machen. Darin müssen die geplanten Verarbeitungsvorgänge und Zwecke der Datenverarbeitung beschrieben sowie die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung und mögliche Risiken für die Rechte und Freiheiten betroffener Personen bewertet werden. Diese Risikoanalyse und geplante Abhilfen in der Organisation komplettieren die Folgeabschätzung.

Mehr zu Datenschutz-Folgenabschätzung

### 4. Datenschutzbeauftragter

Es ist ein Datenschutzbeauftragter verpflichtend zu bestellen, wenn die Kerntätigkeit des Unternehmens eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht – das gilt unabhängig davon zu beurteilen, ob ein Unternehmen als Verantwortlicher oder Auftragsverarbeiter auftritt.

**Beispiele:**
- Haupttätigkeit des Unternehmens ist die Bereitstellung von Website-Analysediensten und die Unterstützung bei zielgruppenorientierten Werbe- und Marketingmaßnahmen
- Haupttätigkeit des Unternehmens ist die Verarbeitung von Daten (Inhalte, Datenverkehrsaufkommen, Standort) durch Telefon- oder Internetdienstleister.

Informationstechnologen und IT-Dienstleister arbeiten oftmals auch mit sensiblen Daten (Gesundheitsdaten, Daten über religiöse Zugehörigkeit der Mitarbeiter eines Unternehmens). Wenn sie das in einem umfangreichen Ausmaß (= große Anzahl der betroffenen Personen, umfassendes Datenvolumen, etc.) tun bzw. diese konkrete Datenverarbeitung die Kerntätigkeit (= wichtigsten Arbeitsabläufe, Haupttätigkeit) dieses Unternehmens darstellt, so hat der IT-Dienstleister einen Datenschutzbeauftragten zu bestellen.

Mehr zu Datenschutzbeauftragter IT-Dienstleister
Mehr zu Allgemeinen Informationen betreffend Datenschutzbeauftragter

WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung·Buchhaltung·IT

**5. Sub-Auftragsverarbeiter**

Sie dürfen keine weiteren Auftragsverarbeiter (Subunternehmer) ohne vorherige schriftliche Genehmigung Ihres Auftraggebers beauftragen. Liegt nur eine allgemeine schriftliche Genehmigung vor, müssen Sie den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch anderer Auftragsverarbeiter informieren. Ihr Auftraggeber hat die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

**Achtung**: Grundsätzlich fiele auch die Nutzung von Cloud-Services zur Datenspeicherung unter diesen Passus! Sie müssen einerseits eine DSGVO-konforme Vereinbarung mit Ihren eigenen Auftragsverarbeitern abschließen und andererseits sicherstellen, dass diese Speicherung mit Ihrem Auftraggeber vereinbart wurde.

**6. Auftragsverarbeiter - Vertrag/Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO**

Sie müssen mit Ihrem Auftraggeber schriftlich einen Vertrag abschließen, wobei elektronisch auch als schriftlich gilt. Der Vertrag kann auf Standardvertragsklauseln beruhen, welche entweder die Europäische Kommission oder die Aufsichtsbehörde festlegen kann und hat Folgendes zu beinhalten:

- Bindung an die Verantwortliche / den Verantwortlichen,
- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte der Verantwortlichen / des Verantwortlichen.

**Tipp:** Verwenden Sie unsere Muster und weiterführenden Informationen
- Mustervertrag IT-Dienstleister (Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO)
- EU-DSGVO-MUSTERVERTRAG-Vereinbarung-Auftragsverarbeitung

Weitere Informationen sind auch hier abrufbar:

- Pflichten des Auftragsverarbeiters
- Verantwortlicher und Auftragsverarbeiter - (Überblick)
- Fragen und Antworten aus dem Chat
- Auftragsverarbeiter
- Verarbeitungsverzeichnis

Sie und jede Ihnen oder dem Verantwortlichen unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur auf Weisung Ihrer Auftraggeberin und Ihres Auftraggebers verarbeiten, es sei denn, dass Sie aufgrund einer gesetzlichen Vorschrift zur Verarbeitung verpflichtet sind. Mitarbeiter sind entsprechend zu belehren (vgl auch: EU-Datenschutz-Grundverordnung (DSGVO): Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen).

### 6.1. Warnpflicht des Unternehmers

Sie unterliegen einer besonderen Warnpflicht, d.h. Sie haben Ihren Auftraggeber unverzüglich zu informieren, falls Sie der Auffassung sind, dass eine Weisung gegen Datenschutzrecht verstößt.

## 7. Informationspflicht und Betroffenenrechte

Als Verantwortlicher müssen Sie den von einer Datenanwendung betroffenen Personen (Betroffene) gewisse Informationen über die Datenanwendungen zur Verfügung zu stellen. Informationen und Betroffenenrechte (v.a. Recht auf Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch) müssen unverzüglich, spätestens aber innerhalb eines Monats gegeben und erledigt werden. Diese Frist kann um höchstens weitere zwei Monate verlängert werden.

Mehr zu Informationspflichten

Mehr zu Betroffenenrechte

Es empfiehlt sich, die Datenschutzerklärung als auch eine Einwilligungserklärung jeweils extra auszuweisen und diese nicht in die AGB zu integrieren.

**Tipp:** Füllen Sie das Muster der Datenschutzerklärung im Online-Ratgeber zu den Informationsverpflichtungen aus und stellen Sie es auf Ihre Webseite. Es reicht nach derzeitigem Stand aus, wenn Sie gegenüber den Betroffenen auf Ihre Datenschutzerklärung verweisen.
Datenschutzerklärung selbst gestalten: Online-Ratgeber zu den Informationsverpflichtungen
Mehr zu Muster zur Datenschutzerklärung

Informationen zur Einwilligungserklärung & Muster: EU-Datenschutz-Grundverordnung (DSGVO): Einwilligungserklärung

## 8. Datenschutzverletzungen

Im Falle von Datenschutzverletzungen (z.B. Verlust eines Datenträgers, Hackerangriff) müssen Unternehmen (Verantwortlicher) dies der Datenschutzbehörde und den betroffenen Personen melden. Und zwar in angemessener Frist – höchstens innerhalb von 72 Stunden nach der Entdeckung.

Ausnahme: Wenn die Datenschutzverletzung voraussichtlich kein Risiko (bzw. im Fall der Betroffenen kein hohes Risiko) für die persönlichen Rechte und Freiheiten der Betroffenen bedeutet.

Mehr zu Datenschutzverletzungen

## 9. Aufbewahrungsfristen

Eine häufige Anfrage von Kunden stellen die Speicherfristen dar. Wenn die Aufbewahrung der Daten tatsächlich aus steuerrechtlichen / gesetzlichen Gründen notwendig ist, können diese Daten natürlich auch aufbewahrt werden. Gleiches gilt für Daten, welche aufgrund von vertragsrechtlichen Überlegungen (Gewährleistung, Schadenersatz, etc.) potentiell

benötigt werden. Pauschal alle personenbezogene Daten aber für sieben Jahre zu speichern würde u.a. gegen den Grundsatz der Speicherbegrenzung verstoßen.

**Tipp:** Einen Überblick über die wichtigsten Speicher- und Aufbewahrungsfristen in Österreich finden Sie hier: Speicher- und Aufbewahrungsfristen

**10. Haftung**

Betroffene Personen haben neben verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfen auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Auftragsverarbeiter im Falle einer Rechtsverletzung durch den Auftragsverarbeiter (zB Ansprüche auf Schadenersatz).

Betroffene Personen können auf materiellen oder immateriellen Schadenersatz klagen. Jeder an einer Verarbeitung Beteiligte haftet für den Schaden, der durch eine unrechtmäßige Verarbeitung verursacht wurde. Die Haftung entfällt, wenn die fehlende Verantwortung für den Umstand, durch den der Schaden eingetreten ist, nachgewiesen werden kann.

Ist mehr als ein Auftragsverarbeiter (oder mehr als ein Verantwortlicher) oder sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für einen Schaden verantwortlich, haftet jeder Auftragsverarbeiter (oder jeder Verantwortliche) für den gesamten Schaden. Es ist jedoch möglich, von den übrigen an derselben Verarbeitung Beteiligten den Teil des Schadenersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht, also Regress zu nehmen.

**11. Geldstrafen**

Es drohen Verwaltungsstrafen bis zu einer Maximalhöhe von EUR 20 Mio. bzw. 4% des weltweiten Konzernumsatzes des vorangegangenen Geschäftsjahres, je nach dem, was höher ist.

**Achtung:** Obwohl diese Verwaltungsstrafen Maximalstrafen sind, werden datenschutzrechtliche Verletzungen in Zukunft sicher einschneidender und teurer werden. Datenschutz darf nicht mehr auf die leichte Schulter genommen werden.

Informationen und weiterführende Links zur DSGVO für IT-Dienstleister

WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

## WKO Unterlagen und Hilfestellung zur DSGVO - wko.at/datenschutz

**Achtung:** Die weiteren angeführten Links sind für IT-Dienstleister ebenso relevant, da sie im eigenen Unternehmen eigenständig verantwortlich sind.

Checkliste

Online-Ratgeber zur Datenschutz-Grundverordnung

Online-Ratgeber zu den Informationsverpflichtungen

**Weitere Musterdokumente:**

Musterschreiben zur Auskunftserteilung

Data Breach Notification - Muster Meldung an die Aufsichtsbehörde

Data Breach Notification - Muster Benachrichtigung der betroffenen Person

**Weitere Links:**

Auskunftspflicht des Verantwortlichen

Bildverarbeitung

Das Datenschutz-Anpassungsgesetz 2018

Datenschutz und Direktmarketing

Datenschutzrechtliche Pflicht zur Datenübertragbarkeit

Datenschutzrechtliche Pflicht zur Umsetzung eines Widerspruches

Datenverarbeitung zu Archivzwecken, zu wissenschaftlichen und historischen

Forschungszwecken sowie zu statistischen Zwecken

Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten

Grundsätze und Rechtmäßigkeit der Verarbeitung

Internationaler Datenverkehr

Meldung von Datenschutzverletzungen (Data Breach Notification)

Pflicht zur Berichtigung, Löschung ("Recht auf Vergessenwerden") und zur Einschränkung der Verarbeitung

Pflichten des Verantwortlichen

Rechtsdurchsetzung und Strafen

Sachlicher und räumlicher Anwendungsbereich

Wichtige Begriffsbestimmungen

KMU DIGITAL BeraterInnen

Informationen und weiterführende Links zur DSGVO für IT-Dienstleister

WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

**UBIT Firmen A-Z mit neuer Suchfunktion: DSGVO-Beratung -** firmen.wko.at/web/ubit

IT-Dienstleister als auch Unternehmensberater dürfen im Kontext ihrer Fachexpertise und ihres Berechtigungsumfangs Beratungsleistungen zur Implementierung von DSGVO Maßnahmen und Maßnahmen zur Datensicherheit in Betrieben anbieten.

Die Expertenliste für DSGVO Projekte auf der WKO Serviceseite zum Thema Datenschutz verweist direkt auf das UBIT Firmen A-Z. Hier können sich Unternehmen über die einfache, erweiterte Suche einen Überblick über alle Dienstleister verschaffen. Insgesamt stehen drei Zertifikate bei der Suche nach DSGVO-Fachexperten zur Verfügung:

- **DSGVO-Beratung**
  UBIT-Mitglieder können diese Kategorie über die Firmen A-Z Wartung (Menüpunkt „Auszeichnungen & Zertifikate“) selbst auswählen. Diese Kategorie steht UBIT-Mitgliedern zur Verfügung, die im Bereich DSGVO als Fachexperten tätig sind und dies in Ihrem Profil (Selbstverwaltung) angegeben haben. Es ist an keine bestimmte Zertifizierung bzw. Qualifikation gebunden.

- **Certified Data & IT Security Expert (CDISE)**
  Dieser Zertifizierungslehrgang der incite wird UBIT-Mitgliedern mit Praxiserfahrung als Datenschutz/IT-Sicherheitsexperte angeboten. Die Absolventen sind mit technischen, organisatorischen und juristischen Grundlagen in Bezug auf IT-Sicherheit und Datenschutz vertraut und geben das Wissen an die Unternehmen (Kunden) in Form von z.B. Datenschutz- und IT-Sicherheitskonzepte, Evaluierung bestehender Maßnahmen bzw. Beratungsleistungen für Datenschutz/IT-Sicherheit bzw. DSGVO weiter. Die Eintragung erfolgt automatisiert.

- **Geprüfte/r Datenschutzexpertin/-experte:**
  Dieser von der incite angebotener Lehrgang dient dazu, um für Unternehmen (Kunden) die Rolle des Datenschutzbeauftragten übernehmen zu können. Die Eintragung erfolgt automatisiert.

Informationen und weiterführende Links zur DSGVO für IT-Dienstleister

WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

## Unterlagen und Hilfestellung zur DSGVO der Datenschutzbehörde – https://www.dsb.gv.at/datenschutz-grundverordnung

Leitfaden - Verordnung

Artikel 29 Datenschutzgruppe - Beschlossene Leitlinien der Artikel-29-Gruppe

- Recht auf Datenübertragbarkeit:
  Leitlinien zum Recht auf Datenübertragbarkeit (PDF, 533 KB)
- Datenschutzbeauftragter:
  Leitlinien in Bezug auf Datenschutzbeauftrage (PDF, 1028KB)
- Federführende Aufsichtsbehörde:
  Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (PDF, 508 KB)
- Datenschutz-Folgenabschätzung und Hohes Risiko:
  Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt" (PDF, 1162 KB)

**Neu: Export-Funktion in DVR-Online**
Mit dem In-Geltung-Treten der EU-Datenschutz-Grundverordnung am 25. Mai 2018 entfällt die Verpflichtung zur Erstattung von DVR-Meldungen an die Datenschutzbehörde. Das Datenverarbeitungsregister wird ab diesem Zeitpunkt (bis zum 31. Dezember 2019) zu Archivzwecken fortgeführt werden.

Um einem Auftraggeber die Möglichkeit zu bieten, seine vorhandenen DVR-Meldungen zu sichern, ist es ab sofort möglich, in der Internet-Applikation DVR-ONLINE elektronisch verfügbare Meldungsinhalte sowohl als PDF-Dokumente als auch als XML-Dateien zu exportieren. Hierfür wurden im DVR-ONLINE-Meldebereich des Auftraggebers entsprechende Funktionen (rote Buttons, siehe Screenshot) eingefügt.
Achtung: für Informationsverbundsysteme besteht diese Möglichkeit nicht.
Mehr zu DVR-Online.

## Unterlagen und Hilfestellung zur DSGVO des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – privacyofficers.at

Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung

## Rechtsinformationssystem (RIS)
Hier finden Sie ausgewählte Entscheidungen der Datenschutzkommission von 1990 bis 2013. Ab 2014 finden Sie hier ausgewählte Entscheidungen der Datenschutzbehörde.
https://www.ris.bka.gv.at/Dsk/