wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Datenschutz Handbuch 2018

wow! solution | Wolfgang Wagner

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Datenschutzleitlinie

Das Team von wow! solution nimmt den Schutz unternehmens- und personenbezogener Daten sehr ernst. Deshalb ist das Einhalten der gesetzlichen Bestimmungen zum Datenschutz für uns selbstverständlich. Im Folgenden möchten wir Ihnen kurz darstellen, wie wir zum Datenschutz stehen, wie Ihre Daten geschützt werden.

Strategie und Grundsatz: Datensparsamkeit

Nur was benötigt wird, wird an personenbezogenen Daten gespeichert und verarbeitet. Durch diese Einstellung wird ein Risiko für betroffenen Personen ausgeschlossen. Wir verarbeiten nur Daten, die kein Risiko für Betroffene beinhalten.

Unsere Einstellung: Daten gehören den Betroffenen

Wirtschaft ist Beziehung zwischen Menschen. Wir wissen es zu schätzen, dass man uns Daten anvertraut. Die Daten der Betroffenen in unseren Unternehmen gehören zu folgenden Kategorien: MitarbeiterInnen, KundInnen, LieferantInnen, InteressentInnen, KooperationspartnerInnen und BesucherInnen unserer Unternehmen und Webseiten.

Das Datenschutz Ziel

Unser Ziel beim Datenschutz ist der respektvolle Umgang mit diesen uns anvertrauten Daten. Wir kennen die Gesetze und nutzen die Unterstützung von ExpertInnen.

Verantwortung der Unternehmensleitung

Die Verantwortung für den Schutz der Daten trägt die Unternehmensleitung.
Jede und jeder kann sich zu diesem Thema jederzeit an jede Unternehmensleitung wenden.

Risiken bewusst niedrig halten

Die Risiken für die verarbeiteten Daten sind ganz besonders niedrig. Die Daten, die wir speichern, haben für Kriminelle keinen besonderen Wert. Gegen unbeabsichtigte Fehler entwickeln wir gemeinsam Maßnahmen. Jedes Jahr werden die Risiken neu bewertet, denn die Welt verändert sich. Wenn wir Bedarf erkennen, werden neue Sicherheitsmaßnahmen festgelegt und umgesetzt.

Die Sicherheit bei der Verarbeitung von Daten ruht bei uns auf 3 Säulen:

- Geschulte MitarbeiterInnen
- Einsatz sicherer Technik mit Unterstützung professioneller Partner Unternehmen
- Das Bewusstsein, worauf es ankommt

Unsere AuftragsverarbeiterInnen und DienstleisterInnen

Sicherheit im Umgang mit Technologie fordert Fachkompetenz. Wir haben professionelle AuftragsverarbeiterInnen und DienstleisterInnen, die wir sorgfältig auswählen.
Sie bieten uns ausreichende Garantien für ihre Kompetenz im Datenschutz und ihren technischen und organisatorischen Maßnahmen.
Wir haben sie vertraglich zum Datenschutz verpflichtet und arbeiten im Interesse der betroffenen Personen zusammen.

Unser Team

Unsere MitarbeiterInnen schulen wir, damit uns allen das richtige Verhalten gelingt. Die Regeln, die im Unternehmen für die Verarbeitung personenbezogener Daten gelten, formulieren wir einfach und verständlich. Bewusstseinsbildung erleichtert uns das Einhalten der Regeln. Denn was man versteht, kann man leichter erfolgreich tun.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Was wir für den Datenschutz tun und wie wir es tun

Unser Datenschutz ist praxisbezogen und verständlich.
Auf den folgenden Seiten erfahren Sie, was wir zum Thema Datenschutz tun.

Datenschutz auf unserer Website

Kontaktaufnahme

Bei der Kontaktaufnahme mit uns (zum Beispiel per Kontaktformular oder E-Mail) werden Ihre Angaben zwecks Bearbeitung der Anfrage sowie für den Fall, dass Anschlussfragen entstehen, gespeichert. Ihre Daten werden dabei nur streng zweckgebunden zur Bearbeitung und Beantwortung Ihrer Anfrage benutzt. Mit dem Absenden des Kontaktformulars oder einer Email an uns erklären Sie sich mit der Verarbeitung einverstanden.

Zugriffsdaten/ Server-Logfiles

Wir (beziehungsweise unser Webspace-Provider) erheben Daten über jeden Zugriff auf das Angebot (so genannte Serverlogfiles). Zu den Zugriffsdaten gehören:

Name der abgerufenen Webseite, Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung über erfolgreichen Abruf, Browsertyp nebst Version, das Betriebssystem des Nutzers, Referrer URL (die zuvor besuchte Seite), IP-Adresse und der anfragende Provider.

Wir verwenden diese Protokolldaten nur für statistische Auswertungen zum Zweck des Betriebs, der Sicherheit und der Optimierung des Angebotes. Wir behalten uns jedoch vor, die Protokolldaten nachträglich zu überprüfen, wenn aufgrund konkreter Anhaltspunkte der berechtigte Verdacht einer rechtswidrigen Nutzung besteht.

Newsletter

Um Sie noch aktueller über alle News des wow! solution Blogs informieren zu können, bekommen Sie, wenn Sie sich zum Newsletter Empfang anmelden, ganz automatisch tagesaktuell die neuesten Blog News per Mail zugesendet sobald ein neuer Eintrag im wow! solution Blog online geht.

Themen des wow! solution Blogs betreffen zb. Hosting, Web Tipps & Tricks, Responsive Webdesign, SEO, Social Networking, Web-Optimierung, wow! solution Referenzen, TYPO3 CMS Sicherheitsmeldungen, TYPO3 CMS Updates uvm.

Anmeldung / Registrierung

Mit der Anmeldung zum Newsletter speichern wir Ihre IP-Adresse und das Datum der Anmeldung. Diese Speicherung dient alleine dem Nachweis im Fall, dass ein Dritter eine Emailadresse missbraucht und sich ohne Wissen des Berechtigten für den Newsletterempfang anmeldet.

Ihre Einwilligung zur Speicherung der Daten, der Email-Adresse sowie deren Nutzung zum Versand des Newsletters können Sie jederzeit widerrufen. Der Widerruf kann über einen Link in den Newslettern selbst, in Ihrem Profilbereich oder per Mitteilung an die oben stehenden Kontaktmöglichkeiten erfolgen.

Spam-Vermeidung / double opt in

E-Mail-Adressen müssen verifiziert werden. Das bedeutet, dass nach Eingabe einer E-Mail-Adresse ein Bestätigungsmail an diesen E-Mail-Account gesendet werden muss, welche durch den rechtmäßigen Besitzer bestätigt werden muss. Wird nicht bestätigt, ist die Anmeldung nicht erfolgt.

Jede E-Mail-Adresse benötigt also ein „double opt in“. Das ist die übliche Methode, um Spam auszuschalten. Nur durch aktive Bestätigung einer Anforderung eines Newsletters aus dem Ziel-E-Mail-Account gilt eine Einwilligung als nachgewiesen.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Cookies

Wir verwenden Cookies, die von der EU-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation erfasst werden. Mit Cookies können wir die Besuchserfahrung in Bezug auf unsere Website verbessern. Ein Cookie entspricht einer kleinen Datei, die auf dem Computer oder Mobilgerät eines Nutzers gespeichert wird. Sie enthält Einstellungen und andere Informationen, die auf besuchten Webseiten für den jeweiligen Nutzer verwendet werden.

Jeder Nutzer hat jedoch die Möglichkeit, den Web-Browser so einzustellen, dass der Web-Browser den Nutzer davon in Kenntnis setzt, wann dieser ein Cookie erhält. Wir weisen allerdings darauf hin, dass bei deaktivierten Cookies oder clientseitig deaktivierten Features bzw. clientseitig aktivierten Sperren u.U. einige Angebote bzw. Dienste nicht oder nur eingeschränkt funktionieren.

a. Cookies zur Verbesserung der Funktionalität unserer Websites

Wir nutzen Cookies unter anderem, um besser zu verstehen, wie unsere Websites genutzt werden, und um so deren Attraktivität, Inhalt und Funktionalität zu verbessern. Cookies helfen uns beispielsweise zu bestimmen, welche Unterseiten unserer Website besucht werden und für welche Inhalte sich Nutzer interessieren. Hierfür setzen wir Flash Cookies und Ladezeit-Optimierungs-Cookies ein. Diese sogenannten „First Party Cookies“ erfassen insbesondere die Anzahl der Zugriffe auf eine Seite, die Anzahl der angesehenen Unterseiten, die auf unseren Websites verbrachte Zeit, die Reihenfolge der besuchten Seiten, welche Suchbegriffe Sie zu uns geführt haben, das Land, die Region und ggf. die Stadt, aus der der Zugriff erfolgt, welches Betriebssystem und welchen Internet-Browser mit welcher Spracheinstellung Sie verwenden sowie den Anteil von mobilen Endgeräten, die auf unsere Websites zugreifen. Ferner erfassen wir Bewegungen, „Klicks“ und das Scrollen mit der Computermaus, um zu verstehen, welche Bereiche unserer Website Besucher besonders interessieren. Die aus technischen Gründen übermittelte IP-Adresse Ihres Rechners wird automatisch anonymisiert und ermöglicht uns keinen Rückschluss auf Sie.

b. Cookies für nutzungsbasierte Online-Werbung

Wir behalten uns vor, Informationen, die wir mittels Cookies aus einer Analyse des Nutzungsverhaltens von Besuchern unserer Websites gewonnen haben, auch zu nutzen, um Ihnen auf unseren eigenen Websites spezifische Werbung für bestimmte unserer Produkte anzuzeigen. Wir sind der Auffassung, dass Sie als Nutzer hiervon profitieren, weil wir Werbung oder Inhalte einblenden, von denen wir aufgrund Ihres Surf-Verhaltens annehmen, dass sie zu Ihren Interessen passen und Sie so weniger zufällig gestreute Werbung oder bestimmte Inhalte, die Sie wahrscheinlich weniger interessieren, angezeigt bekommen.

c. So verhindern Sie, dass „Cookies“ auf Ihrer Festplatte gespeichert werden, bzw. löschen diese

Sie können Ihren Internet-Browser so einstellen, dass das Speichern von Cookies auf Ihrer Festplatte verhindert wird bzw. Sie jedes Mal gefragt werden, ob Sie mit dem Setzen von Cookies einverstanden sind. Einmal gesetzte Cookies können Sie auch jederzeit wieder löschen. Wie all dies im Einzelnen funktioniert, können Sie der Bedienungsanleitung Ihres Browsers entnehmen. Eine Erklärung in Wort und Bild finden Sie für die Internet-Browser Firefox, Microsoft Internet Explorer und Google Chrome unter diesem Link: http://www.aboutcookies.org/Default.aspx?page=2 . Wenn Sie das Speichern von Cookies nicht akzeptieren, kann dies gegebenenfalls zu Funktionseinschränkungen unserer Angebote führen.

Von uns verwendete Third Party Cookies

(1) Google Analytics

Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA („Google“). Google Analytics verwendet eine spezifische Form von „Cookies“, Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse Ihrer Benutzung der Website ermöglichen. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website werden in der Regel an einen Server von Google in den USA übertragen und dort gespeichert. Wir weisen Sie darauf hin, dass auf dieser Website Google Analytics um den Code „gat._anonymizeIp();“ erweitert wurde, um eine anonymisierte Erfassung von IP-Adressen (sog. „IP-Masking“) zu gewährleisten. Durch die IP-Anonymisierung auf dieser Website wird Ihre IP-Adresse von Google innerhalb des Gebiets der EU bzw. der Vertragsstaaten der Europäischen Wirtschaftsgemeinschaft gekürzt. Nur in Ausnahmefällen wird die volle IP-Adresse an einen Server von Google in den USA übertragen und dort gekürzt.

Google wird diese Informationen in unserem Auftrag benutzen, um Ihre Nutzung dieser Website auszuwerten, um Reports über die Websiteaktivitäten zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen gegenüber dem Websitebetreiber zu erbringen. Die im Rahmen von Google Analytics von Ihrem Browser übermittelte IP-Adresse wird nicht mit anderen Daten von Google zusammengeführt. Sie können die Speicherung der Cookies durch eine entsprechende Einstellung Ihrer Browser-Software verhindern, siehe oben Ziffer 7. c. Sie können darüber hinaus die Übertragung der durch das Cookie erzeugten und auf Ihre Nutzung der Website bezogenen Daten (inkl. Ihrer IP-Adresse) an Google sowie die Verarbeitung dieser Daten durch Google verhindern, indem sie das unter dem Link tools.google.com/dlpage/gaoptout verfügbare Browser-Plug-in herunterladen und installieren. Nähere Informationen zu Nutzungsbedingungen und Datenschutz finden Sie unter http://www.google.com/analytics/terms/de.html bzw. unter http://www.google.com/intl/de/analytics/privacyoverview.html .

(2) Google Maps

Wir verwenden auf unseren Websites die Google Maps API, um geographische Informationen visuell darzustellen. Bei der Nutzung von Google Maps werden von Google auch Daten über die Nutzung der Maps-Funktionen durch Besucher der Webseiten erhoben, verarbeitet und genutzt. Nähere Informationen über die Datenverarbeitung durch Google können Sie den Datenschutzhinweisen von Google entnehmen. Dort können Sie im Datenschutzcenter auch Ihre Einstellungen verändern, so dass Sie Ihre Daten verwalten und schützen können.

(3) Google DoubleClick

Wir verwenden auf unseren Websites die Funktion DoubleClick von Google, um die Nutzung der Website auszuwerten und es Google und anderen Werbetreibenden, die mit DoubleClick zusammenarbeiten, zu ermöglichen, Ihnen nutzerrelevante Werbung präsentieren zu können. Hierzu wird ein Cookie auf der Festplatte Ihres Computers installiert. Mithilfe dieses Cookies wird Ihrem Browser eine pseudonyme Identifikationsnummer zugewiesen und es werden Informationen über die in Ihrem Browser eingeblendete Werbung und deren Aufruf gesammelt. Die durch den Cookie gesammelten Informationen über Ihre Nutzung von Websites werden in der Regel an einen Server von Google in den USA übertragen und dort gespeichert. Auf Basis der gesammelten Informationen werden Ihrem Browser interessensrelevante Kategorien zugewiesen. Diese Kategorien werden zur Schaltung von interessensbezogener Werbung genutzt.

Neben der Änderung Ihrer Browsereinstellungen können Sie auch mithilfe eines Browser-Plug-in das DoubleClick-Cookie dauerhaft deaktivieren. Mit dem Plug-in bleiben Ihre Deaktivierungseinstellungen für diesen Browser erhalten, auch wenn Sie sämtliche Cookies löschen. Das Browser-Plug-in für eine dauerhafte Deaktivierung erhalten Sie hier: www.google.com/settings/ads/plugin

Mit der Nutzung unserer Website willigen Sie ein, dass das DoubleClick-Cookie eingesetzt und damit Nutzungsdaten von Ihnen in der zuvor beschriebenen Art und Weise zu dem genannten Zweck erhoben, gespeichert und genutzt werden. Weiter willigen Sie ein, dass Ihre Daten in Cookies über das Ende der Browser-Sitzung hinaus gespeichert werden und beispielsweise bei Ihrem nächsten Website-Besuch wieder aufgerufen werden können. Diese Einwilligung können Sie jederzeit mit Wirkung für die Zukunft durch die Löschung des DoubleClick-Cookies und die dauerhafte Deaktivierung widerrufen.

Mehr Informationen über die von uns eingesetzten Cookies finden Sie in unserer Cookie Richtlinie.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Informationen für Datenschutzverantwortliche

Damit für alle Mitarbeiter der Datenschutz einfach und gut funktioniert, gibt es hier für wichtige Themen Informationen.

Hilfreicher Link zur DSGVO zum Nachlesen: https://dsgvo-gesetz.de

Die Grundsätze des Datenschutzes

nach Artikel 5 der DSGVO:

- Rechtmäßigkeit der Daten. Ohne Rechtmäßigkeit keine Nutzung von personenbezogenen Daten. Es gibt 6 verschiedene Arten der Rechtmäßigkeit.
- Zweckbindung. Legitime Daten dürfen nur für eindeutige Zwecke genutzt werden.
- Datenminimierung. Nur die für den Zweck erforderlichen Daten sind erlaubt.
- Richtigkeit. Die Daten müssen dem Zweck entsprechend richtig sein.
- Speicherbegrenzung. Daten dürfen solange wie notwendig genutzt werden.
- Integrität und Vertraulichkeit. Daten müssen vor Beschädigung, Verlust und gegen Unbefugte geschützt werden.
- Rechenschaftspflicht. Gegenüber Betroffenen und der Behörde gibt es verschiedene Pflichten über Nachweise.

Vertraulichkeit: Die Pflicht

Artikel 29 DSGVO sagt: Jede unterstellte Person (bei Verantwortlichen und auch bei Auftragsverarbeitern), die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Diese Weisung und die Verpflichtung zur Vertraulichkeit (auch über das Ende des Arbeitsverhältnisses hinaus) muss vereinbart werden.

Bei MitarbeiterInnen im Dienstvertrag, bei externen Personen, die Zugang zu personenbezogenen Daten haben könnten (Steuerberater, IT etc.) im Vertrag.

Einhaltung Datenschutz - Vertrag für externe Auftragnehmer

Der Auftragnehmer / die Auftragnehmerin erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne der geltenden Datenschutzgesetze verpflichtet hat. Der Auftragnehmer / die Auftragnehmerin bestätigt, dass alle für ihn tätigen Personen die rechtlichen Vorgaben der DSGVO und des Datenschutzgesetzes in der geltenden Fassung kennen und einhalten. Die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen bleibt auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer/ bei der Auftragnehmerin aufrecht.

Einhaltung Datenschutz - Vertrag für MitarbeiterInnen

VERPFLICHTUNGSERKLÄRUNG für Datenschutz und Vertraulichkeit:

Im Zuge Ihres Dienstverhältnisses erhalten Sie voraussichtlich Kenntnis über Personen und personenbezogene Umstände und alle diese Daten sind absolut vertraulich zu behandeln.
Personenbezogene Daten dürfen Sie nur auf Weisung Ihrer Vorgesetzten verwenden.
Mit Ihrer Unterschrift verpflichten Sie sich

- das Datengeheimnis gemäß den Bestimmungen der DSGVO und des Datenschutzgesetzes in den geltenden Fassungen zu wahren,
- zu absoluter Verschwiegenheit über alle Ihnen anlässlich Ihrer Tätigkeit bekannt gewordenen, nicht von den zuständigen Personen ausdrücklich als unbedenklich bezeichneten Informationen,
- diese Verpflichtung auch nach Beendigung dieses Vertragsverhältnisses und dem Ausscheiden aus dem Unternehmen einzuhalten.

Sie nehmen durch Ihre Unterschrift zur Kenntnis, dass Verstöße gegen diese Verpflichtung zu strafrechtlicher Verfolgung führen können, schadenersatzpflichtig machen und auch arbeitsrechtliche Folgen haben können (z.B. Entlassung gemäß § 27 Angestelltengesetz).
(ArbeitgeberIn und ArbeitnehmerIn erhalten jeweils eine unterzeichnete Version)

Übersicht über Verarbeitungen

DSGVO Art 30 fordert ein „Verzeichnis aller Verarbeitungen personenbezogener Daten".
Es ist die Basisinformation über die Datenverarbeitungen und aller Maßnahmen.
Das Verzeichnis ist die Grundlage aller Argumentationen, warum die Maßnahmen als angemessen bewertet werden.

Das Verzeichnis wird vom Verantwortlichen für alle Verarbeitungen geführt, für die er Zwecke und Mittel definiert.
Ebenfalls wird ein Verzeichnis auch von Auftragsverarbeitern für deren Verarbeitungen im Auftrag von Verantwortlichen geführt.

Rechte der Betroffenen

DSGVO Art 15-22

Hinweis: Für jedes Recht ist die Prüfung der Identität der Person, die dieses Recht einfordert wichtig. Falls berechtigte Zweifel an der Identität der berechtigten Person bestehen, muss ein Nachweis gefordert werden.

Idealerweise haben wir

1) eine Adresse
2) eine E-Mail-Adresse
3) eine Telefonnummer

Diesen Identitätsnachweis kann man (ohne Portal mit Registrierung und Profil) am besten mit einer Rückfrage auf einem anderen Kanal absichern. Hat jemand per E-Mail um Auskunft gebeten, kann man telefonisch rückfragen, ob die Anfrage tatsächlich vom Betroffenen stammt.

Die Zusendung einer Kopie eines amtlichen Dokuments, das mit Sicherheit nur der Berechtigte hat ist ebenfalls eine Möglichkeit die Identität zu prüfen. Nach der Prüfung sollte das Ergebnis protokolliert werden und die Kopie unbedingt gelöscht, damit nicht die Kopie zu einem sensiblen Datenbestand wird.

Auskunftsrecht der betroffenen Person Art.15

Betroffene haben Recht auf Bestätigung, ob Daten verarbeitet werden.
Wenn ja, so haben sie ein Recht auf Auskunft mit folgenden Inhalten:

- Die gespeicherten personenbezogenen Daten
- Zweck der Verarbeitung
- Kategorie der Daten
- Empfänger / Kategorien der Empfänger
- Dauer / Kriterien für die Dauer
- Information über das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Beschwerderecht
- Herkunft der Daten
- Das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, der Logik, Tragweite und Auswirkungen
- Bei Übermittlung an ein Drittland / internat. Organisation die geeigneten Garantien

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Da Betroffene nicht wissen, welche Daten in welchem Unternehmen der Gruppe verarbeitet werden, kümmern wir uns im Falle einer Auskunftsanfrage um einen Rundlauf, der alle personenbezogenen Daten aller Dienstleiter von wow! solution beauskunftet.

Recht auf Berichtigung Art 16

Betroffene haben das Recht auf unverzügliche Berichtigung und Vervollständigung.

Für den Fall, dass Daten rechtmäßig weitergegeben wurden, informieren wir bei gewünschter Berichtigung auch die Empfänger dieser Daten über den Berichtigungsauftrag.

Recht auf Löschung Art 17

Ein Prozess für das Recht auf Löschung sollte mit einer vorherigen Auskunft kombiniert werden, um zu vermeiden, dass Betroffene Daten löschen lassen, die sie eigentlich nicht löschen wollten, weil sie nicht mehr wussten, welche Daten verarbeitet werden.

Für den Fall, dass vom Betroffenen eine Löschung gefordert ist und diese nicht unverzüglich möglich ist, ist die Verarbeitung dieser Daten nach Datenschutzanpassungsgesetz §4(2) durch den Verantwortlichen unverzüglich einzuschränken.

Für den Fall, dass Daten rechtmäßig weitergegeben wurden, informieren wir bei gewünschter Löschung auch die Empfänger dieser Daten über den Löschauftrag.

Recht auf Einschränkung der Verarbeitung Art 18

Einschränkung bedeutet, dass die Daten unverändert aufbewahrt und nicht verarbeitet werden dürfen.

Betroffene haben Recht auf Einschränkung der Verarbeitung in 4 Situationen:

1) Die Richtigkeit der Daten wird bestritten
2) Die Daten sind unrechtmäßig und d. Betroffene verlangt Einschränkung statt Löschung
3) Die Daten werden vom Verantwortlichen nicht mehr benötigt, vom Betroffenen aber für Rechtsansprüche benötigt
4) Der Betroffene hat Widerspruch gegen berechtigte Interessen eingelegt, solange das überwiegende Interesse nicht feststeht

Für den Fall, dass Daten rechtmäßig weitergegeben wurden, informieren wir bei gewünschter Einschränkung auch die Empfänger dieser Daten über den Einschränkungsauftrag.

Recht auf Datenübertragbarkeit Art 20

Betroffene dürfen Daten, die sie uns bereitgestellt haben in strukturierter, gängiger, maschinenlesbarer Form fordern, wenn

1) die Daten mit Hilfe automatisierter Verfahren verarbeitet werden und
2) die Verarbeitung auf Basis einer Einwilligung oder eines Vertrages erfolgt

Auch die direkte Übertragung an einen anderen Verantwortlichen ist durchzuführen.

Widerspruchsrecht Art 21

Betroffene Personen dürfen Widerspruch einlegen bei

1) Datenverarbeitung aus 6.1.e Öffentlichem Interesse
2) Datenverarbeitung aus 6.1.f Berechtigtem Interesse
3) Datenverarbeitung aus 6.1.e oder 6.1.f gestützt auf Profiling

aus ihrer besonderen Situation.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Widerspricht die Person, werden die Daten nicht mehr verarbeitet, es sei denn, der Verantwortliche kann zwingende, überwiegende Interessen nachweisen oder Rechtsansprüche.

Betroffene Personen dürfen Widerspruch einlegen bei

1) Datenverarbeitung für Direktwerbung oder
2) Datenverarbeitung für Direktwerbung gestützt auf Profiling

Widerspricht die Person, werden die Daten nicht mehr verarbeitet.

Profiling bedeutet, dass bestimme Aspekte einer Person analysiert oder vorhergesagt werden. Details siehe Art 4, Begriff 4. „Profiling“

Link: https://dsgvo-gesetz.de/art-4-dsgvo/

Widerspruchsrecht gegen automatisierte Entscheidungsfindung und Profiling Art 22

Derzeit nicht anwendbar, da weder automatisierte Entscheidungsfindung noch Profiling durch wow! solution erfolgt.

Automatisierte Entscheidungsfindung darf aus 3 Bedingungen (Absatz 2 a,b,c) erfolgen, wenn die Absätze 3) und 4) berücksichtig werden. Siehe Link

Profiling bedeutet, dass bestimme Aspekte einer Person analysiert oder vorhergesagt werden. Siehe Art 4, Begriff 4. „Profiling“

Link zum Artikel: https://dsgvo-gesetz.de/art-22-dsgvo/

Einwilligungen

DSGVO Art 7

Beruht die Verarbeitung auf einer Einwilligung, muss die Einwilligung nachweisbar sein.

ACHTUNG: Da sich diese Pflicht auf die Verarbeitung (nicht auf die Erhebung) bezieht, gilt sie bei jeder Verarbeitung, egal, wann die Daten erhoben worden sind.

Eine Einwilligung muss

freiwillig

für den konkreten Fall

in informierter Weise

unmissverständlich

durch Auswahl / Erklärung oder Verhaltensweise geschehen.

Eine Einwilligung setzt eine aktive Handlung voraus. Inaktivität zählt nicht als Einwilligung. Eine Vorbelegung von Klickboxen ist nicht geeignet.

Wenn mehrere Sachverhalte dargestellt werden, müssen das Ersuchen um Einwilligung klar zu unterscheiden sein.

Bezieht sich die Verarbeitung auf mehrere Zwecke, soll für jeden Zweck eine Einwilligung gegeben werden. (Erwägungsgrund 32)

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Widerruf

Eine Einwilligung kann jederzeit widerrufen werden.

Der Widerruf muss so einfach wie die Einwilligung sein.

Der Widerruf gilt ab diesem Zeitpunkt.

Koppelungsverbot

Eine Vertragserfüllung oder eine Dienstleistung darf nicht von einer auf Freiwilligkeit basierenden Verarbeitung abhängig gemacht werden, die nicht für die Erfüllung des Vertrages notwendig ist.

Zwanglos

Die betroffene Person hat nur dann eingewilligt, wenn bei Verweigerung der Einwilligung keine Nachteile erwartet werden.

Zur Orientierung: https://www.lda.bayern.de/media/oh_einwilligung.pdf

Risikobewertung

Mit der DSGVO werden Maßnahmen gefordert, die dem Risiko für die Betroffenen angemessen sind. Eine praktikable Methode für die Bewertung des Risikos ist folgende:

1) Die Kritikalität der Daten steht im Vordergrund, weil man sie einschätzen kann
2) Die Wahrscheinlichkeit eines Schadens ist sehr schwierig zu bewerten – wir vernachlässigen sie. Der Unterschied in den Maßnahmen ist marginal.

Damit es praktisch anwendbar ist, verwenden wir 5 Klassen von Daten:

1) Öffentliche Daten: Kein Risiko
2) Daten, für die jemand berechtigte Vertraulichkeits-Interessen hat.
   Beispiel: „interne Daten“ = Namen und deren Funktion im Unternehmen.
   Risiko bei nicht widmungsgemäßer Verwendung: Gering
3) Daten, geeignet das Ansehen zu schädigen. „Insider-Infos“ und Daten über Verhaltensmängel, die zu sozialer Ablehnung führen können.
   Risiko: Mittel - Hoch, abhängig von der Wichtigkeit des Ansehens für die Person
4) Daten, geeignet die Existenz zu bedrohen. Nicht tolerierte Eigenschaften.
   Risiko: Hoch. Langfristiger Schaden, Verlust des Berufs, Ausschluss aus Gruppen
5) Daten, die Leib & Leben gefährden. Emotionale, unberechenbare Konsequenzen.
   Risiko: Sehr hoch

Für eine praktikable Risikobewertung stellt man die Frage: „Was bedeutet der worst case für die Betroffenen, zB für meinen Partner / für Kinder“?

Für den Schutz der Daten gegen die Risiken sind „Technische & Organisatorische Maßnahmen festzulegen.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Checkliste für „Risiko / hohes Risiko“

Für den Fall, dass in der Zukunft Daten mit Risiko / hohem Risiko verarbeitet werden sollten, gibt es eine Checkliste mit 18 Fragen zu detaillierten Bewertung.

Diese Checkliste wird sowohl bei einer Schutzverletzung (zum aktuellen Fall) oder bei einer Datenschutzfolgenabschätzung (im Projekt) verwendet.

Vor der Risikobewertung klärt man die Fakten der Schutzverletzung, um genau zu wissen, a) wer die konkret Betroffenen sind und b) welches Risiko eintreten kann.

Man schätzt den worst case ein, der konkret für die Betroffenen
a) im Einzelfall (wenn spezifische Risiken bestehen) oder
b) für alle Betroffenen (wenn alle gleich betroffen sind) eintreten kann:

RISIKO	Konkrete Beschreibung der Auswirkung im worst case
Physische Schäden	Beschreibung:
Materielle Schäden	Beschreibung:
Immaterielle Schäden	Beschreibung:
Diskriminierung	Möglich JA / NEIN
Identitätsdiebstahl	Möglich JA / NEIN
Identitätsbetrug	Möglich JA / NEIN
Finanzieller Verlust	Schätzung maximal:
Rufschädigung	Beschreibung:
Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten	Möglich JA / NEIN
Unbefugte Aufhebung der Pseudonymisierung	Möglich JA / NEIN
Erhebliche wirtschaftliche Nachteile	Nachteile beschreiben:
Erhebliche gesellschaftliche Nachteile	Nachteile beschreiben:
Betroffenen können um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren	Welche Rechte können beschnitten werden:
Verarbeitung von Art 9 / Art 10 Daten	JA / NEIN
Bewertung von Aspekten nach Art 22 / Profiling um persönliche Profile zu erstellen oder zu nutzen	Welche Aspekte sind in Daten enthalten:
Verarbeitung von personenbezogenen Daten besonders schutzbedürftiger Personen, insbesondere Kinder	JA / NEIN
Verarbeitung einer großen Menge von Daten	Menge der Daten:
Verarbeitung der Daten einer großen Anzahl betroffener Personen	Anzahl der Betroffenen:

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Notfall / Schutzverletzung

Nach Auflistung aller Bewertungen der 18 Risiken protokolliert die Geschäftsführung der für die Verarbeitung Verantwortlichen die Gesamteinschätzung als

KEIN RISIKO für Betroffene

RISIKO für Betroffene

HOHES Risiko für Betroffene

Bei der Bewertung „RISIKO für Betroffene“ muss nach Art 33 eine Meldung an die Behörde erfolgen.

Für diese Meldung enthält folgende Informationen:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten,
2. soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen,
3. der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
4. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
5. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
6. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und
7. gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Link zum Artikel: https://dsgvo-gesetz.de/art-33-dsgvo/

Bei der Bewertung „HOHES RISIKO für Betroffene“ muss eine Benachrichtigung der betroffenen Person nach Art 34 erfolgen. https://dsgvo-gesetz.de/art-34-dsgvo/

Diese Benachrichtigung muss nicht erfolgen, wenn

a) die Daten durch Sicherheitsmaßnahmen für Unbefugte unzugänglich sind oder
b) nachfolgende Maßnahmen das hohe Risiko wahrscheinlich nicht mehr besteht oder
c) wegen Unzumutbarkeit über eine öffentliche Bekanntmachung informiert wird

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Regeln für sicheres Verhalten

Eine organisatorische Maßnahme für den Datenschutz ist die Erstellung einer Liste von Regeln, um sie schulen zu können.

95% aller Schutzverletzungen passieren durch Verhaltensfehler.

Mitarbeiterinnen brauchen eine Einschulung zu diesen Regeln, denn Missverständnisse und Fehler sind gefährlich. Betrüger nutzen die Unsicherheit der MitarbeiterInnen aus.

Hier die wichtigsten Regeln für alle MitarbeiterInnen im Umgang mit Technologie, im privaten Bereich und im Unternehmen:

1) Für jedes Login-System braucht es ein eigenes Passwort. Ein Passwort für mehrere Systeme zu verwenden, ist gefährlich, wenn ein Passwort gestohlen wurde.
   Man muss das Passwort nicht regelmäßig ändern, (Wir ändern ja auch nicht regelmäßig einen guten Schlüssel, nur, weil jemand ihn nachgemacht haben könnte). Wichtig ist, dass das Passwort gut ist: Ca. 16 Zeichen und kein Wort, das man erraten kann.

2) Das Passwort darf kein Wort aus dem Wörterbuch, kein Geburtsdatum und kein Name sein. Es muss Groß und Kleinbuchstaben enthalten, mindestens 1 Zahl und ein Sonderzeichen (eines, dass man auch am Smartphone findet).
   Ein Tipp: Bilden Sie Ihre Passworte mit einem Satz.
   So kann man sich unendlich viele Passworte merken

3) Bei Eingabe eines Passworts oder eines PINs darf niemand zusehen.

4) Updates („Patches“) für die Software immer sofort einspielen.

5) Backups machen und an einem sicheren Ort aufbewahren.

6) Links in Mails nur anklicken, wenn Sender bekannt und das Mail erwartet wird. Denn die Sender könnten Sie auf eine falsche Seite locken, um Ihr Passwort abzufangen.
   Besser ist, die Seite über Google oder gespeicherte Favoriten aufzurufen.

7) Makros in Dateien nie sofort aktivieren. Erst wenn die benötigte Funktion leidet.

8) Bei Security Warnings IMMER in der IT nachfragen

9) Fremde USB-Geräte nicht am Firmen-PC anstecken, Daten besser per Mail fordern. Mails werden am Server und am Endgerät geprüft.

10) Vorsicht = Rückfragen: Wenn eine sehr ungewöhnliche Sache von Ihnen „streng geheim“ gefordert wird und der Auftraggeber nicht erreichbar ist. Betrüger arbeiten so.

11) Vorsicht = Rückfragen, wenn man Sie stark unter Druck setzt, zB „sehr dringend“ und außergewöhnliche Handlungen gefordert werden (zB Kontoänderungen, hohe Überweisungen oder die Herausgabe einer wichtigen Information).

12) Anti-Malware-Scan laufen lassen (1 x je Woche). Fragen Sie Ihre IT, wie das geht.

13) Rechnen Sie immer mit einem Taschendieb. Achten Sie auf Smartphone & Laptop

14) E-Mails mit heiklen Daten: Verteiler doppelt prüfen vor dem Versand. Ein Versandfehler an eine falsche Adresse ist ein schwer wiegender Fehler.

15) E-Mails an viele Personen, die sich nicht kennen: Immer alle in BCC schreiben, denn die E-Mail-Adressen der Empfänger dürfen den anderen Empfängern nicht einfach öffentlich gemacht werden.

16) Wenn Sie Unbekannte in Bereichen treffen, wo Personendaten aufbewahrt werden, fragen Sie nach dem zuständigen Mitarbeiter, für den die Person im Haus tätig ist. Fragen Sie bei dem Mitarbeiter dann nach, ob das in Ordnung ist. Diebe arbeiten so.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Verantwortliche, Auftragsverarbeitung & Dienstleister

Die Unternehmensleitung hat die Verantwortung für die personenbezogenen Daten im Unternehmen. Verantwortliche bestimmen die Zwecke und Mittel der Verarbeitung.

Die Unternehmensleitung muss zuerst prüfen, ob Beauftragte „geeignete Garantien“ für den Schutz der Daten vorweisen können. Es ist deshalb wichtig, dass Dienstleister im Vertrag oder in den verbindlichen AGBs und der Datenschutzerklärung dokumentieren, wie sie den Datenschutz sicherstellen.

Ein Widerspruch in AGBs oder Datenschutzerklärung zu den geltenden Datenschutzgesetzen muss auf seine Bedeutung im konkreten Fall überprüft werden.

Von den Verantwortlichen dürfen nur Unternehmen und Personen für die Verarbeitung personenbezogener Daten beigezogen werden, die vertraglich zum geltenden Datenschutzrecht verpflichtet wurden. Diese Verträge sind als Nachweis aufzubewahren.

Zwei Arten Auftrag: Auftragsverarbeiter und Verantwortliche

Auftragsverarbeitung

bedeutet, dass der Verantwortliche die volle Verantwortung für die Datenverarbeitung behält und der Auftragsverarbeiter nach strikten Vorgaben und ohne jeden Spielraum was Mittel und Zwecke anbelangt agieren muss.

Ein spezieller Vertrag nach Art 28 ist verpflichtend.

(Zur Veranschaulichung: Wenn mehrere Auftragsverarbeiter ihre Aufträge zeitgleich und ohne voneinander zu wissen abarbeiten, ist verständlich, warum hier die Aufträge exakt vom Verantwortlichen zu vergeben sind.)

Der Auftrag bezieht sich dabei auf die Verarbeitung der personenbezogenen Daten.

Wenn ein Auftragsverarbeiter den Vertrag verlässt, indem er eine Vereinbarung bricht, wird er automatisch zum Verantwortlichen

Eine Auftragsverarbeitung liegt zum Beispiel regelmäßig vor bei:

- Telefonmarketing und andere Callcenterleistungen soweit nicht vom Unternehmen selbst durchgeführt.
- externer Datenhaltung, insbesondere beim teilweisen oder gesamten Outsourcing eines Rechenzentrums.
- Implementierung neuer IT-Systeme mit Migration bestehender Datenbanken durch den Auftragnehmer.
- Nutzung von Cloudsystemen zur Personal- oder Kundenverwaltung.
- externe Druckdienstleistung.
- manuellem oder elektronischem Archivierungsservice.
- Aktenvernichtung, Vernichtung von Datenträgern.

„Wer keinen spezifischen Auftrag hat, ist Verantwortlicher“

Steuerberater und Rechtsanwälte die durch ihre Standesregeln frei von allen Weisungen sind, sind voll selbst Verantwortliche mit allen Pflichten gegenüber den Betroffenen.
Für weisungsfreie Berufsgruppen und alle Auftragnehmer, die nicht eine Auftragsverarbeitung an personenbezogenen Daten durchführen, ist ein Vertrag sinnvoll, der die Pflichten bei Berührung mit personenbezogenen Daten regelt.

Verträge, die keinen Auftrag zur Verarbeitung beschreiben

Sollte ein Unternehmen, das keinen spezifischen Auftrag zur Verarbeitung von personenbezogenen Daten hat, unbedingt einen Vertrag abschließen wollen, ist das kein Nachteil, wenn sich alle Inhalte des Vertrages nach Art 28. vereinbaren lassen.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Verträge sind auch Bindungsinstrumente: Wer einen Vertrag eingeht, ist in einer engeren Beziehung gebunden als Verantwortliche, die nach Prüfung ihrer geeigneten Garantien ohne Art.28 Vertrag Daten für Verantwortliche verarbeiten.

Hier finden Sie Beschreibungen, wo keine Auftragsverarbeitung gesehen wird:

https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf

Siehe Seite 22 und 23, Überschrift 1.3 und folgende.

Gemeinsam Verantwortliche: Kooperationen

Die DS-GVO geht in Art. 4 Nr. 7 davon aus, dass Verantwortlicher derjenige ist, der »allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (...)«.

Auftragsverarbeiter ist diejenige Person oder Stelle, die (so Art. 4 Nr. 8) »personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet«.

Aus Art. 4 Nr. 7 DS-GVO ergibt sich, dass neben der alleinigen Verantwortung auch ein arbeitsteiliges Zusammenwirken möglich ist.

Ohne ein solches Zusammenarbeiten kommen selbst kleinere und mittlere Unternehmen heute nur noch selten aus, denn es ermöglicht die Inanspruchnahme besonderer Kenntnisse und Erfahrungen.

Dabei ist das Zusammenwirken nicht zahlenmäßig beschränkt: Art. 26 DS-GVO, die Kernbestimmung über gemeinsam Verantwortliche, nennt »zwei oder mehr Verantwortliche« und verzichtet auf eine Obergrenze.

Cloud & Software: Prüfen gegen Vertragsvorlage

Eine Unternehmensleitung, die personenbezogen Daten verarbeitet, ist laut Artikel 32 für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten verantwortlich, was Vertraulichkeitserklärungen und die Einhaltung der Datenschutzgesetze bei den Auftragnehmern erfordert.

Bei Cloud-Diensten, wo Auftragsverarbeiter ihre Kompetenzen mittels AGBs und Datenschutzerklärungen darstellen, muss geprüft werden:

1) Ist das Land der Niederlassung des Providers genehmigungsfrei (EWR bzw. Art 45)?
2) Welches Risiko für die Betroffenen besteht, wenn der Cloud-Dienst entgegen den Beschreibungen (AGBs, Datenschutzerklärung) agiert?
3) Ist die Webseite (auf der personenbezogene Daten verarbeitet werden), die App oder die Software ausreichend und dem Risiko für die Betroffenen durch Nachweis geeigneter Garantien angemessen sicher (zB durch Nachweise externer Zertifizierer oder Tests in Fachmedien dokumentiert)?

Im Dokument „VertragAuftragsverarbeitung_VV-AV-DSGVO“ sind alle Varianten abbildbar.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Datenschutz & MitarbeiterInnen

Wer neu ins Unternehmen kommt, bekommt 4 Informationen zum Datenschutz:

1. Vertraulichkeitserklärung im Dienstvertrag
2. Eine Einweisung zum Datenschutz durch Selbststudium des Datenschutz-Handbuchs
3. Erklärung der Regeln für sicheres Verhalten durch die / den Vorgesetzten
4. Awareness-Schulung über den Sinn der Regeln

In den folgenden Jahren finden diese 3 organisatorischen Maßnahmen jährlich statt:

1. Besprechung und Bewertung der Erfahrungen mit Regeln für sicheres Verhalten im Team
2. Awareness-Schulung über den Sinn der Regeln
3. Information an die Unternehmensleitung über die Bewertung

Daten in Drittländer & an internationale Organisationen

Wenn Daten außerhalb des Europäischen Wirtschaftsraums übermittelt werden sollen, gibt es zwei Prüfungen:

1) Das Land, in das die Daten übermittelt werden sollen
2) Die geeigneten Garantien des Verantwortlichen / Auftragsverarbeiters, dem die Daten übermittelt werden

Hier finden die Artikel 44-49 Anwendung.

Im Vertrag, den Sie mit dem Verantwortlichen / Auftragsverarbeiter vereinbaren müssen, finden Sie alle erforderlichen Fragen.

Siehe Vertragsvorlage „VertragAuftragsverarbeitung_...“ unter der
Überschrift (2) Ort der vorgesehenen Verarbeitung von Daten“

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Checkliste technische & organisatorische Maßnahmen

TOM Vertraulichkeit

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen
  - ☐ Schlüssel
  - ☐ Magnet- oder Chipkarten
  - ☐ elektrische Türöffner
  - ☐ Empfang/Portier
  - ☐ Sicherheitspersonal
  - ☐ Alarmanlagen
  - ☐ Videoanlagen

- Zugangskontrolle: Schutz vor unbefugter Datennutzung
  - ☐ Passworte & Passwortpolicy
  - ☐ automatische Sperrmechanismen, Verzögerung für wiederholte Fehleingaben
  - ☐ Zwei-Faktor-Authentifizierung
  - ☐ Verschlüsselung von Datenträgern
  - ☐ Clean Desk

- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen innerhalb des Systems
  - ☐ Standard-Berechtigungsprofile
  - ☐ „need to know“ als Prinzip
  - ☐ Standardprozess für Berechtigungsvergabe
  - ☐ Protokollierung von Zugriffen
  - ☐ periodische Überprüfung der vergebenen Berechtigungen
  - ☐ periodische Überprüfung der administrativen Benutzerkonten
  - ☐ Freigaben / 4-Augen-Prinzipien
  - ☐ mehrteilige Passworte bei hohem Risiko

- Datensparsamkeit
  - ☐ Bewertung von personenbezogenen Daten auf Möglichkeiten der Anonymiserung
  - ☐ Datensparsamkeit wird in Projekten thematisiert

- Pseudonymisierung
  - ☐ Identifikationsmerkmale der personenbezogenen Daten werden standardmäßig entfernt und gesondert aufbewahrt.

- Klassifikationsschema für Daten
  - ☐ Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich)
  - ☐ Risikoklassen nach Impact auf betroffene Personen (öffentlich/berechtigtes Interesse/Ansehen/Existenz/Leib&Leben).

- Awareness-Maßnahmen für die Bildung eines Datenschutz-Bewusstseins
  - ☐ Jährliche Awareness-Schulung

TOM Integrität

- Weitergabekontrolle / Transportkontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - ☐ Verschlüsselung
  - ☐ Virtual Private Networks (VPN)
  - ☐ elektronische Signatur
  - ☐ USB-Ports managen
  - ☐ Schnittstellenkontrolle
  - ☐ Data Loss Prevention

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
  - ☐ Authentifizierung / Identitätsmanagement
  - ☐ Zugriffsprotokollierung bei nur lesendem Zugriff
  - ☐ Zugriffsprotokollierung bei Änderungen
  - ☐ Zugriffsprotokollierung bei Löschung
  - ☐ Unveränderbarkeit der Zugriffsprotokolle
  - ☐ Dokumentenmanagement
  - ☐ Datenschutzfreundliche Voreinstellungen

- Anti-Malware-Protection
  - ☐ auf allen Geräten
  - ☐ Virenschutz-Updates automatisch
  - ☐ Virenschutz-Scan (durch manuellen Aufruf)
  - ☐ Sandbox für verdächtige Dateien

- Awareness-Maßnahmen zur Bewusstseinsbildung
  - ☐ Informationen über Vorfälle mit verdächtigen Sendungen
  - ☐ Informationen über Betrugsfälle
  - ☐ Informationen über neue Methoden Cybercrime
  - ☐ Analyse der Sinnhaftigkeit / Wirksamkeit / Belastung durch/von Regelungen

TOM Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust,
  - ☐ Sicherungskonzept (online/offline; on-site/off-site)
  - ☐ unterbrechungsfreie Stromversorgung
  - ☐ Virenschutz
  - ☐ Firewall
  - ☐ Security Checks auf Infrastruktur- und Applikationsebene
  - ☐ Mehrstufiges Sicherungskonzept mit Auslagerung der Sicherungen
  - ☐ Ausweichrechenzentrum
  - ☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

- Rasche Wiederherstellbarkeit
  - ☐ Meldewege & Notfallpläne
  - ☐ Incident Response / Emergency Response
  - ☐ Disaster Recovery Konzept
  - ☐ Business Continuity Management

- Löschung
  - ☐ Personenbezogene Daten mit Löschfrist erfassen / Projektstandard
  - ☐ Metadaten
  - ☐ Logfiles
  - ☐ Daten-Architektur zur Machbarkeit der Löschung
  - ☐ Einschränkung von Daten bei nicht unverzüglicher Löschbarkeit

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

TOM Systematik

- Datenschutz-Management
  - ☐ Statement der Unternehmensleitung zum Datenschutzziel
  - ☐ Datenschutzstrategie
  - ☐ Datenschutzbeauftragung
  - ☐ Projektstandards für Datenschutz
  - ☐ Reifegrade Datenschutz für relevante Teams (IT, HR, Zutritt...) (undefiniert/Experten/definiert/nachhaltig/gemanagt/optimal)
  - ☐ Experten Schulungen
  - ☐ Mitarbeiter Schulungen
  - ☐ Assessments / Audits zur Überprüfung des Systems
  - ☐ Bewertung der Wirksamkeit des Systems
  - ☐ Management Report
  - ☐ Zertifizierung
  - ☐ Incident-Response-Management für Vorfall / Notfall / Krise

- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers
  - ☐ Privacy by default bei der Vertragsgestaltung
  - ☐ Auftragsmanagement für Datenschutzaufträge
  - ☐ Auswahl der Auftragsverarbeiter Art 28
  - ☐ Auswahl der gemeinsam Verantwortlichen Art 26
  - ☐ Vorabüberzeugungspflicht
  - ☐ Nachkontrollen

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Checkliste Jahresüberprüfung

Jährlich wird die beschriebene Datenschutz-Situation überprüft und auf ihre Angemessenheit bewertet. Diese Checkliste hilft Ihnen dabei:

Planung: Die Überprüfung findet im Monat ..... statt.

Zuständig: Verantwortlich für die Überprüfung ist: .....

Folgende Fragen werden gestellt und protokolliert:

Handbuch

1) Ist das Handbuch richtig?

Strategie

2) Ist die Strategie für den Datenschutz noch gültig?

Datenschutz Auftrag

3) Macht die Unternehmensleitung den Datenschutz selbst oder gibt es einen schriftlichen Auftrag an eine interne oder externe Person?
4) Gibt es eine(n) Datenschutzbeauftragte(n) im Sinne der DSGVO Abschnitt 4?
5) Ist d. Datenschutzbeauftragte (DSB) der Behörde gemeldet?
6) Wird d. DSB bei der Erhebung von Daten bei Betroffenen genannt?
7) Wird d. DSB genannt, wenn Daten nicht bei Betroffenen erhoben werden?
8) Wird d. DSB im Verfahrensverzeichnis d. Verantwortlichen Art. 30 genannt?
9) Wird d. DSB im Verfahrensverzeichnis d. Auftragsverarbeiter Art. 30 genannt?
10) Wird d. DSB in der Meldevorlage für Schutzverletzung Art. 33 genannt?
11) Wird d. DSB bei Datenschutzfolgenabschätzung Art. 35 zu Rate gezogen?
12) Wird d. DSB im Zuge einer Konsultation Art. 36 der Behörde genannt?
13) Ist d. DSB konform Art. 37 ausgewählt?
14) Ist die Stellung d. DSB konform Art. 38?
15) Sind die Aufgaben konform Art. 39 nachvollziehbar?
16) Sind d. Aufgaben d. DSB betr. verbindlicher interner Datenschutzvorschriften Art. 47 dokumentiert?

Verfahrensverzeichnis

Check mit Datei „Verfahrensverzeichnisse“

17) Sind die Beschreibungen der Verfahren richtig?
18) Gibt es neue Zwecke und Verfahren, die aufgenommen werden müssen?
19) Haben die Auftragsverarbeiter, die an der Verarbeitung beteiligt sind, ihre Verfahrensverzeichnisse aktuell für die Verfahren?
20) Wie ist die aktuelle Risikobewertung je Verfahren?
21) Die neuen Risikobewertungen sind in den Verfahren zu dokumentieren.
22) Sind die technischen und organisatorischen Maßnahmen korrekt beschrieben?
23) Gibt es neue technische Maßnahmen, die dokumentiert werden müssen?
24) Gibt es neue organisatorische Maßnahmen, die dokumentiert werden müssen?
25) Welche Maßnahmen sind nicht mehr notwendig und können entfernt werden?

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Regeln für sicheres Verhalten

Check mit Handbuch, Kapitel „Regeln für sicheres Verhalten“

26) Die Ergebnisse der Bewertung aus den Teams über die Sinnhaftigkeit werden eingeholt
27) Sind alle Regeln notwendig?
28) Was ist im letzten Jahr passiert (Vorfälle / Notfälle)?
29) Was haben wir daraus gelernt?
30) Sind neue Regeln sinnvoll und hinzuzufügen (IT fragen)?
31) Wann wurden die neuen MitarbeiterInnen (Eintritt seit der letzten Jahresüberprüfung) geschult?
32) Wann haben alle MitarbeiterInnen seit der letzten Jahresüberprüfung den Sinn der Regeln erklärt bekommen (Awareness-Schulung)?
33) Für welchen Monat ist die nächste Awareness-Schulung geplant?

Verträge mit Auftragsverarbeitern

Check der Verträge gegen das Dokument
„VertragAuftragsverarbeitung_VV-AV-DSGVO“

34) Ist die Vertragsvorlage richtig zur geltenden Fassung der Datenschutzgesetze?
35) Sind die bestehenden Verträge richtig zur geltenden Fassung der Datenschutzgesetze?

Datenschutzerklärungen

36) Gibt es für jedes Unternehmen eine Datenschutzerklärung auf der Webseite?

37) Sind die Datenschutzerklärungen (DSE) auf den Webseiten richtig?
Vergleiche mit https://datenschutz-generator.de (mit Erwähnung des Urhebers)

38) Sind in jeder DSE die eingesetzten Cookies erwähnt?

39) Ist die Datenschutzerklärung im Webshop richtig?

40) Ist die DSE widerspruchsfrei zu den DSEs auf den Portalen, auf denen angeboten wird?

Ergebnisbericht

Das Ergebnis dieser Jahresprüfung wird der Unternehmensleitung mit Vorschlägen zur Verbesserung berichtet

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

To do´s Projekt Datenschutz bis zum 25. Mai 2018

To do 1: Datenschutzerklärung

Die Datenschutzerklärung ist der richtige Platz für alle Aussagen zum Datenschutz. Menschen, die Wert auf Datenschutz legen, suchen diese Seite.

Cookies müssen erwähnt werden.

Die Rechte der Betroffenen müssen erklärt werden.

Vorschläge, wie das gestaltet werden kann zur Orientierung:

1) https://www.cms-typo3.at/kontakt-info/datenschutz.html
2) https://www.sonnentor.com/de-at/datenschutzerklaerung
3) http://www.gorelate.com/de/info/datenschutz/
4) http://weingut-steininger.at/datenschutz-und-vertraulichkeit/
5) http://www.adobe.com/de/privacy.html
6) https://datenschutz-generator.de

To do 2: Newsletter & Registrierung: Spam-Vermeidung

E-Mail-Adressen müssen verifiziert werden.

Das bedeutet, dass nach Eingabe einer E-Mail-Adresse ein Bestätigungsmail an diesen E-Mail-Account gesendet werden muss, das durch den rechtmäßigen Besitzer bestätigt werden muss.
Wird nicht bestätigt, ist die Anmeldung nicht erfolgt.

So wird ausgeschlossen, dass unter fremden E-Mail-Adressen in Webshops eingekauft wird und Unbeteiligte sich gegen etwas wehren müssen, was sie nicht beantragt haben.

Jede E-Mail-Adresse benötigt also ein „double opt in“. Das ist die übliche Methode, um Spam auszuschalten.
Nur durch aktive Bestätigung einer Anforderung eines Newsletters aus dem Ziel-E-Mail-Account gilt eine Einwilligung als nachgewiesen.

Z.B.: https://www.cms-typo3.at/typo3-news/newsletter-anmeldung.html

To do 3: Informationspflicht bei Erhebung

DSGVO Art 13-14 -> Transparenz, Datenschutzerklärung

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

Vereinbarung über die Informationspflichten

Jede und jeder Verantwortliche informiert bei der Erhebung von personenbezogenen Daten die Betroffenen mit einem Informationstext, der folgende Inhalte hat:

1) Name und Kontaktdaten der/des Verantwortlichen
2) Name und Kontaktdaten der/des Datenschutzbeauftragten
3) Die Zwecke, für die die Daten verarbeitet werden und die Rechtsgrundlage (= Einwilligung, Vertrag, Gesetz, berechtigte Interessen)
4) Eventuelle Empfänger / Kategorie der Empfänger
5) Eventuelle Absichten, Daten in Drittländer / internat. Organisationen zu übermitteln
6) Die Dauer der Verarbeitung
7) Das Recht auf Auskunft
8) Das Recht auf Berichtigung
9) Das Recht auf Löschung
10) Das Recht auf Einschränkung der Verarbeitung
11) Das Recht auf Widerspruch
12) Das Recht auf Datenübertragung
13) Das Recht auf Widerruf der Einwilligung
14) Das Recht auf Beschwerde bei der Behörde
15) Ob die Bereitstellung vertraglich / gesetzlich erforderlich ist, ob es eine Pflicht gibt und was die Folgen der Nichtbereitstellung wäre
16) Das Bestehen einer Automatisierten Entscheidungsfindung / eines Profilings und der Logik, Tragweite und Auswirkungen
17) Wenn Daten nicht bei Betroffenen erhoben = § 14: Die Quelle
18) Wenn Daten nicht bei Betroffenen erhoben = § 14: Die Kategorien der Daten

Diese Informationen muss man nicht mehr geben, wenn die betroffene Person diese Info bereits hat.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

To do 4 für Fachbereichs-Verantwortliche:
Analyse & Abstimmung mit allen externen Dienstleistern zur Synchronisation betreffend DSGVO bis Mai 2018

Jeder Fachbereich nimmt Kontakt mit seinen externen Dienstleistern auf, die mit personenbezogenen Daten des Unternehmens in Kontakt kommen können.
Es ist wesentlich, dass deren AGBs und Datenschutzerklärungen nicht im Widerspruch zur DSGVO stehen.

Beispiele für mögliche Schnittstellen von / nach außen:

1. Print-Dienstleister für Druck und Versand von Mailings
2. Daten-Zulieferer: AMS, Personalbereitsteller
3. IT-Dienstleister Auftragsverarbeitung
4. IT-Dienstleister Verantwortlicher / Systemwartung / ...
5. Steuerberatung / Lohnverrechnung / ...
6. Unternehmensberatung / Due dilligence / Potenzialanalysen / Change-Beratung / ...
7. Personalberatung / Personalsuche / Recruiting / Outplacement / ...
8. Versicherungsberatung
9. Magistrate, Sozialversicherung, Behörden
10. Online-Marketing / Analytics / Kundensegmentierung / ...

To do 5 für Fachbereichs-Verantwortliche:
Prüfung der Software-Produkte für die Verarbeitung personenbezogener Daten auf „privacy by design“ bis Mai 2018

Jede Software, die für die Verarbeitung von Personendaten eingesetzt wird, wird geprüft auf Widersprüche zur DSGVO. Zu erfragen / prüfen sind:

1. Vertrag (bei beauftragter Software)
2. AGB
3. Lizenz
4. Datenschutzerklärung
5. Beschreibung des eingebauten „Datenschutzes durch Technikgestaltung“

Anzuwenden bei: Webseiten / Software / Apps / Cloud-Services für pers. bez. Daten.

Bei Apps ist der Zugriff auf die Kontaktdaten und die Datenverwendung zu klären.

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

ANHANG

Hilfreiche Links

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

https://dsgvo-gesetz.de

Privacyshield - USA Selbstzertifizierung als Basis für die Zulässigkeit der Nutzung amerikanischer Datenverarbeiter
https://www.privacyshield.gov/welcome

Standard- und Musterverordnung als Argumentationsgrundlage genehmigungsfreier üblicher Datennutzung für Verarbeitungsverzeichnisse (Zwecke, Empfängerkategorien, Speicherfristen etc. für die Herleitung von Rechtmäßigkeit)
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495

E-Mail-Marketing und Rechtmäßigkeit
https://www.mailjet.de/dsgvo/email-marketing/

Auftragsverarbeitung & Fernwartung
https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf

Videoüberwachung
https://www.datenschutzbeauftragter-info.de/fachbeitraege/videoueberwachung-und-datenschutz/

https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/OH_VideoueberwachungNichtOeffentlicheStellen.pdf;jsessionid=031407CD8BEEC1A24B3BA3170F0142E8.1_cid319?__blob=publicationFile&v=8

Juristen mit Spezialwissen
https://drschwenke.de
https://www.wbs-law.de/it-recht/datenschutzrecht/

Datenschutzbehörde AT & Datenschutzgesetz & Datenschutzanpassungsgesetz
https://www.dsb.gv.at
https://www.dsb.gv.at/gesetze-in-osterreich

BSI Das deutsche Bundesamt für Sicherheit in der Informationstechnologie
https://www.bsi.bund.de/DE/Home/home_node.html

Datenschutz Bayern
https://www.datenschutz-bayern.de/datenschutzreform2018/

Datenschutz und Logfiles
https://www.datenschutz.org/logfiles/

Stand der Technik – die Suche nach der Definition
http://fokus.genba.org/dsgvo-stand-der-technik

wow! solution | Wolfgang Wagner
St. Ulrichsplatz 6, 1070 Wien
Tel.: +43 650 799 88 77
Fax: +43 1 205 115 110 26
E-Mail: wow@wow-solution.at

E-Mail & Datenschutz

Der Tätigkeitsbericht des Hessischen Datenschutzlandeamtes, er gibt zu vielen Themen die Praxis der Behörde wieder:
https://www.datenschutz.hessen.de/tb45inhalt.htm

Öffentlicher Verteiler und ärztliche Schweigepflicht an einem Beispiel aus dem Tätigkeitsbericht in 6.2.1. (Zahnarzt, Erinnerungsmails an Verteiler)
https://www.datenschutz.hessen.de/tb45k06.htm#entry4904

Administration, Hoster etc. (OHNE spezifischern Auftrag zur Verarbeitung von personenbezogenen Daten) & Auftragsverarbeitung

Hier ist eine Abgrenzung auf Seite 22, Kapitel 1.3. :

Wer nur Systeme im Betrieb hält und keinen Auftrag hat, personenbezogene Daten zu verarbeiten, ist KEIN Auftragsverarbeiter und wird nur a) auf Verschwiegenheit und b) Einhaltung DSGVO verpflichtet. Bitkom erklärt den Unterschied:

https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf

Datenschutzbeauftragte(r) : Wer muss DSB nominieren? Fallbeispiele hier

https://www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf

Übermittlung von Daten in ein Drittland oder eine internationale europäische Organisation, die auch Niederlassungen außerhalb des EWR hat

EU-Seite, die alle wichtigen Sachverhalte offiziell erklärt:

https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu_de

Hier die Übersicht in verständlicher Sprache:

https://www.fsdz.ch/file-docs/lf-verarbeitung-personenbezogener-daten-de-online-final.pdf

Beispiel eines internationalen Unternehmens mit „verbindliche genehmigte interne Datenschutzvorschriften“ Binding Corporate Rules:

https://www.firstdata.com/en_us/privacy/binding-corporate-rules.html

Link zur Liste aller internationalen Unternehmen, die auf EU-Seite mit Binding Corporate Rules geführt werden:

https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/binding-corporate-rules_de