HilCon Büroservice e.U.

EU-Datenschutz-Grundverordnung

DSGVO

Erstellt von Christoph Hilberger © am 27 April 2018

Inhalt

Grundlagen

Ab dem 25.5.2018 gelten die EU-Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) in der Fassung des Datenschutz-Anpassungsgesetz 2018. Das bedeutet für alle Unternehmen zum einen Handlungsbedarf bei Verträgen, internen Abläufen sowie Datensicherheitsmaßnahmen und zum anderen verschärfte Strafdrohungen.

Interne Abläufe

Die Firma HilCon verarbeitet personenbezogene Daten und Sensible Daten Ihrer Kunden und Auftraggeber. Wir verarbeiten keine Daten im umfangreichen Ausmaße, es werden auch keine strafrechtlichen relevanten Daten für die Arbeit benötigt oder gespeichert. Wir bieten für Kinder unter 14 Jahren keine Dienstleistung an, jedoch ist zu beachten das die Homepage http://www.hilcon.co.at sowie das LinkedIn und Google+ Profil im Internet aufgerufen werden kann.

Ab 01 Mai 2018 werden für alle relevanten Daten eine klare und deutlich verständliche Einwilligung der Betroffenen eingeholt.

Aufgrund der Datenminimierung, werden vom Kunden nur diese Daten erhoben, welche für die Weiterverarbeitung erforderlich sind. Die Speicherung der Daten erfolgten gemäß Bundesabgabenordnung und ist somit maximal 7 Jahre. Wir werden einmal jährlich erheben welche Kundendaten wir wie und wann löschen, weiters ist es dem Kunden möglich eine Löschung zu beantragen.

Geprüft werden muss ob die Datenspeicherung den Anforderungen genügen, besonders die sensiblen Daten in Papierform und Elektronisch.

Die Firma HilCon tritt gemäß österreichischem DSG 2000 als Dienstleister auf.

Benötigte Kundendaten

Rechnungserstellung

Hierfür werden folgende Daten benötigt und die Speicherung der Daten/Anforderung haben eine rechtliche Grundlage

- Name und Anschrift des Leistungsempfängers und Lieferanten
- Umsatzsteueridentifikationsnummer (UID-Nummer) des Ausstellers der Rechnung
- Bankverbindung
- E-Mail-Adresse es Empfängers und des Lieferanten (bei elektronischer Übermittlung

Gewerbeanmeldung, Versicherungserklärung

Hierfür werden folgende Daten benötigt und die Speicherung der Daten/Anforderung haben eine rechtliche Grundlage

- Zuständige Bezirkshauptmannschaft
- Familiennamen, Vornamen, Geburtsdatum, Geburtsland, Geburtsort, Staatsangehörigkeit und Geschlecht.
- Straße, Hausnummer, Postleitzahl, Ort und Staat der Wohnadresse sowie Gewerbewohnsitz.
- Telefonnummer und E-Mail-Adresse

Finanzamt

Hierfür wird die Steuernummer des Klienten benötigt.

Dokumentation

Dokumentation der erteilten Einwilligungen

Elektronische Ablage der Einwilligungen erfolgt in elektronischer oder in Papierform, je nach Einlagen.

Es muss eine nachträgliche Einwilligung der Kunden erfolgen.

Verarbeitungsverzeichnis

Liste der Datenverarbeitungen mit personenbezogenen Daten, den Rechtsgrundalgen etc.

Siehe Anhang

WKO Online Ratgeber

Zusammenfass sende Information

Siehe Anhang

WKO-Online-Ratgeber.pdf

Datenverarbeitungsverzeichnis nach Art 30 Abs 2 EU-Datenschutz-Grundverordnung (DSGVO)

Stammblatt des Auftragsverarbeiters

Name und Anschrift

Firma HilCon Büroservice e.U.

Unterm Kirchbichl 1

8733 St. Marein – Feistritz

E-Mail-Adresse / Telefonnummer

Mail: office@hilcon.co.at Tel.: +43 0664 / 59 55 928

Datenschutzbeauftragter

Da die Kerntätigkeit des Unternehmens nicht eine umfangreiche regelmäßige uns 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. Es werden lediglich personenbezogene Daten manuell von einer Person bearbeitet.

Stammblatt des Verantwortlichen und Angaben zur Auftragsdatenverarbeitung

Auftraggeber werden gem. Kundenliste geführt und unterfertigen den Vertrag für Auftragsdatenverarbeitungen.

Inhalt des Vertrages siehe Anhang!

Allgemeine Beschreibung der organisatorisch-technischen Maßnahmen

Die allgemeinen Beschreibungen werden im Anhang erläutert, und dem Auftraggeber angepasst. Es erfolgt eine Unterzeichnung beiderseits.

Datenverarbeitungen / Datenverarbeitungszwecke

Zweck und Beschreibung der Datenverarbeitung

Rechnungswesen und Geschäftsabwicklung

Verarbeitung und Übermittlung von Daten im Ramen von Geschäftsbeziehung mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenzen oder Verträge) in diesen Angelegenheiten.

Marketing

Sollte der Kunde einverstanden sein erfolgt eine gelegentliche e-mail Marketing oder Post Marketing Zusendung. Welche jederzeit aufgelöst werden kann.

Geschäftspartnerdatenbank

Es werden keine Daten an Dritte weitergegeben! Keine Übermittlung personenbezogener Daten ohne ausdrücklicher schriftlicher Aufforderung vom Kunden, für die Kommunikation mit der Kammer, Versicherung etc.

Wurde eine Datenschutz-Folgeabschätzung durchgeführt?

NEIN

Die Firma HilCon arbeitet nicht mit Sicherheitstechnologien, welche ein hohes Risiko verbirgt. Weiters wird kein Profiling betrieben oder umfangreiche sensible Daten verarbeitet.

Kategorien der betroffenen Personen

Kategorie	*Beschreibung*
1	Geschäftskunden – inkl. Kontaktpersonen
2	Privatkunden
3	Geschäftskunden – von denen personenbezogene Daten überlassen werden, für die weitere Verarbeitung.

Rechtsgrundalgen

DSGVO Art 6 Abs1 lit a Einwilligung der Betroffenen

Es werden von jedem neuen Geschäftspartner eine Einwilligung eingeholt

DSGVO Art 6 Abs1 lit b gesetzliche Verpflichtung nach der BAO und UGB

§ 132 Bundesabgabenordnung

§§ 190, 212 Unternehmergesetzbuch

Verträge

Anhang

Datenverarbeitungen / Datenverarbeitungszwecke

Kategorie	Lfd Nr	Datenkategorie	Strafrecht	Rechnungs-erstellung	Behörde	Aufbewahrung
1	1	Name und Anschrift des Geschäftskunden	Nein	X		7 Jahre
	2	Umsatzsteueridentifikationsnummer	Nein	X		7 Jahre
	3	E-Mail-Adresse und Telefonnummer	Nein	X		7 Jahre
	4	Bankverbindung	Nein	X		7 Jahre
	5	Bankverbindung	Nein		X	1 Jahr
	6	Zuständige Bezirkshauptmannschaft	Nein		X	1 Jahr
	7	Geburtsdatum			X	1 Jahr
	8	Geburtsland			X	1 Jahr
	9	Geburtsort			X	1 Jahr
	10	Staatsangehörigkeit			X	1 Jahr
	11	Geschlecht			X	1 Jahr
	12	Steuernummer			X	7 Jahre
2	13	Name und Anschrift des Privatkunden	Nein	X		7 Jahre
	14	E-Mail-Adresse und Telefonnummer	Nein	X		7 Jahre
	15	Bankverbindung	Nein		X	1 Jahr
	16	Staatsangehörigkeit			X	1 Jahr
	17	Steuernummer			X	7 Jahre
3	18	Name und Anschrift des Geschäftskunden	Nein	X		7 Jahre
	19	Umsatzsteueridentifikationsnummer	Nein	X		7 Jahre
	20	E-Mail-Adresse und Telefonnummer	Nein	X		7 Jahre
	21	Bankverbindung	Nein	X		7 Jahre
1-3	22	Anschrift & e-mail Adressen	Nein	**Werbung**		**Solange eine Geschäftsverbindung Besteht 1 bis 7 Jahre**

Begriffserklärung

Sensible Daten

„Sensible Daten" (besondere Kategorien personenbezogener Daten) sind personenbezogene Daten, aus denen die rassische und ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Datenverarbeitung im umfangreichen Ausmaß

Beispiel: Die Patienten-Datenverarbeitung eines Krankenhauses gilt als umfangreich, die eines Hausarztes nicht; die Kundendatenverarbeitung einer Versicherung ja, die eines Versicherungsmaklers nicht.

Eine Verarbeitung großer Mengen personenbezogener Daten, eine große Anzahl an betroffenen Personen, die Datenverarbeitung ist dauerhaft ausgelegt, oder hat eine weite geographische Ausdehnung.

Treu und Glauben

Die Verarbeitung personenbezogener Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche personenbezogenen Daten der betroffenen Person verarbeitet werden.

Datenminimierung

Beispiel: Unzulässig ist die Verarbeitung des vollständigen Geburtsdatums, wenn nur Geburtsjahr für die Erreichung des Zweckes notwendig wäre.

Personenbezogene Daten müssen dem Zweck angemessen und auf das notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Speicherung

Beispiel: 7 Jahre Aufbewahrungspflicht für steuerrelevante Geschäftspapiere

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich sind. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Für die regelmäßigen Überprüfungen und Löschungen sollten Fristen vorgegeben sein. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

Vertraulichkeit

Sorgen Sie technisch und organisatorisch für den Schutz der Daten vor unbefugtem Zugriff?
Beispiel: Passwortschutz, Zutrittskontrolle, abgesperrte Räumlichkeiten

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Dokumentation

Beispiel: Dokumentation der erteilten Einwilligungen, Verarbeitungsverzeichnis (Liste der Datenverarbeitungen mit personenbezogenen Daten, den Rechtsgrundlagen, etc.)

Der Verantwortliche ist zur Einhaltung der Grundsätze (Rechtmäßigkeit, Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Ingetrität und Vertraulichkeit) verpflichtet. Weiters muss er die Einhaltung dieser Grundsätze auch nachweisen können.

Auftragsverarbeiter

Beispiel: Buchhalter, Provider

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

Dieser Begriff entspricht dem „Dienstleister“ nach dem derzeitigen österreichischem DSG 2000.

Verträge

Stammblatt zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung

Name und Kontaktdaten

E-Mail-Adresse und Telefonnummer

Name und Kontaktdaten des Vertreters

Kategorien von Verarbeitungen, die am Auftrag des konkreten Verantwortlichen durchgeführt werden

Übermittlung von personenbezogenen Daten in Drittländer, inkl. Internationale Organisationen

Nein

Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

Vertraulichkeit:

Offenlegung oder unbefugten Zugang zu personenbezogenen Daten wird elektronische durch Passwortsicherheit und Verschlüsselung sichergestellt. Weiters werden Daten nur solange wie unbedingt notwendig gespeichert.

Integrität

Durch eine Passwortsicherung, Firewall und Antivirenschutz wird eine Zerstörung/Vernichtung bzw. Schädigung durch dritte verhindert. Die Ablage in Papierform erfolgt in einem versperrten Holzkasten, in einem Versperrbaren Büro.

Verfügbarkeit und Belastbarkeit

Die Verfügungstellung der Daten erfolgt im Vertragszeitraum längstens 7 Jahre, gem. der Bundesabgabenordnung. Daten, die man nicht mehr benötigt, werden dem Auftraggeber übermittelt und in weiterer Folge gelöscht.

Pseudonymisierung und Verschlüsselung

Daten werden über mittels gesicherten *pdf übermitteln, Verschlüsselung erfolgt über das Programm DATEV, über dieses wir Kommunizieren

Evaluierungsmaßnahmen

Sollte es Änderungen oder Verbesserungen im Übermittlungsverfahren geben, werden diese sofort umgesetzt, ansonsten wird eine jährliche Evaluierung durchgeführt.

EU-Datenschutz-Grundverordnung (DSGVO) – Einwilligungserklärung

Gesetzliche Grundlagen

Einkommensteuergesetzbuch
Umsatzsteuergesetzbuch
Bundesabgabenordnung

Vertragliche Grundlage

Erstellung eines Vertrages inkl. Vollmacht

(Privatkunde / Geschäftskunde

Einwilligungserklärung

Erstellung einer Einwilligung inkl. Stammdatenblatt