Handout zum DSGVO Vortrag

Themen des DSGVO Vortrags –

„Schwerpunkte aus dem Erwartungsspeicher“

Grundsätzliches

Datenschutzerklärung Ihrer Website

Impressumspflicht und die Ausprägung

Verfahrensverzeichnis und TOM‘s

Grundsätzliches

Jede Verarbeitung personenbezogener Daten ist verboten, es sei denn der Betroffene oder eine Rechtsvorschrift erlauben dieses!!

Die EU-DSGVO ist für alle Unternehmungen verbindlich. Inhaltlich gibt es Abweichungen durch die Kirchen. Diese haben die Öffnungsklausel genutzt und eigene Gesetze umgesetzt (DSG-EKD/KathDSG)

Ab einer Anzahl von mehr als 9 Mitarbeitern muss ein Datenschutzbeauftragter benannt werden. Dies kann intern, oder extern erfolgen.

Abweichend hiervon muss ebenfalls ein Datenschutzbeauftragter benannt werden, wenn hochsensible Daten verarbeitet werden.

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeiten
- Genetische oder biometrische Daten
- Kinder
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Einen guten Leitfaden zur Umsetzung der EU-DSGVO finden Sie unter

https://vds.de/de/cyber/dsgvo/

Hier die Richtlinie VdS 10010 nutzen. Die Health365 AC GmbH hat hier maßgeblich an der Entwicklung mitgearbeitet und arbeitet nach diesem System.

Im Rahmen der EU-DSGVO ist ein Verfahrensverzeichnis zu erarbeiten. Hier sind alle Verarbeitung von personenbezogenen Daten aufzunehmen und deren Risiken einzuschätzen.

Sie sollten sich immer nach dem Zweck und dessen Berechtigung bei der Datenerhebung fragen. Denn wenn Sie keinen rechtmäßigen Zweck haben dann dürfen Sie die Daten auch nicht erheben.

Wenn Sie Daten erheben beschreiben Sie den kompletten Prozess und wer im Unternehmen darauf zugreifen darf bzw. wie Sie die Daten schützen.

Beachten Sie das Gebot der Datensparsamkeit und der Datentrennung!

Impressum und die Datenschutzerklärung müssen sofort ersichtlich sein und nach maximal nach zwei Klicks geöffnet sein.

Wenn Sie ein Kontaktformular nutzen, senden Sie dem Eintragenden seine Daten inkl. der Datenschutzerklärung und Ihren AGBs

Erstellen Sie eine aktive Einwilligung in Form von Checkboxen, jedoch mit der Möglichkeit des Aufrufens einer Erklärung zur Verarbeitung und der dazu passenden Transparenz.

Das Speichern oder Verarbeiten von Daten in Ländern außerhalb der EU bzw. des EWG ist nicht zulässig. Es sei denn über die EU Standardvertragsklauseln

https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32010D0087

Als Beispiel verweisen wir auf die Dropbox. Diese speichert alle Daten in den USA und ist damit nicht DSGVO konform.

Nutzen Sie hier andere Lösungen.

NOCH FRAGEN:

Health365 AC GmbH
Frank Nelles
Friedrichstraße 68
10117 Berlin
030/809332855 oder 0175/5870326

Die Datenschutzerklärung

Bitte überprüfen Sie Ihre Website auf alle Funktionalitäten. Aus dieser Liste von Funktionalitäten können Sie dann die etwaige Form der Datenschutzerklärung festlegen.

Im Folgenden die Beispiele aus meinem Vortrag:

Die Kurzform

Wenn Sie unsere Webseite besuchen...
...freuen wir uns über Ihr Interesse. Wir möchten nichts weiter über Sie wissen. Wer Sie sind, welche Seite Sie sich wie lange ansehen, welche Webseiten Sie vorher besucht haben, welche Werbung wir Ihnen einblenden könnten und was Ihre persönlichen Interessen sind? Es ist uns egal.
Deshalb loggen wir Ihre Zugriffe nur, wenn dabei ein Fehler auftritt. Diese Protokolldaten nutzen wir ausschließlich für die Fehlersuche und um unsere Schutzmechanismen zu verbessern.
Logdateien werden in aller Regel nach 12 Monaten gelöscht (weil sie sonst nur Speicherplatz belegen - wer liest schon alte Logfiles?).

Wenn Sie Kontakt mit uns aufnehmen...
...entscheiden Sie selbst, ob und welche personenbezogenen Daten Sie uns zur Verfügung stellen (z. B. Ihre Mailadresse, wenn Sie unser Kontaktformular nutzen). Wir nutzen diese Daten nur, um Ihre Anfrage zu bearbeiten.
Bitte bachten Sie: Ihre Anfragen (wie z. B. eintreffende Mails oder Telefonnotizen) werden von uns in aller Regel aufgehoben, weil ein zielgerichtetes Löschen zu aufwändig wäre und weil wir mit Hilfe einer Historie zukünftige Anfragen schneller und zielgerichteter beantworten können.

Wenn Sie uns brisante Informationen übermitteln...
...(oder wir derartige Informationen z. B. im Verlauf eines Projekts ermitteln) löschen bzw. anonymisieren wir diese so bald als möglich. Dieses Vorgehen gilt für personenbezogene und nicht-personenbezogene Daten gleichermaßen. So werden die Daten jedes

Projekts nach dessen Beedigung generell anonymisiert. Nicht anonymisierte Daten weden von allen Speichermedien (inkl. aller Backup-Medien) gelöscht.

Wenn Sie Fragen haben oder eine Bitte...
...kontaktieren Sie uns über unser Webformular oder rufen Sie uns an (sie finden unsere Kontaktdaten im Impressum). Wir geben Auskunft, beraten Sie und löschen gerne - wann immer möglich - Ihre personenbezogenen Daten (das spart Speicherplatz und Nerven). Wir stehen (nicht nur in Sachen Datenschutz) auf Ihrer Seite

(Quelle: www.mark-semmler.de/datenschutz)

Diese Form können Sie nutzen wenn Sie auf Ihrer Website nur begrenzt Daten verarbeiten oder Tools zur Auswertung verwenden.

Die Langform (noch immer möglichst kurz)

Mit dieser Erklärung informieren wir Sie über Art, Umfang und Zweck der von uns im Zuge der Nutzung dieser Webseite erhobenen, genutzten und verarbeiteten personenbezogenen Daten und klären über die Ihnen zustehenden Rechte auf.

1. Grundsätzliches
Wir arbeiten stets nach dem Prinzip der Datensparsamkeit. Wir erheben und verarbeiten personenbezogene Daten nur dann, wenn dies für unsere Geschäftsprozesse (dem Erbringen von Dienstleistungen im Bereich der Informationssicherheit) unbedingt notwendig ist.

2. Name und Anschrift des für die Verarbeitung Verantwortlichen
Verantwortlicher im Sinne der Datenschutz-Grundverordnung, sonstiger in den Mitgliedstaaten der Europäischen Union geltenden Datenschutzgesetze und anderer Bestimmungen mit datenschutzrechtlichem Charakter ist die:

Kontaktieren Sie die Health365 AC GmbH.
Rufen Sie das Impressum der Health365 AC GmbH auf.

3. Grundlagen der Verarbeitung personenbezogener Daten
Die von Ihnen im Zuge der Nutzung dieser Webseite überlassenen personenbezogenen Daten werden aufgrund folgender gesetzlicher Bestimmungen verarbeitet:

- Zur Erfüllung vertraglicher Pflichten
  Die umfasst z. B. die Einleitung vorvertraglicher Maßnahmen, die einer vertraglich geregelten Geschäftsbeziehung vorausgehen oder die Erfüllung der Pflichten aus einem mit Ihnen geschlossenen Vertrag.
- Aufgrund gesetzlicher Vorgaben
  Dies kann z. B. die Einhaltung von steuerlichen Aufbewahrungspflichten sein.
- Im Rahmen der Interessensabwägung:
  Unser berechtigtes Interesse kann im Einzelfall z. B. die Geltendmachung rechtlicher Ansprüche, Abwehr von Haftungsansprüchen oder die Verhinderung/Aufklärung von Angriffen auf unsere Informationsverarbeitung oder von Straftaten sein.

4. Schutz Ihrer personenbezogene Daten
Wir stellen die angemessenen Verfügbarkeit, Integrität und Vertraulichkeit aller Informationen sicher, die von unserem Unternehmen gespeichert, verarbeitet oder übertragen werden. Hierfür haben wir ein Informationssicherheitsmanagementsystem (ISMS) implementiert, mit dem wir die die hierfür notwendigen technischen und organisatorischen Maßnahmen identifizieren, umsetzen, überprüfen und stetig verbessern. Dennoch kann keine absolute Sicherheit garantiert werden.

5. Kategorien personenbezogener Daten und deren Verarbeitungszweck
Wir verarbeiten bei der Nutzung dieser Webseite und bei einer Kontaktaufnahmen durch Sie die folgenden Kategorien personenbezogener Daten:

a) Automatisch erfasste Nutzungsdaten (Logdateien des Webservers)

Diese Webseite erfasst nur beim Auftreten eines Fehlers (!) eine Reihe von Informationen. Diese allgemeinen Daten und Informationen werden in den Logfiles des Servers gespeichert. Erfasst werden im Fehlerfall

- die verwendeten Browsertypen und Versionen
- das vom zugreifenden System verwendete Betriebssystem
- die Internetseite, von welcher ein zugreifendes System auf unsere Internetseite gelangt (sogenannte Referrer)
- die Unterwebseiten, welche über ein zugreifendes System auf unserer Internetseite angesteuert werden
- das Datum und die Uhrzeit eines Zugriffs auf die Internetseite
- eine Internet-Protokoll-Adresse (IP-Adresse) und
- sonstige ähnliche Informationen, die der Analyse und Gefahrenabwehr im Falle von Fehlern und Angriffen dienen (wie z. B. der aufgetretene Fehler und seine Beschreibung).

Bei der Nutzung dieser Informationen zieht wir keine Rückschlüsse auf die betroffene Person. Diese Informationen werden vielmehr benötigt, um die Sicherheit Informationsverarbeitung zu gewährleisten und um Strafverfolgungsbehörden im Falle eines Angriffes die zur Strafverfolgung notwendigen Informationen bereitzustellen.

b) von Ihnen zur Verfügung gestellte Informationen bei Kontaktaufnahme

Unsere Internetseite enthält Angaben, die eine schnelle Kontaktaufnahme sowie eine unmittelbare Kommunikation mit uns ermöglichen (Telefonnummer, E-Mail-Adresse, Postanschrift). Darüber hinaus enthält sie die Möglichkeit, uns über ein Kontaktformular Textnachrichten zu senden. Wenn Sie Kontakt mit uns aufnehmen werden verschiedene personenbezogenen Daten (wie z. B. die anrufende Telefonnummer, die absendende E-Mail-Adresse, der Absender eines Briefes) und sämtliche andere übermittelte personenbezogene Daten bei uns verarbeitet. Die Verarbeitung ist notwendig,weil wir sonst Ihre Anfragen nicht bearbeiten und beantworten können.

6. Offenlegung und Weitergabe

Personenbezogene Daten werden von uns nur offengelegt oder weitergegeben, wenn wir dazu gesetzlich verpflichtet sind oder wenn wir dadurch in einem konkreten Fall (wie z. B. bei einem Angriff auf unsere IT-Infrastruktur) die Arbeit von Ermittlungsbehörden unterstützen können bzw. wollen.

7. Dauer der Speicherung
a) Automatisch erfasste Nutzungsdaten (Logdateien des Webservers)

Sämtliche Einträge in den Logdateien des Webservers werden nach 6 Monaten automatisch auf unseren Produktivsystemen und unserer Datensicherung wieder gelöscht.

b) von Ihnen zur Verfügung gestellte Informationen bei Kontaktaufnahme

Wir löschen nach dem Ende eines Projekts in aller Regel sämtliche sensitiven Daten (z. B. über Sicherheitsvorfälle, technische oder organisatorische Schwachstellen oder offensichtlich vertrauliche Informationen) von oder über unserer Kunden von unseren Produktivsystemen und aus unserer Datensicherung.
Um auf neue Anfragen schnell und korrekt reagieren zu können, behalten wir uns allerdings vor, allgemeine und nicht sensitive bzw. vertrauliche Informationen (z. B. Kontaktdaten, Informationen über Ansprechpartner und Projektverläufe, technische Vorgehensweisen oder spezielle Wünsche/Anforderungen des Kunden) beliebig lange zu speichern.

8. Ihre Rechte
Wenn wir personenbezogene Daten von Ihnen verarbeiten, so besitzen Sie die untenstehenden Rechte. Möchte Sie eines dieser Rechte in Anspruch nehmen, können sie sich jederzeit an uns wenden. Diese Rechte sind:

a) Recht auf Bestätigung
Sie können jederzeit unentgeltlich Auskunft erhalten, ob wir personenbezogene Daten von Ihnen verarbeiten.

b) Recht auf Auskunft
Sie können jederzeit unentgeltlich Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten erhalten.
c) Recht auf Berichtigung
Sie haben das Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten bzw. deren Vervollständigung zu verlangen.
d) Recht auf Löschung (Recht auf Vergessen werden)
Sie habe das Recht, zu verlangen, dass wir die sie betreffenden personenbezogenen Daten unverzüglich löschen.
e) Recht auf Einschränkung der Verarbeitung
Sie dürfen von der Health365 AC GmbH die Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen.
f) Recht auf Datenübertragbarkeit
Wir stellen Ihnen auf Wunsch die Sie betreffenden personenbezogenen Daten, welche Sie der Health365 AC GmbH bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung. Gerne stellen wir diese Daten einer Stelle Ihrer Wahl direkt zur Verfügung.
g) Recht auf Widerspruch
Sie haben das Recht, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen.
h) Recht auf Widerruf einer datenschutzrechtlichen Einwilligung
Sie haben das Recht, eine Einwilligung zur Verarbeitung ihrer personenbezogenen Daten jederzeit zu widerrufen.
Sie haben natürlich auch das Recht, sich über die Verarbeitung Ihrer personenbezogenen Daten bei uns bei der zuständigen Aufsichtsbehörde zu beschweren

(Quelle: www.mark-semmler.de/datenschutz)

Diese Form können Sie Nutzen wenn Sie auf Ihrer Website Daten verarbeiten und Tools zur Auswertung verwenden.

BITTE beachten Sie!!

- *Bei Verarbeitung personenbezogener Daten auf Ihrer Website, muss diese verschlüsselt werden über https erreichbar sein!!*
- *Bei Verwendung von Bildern achten Sie darauf das Bilder von Personen geschützt werden müssen. Dies bedeutet das der Download über Rechtsklick gesperrt werden sollte.*
- *Bei Bildern unter 5 Personen, benötigen Sie eine Einwilligungserklärung der dargestellten Person.*

Die Impressumspflicht und dessen Ausprägung gem. DSGVO

Die Impressumspflicht besteht schon auf Grundlage des Telemediengesetzes und des HGB. Hier sollten in Zukunft die Verknüpfungen zur Datenschutzerklärung sichergestellt sein.

Denn es muss gewährleistet sein das die verantwortliche Stelle und/oder der Datenschutzbeauftragte genannt werden.

Gesetzeskonforme Vorlagen finden Sie unter:

http://www.bmjv.de/DE/Verbraucherportal/DigitalesTelekommunikation/Impressumspflicht/Impressumspflicht_node.html

Das Verfahrensverzeichnis und TOMs

Es ist jeglicher Verarbeitung von personenbezogenen Daten ob analog oder digital ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Dies bedeutet das jeder Prozess bzw. Datenfluss beschrieben werden muss und das dazugehörige Risiko eingeschätzt werden muss.

Beispiel:

Prozessschritt	Art der Verarbeitung/ Betroffene Daten	Zweck	Alte Rechtsgrundlage	Neue Rechtsgrundlage
1 Erstkontakt (Ein potentieller Neukunde meldet sich idR telefonisch oder per Email.)	Direkterhebung/ jeweilige Kontaktdaten (z.B. Email-Adresse, Telefonaten), Daten zum Kundenanliegen	Begründung eines Vertragsverhältnisses	§ 28 Absatz 1 Satz 1 Ziffer 1 BDSG	Artikel 6 Absatz 1 lit. b DSGVO
2 Rückruf/ Angebot (Es erfolgt ein Rückruf, bei dem weitere Informationen erfragt und nach dem gf. Ein Angebot erstellt wird)	Speicherung, Nutzung, Übermittlung/ Kontaktdaten, Auftragsdaten	Begründung eines Vertragsverhältnisses	§ 28 Absatz 1 Satz 1 Ziffer 1 BDSG	Artikel 6 Absatz 1 lit. b DSGVO

Prozessschritt	Art der Verarbeitung/ Betroffene Daten	Zweck	Alte Rechtsgrundlage	Neue Rechtsgrundlage
3a Aufbewahrung bei Nicht zustande-kommen (Kommt der Vertrag nicht zustande, werden die Daten archiviert und nach Ablauf der Löschfrist gelöscht)	Sperrung, Löschung/ sämtliche bereits gespeicherte Daten	Vorvertragliche Maßnahme, Wahrung der Aufbewahrungsfristen	§ 147 Absatz 1, Absatz 3 AO, § 35 Absatz 2 Satz 2 Ziffer 1 BDSG	§ 147 Absatz 1, Absatz 3 AO, § Artikel 17 Absatz 1, 2. HS lit. a DSGVO
3b Kommunikation, Dokumentation bei Zustande-kommen (Kommt der Vertrag zustande, erfolgt die vertrgasbezogene Kommunikation, Dokumentation)	Verarbeitung/ sämtliche bereits gespeicherte Daten und neue Daten	Durchführung des Vertragsverhältnisses	§ 28 Absatz 1 Satz 1 Ziffer 1 BDSG	Artikel 6 Absatz 1 lit. b DSGVO

Prozessschritt	Art der Verarbeitung/ Betroffene Daten	Zweck	Alte Rechtsgrundlage	Neue Rechtsgrundlage
4 Aufbewahrung nach Vertragsende (Nach Vertragsende werden die Daten archiviert und nach Ablauf der Löschfrist gelöscht)	Sperrung, Löschung/ sämtliche bereits gespeicherte Daten	Vertragliche Maßnahme, Wahrung der Aufbewahrungsfristen	§ 147 Absatz 1, Absatz 3 AO, § 35 Absatz 2 Satz 2 Ziffer 1 BDSG	§ 147 Absatz 1, Absatz 3 AO, § Artikel 17 Absatz 1, 2. HS lit. a DSGVO

Hinzu kommen dann die TOMs (Technische und organisatorische Maßnahmen)

Diese organisieren den technischen und organisatorischen Schutz der verarbeiteten Daten.

Beispiel:

Lfd. Nr.	Datenfluss	Schadensschwere	Eintrittswahrscheinlichkeit	Rechte und Freiheiten	Art, Umfang, Zweck	Risikobewertung (insgesamt)
1	Erstkontakt	mittel, da weder unbedeutende noch besonders sensible Daten erhoben werden	hoch, weil in den vergangenen Jahren vermehrt Angriffe auf Unternehmen derselben Branche verübt worden (Quelle: www.xyz.de)	mittel, da weder untergeordnete noch besondere Rechte beeinträchtigt sind	hoch, da besonders viele Daten betroffen sind	gering: 0 mittel: 2 hoch: 2 **Gesamt: hoch**
2	Rückmeldung	gering, da nur die Kontaktdaten verarbeitet werden	hoch, da gerade bei Rückantworten in den vergangenen Jahren vermehrt Angriffe auf Unternehmen derselben Branche verübt worden (Quelle: www.xyz.de)	gering, da die für diesen Prozessschritt erforderlichen Daten keine besonderen Freiheiten tangieren	mittel, da zwar viele Betroffene, aber nur wenige Daten betroffen sind	gering: 2 mittel: 1 hoch: 1 **Gesamt: mittel**

Das eingeschätzte Risiko ergibt dann den Schutzbedarf. Einteilen lassen sich die Daten in 4 Schutzstufen:

<u>Stufe 1: Niedriger oder geringer Schutzbedarf</u>

Darunter fallen personenbezogene Daten, deren Verarbeitung keine besondere Beeinträchtigung des informationellen Selbstbestimmungsrechts erwarten lässt.

Bsp.:

Anschrift, Beruf, Geburtsjahr, Telefonnr., Titel, akademischer Grad, öffentliche Register, Telefonverzeichnisse, Branchen- und Geschäftsbezeichnungen, Adressbuchangaben,

Branchenverzeichnisse, Bankverbindungen, Adressdaten von Funktionsträgern einer Gemeinde (Gemeinderatsmitglied, Vereinsvorsitzende)

Stufe 2: Mittlerer Schutzbedarf

Darunter sind personenbezogene Daten zu verstehen, deren Verarbeitung eine besondere Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern erwarten lässt, als der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.

Bsp.:

Daten über Mietverhältnisse, Daten über Geschäfts- und Vertragsbeziehungen, Telefonverbindungsdaten, Gleitzeitdaten, Kontenstände, Mitgliederverzeichnisse, Familienstand, Zeugnisse, Prüfungsergebnisse, Versicherungsdaten, Wehrdienstzeit, Grad der Behinderung, verwandtschaftliche Beziehungen, Bekanntenkreis, Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen, berufliche Laufbahn,

nähere Angaben über Behinderung und dergleichen), Kreditauskünfte, rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen, politische Meinungen, Gewerkschaftszugehörigkeit, Sexualleben, Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen), Schülerdaten, Verkehrsordnungswidrigkeiten, Melderegister

Stufe 3: Hoher Schutzbedarf

personenbezogene Daten fallen dann unter die Kategorie des hohen Schutzbedarfs, wenn deren Verarbeitung eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern zu erwarten ist, als dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann oder die Daten aufgrund ihrer besonderen Sensibilität bzw. ihres Verwendungszusammenhangs einen höheren Schutzbedarf als Stufe 1 erfordern.

Bsp.:

Patientendaten (besonders sensible Diagnosedaten wie Aids, Krebs, psychischer Erkrankungen und dergleichen) soweit nicht Stufe 1, besonders sensible Sozialdaten, Steuerdaten, strafbare Handlungen, Daten, die einem Berufs-, Geschäfts-, Fernmelde- oder Mandantengeheimnis unterliegen,

Personalverwaltungsdaten (dienstliche Beurteilungen, berufliche Laufbahn und dergleichen) soweit nicht Stufe 1, Verwaltungsdaten entsprechend der „VS-Vertraulich

Stufe 4: Sehr hoher Schutzbedarf

Hierunter fallen personenbezogene Daten, deren Verarbeitung eine sehr hohe Gefährdung des informationellen Selbstbestimmungsrechts insofern erwarten lässt, als eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.

Bsp.:

Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren.

Zur Umsetzung der Schutzanforderungen raten wir zu einem IT Sicherheitskonzept. Hierbei bedienen wir uns in der Beratung der VdS 3473

https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf