QS Kornmann quality solutions

Schön, dass Sie dabei sind.

- Es folgen ca. 30 Minuten Vortrag
- Im Anschluss haben wir 30 Minuten Q&A reserviert
- Bei Fragen während des Vortrags bitte die Hand heben - über die entsprechende Funktion in Zoom
- Schreiben Sie auch gerne Fragen direkt in den Chat, diese beantworten wir nach dem Vortrag

  (während des Vortrags haben wir keinen Zugriff auf die Chatfragen)
- Wenn Sie die Folien als PDF erhalten möchten, senden Sie uns bitte eine E-Mail an: kontakt@qs-kornmann.de

QS Kornmann quality solutions

Datenschutz-Tipp

Die Datenschutzerklärung

Mai 2022

QS Kornmann quality solutions

IHR Ansprechpartner für Datenschutz, Qualitätsmanagement & Informationssicherheit

Die in diesem Dokument gezeigten Informationen und Empfehlungen basieren auf unserer Erfahrung und stellen keine rechtssichere Umsetzung sicher. Wir übernehmen keine Haftung.

Vorstellung QS-Kornmann

- Gründung in 2017
- Sitz in Mittelhessen zwischen Frankfurt und Kassel
- 5 Mitarbeiter
- Datenschutz
- Informationssicherheit nach ISO-27001
- Managementsysteme 9001/13485
- Betreuung von IMS Systemen auf SW-Basis
- Projektmanagement, Produktentwicklung Medizintechnik

QS-Kornmann
Sudetenstrasse 33
35625 Hüttenberg
06403 / 92 95 287

info@qs-kornmann.de
www.qs-kornmann.de

Unser Fokus liegt auf der Betreuung von Unternehmen in den Bereichen Datenschutz und Informationssicherheit

QS Kornmann quality solutions

Vita Michael Kornmann

- 2001 Erster Kontakt zu Managementsystemen
- 2002 Einstieg in die Medizintechnik - Fertigung und Technischer Service von Medizinprodukten sowie Betreuung Pharmastudien
- 2007 Wechsel zur Pharmaindustrie - FDA Audits, Montage weltweit mit Projektverantwortung
- 2017 Selbstständig in den Bereichen Datenschutz und Managementsystem
- 2018 Datenschutzbeauftragter
- 2019 Lead Auditor ISO13485:2016
- 2020 Lead Auditor ISO27001
- 2020 QMB ISO9001:2015
- 2022 Risikomanager

Allianz für Cyber-Sicherheit Teilnehmer

BvD e.V. Datenschutzbeauftragter nach Verbandskriterien verpflichtet Nr.: 100410

GDD Mitglied

DGQ Deutsche Gesellschaft für Qualität

DEKRA

Kornmann quality solutions

Jede gewerbliche Webseite benötigt eine Datenschutzerklärung.
In Deutschland ergibt sich dies aus den Informationspflichten der DSGVO Art. 13-14

- Viele Datenschutzerklärungen sind aber vollkommen überlaufen oder haben keine ausreichende Transparenz

- Weiterhin sind viele Datenschutzerklärungen so geschrieben, das keiner mehr einen Durchblick erhält

- Eine Datenschutzerklärung auf der Webseite gilt primär für die Webseite.
  Kann aber auch auf andere Bereiche ausgedehnt werden, wenn korrekt beschrieben

Datenschutz-Tipp 3 –Die Datenschutzerklärung-
Rechtlicher Hintergrund

QS Kornmann quality solutions

DSGVO Art. 13 und 14 beschreiben die Pflicht zu Beginn einer Verarbeitung, die betroffene Person zu informieren, wie, warum und welche Daten verarbeitet werden.

Die betrifft jede Verarbeitung und ist nicht pauschal auf „eine Webseite“ zu sehen.

- Newsletter
- Kontaktformular
- Allgemeiner Besuch
- Tracking
- Cookies
- ....

Art. 13 DSGVO

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Art. 14 DSGVO

Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder

Mögliche Umsetzung

QS Kornmann quality solutions

Folgende Punkte können hilfreich sein:

- Arbeiten Sie die Punkte aus Art.13-14 durch
- Definieren Sie den Umfang, über was die Datenschutzerklärung informieren soll
- Nutzen Sie gerne einen Generator, vertrauen Sie dem Generator aber nicht blind
- Geben Sie einen Hinweis auf Cookies
- Beschreiben Sie allgemeine Angaben wie Ihre Kontaktdaten, die des DSB, falls vorhanden, und belehren Sie über die Betroffenenrechte
- Beschreiben Sie für jede Funktion Ihrer Webseite Rechtsgrundlage, Zweck, Löschfrist, Empfänger, bei Übermittlung außerhalb des EWR die Rechtsgrundlage der Übermittlung, Infos über Profiling.
- Beschreiben Sie bei der Erhebung über Dritte die Kategorien und die Quellen.

Kornmann quality solutions

Häufige Fehler:

- Der Zweck der Datenschutzerklärung ist nicht eindeutig ersichtlich
- Es fehlen die Kontaktdaten der verantwortlichen Person
- Anfragen zum Datenschutz sollten nur die verantwortliche Person im Sinne der DSGVO erreichen und nicht an eine allgemeine Adresse, wie z.B. info@.... gesendet werden
- Es wird kein Kontakt zur zuständigen Behörde benannt
- Begriffe werden nicht erklärt
- Die Rechte werden nicht erklärt
- Die Datenschutzerklärung ist nicht mit einem Klick erreichbar
- Bei einem Kontaktformular muss vor dem Senden die Datenschutzerklärung eingewilligt werden
- Es wird zu viel beschrieben
- Es wird nicht das beschrieben was wirklich passiert

Datenschutz-Tipp 3 –Die Datenschutzerklärung-

Hilfreiche Links

- https://dsgvo-gesetz.de/art-14-dsgvo/
- https://dsgvo-gesetz.de/art-13-dsgvo/
- https://www.site-verifier.com
- https://www.datenschutzexperte.de/datenschutzerklaerung-generator/
- https://datenschutz-generator.de

Nutzen

Beschreibung	gering	mittel	hoch
Gute Außenwirkung		X	
Transparente Information		X	
Rechtssicherheit			X
Erfüllung DSGVO			X

Risiken

Beschreibung	gering	mittel	hoch
Scan Ihrer Seite mit entsprechender Abmahnung			X
Beschwerde von Webseiten-Besuchern		X	
Falsche Inhalte		X	
Falsche Rechtsgrundlagen			X

Zusammenfassung

Kosten

Beschreibung	Schätzkosten
Anschaffung	ggf. Anwaltskosten
Umsetzung	4-6h
laufende Lizenz-Kosten	-Keine-

Aufwand

Beschreibung	gering	mittel	hoch
Umsetzung selbst			X
Umsetzung mit Generator		X	
Umsetzung mit Anwalt, DSB		X	
Definition was wirklich in die Datenschutzerklärung gehört		X	

Fazit und Empfehlung

- Beachten Sie unsere Punkte zur möglichen Umsetzung
- Eine Datenschutzerklärung muss leicht zugänglich sein (1 Klick)
- Eine Datenschutzerklärung muss transparent beschreiben was Sie tun
- Eine Datenschutzerklärung muss verständlich sein
- Eine Datenschutzerklärung muss NICHT bestätigt werden,
  es ist ein Hinweis. (Kontaktformular)
- Eine Datenschutzerklärung zu bestätigen ist in der Regel auch KEINE wirksame Einwilligung

Fazit und Empfehlung

- Sie bleiben verantwortlich für Ihre Webseite. Eine Webagentur und auch Ihr DSB werden keine Verantwortung übernehmen
- Eine Datenschutzerklärung ist eine Visitenkarte für Ihr Unternehmen
- Beschreiben Sie Verfahren wie Bewerbung, online-Meeting usw. in getrennten Informationen um die Übersicht zu wahren.

Kornmann
quality solutions

News rund um das Thema Datenschutz und Informationssicherheit

- https://qs-kornmann.de
- https://qs-kornmann.de/blog
- https://qs-kornmann.de/newsletter
- https://qs-Kornmann.de/event
- https://qs365.de

Kostenfrei und nützlich

Zeit für Fragen und offene Diskussion

QS-Kornmann

Michael Kornmann
Sudetenstrasse 33
35625 Hüttenberg
06403 / 92 95 287

info@qs-kornmann.de
www.qs-kornmann.de

Vielen Dank für Ihre Aufmerksamkeit

Ihr Profi in Sachen
Datenschutz und Qualitätsmanagement