kisscal

STUDIO MANAGER
TATTOO & PIERCING

DS-Folgenabschätzung zu Risikofaktoren der Kunden

Stand 21.05.2018

Inhalt

Einleitung

Für eine sachgerechte Erstellung eines Tattoos bzw. Anbringen eines Piercings ist die vorherige Abfrage – bzw. deren Ausschluss – von sog. Risikofaktoren erforderlich. Diese umfassen im Wesentlichen:

- Allergien
- Ansteckende Infektionskrankheiten
- Medikamente (insb. Blutverdünner)

Daher ist es erforderlich, diese Informationen

- von den Kunden zu erheben (schriftlich mit Unterschrift),
- zu speichern (für die Termine(e) und aufbewahren hinsichtlich etwaiger Haftungsansprüche),
- den jeweiligen Tätowierern/Piercern zur Verfügung zu stellen.

Da es sich hierbei um sensible personenbezogene Daten handelt (Gesundheitsdaten), ist zu diesen Daten nach der aktuellen DSGVO eine Risikofolgenabschätzung erforderlich.

Gegenstand der DSFA

Gegenstand dieser Folgenabschätzung sind sämtliche Verarbeitungsvorgänge, welche die Risikofaktoren der Kunden (ggf. nur Teilweise) zum Gegenstand haben.

Betroffene Daten

Die Kundendaten werden über ein Erfassungsformular erhoben, welches der Kunde unterzeichnen muss:

Deine Daten (Your Data):

Name	Geschlecht (Gender)	Geburtstag (Birthday)
Adresse / Land (Address / Country)	Mobil (Mobile)	
	Festnetz (Landline)	
	EMail	
Beruf (professtion) Falls wir mal Deine professionelle Unterstützung gebrauchen können		

Krankheiten und Allergien (Deseases and Allergies)

Die Daten auf diesem Erfassungsbogen benötigen wir zur ordnungsgemäßen Durchführung unserer Arbeit. Mit Deiner Unterschrift willigst Du in die Nutzung und Speicherung dieser Daten ein. Um mögliche individuelle Risiken rechtzeitig erkennen und einschätzen zu können, ist zudem die sorgfältige Beantwortung der folgenden Fragen unerlässlich. Zutreffendes bitte ankreuzen:

[ ] Es besteht eine Bluterkrankung oder erhöhte Blutungsneigung.
[ ] Es besteht eine Hauterkrankung (Neurodermitis, Schuppenflechte etc.).
[ ] Ich nehme Medikamente zur Blutverdünnung (Marcumar, Aspirin, Heparin etc.).
[ ] Es bestehen folgende Allergien:
_____
[ ] Es bestehen Überempfindlichkeitsreaktionen (z.B. gegen Latex, Medikamente).
[ ] Ich habe eine Herz- oder Kreislauferkrankung bzw. neige zu Ohnmachtsanfällen.
[ ] Es besteht eine chronische Infektionskrankheit (z.B. AIDS, Hepatitis, MRSA).
[ ] Es besteht eine akute Infektionskrankheit (grippaler Infekt etc.).
[ ] Es bestehen andere schwerwiegende chronische Leiden (z.B. Epilepsie oder Lähmungen).
[ ] Ich könnte schwanger sein.
[ ] Ich stille derzeit mein Kind.

Uns bislang von Dir bekannt ist:

_____ _____
Ort, Datum Unterschrift

Bei den Risikofaktoren handelt es sich um die Angaben zu „Krankheiten und Allergien (Deseases and Allergies)“

Verarbeitungszweck

Diese Risikofaktoren werden u.a. benötigt, um

- Einen geplanten Eingriff (Tattoo/ Piercing) bei erhöhtem Risiko gar nicht erst stattfinden zu lassen (Schwangerschaft, Stillzeit, Infektionserkrankungen).
- Vor dem Angriff die Expertise des betreuenden Arztes einholen zu lassen (jede Art von Erkrankungen sowie blutverdünnende Medikamenteneinnahme).
- Die richtigen Hilfsmittel und Arbeitsmittel (Farben) zu verwenden (Allergien).
- Ggf. verschärfte Hygienemaßnahmen stattfinden zu lassen.

Außerdem muss der Artist bei evtl. Haftungsansprüchen in der Lage sein, nachweisen zu können, was ihm vom Kunden (in Treu und Glauben) mitgeteilt wurde und was nicht.

Notwendigkeit und Verhältnismäßigkeit

Da hier die Gesundheit des Kunden sowie anderer Kunden und Kollegen gefährdet sein kann, ist die Erhebung dieser Risikofaktoren für eine gewissenhafte Arbeit unerlässlich.

Rechtsgrundlage

Rechtsgrundlage dieser Risikofolgenabschätzung ist § 6 Abs. 1, UAbs. 1, lit b) und lit. f) der DSGVO vom 25.5.2018.

Risikobewertungen

Grundsätzliche Einstufungen

Aus „privacy officers“, Verein österreichischer betrieblicher & behördlicher Datenschutzbeauftragter

Eintrittswahrscheinlichkeit des Risikos

Einstufung	Beschreibung
Vernachlässigbar	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Datendiebstahl von den Servern des Betreibers des Studio-Management-Systems, gesichert durch SSL-Tunnel, Firewall, etc.).
Eingeschränkt	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl der Erfassungsformulare aus dem verschlossenen Schrank in einem Raum des Studios außerhalb des Publikumsverkehrs).
Signifikant	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl des Termin-Ordners (mit Erfassungsformularen) vom Arbeitsplatz des Tätowierers/Piercers.
Maximal	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Erfassungsformularen von der Theke im Empfang).

Auswirkungen aus Sicht des Betroffenen

Einstufung	Beschreibung
Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
Eingeschränkt	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Signifikant	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Bei diesem Risiko sind die Auswirkungen aus Sicht des Betroffenen grundsätzlich als Signifikant eingestuft werden, da es bei konkreten Erkrankungen (z.B. HIV, Hepatitis etc.) zu Diskriminierungen kommen kann, denen man sich nur mit viel Geduld oder durch einen Umzug entziehen kann.

Risikomatrix

Auswirkungen aus Sicht des Betroffenen	Maximal	Mittel	Mittel	Hoch	Hoch
	Signifikant	Mittel	Mittel	Mittel	Hoch
	Eingeschränkt	Gering	Mittel	Mittel	Mittel
	Vernachläss.	Gering	Gering	Mittel	Mittel
		Vernachläss.	Eingeschränkt	Signifikant	Maximal

Arten der Risikobehandlung

Risikominimierung	durch Setzen von Maßnahmen
Risikovermeidung	durch Unterlassen der risikobehafteten Aktivität, z. B. keine Erfassungsbögen mehr in physischen Terminordnern
Risikotransfer	durch Auslagerung von Risikofolgen auf Dritte, z. B. Versicherung bei Datenverlust
Risikoakzeptanz	bewusste Entscheidung, keine weiteren Maßnahmen zu treffen

Ausschließbare Risikos

Der Grundsatz der Datenminimierung ist beim Thema „Risikofaktoren“ grundsätzlich gesichert, da nur diejenigen Faktoren abgefragt werden, die eine Relevanz für den geplanten Eingriff (Tattoo/Piercing) haben.

Der Grundsatz der Intervenierbarkeit ist beim Thema „Risikofaktoren“ grundsätzlich gesichert, da die Risikofaktoren bei jedem neuen Termin erneut abgefragt werden müssen.

Risikobewertung: Vertraulichkeit

Diebstahl Erfassungsformulare durch Dritte

Risikobewertung	
Beschreibung der Bedrohung	Die Erfassungsformulare mit den Risikofaktoren des Kunden können durch Diebstahl in die falschen Hände geraten.
Eintrittswahrscheinlichkeit inkl. Begründung	Wenn diese unverschlossenen, wohl möglich im Einzugsbereich der Rezeption (Kundenverkehr) aufbewahrt werden, ist die Eintrittswahrscheinlichkeit Maximal.
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Hoch
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikominimierung
Begründung für die Auswahl der Risikobehandlung	Ausgefüllte Kundenerfassungsformulare werden in abgeschlossenen Schränken abseits des Kundenverkehrs aufbewahrt. Hier besteht eine Aufbewahrungspflicht (Haftung).
Dokumentation der Maßnahmen	Verarbeitungsverzeichnis
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	Eingeschränkt
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Diebstahl Erfassungsformulare durch Guest-Artists

Risikobewertung	
Beschreibung der Bedrohung	Die Erfassungsformulare mit den Risikofaktoren des Kunden können durch Diebstahl in die falschen Hände geraten.
Eintrittswahrscheinlichkeit inkl. Begründung	Für einen Guest-Artist ist es äußerst einfach, diese Formulare nach Ende seines Guest-Spots mitzunehmen, wenn diese (in Kopie) in seinem Terminordner abgelegt sind. Daher: maximal.
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Hoch
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikovermeidung
Begründung für die Auswahl der Risikobehandlung	Die Risikofaktoren sind NICHT mehr Bestandteil der Terminordner der Artists. Dort erfolgt lediglich eine Kennzeichnung, dass es zu einem bestimmten Kunden Risikofaktoren gibt, die der Artist dann von befugtem Personal des Studios abrufen kann.
Dokumentation der Maßnahmen	Verarbeitungsverzeichnis
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	Vernachlässigbar
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Weitergabe der „Risikofaktoren“ zu Kunden durch KissCal-Anwender

Risikobewertung	
Beschreibung der Bedrohung	Ein Mitarbeiter des Studios mit Zugriff auf KissCal kann die Risikofaktoren der Kunden einsehen und weitergeben.
Eintrittswahrscheinlichkeit inkl. Begründung	Es besteht grundsätzlich kein Anreiz für einen Mitarbeiter, die Informationen weiterzugeben. Ein Export dieser Informationen aus dem System ist nur für Administratoren möglich. Daher: vernachlässigbar.
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikominimierung
Begründung für die Auswahl der Risikobehandlung	Verschwiegenheitserklärungen
Dokumentation der Maßnahmen	Arbeitsverträge, Platzmietverträge
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	Vernachlässigbar
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Unbefugter Systemzugriff

Risikobewertung	
Beschreibung der Bedrohung	Nicht befugte greifen über KissCal auf die Risikofaktoren der Kunden zu und geben diese weiter.
Eintrittswahrscheinlichkeit inkl. Begründung	KissCal ist durch ein zweistufiges Login-Verfahren geschützt (Studio mit Passwort und Artist mit Passwort). Daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikoakzeptanz
Begründung für die Auswahl der Risikobehandlung	Weitere Maßnahmen sind im wirtschaftlichen Rahmen nicht möglich.
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	-
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Datenübertragung

Risikobewertung	
Beschreibung der Bedrohung	Daten können von unberechtigten Dritten abgegriffen werden, da die Übertragung zum Server unverschlüsselt und drahtlos erfolgt.
Eintrittswahrscheinlichkeit inkl. Begründung	Die Datenübertragung erfolgt verschlüsselt (SSL-Tunnel), daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikoakzeptanz
Begründung für die Auswahl der Risikobehandlung	Weitere Maßnahmen sind im wirtschaftlichen Rahmen nicht möglich.
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	-
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Risikobewertung: Integrität

Risikobewertung	
Beschreibung der Bedrohung	Die Risikofaktoren zum Kunden können durch Systemanwender jederzeit manipuliert werden.
Eintrittswahrscheinlichkeit inkl. Begründung	Zum einen besteht keine Motivation für Systemanwender, dies zu tun, zum anderen fragt der Artist vor dem Eingriff evtl. Risikofaktoren nochmals ab. Daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikoakzeptanz
Begründung für die Auswahl der Risikobehandlung	Weitere Maßnahmen sind im wirtschaftlichen Rahmen nicht möglich.
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	-
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Risikobewertung: Verfügbarkeit

Risikobewertung	
Beschreibung der Bedrohung	Die Daten stehen zum Termin nicht zur Verfügung, da die Verbindung zum Server (Internet) abgebrochen ist.
Eintrittswahrscheinlichkeit inkl. Begründung	Zum einen kann auf die Original-Formulare zurückgegriffen werden, zum anderen fragt der Artist vor dem Eingriff evtl. Risikofaktoren nochmals ab. Daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikoakzeptanz
Begründung für die Auswahl der Risikobehandlung	Weitere Maßnahmen sind im wirtschaftlichen Rahmen nicht möglich.
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	-
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Risikobewertung: Nichtverkettung

Risikobewertung	
Beschreibung der Bedrohung	Die sensiblen Kundendaten gelangen über Schnittstellen in andere Systeme und reichern dort bestehende Daten des Betroffenen an.
Eintrittswahrscheinlichkeit inkl. Begründung	KissCal gibt von sich aus diese Daten an kein System weiter. Ein Export der Daten ist lediglich für System-Administratoren möglich, die diese Daten manuell an andere Stellen weitergeben müssten. Daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikoakzeptanz
Begründung für die Auswahl der Risikobehandlung	Weitere Maßnahmen sind im wirtschaftlichen Rahmen nicht möglich.
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	-
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein

Risikobewertung: Transparenz

Risikobewertung	
Beschreibung der Bedrohung	Für den Betroffenen ist es nicht ersichtlich, was mit seinen Daten genau geschieht und wer alles Zugriff darauf hat.
Eintrittswahrscheinlichkeit inkl. Begründung	Wenn ein vollständiges VV vorliegt, ist dies ausgeschlossen, da jeder Kunde auf Grundlage der DSGVO Einsicht darin einfordern kann. Daher: Vernachlässigbar
Auswirkungen inkl. Begründung	Signifikant (s.o.)
Risikowert	Mittel
Abhilfemaßnahmen/Risikobehandlung	
Art der Risikobehandlung	Risikovermeidung
Begründung für die Auswahl der Risikobehandlung	Das VV liegt vor und wird laufend aktuell gehalten.
Dokumentation der Maßnahmen	Verarbeitungsverzeichnis
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (nach obigen Maßnahmen)	Vernachlässigbar
Risikowert	Mittel
Konsultation der Aufsichtsbehörde erforderlich?	Nein