Sensible Daten nach der EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

1. Was versteht man genau unter sensiblen personenbezogenen Daten für Unternehmen?

Die Verarbeitung personenbezogener Daten, „aus denen die rassische und ethnische 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" sind sensible Daten (siehe Artikel 9 DSGVO „Verarbeitung besonderer Kategorien personenbezogener Daten". Die „Verwendung des Begriffs ‚rassische Herkunft' in dieser Verordnung bedeutet nicht, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt", siehe Erwägungsgrund 51 DSGVO).

Beispiele: Fingerabdruck, Irisscan, Krankengeschichte.

2. Gilt das Erfassen des Geburtsdatums als sensibel? Oder "nur" personenbezogen?

Das Geburtsdatum selbst ist kein sensibles Datum. Es ist allerdings personenbezogen.

3. Personendaten: zählt das Geschlecht (female, male, other) zu den sensiblen Daten?

Nein.

4. Sind Passdaten sensible Daten?

Die abgedruckten Informationen im Pass selbst sind keine sensiblen Daten. Allerdings enthalten neuere Pässe einen Chip mit biometrischen Daten, sodass der Pass selbst Träger sensibler Daten ist.

5. Wir sind ein Sprachinstitut. Gelten Daten, wie das jeweilige Sprachniveau des Studenten oder sein Schulungsverlauf als sensible Daten?

Nein

6. Wir betreiben ein Online-Buchungstool und verarbeiten neben den allgemeinen Personendaten (Name, Adresse, Telefon, EMail, etc.) auch spezielle Informationen wie zB Laktoseintoleranz, Vegetarier, die uns die Kunden mitteilen, damit die Verpflegung in den gebuchten Betrieben entsprechend angepasst werden kann. Zählen diese Daten bereits zu "sensiblen" Daten?

Während Ernährungsgewohnheiten, die ohne zwingender Verbindung zum Gesundheitszustand stehen, keine sensiblen Daten sind, handelt es sich bei Allergien, Lebensmittelunverträglichkeiten udgl um Daten zur Gesundheit und damit um sensible Daten. Im konkreten Fall ist die Einholung der Einwilligung des Kunden eine praktikable Lösung.

7. Ich bin als Humanenergetiker tätig. Wir müssen eine Klientenaufklärung unterschreiben lassen und einen Klientenakt führen. Im Klientenakt ist die Vorgeschichte des Klienten auf zu zeichnen. d.h. der Klient schildert auch Beschwerden, Erkrankungen, Unfälle usw. Wie ist mit diesen Gesundheitsdaten genau umzugehen?

§ 3 Standesregeln der Humanenergetiker schreiben die Führung eines Klientenaktes vor; dieser ist sieben Jahre aufzubewahren. Es gibt daher eine gesetzliche Grundlage für die Datenverarbeitung.

Bei der Verarbeitung ist ua auf die Grundsätze und die Datensicherheitsmaßnahmen Bedacht zu nehmen.

8. Würden Sie die Daten einer Potenzialanalyse bzw. einer Persönlichkeitsanalyse als sensible Daten oder "nur" als personenbezogene Daten bezeichnen?
Was ist zu berücksichtigen, wenn sich Mitarbeiter mittels Fingerprint-Sensor an Laptops anmelden?

Sensible Daten sind personenbezogene Daten, aus denen die rassische und ethnische 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. Wenn sich aus einer Persönlichkeitsanalyse eine Krankheit ableiten lässt, dann enthält diese auch sensible Daten.

Die Identifizierung mittels Fingerprint wird in der Regel nur dann zulässig sein, wenn sich die Mitarbeiter aussuchen können, ob sie dieses Mittel verwenden und wenn das Template nur lokal gespeichert wird.

9. Ich bin Sportwissenschafterin und erfasse sensible Daten wie Blutdruck, Größe, Gewicht, Ruhefrequenz meiner Kunden - was muss ich konkret beachten?

Wenn es keine geeignete gesetzliche Grundlage gibt, brauchen Sie eine Einwilligung der Kunden.

Bei der Verarbeitung ist ua auf die Grundsätze und die Datensicherheitsmaßnahmen zu nehmen.

10. Wir sind eine medizinische Hilfsmittelfirma und erhalten Verordnungsscheine und Diagnosen per Mail und Fax. Wie sollen wir da vorgehen? / Ich bin Versicherungsmakler und leite auch sensible Daten an Versicherungsunternehmen weiter. Ist das per Mail erlaubt?

Unverschlüsselte E-Mails sind grundsätzlich keine geeignete Übermittlungsform für sensible Daten, insbesondere wenn die mitgeschickten Dateien ebenfalls unverschlüsselt sind. Gerade im Gesundheitsbereich wäre eine andere Handhabe zu empfehlen.

11. Was bedeutet das jetzt für einen selbstständigen Heilmasseur, der seine Dokumentationen (Gesundheitsdaten) der Therapien in einem Word Dokument speichert und keine weitere Verwendung damit hat (nur nachlesen was er an den jeweiligen Tagen mit den Patienten gemacht hat und vervollständigen)?

§ 3 Medizinischer Masseur- und Heilmasseurgesetz verpflichtet den Masseur zur Dokumentation seiner Tätigkeit. Eine gesetzliche Grundlage ist somit vorhanden.

Bei der Verarbeitung ist ua auf die Grundsätze und die Datensicherheitsmaßnahmen Bedacht zu nehmen.

Im geschilderten Fall wäre dies zum Beispiel: Löschen von Dokumentationen nach Ablauf der gesetzlichen Aufbewahrungsfrist, Absicherung des Endgerätes gegen unbefugte Inbetriebnahme (zB Passwortschutz), Back-Ups.

12. Wenn sensible (Gesundheits-) Daten - nur auf Papier - vorhanden sind, wie müssen diese physisch verwahrt werden (unter Verschluss)? Was muss hier zusätzlich beachtet werden?

Auf Papierakten ist die DSGVO genauso anwendbar, wenn es sich um sogenannte „Dateisysteme" handelt, das sind strukturierte Sammlungen personenbezogener Daten, die nach bestimmen Kriterien geordnet sind. Aus Datensicherheitsüberlegungen sind sensible Papierdokumente sicher aufzubewahren. Der Grad der Sicherheit (zB normaler Bürokasten oder Tresor) muss im Einzelfall bestimmt werden, aber der Verschluss des jeweiligen Aufbewahrungsorts mit entsprechender Zugriffsberechtigung ist ein guter erster Ansatz.

13. Fällt die Erfassung des Religionsbekenntnis unter die sensiblen Daten?

Ja.

14. Wir bieten Englischkurse für Kinder an. Für die Sicherheit des Kindes fragen wir, ob die Kinder Allergien haben oder ob es etwas gibt, was wir wissen sollen. Sind das "sensible Daten" auf einem Anmeldeformular, der sonst Kontaktdaten beinhaltet?

Vorausgesetzt Sie sind ein privater Anbieter: Adaptieren Sie das Anmeldeformular so, dass es als Einwilligungserklärung dienen kann.

Muster finden Sie hier. Allergien sind Gesundheitsdaten, sind sensible Daten, dh Sie brauchen eine gesetzliche Grundlage für die Verarbeitung oder eine Einwilligung des Betroffenen.

15. Sind die Daten beim Tierarzt (Behandlungsdaten, Labordaten, Röntgen, etc.) als sensible Daten anzusehen?

Sofern sich die Frage auf die Daten eines Tieres bezieht, nein. Die DSGVO ist nur auf die Daten von Personen anwendbar.

16. Welche IT Maßnahmen sind notwendig, um sensible Daten zu schützen? zB wie muss der Passwortschutz sein oder ist es erlaubt, dass auch ein IT-Administrator auf sensible Daten zugreifen kann oder wirklich nur der zB Personalverantwortliche

Dazu kann keine allgemeine Aussage getroffen werden, da es sehr stark vom jeweiligen Einzelfall abhängt (welche Daten, welche Risiken, welche Branche, welche technischen Möglichkeiten,...). Gibt es nachvollziehbare technische Gründe, warum der IT-Administrator Zugriff benötigt, wird dies im Regelfall auch erlaubt sein.

Mehr dazu hier.