CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Datenschutz und -Ethik: Das Quiz

Frage 1 – Wie viele Unternehmen in Deutschland haben die DSGVO komplett umgesetzt (Stand Sep. 20)?
Antwort: 20 Prozent – trotz drohender Sanktionen!

Frage 2 – Nenne einen der Gründe, warum deutschen Unternehmen die Umsetzung der DSGVO so schwerfällt.
Antwort:

1. *Anhaltende Rechtsunsicherheit (74%)*
2. *Änderungen und Anpassungen bei der Auslegung (68%)*
3. *Fehlende Umsetzungshilfen durch Aufsichtsbehörden (59%)*
4. *Uneinheitliche Auslegung der Regeln in der EU (45%)*
5. *Fehlendes Fachpersonal (26%)*

Frage 3 – Wann wurde der Datenschutz in Deutschland erstmals eingeführt?
Antwort: 1977 – mit dem ersten Bundesdatenschutzgesetz.

Frage 4 – Seit wann gilt die DSGVO?
Antwort: 2018 – der Beschluss selbst trat aber bereits 2016 in Kraft.

Frage 5 – Aus welchen verfassungsrechtlichen Grundsätzen ergibt sich der Datenschutz?
Antwort: Art 1 I. – Die Würde des Menschen ist unantastbar – und Art 2 I. – Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, die zusammen das Allgemeine Persönlichkeitsrecht (APR) ergeben.

Frage 6 – Was ist der Unterschied zwischen Datenschutz und Datensicherheit?
Antwort: Als Datenschutz bezeichnet man den Schutz der verfassungsrechtlich garantierten Persönlichkeitsrechte, während mit Datensicherheit die praktische Umsetzung des Datenschutzes durch strukturelle Maßnahmen und eine funktionierende IT gemeint ist.

Frage 7 – Welche Datenschutzrichtlinie gilt für die Katholische Stiftungshochschule in München im Gegensatz zur Technischen Universität München?
Antwort: Für Erstere gilt das Gesetz über den Kirchlichen Datenschutz (KDG), für Letztere das Bayrische Hochschulgesetz (BayHSchG).

Frage 8 – Welche zwei Prinzipien gelten bei der Anwendung von Datenschutzrichtlinien mit demselben Schutzbereich?
Antwort: Das Subsidiaritätsprinzip und die Normenhierarchie, die besagen, dass zwar grundsätzlich das speziellste Datenschutzgesetz anzuwenden ist, bei Auslegungsfragen oder (eigentlich zu vermeidenden) Widersprüchen die DSGVO anzuwenden ist.

Frage 9 – Welche Daten werden von der DSGVO geschützt?
Antwort: Personenbezogene Daten, also „alle Informationen, durch die eine natürliche Person, also Menschen, direkt oder indirekt identifiziert werden oder identifizierbar sind, also durch Merkmale, die Ausdruck der physischen, physiologischen, genetischen,

psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind". Daten von nicht-natürlichen, also juristischen Personen, wie Vereinen und Unternehmen sind also nicht von der DSGVO geschützt. Hier gelten ggf. das Geschäftsgeheimnisgesetz (GeschGehG) sowie bilateral getroffene Vereinbarungen zur Datenverarbeitung.

Frage 10 – Was versteht die DSGVO unter Datenverarbeitung?
Antwort: Das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung, Veränderung, das Auslesen, Abfragen, die Verwendung, Offenlegung, den Abgleich, die Verknüpfung, Einschränkung, Löschung oder Vernichtung in automatisierten und nicht-automatisierten Vorgängen – also eigentlich alles, was man mit Daten tun kann.

Frage 11 – Welche sieben Kernpflichten umfasst die DSGVO?
Antwort: Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Datenreduktion, Vertraulichkeit und Rechenschaft

Frage 12 – Da Ihr Euch leicht fiebrig fühlt, besucht Ihr eine neue Ärztin unweit Eurer Wohnung. Bevor sie Euch behandelt, bittet Euch der Arzthelfer den Anamnesebogen auszufüllen. Anbei findet Ihr eine Einwilligungserklärung zur Datenverarbeitung. Abgefragt werden im Anamnesebogen Kontaktdaten, Eure gesundheitliche Historie und Eure derzeitigen Beschwerden. Sind die Dokumente aus rechtlicher Sicht unbedenklich? Könnt Ihr die Einwilligung ablehnen und trotzdem eine Behandlung verlangen?
Antwort: Anamnesebogen und Einwilligungserklärung sind zwar rechtlich unbedenklich, aber auch nicht erforderlich. Zwar handelt es sich hierbei um Gesundheitsdaten, deren Verarbeitung auf Grund der besonderen Schutzwürdigkeit gem. Art. 9 I DSGVO prinzipiell verboten ist, jedoch gilt dies nicht, wenn dies zum Zweck der Gesundheitsvorsorge erforderlich ist (Art. 9 II h). Eure Einwilligung ist also gar nicht notwendig, um Eure Daten zu verarbeiten. Die ärztliche Behandlung darf Euch dabei auf keinen Fall verweigert werden – es gilt auch in Deutschland trotz DSGVO noch der Grundsatz des Hippokratischen Eides.

Frage 13 – Wie viele Gruppenmitglieder braucht es pro Merkmalskombination, um bei aggregierten Daten von einer Anonymisierung auszugehen?
Antwort: Gem. §16 Bundesstatistikgesetz (SAFE) mindestens drei – oder gar keine.

Frage 14 – Weil Ihr den morgendlichen und bitter benötigten Kaffee über Euren Arbeitslaptop verschüttet, verliert Ihr die Mitgliedsdaten Eures 20 Mitglieder starken Vereins, die Ihr lokal in einer Excel gespeichert hattet. Die Daten sind unwiderruflich verschwunden. „Kein Problem", denkt Ihr, „für von Kaffee eliminierte Daten bin ich ja nicht haftungspflichtig." Ist das richtig?
Antwort: Nein. Eure sieben Kernpflichten (Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Datenreduktion, Vertraulichkeit und Rechenschaft) beinhalten gem. Art. 5 DSGVO auch den Grundsatz der Vertraulichkeit. Damit seid Ihr verpflichtet Daten durch dem Risiko angemessene technische und organisatorische Maßnahmen vor Zugriff und Verlust zu sichern. Dass Endgeräte kaputtgehen, ist durchaus zu erwarten. Eine doppelte Datensicherung durch externe, digitale Speicher wie USB oder Cloud-Lösung ist notwendig. Die Datenpanne (Art. 4 DSGVO) könnt, müsst Ihr aber nicht innerhalb von 72h der zuständigen Behörde melden, da das Risiko für

Betroffene hier nicht weiter beachtlich ist. Den Vorfall sowie Eure Überlegungen zur Meldepflicht solltet Ihr trotzdem dokumentieren.

Frage 15 – Zum Austausch von personenbezogenen Daten nutzt die HR-Abteilung Eures Unternehmens passwortgeschützte Ordnerstrukturen in der Google Cloud. Zugang haben lediglich Mitarbeitende der Personalabteilung. Ist das unbedenklich?
Antwort: Nein. Es ist zwar lobenswert, dass die hochsensiblen Daten durch Passwörter geschützt werden, aber Google ist ein US-Amerikanischer Anbieter, weshalb mit dem Kippen des Privacy Shields 2020 (Schrems I) das Nutzen von US-Amerikanischen Tools zur Speicherung personenbezogener Daten unzulässig ist. Das ist zwar erstmal eine ziemlich schlechte Nachricht, aber auch wir sind derzeit noch in der Umstellung – und erwarten hier auch Korrekturen und Eingriffe der Gesetzgebenden. Bis dahin fördern wir – wo möglich – digitale Tools aus der EU oder hosten Alternativen, wie z.B. IDGARD oder eine eigene Instanz von NextCloud.

Frage 16 – Eurer Projektpartner bittet Euch bei der geplanten Datenanalyse zur Polizeilichen Kriminalitätsstatistik (PKS) vorhandene demographische Merkmalen (Geschlecht und Nationalität) zu berücksichtigen. Ihr findet das Ganze etwas fishy – zu Recht? Was könnt Ihr tun?
Antwort: Die Polizeiliche Kriminalstatistik enthält viele spannende Daten – allerdings kann die geplante Analyse – falls statistische signifikante Beobachtungen gemacht werden - leicht politisiert werden, z.B. um für die Ausweisung von Migrant:innen zu werben. Besonders kritisch ist hier auch, dass die Polizeistatistik neben den genannten Merkmalen wenig Informationen zu sonstigen demographischen Merkmalen enthält, weshalb sog. Confounding Variables (zu dt. Störfaktoren) wie Alter und Einkommen nicht identifiziert werden können. Am besten meldet Ihr Euch in solchen Fällen an CorrelAid's Ethikbeauftragte Nina Hauser (nina.h@correlaid.org).

Frage 17 – In einer geplanten Feedback-Umfrage fragt Ihr nach dem Geschlecht der Mitglieder. Ihr überlegt Euch folgende Fragestellung:

Was ist dein Geschlecht?
- Männlich
- Weiblich
- Das möchte ich nicht angeben.

Was könnten hierbei Herausforderungen sein?
Antwort: Zunächst könnte man hier hinterfragen, ob es überhaupt notwendig ist, nach dem Geschlecht zu fragen. Ein Grund könnte sein, dass Ihr Frauen besonders fördern möchtet, weshalb Ihr Feedback für Euch besonders wichtig ist. Andernfalls lasst die Frage lieber weg. Die Formulierung sollte außerdem angepasst werden:

Was ist dein Geschlecht?
- *Das möchte ich nicht angeben (Opt Out)*
- *Weiblich (es muss auch nicht immer der Mann zuerst kommen)*
- *Männlich*
- *Non-binary (Allgemeines Alternativfeld)*
- *Mein Geschlecht ist: [Freitextfeld] (zur Selbstidentifikation)*

Schön fanden wir auch die Überlegungen und Ausführungen hier.