Überblick über die Datenschutz-Grundverordnung der EG (DSGVO)

Strafen von bis zu €20.000.000 oder bis zu 4% des jährlichen weltweiten Gesamtumsatzes, je nachdem, welcher Betrag höher ist.

Personenbezogene Daten

''Ist die Verarbeitung von personenbezogenen Daten erlaubt?'

Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten Die Rechtmäßigkeit ist gegeben, wenn eine eindeutige Einwilligung erteilt wird bzw. wenn sie für die Vertragserfüllung, Erfüllung einer gesetzlichen Verpflichtung, zum Schutz lebenswichtiger Interessen, für die Durchführung von Aufgaben im öffentlichen Interesse oder für den Zweck eines berechtigten Interesses erforderlich ist. Ein berechtigtes Interesse besteht bei Behörden nicht mehr.	6
Grundsätze für die Verarbeitung von personenbezogenen Daten Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Verantwortlichkeit.	5
Nachweisliche Zustimmung für bestimmte Zwecke (falls die Zustimmung als rechtmäßiger Grund für die Verarbeitung verwendet wird). Organisationen müssen nachweisen können, dass sie Zustimmung erhalten haben. Die Zustimmung kann jederzeit zurückgezogen werden. Schriftliche Einwilligungserklärungen müssen unmissverständlich sein und von anderen Angelegenheiten deutlich abgegrenzt sein.	7
Übermittlung von personenbezogenen Daten Die Übermittlung außerhalb der EU ist nur unter bestimmten Bedingungen gestattet. Multinationale Unternehmen können verbindliche unternehmensinterne Vorschriften erstellen, die die Zustimmung einer zuständigen Aufsichtsbehörde erfordern.	45-47
Spezielle Kategorien von personenbezogenen Daten (wie politische Meinungen, religiöse Ansichten, Gesundheit, sexuelle Orientierung etc.) Die Verarbeitung von speziellen Kategorien personenbezogener Daten ist untersagt bzw. unterliegt strengen Auflagen.	9
Zusätzlicher Schutz für Kinder unter 16 Jahren Die Verarbeitung von persönlichen Informationen von Kindern unter 16 ist nur mit Zustimmung oder Erlaubnis des gesetzlichen Vertreters gestattet. Organisationen müssen angemessene Anstrengungen unternehmen, um die Zustimmung zu überprüfen.	8
Profiling Das Profiling mit rechtlichen Folgen ist nur unter bestimmten Umständen erlaubt. Falls das Profiling einen wesentlichen Einfluss auf die betroffene Person hat, hat er/sie das Recht, sich einer solchen Entscheidung nicht zu unterwerfen, wenn sie nur auf einer automatisierten Verarbeitung beruht.	22
Ausnahmen für bestimmte Zwecke Die Regelung gilt nicht für die Archivierung für Zwecke im öffentlichen Interesse sowie für wissenschaftliche, geschichtliche oder statistische Zwecke.	5/89

Umgang und Pflege

'Wie wird die Privatsphäre aufrecht erhalten?'

Implementierung und Dokumentation Organisationen müssen unter anderem die von ihnen selbst oder von ihren Lieferanten durchgeführte Verarbeitung, die Art der betroffenen Personen, die Zwecke der Verarbeitung und die getroffenen Sicherheitsmaßnahmen analysieren. In einigen Fällen müssen Organisationen Aufzeichnungen über die Verarbeitungstätigkeiten führen.	5/24/ 30
Prüfung, Bearbeitung und Abschluss von Datenverarbeitungsverträgen Die Verarbeitung von personenbezogenen Daten unterliegt einem Vertrag (Datenverarbeitungsvertrag) zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter.	28/ 29
Risikoanalyse und DSFA (DSFA/Einhaltungsprüfung) Sowohl für vorhandene als auch neue Dienstleistungen muss eine Risikoanalyse durchgeführt werden. Für Dienstleistungen oder Systeme mit hohem Risiko muss eine Datenschutzfolgenabschätzung (DSFA) durchgeführt werden.	24/ 35
Informationssicherheit Organisationen müssen geeignete technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten zu schützen.	24/ 32/ 35
Verwaltung von Zustimmungen und Rechten der betroffenen Personen Systeme und Verfahren müssen so konzipiert und verwaltet werden, dass Betroffenenrechte gewährleistet werden.	7/15-19
Datenübertragbarkeit Die betroffenen Personen haben das Recht eine Kopie ihrer personenbezogenen Daten in elektronischer und verwendbarer Form zu erhalten.	20
Richtlinien und die Implementierung von technischen und organisatorischen Maßnahmen Organisationen sollten Richtlinien erstellen und müssen in der Lage sein, den Einsatz von angemessenen technischen und organisatorischen Maßnahmen nachweisen zu können, durch die Compliance und transparente Verarbeitung personenbezogener Daten sichergestellt wird.	24/ 32
Aufbewahrung Beschränken Sie den Speicherzeitraum und löschen oder archivieren Sie die Daten (falls erlaubt) rechtzeitig.	5/89

Organisation

'Wie wird der Datenschutz in Ihre Organisation eingebettet?'

Datenschutzbeauftragter In einigen Fällen müssen die Organisationen einen Datenschutzbeauftragten ernennen, zum Beispiel, wenn die Verarbeitung von öffentlichen Stellen durchgeführt wird, wenn Verarbeitung ein Kerngeschäft ist oder wenn große Mengen von speziellen personenbezogenen Daten verarbeitet werden.	37-39
Die Rechte der betroffenen Personen (Zugang, Berichtigung, Löschung, Entschädigung, Einspruch) Implementieren Sie Verfahren in Bezug auf die Ausübung von Rechten. Die betroffenen Personen können Informationen über Verarbeitungszwecke, Datenkategorien, Empfänger und Aufbewahrung verlangen sowie deren Berichtigung oder Löschung beantragen. Betroffene Personen haben das Recht eine Beschwerde einzureichen und können gegen eine automatisierte Entscheidungsfindung (Profiling) Einspruch erheben.	15-18 21/ 22/ 24
Meldung von Datenschutzverletzungen Implementieren Sie Verfahren zur Meldung von Datenschutzverletzungen.	33/ 34
Geschultes Personal und eine datenschutzbewusste Organisation Um Risiken zu minimieren, müssen Organisationen und ihre Mitarbeiter die Schlüsselelemente der Gesetzgebung kennen und entsprechend handeln.	5/24/ 28
Relevanz des Datenschutzes für (die Entwicklung) von Produkten und Dienstleistungen (Datenschutz durch Technikgestaltung/Voreinstellungen) Integrieren Sie Datenschutz in die Entwicklung von neuen Produkten und Dienstleistungen.	25
Zertifizierung Die Organisationen werden ermutigt, sich im Bereich Datenschutz zertifizieren zu lassen (zum Nachweis der Einhaltung der Vorgaben). Ein Zertifikat kann von Zertifizierungsstellen ausgestellt werden, die durch die Aufsichtsbehörde und/oder die nationale Akkreditierungsstelle anerkannt sind.	42/ 43/ 83
Beaufsichtigung Die Aufsichtsbehörde im Land der Hauptniederlassung der Organisation übernimmt die Verantwortung für die Beaufsichtigung.	56/ 60

Kommunikation

'Wie wird über Datenschutz kommuniziert?'

Klare und verständliche Kommunikation über Daten Informationen und Kommunikation über die Datenverarbeitung, die Rechte der betroffenen Personen und die Datenschutzerklärung sollten verständlich sein und in einfacher (allgemeiner) Sprache verfasst werden, besonders wenn sie sich an Kinder richten.	7/8/ 14/ 15/ 21
Meldung von Datenschutzverletzungen an die Aufsichtsbehörde und Stakeholder Datenschutzverletzungen müssen der Aufsichtsbehörde innerhalb von 72 Stunden gemeldet werden und erfordern in einigen Fällen eine sofortige Benachrichtigung der betroffenen Personen. Falls die Meldung an die Aufsichtsbehörde nicht innerhalb von 72 Stunden erfolgt, müssen die Gründe für die Verspätung genannt werden.	33/ 34
Kontaktdaten des Datenschutzbeauftragten Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht und an die zuständige Aufsichtsbehörde gesandt werden. Stakeholder müssen in der Lage sein, den Datenschutzbeauftragten zu kontaktieren, um ihre Rechte ausüben zu können.	37
Kommunikation mit der Aufsichtsbehörde Die Aufsichtsbehörde kann Dokumente und Informationen anfordern und hat das Recht, Zugang zu allen personenbezogenen Daten und zu den entsprechenden Speicherorten zu erhalten.	31/ 58
Einspruch gegen das Profiling Die betroffenen Personen müssen ausdrücklich über ihr Einspruchsrecht gegen das Profiling informiert werden.	22
Offenheit über die Aufzeichnung von Verarbeitungstätigkeiten Auf Anfrage müssen Aufzeichnungen der Aufsichtsbehörde zur Verfügung gestellt werden. Alternativ kann die Aufzeichnung der Verarbeitungstätigkeiten oder ein Überblick der Verarbeitungstätigkeiten veröffentlicht werden. Dies fördert Transparenz und Verantwortlichkeit.	30
Informationen zur Einholung einer gültigen Zustimmung Beruht eine Verarbeitungstätigkeit auf Zustimmung, muss der Verwendungszweck vorher klar und verständlich erklärt werden.	6