WIRTSCHAFTSKAMMER WIEN
Die Kaffeehäuser

Datenschutzleitfaden

Fachgruppe Wien der Kaffeehäuser
Sparte Tourismus und Freizeitwirtschaft

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

Inhaltsverzeichnis

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

1 Einleitung

Mit 25. Mai 2018 tritt die neue Datenschutz-Grundverordnung (DSGVO) in Kraft. Kaffeehäuser müssen so wie alle anderen Unternehmer künftig detailliert darlegen, welche personenbezogenen Daten von ihnen verarbeitet werden, wo diese liegen und wohin sie weitergeben werden.

Die wichtigsten Punkte betreffen folgende Bereiche:

- **Umgang mit Kundendaten:** In vielen Betrieben werden persönliche Daten verarbeitet und die Gäste müssen sich grundsätzlich damit einverstanden erklären. Bisher genügte es, dass der Gast der Nutzung nicht aktiv widersprach. Das beutet auch, dass ein Newsletter-Versand in der Regel nur mit ausdrücklicher Zustimmung des künftigen Empfängers möglich ist.
- **Dokumentationspflicht:** Zu mehr bürokratischem Aufwand für Kaffeehäuser dürfte die Neureglung der Nachweis- und Rechenschaftspflichten führen. So muss dokumentiert werden, dass alle geeigneten Maßnahmen ergreifen werden, um personenbezogene Daten rechtskonform zu bearbeiten. Der Betrieb muss also beweisen, dass er alles richtig gemacht hat.
- **Mitarbeiter:** Die Wahrung des Datenschutzes ist auf Anforderung der Datenschutzbehörde jederzeit nachzuweisen. Ein solcher Nachweis kann über verabschiedete bzw. nachweislich zur Kenntnis gebrachte Regeln & Richtlinien für Mitarbeiter und den Nachweis deren Einhaltung (Monitoring, Protokollierung) erbracht werden.
- **Bewerbungsunterlagen:** Grundsätzlich ist die Verarbeitung von personenbezogenen Daten während und im Zuge einer Stellenbesetzung vom Datenschutzrecht gedeckt und auch zulässig. Nach Besetzung der ausgeschriebenen Stelle erlischt allerdings der Verwendungszweck zur weiteren Verarbeitung der Bewerbungsunterlagen und sämtliche Bewerbungsunterlagen wären unverzüglich und unwiederbringlich zu vernichten.
- **Videoüberwachung:** Der Einsatz von Videoüberwachungssystemen ist in den geltenden Datenschutzregularien streng geregelt und Anlagen nur dann datenschutzrelevant, wenn Daten aufgezeichnet werden. Reine Live Bilder ohne Aufzeichnung sind (meist) nicht vom Datenschutzgesetz betroffen (Ausnahmen: sie überwachen fremde private oder öffentliche Bereiche und sie können zur Begehung von Straftaten herangezogen werden).
- **Datenschutzerklärungen:** Eine Datenschutzerklärung erfüllt einen Teil der Informationspflicht für Betroffene wird immer dann benötigt, wenn ein Unternehmen über ein Onlinemedium in die „Öffentlichkeit“ tritt. Traditionell geschieht das bei Webseiten oder beim Versand von Newslettern. Die Datenschutzerklärung hat zu beschreiben, welche personenbezogenen Daten das Unternehmen bzw. die Webseite verarbeitet.

Um die notwendigen Maßnahmen treffen zu können, ist in einem ersten Schritt die Erhebung über den Status Quo der derzeitigen Datenverarbeitungen erforderlich. Zu erheben ist im Wesentlichen, welche Daten verarbeitet, wie diese gesammelt und wie lange diese aufbewahrt oder eventuell auch noch ob diese weitergegeben werden.

Auf den folgenden Seiten wird neben einer Einführung in die relevanten Grundbegriffe auch ein Verständnis für die wichtigsten Themen geschaffen, die für Kaffeehäuser von Relevanz sind.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

2 Europäische Datenschutz Grundverordnung (EUDSGVO)

Die EU hat eine, für alle Mitgliedsstaaten gültige, Verordnung zum Zweck der Aufrechterhaltung, bzw. zur Erreichung, eines einheitlichen Datenschutzlevels erlassen. Damit wird in der gesamten EU dasselbe Datenschutzgesetz mit identischen Regeln gelten. Da es sich hier um eine Verordnung handelt, ist diese direkt in nationales Recht zu überführen. Diese Verordnung wurde im Mai 2016 erlassen. Wie bei EU Verordnungen üblich, gibt es eine Art Schonfrist von 2 Jahren, d.h. die Gesetze dieser Verordnung wurden zwar schon in Kraft gesetzt, sind aber noch nicht anwendbar. Die Anwendbarkeit dieser Gesetze beginnt am 25. Mai 2018.

In dieser Verordnung wurde Datenschutz zu einem europäischen Grundrecht erklärt. Auch wurde ein erweiterter Anwendungsbereich definiert. Die entsprechenden Gesetze gelten nun auch außerhalb der EU, wenn Betroffene innerhalb der EU beteiligt sind.

Generell definiert die EUDSGVO eine wesentlich verstärkte Eigenverantwortlichkeit für Unternehmen, d.h. viele Aufgaben, die bisher von Behörden zu erfüllen waren, sind nun Aufgabe der Unternehmen. Dadurch erhöht sich natürlich der Aufwand für die Aufrechterhaltung des Datenschutzes in den Unternehmen, was derzeit von vielen sträflich unterschätzt wird.

Das Strafmaß für Verstöße gegen die EUDSGVO wurde drastisch erhöht. Durch diese Strafen sind grundsätzlich alle in der EUDSGVO enthaltenen Rechte, Pflichten und Bestimmungen bedroht, d.h. je nach Verstoß können bis zu € 10 Mio. bzw. 2% des weltweiten Jahresumsatzes oder bis zu € 20 Mio. bzw. 4% des weltweiten Jahresumsatzes fällig werden. Verwarnungen oder Vorwarnungen sind in der EUDSGVO stark eingeschränkt bzw. gar nicht vorgesehen!

2.1 Grundbegriffe

Im Sprachgebrauch der DSGVO werden wiederholt diverse Begriffe verwendet. Zum besseren Verständnis, werden die wichtigsten Begriffe im Folgenden erklärt.

2.1.1 Personenbezogene Daten

Personenbezogene Daten sind alle Daten, die zur Identifizierbarkeit einer Person beitragen können, z.B. persönliche Interessen, Standortdaten, Schulden, Einkommen, Bilder der Statur, etc.

Beispiele für personenbezogene Daten:

Name	Gewicht	Zuverlässigkeit	Persönliche Interessen
Geburtsdatum	Haar- und Augenfarbe	Karriereplanung	Freizeitverhalten
Geburtsort	Kleidergröße	Persönliche Verhältnisse	Standortdaten
Wohnanschrift	Familienverband	Unwahrheiten	Ortswechsel
Beruf	Wirtschaftliche Lage	Beschimpfungen	Lebenslauf
Staatsangehörigkeit	Kreditwürdigkeit	Verspottung	Schulbesuche
Geschlecht	Charaktereigenschaften	Verleumdungen	Kontaktdaten
Körpergröße	Arbeitseinstellung	Vorlieben	E-Mail-Adresse
Online-Kennung	Sozialversicherungsnummer	Schulden	Aufnahmen des äußeren Erscheinungsbildes (Gesicht, Statur, Haltung)
Benutzernamen	Kontoinformationen	Rechtliche Verhältnisse	Video- und Audioaufnahmen
IP Adresse	Kreditkartennummer	Melderegisternummer	….
Telefonnummer	Einkommen/Gehalt	Personenkennzeichen	

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

2.1.2 Sensible Daten

Sensible Daten bzw. besondere Datenkategorien sind eine Spezialform der personenbezogenen Daten. Diese Datenarten bergen für Betroffene ein besonders hohes Risiko für die Beeinträchtigung ihrer Integrität und ihrer informationellen Selbstbestimmung. Daher sind diese Daten auch mit besonderer Sorgfalt zu behandeln und von hohen Strafen bedroht. Ist deren Verarbeitung für ein Unternehmen nicht zwingend notwendig, so sollte die Verarbeitung unterlassen werden. Eventuell bereits vorhandene Daten dieser Art sollten daraufhin auch unwiederbringlich vernichtet werden. Die Art und der Umfang dieser Daten ist, anders als bei den personenbezogenen Daten, endlich bzw. abgeschlossen, d.h. zu den sensiblen Daten bzw. den besonderen Datenkategorien gehören ausschließlich folgende Datenarten:

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Gesundheitsdaten
- Sexualleben und sexuelle Orientierung
- Biometrische Informationen (Gesichtsbild, Stimmbild, Papillarlinien, Irismuster, etc.)
- Genetische Informationen

2.1.3 Auftraggeber bzw. Verantwortlicher

Der Auftraggeber bzw. Verantwortliche ist jene Person oder jenes Unternehmen, die personenbezogene Daten verarbeiten, also sammeln, speichern, verwenden, auswerten, etc.

2.1.4 Dienstleister bzw. Auftragsverarbeiter

Eine Dienstleister oder Auftragsverarbeiter ist jene Person oder jenes Unternehmen, das personenbezogene Daten im Auftrag einer anderen Person oder eines anderen Unternehmens verarbeitet.

2.1.5 Betroffener

Ein Betroffener ist jene Person, deren personenbezogene Daten verarbeitet werden, die also sozusagen der Eigentümer der personenbezogenen Daten ist.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

3 Anforderungen aus der EUDSGVO

In der europäischen Datenschutz Grundverordnung sind diverse Anforderungen und Aufgaben festgelegt, die von Verantwortlichen/Auftraggebern bzw. Auftragsverarbeitern/Dienstleistern (siehe Kapitel 1.1.3 und 1.1.4) zu erfüllen sind. Meist handelt es sich hierbei um zu erstellende Dokumente und Dokumentationen, aber es sind auch technische Rahmenbedingungen und Pflichten definiert. Diese Anforderungen bzw. Aufgaben werden im Folgenden kurz erläutert.

3.1 Datenerhebung

Eine Erhebung bzw. Analyse der IST Situation im Umgang und bei der Verarbeitung personenbezogener Daten (siehe Kapitel 2.1.1 und 2.1.2) ist durchzuführen und zu dokumentieren. Dabei ist zu dokumentieren, welche personenbezogenen und/oder sensiblen Daten derzeit auf welche Art („Verfahren“) verwendet werden, wer darauf Zugriff hat und wo bzw. wie sie gespeichert sind, z.B. Kunden-/Lieferantenlisten mit Kontaktinformationen, Bewerbungen, Dienstverträge oder .

Im Zuge dessen sind auch die technischen und organisatorischen Gegebenheiten festzuhalten. Dazu gehören Beschreibungen der eingesetzten technischen Infrastruktur (Server, PC, Netzwerk, WLAN, Videoüberwachung, Software, mobile Geräte, Internet, Email, Social Media, Cloud, etc.) und der organisatorischen Rahmenbedingungen (Regeln & Richtlinien für Mitarbeiter, Dienstleister, Verantwortlichkeiten, Berechtigungen, Vertragsverhältnisse, Prozesse, Aufbewahrungsfristen, etc.) Zu erheben ist auch woher die Daten stammen, zu welchem Zweck sie verarbeitet werden, an wen sie übermittelt werden, wo sie gespeichert sind und wie lange sie aufbewahrt werden.

Im Zuge der Erhebung empfehlen wir auch die Vernichtung aller personenbezogenen Daten, die nicht unbedingt weiterhin benötigt werden. Dies gilt sowohl für digitale Daten als auch Daten auf Papier.

3.2 Verfahrensverzeichnis

Die Verarbeitungen von personenbezogenen Daten sind lt. EUDSGVO zu dokumentieren. Zu diesem Zweck wird die Erstellung eines sogenannten Verfahrensverzeichnisses gefordert. Darin sind alle „Verfahren“, in denen personenbezogene und/oder sensible (siehe Kapitel 2.1.1 und 2.1.2) Daten verarbeitet werden, zu beschreiben. Besonders wichtig sind hier Verfahren, in denen sensible Daten verarbeitet werden. Diese sollten so vollständig und exakt wie möglich im Verfahrensverzeichnis dokumentiert werden. Als Beispiele sind hier der Bewerbungsprozess, eine ev. Videoüberwachung, ein ev. Newsletter oder die Personalverrechnung zu nennen.

Für alle relevanten Datenverarbeitungen ist ein solches Verfahrensverzeichnis mit diversen Detailangaben anzulegen. Es wird zwar nicht beschrieben, wie dieses Verfahrensverzeichnis zu führen ist, sehr wohl aber was darin beinhaltet sein muss. Es hat zumindest folgende Informationen zu enthalten:

- Kontaktdaten der Beteiligten (Verantwortliche inkl. deren Vertretung, Empfänger, Zuständige, ev. Auftragsverarbeiter, ev. Datenschutzbeauftragte)
- Legitimer Zweck der Verarbeitung bzw. die Rechtsgrundlage der Verarbeitung
- verwendete Daten (Kategorien)
- Betroffene (Kategorien)
- beteiligte Empfänger (Kategorien)
- Datenübermittlungen
- die Speicherdauer (Aufbewahrungsfristen, Löschfristen
- getroffene Datensicherheitsmaßnahmen (technisch und organisatorisch)

Die Informationen aus der Erhebung (siehe Kapitel 3.1) können für die Erstellung dieses Verzeichnisses herangezogen werden.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

3.2.1 Beispiel für ein Verfahrensverzeichnis

Verarbeitung/ Applikation	Verantwortliche Stelle	Verantwortlicher	Vertretung des Verantwortlichen	Kontaktdaten	Zweck der Verarbeitung	Rechtsgrundlage	(Kategorien) personenbezogene(r) Daten	(Kategorien) sensible(r) Daten	Datenquellen
Bewerbungsprozess	Leiter Personalabteilung	XY GmbH, XY Strasse1 AT 1234 St. Umleitung		office@XY.at Tel.: +43 1234 56789-0 Fax: +43 1234 56789-1	Abwicklung eines Bewerbungsprozesses	benötigte personenbezogene Daten zur Besetzung einer ausgeschriebenen Stelle	Name, Adresse, Telefonnummer, Emailadresse, Geburtsdatum, Familienstand, Geschlecht, Lebenslauf, Bewerberfoto, Strafregisterauszug, Zeugnisse	Religionsbekenntnis	Bewerber (sendet Daten via Bewerbungsplattform, Email oder postalisch) Onlineplattformen (Xing, Linkedin, Facebook)

Betroffene (Kategorien)	Datenübermittlungen intern	Datenübermittlungen extern	Empfänger (Kategorien)	Zugriffsberechtigte	Löschkonzept	Risikoabschätzung	Schutzmaßnahmen/Datensicherheitsbeschreibung	Stellungnahme des Datenschutzverantwortlichen
Bewerber	ja	nein	Personalabteilung Leiter Fachabteilung Geschäftsleitung	lesend: Personalabteilung Leiter Fachabteilung Geschäftsleitung schreibend: Personalabteilung IT	Alle eingelangten Bewerberdaten werden, nach Abschluss des Bewerbungsprozesses, d.h. nach Auswahl der einzustellenden Person, unverzüglich bzw. nach Ablauf der (vom Bewerber; siehe "Risikoabschätzung") genehmigten oder gesetzlichen Aufbewahrungsfrist, unwiederbringlich auf allen Datenträgern vernichtet. Personenbezogene Bewerberdaten in Papierform werden, unter Verantwortung des Leiters der Personalabteilung, einem entsprechenden Entsorgungsunternehmen übergeben. Personenbezogene Bewerberdaten in digitaler Form (Email, Bewerberplattform) werden, unter gemeinsamer Verantwortung des Leiters Personalabteilung und des Leiters IT, von damit beauftragten und eingewiesenen Mitarbeitern unwiederbringlich gelöscht. Die jeweilige Löschung wird vom Löschenden protokolliert und vom Datenschutzverantwortlichen überwacht bzw. stichprobenartig kontrolliert.	Risiko für Betroffene: gering Eintrittswahrscheinlichkeit: gering Schadenspotential: moderat Begründung: eingelangte Bewerberdaten werden verschlüsselt (Bewerberportal, Email) übertragen und gespeichert, unter Verschluss gehalten (postalische Bewerbungen) und sind nur von speziell berechtigten und eingewiesenen Mitarbeitern einsehbar bzw. werden nur an diese gesichert (Verschlüsselung, Passwort) übermittelt (Email, Bewerberportal, Bewerbung in Papierform). Die Wahrscheinlichkeit, dass unberechtigte Personen auf diese Daten Zugriff bekommen oder dass sie auf unberechtigte Weise verwendet werden, ist somit sehr gering. Weiters werden von allen Bewerbern datenschutzkonforme Datenschutzerklärungen nachweislich zur Kenntnis genommen sowie ordnungsgemäße Zustimmungserklärungen zur Verarbeitung der Daten, und die Erlaubnis zur Aufbewahrung für eine Zeitspanne von 2 Jahren, eingeholt.	Datenverschlüsselung: AES, EFS, Zertifikate Transportverschlüsselung: SSL/HTTPS, IPSEC/AES Berechtigungssystem mit Zugriffsschutz Enpointsecurity: Virenscanner, Verschlüsselung, Passwortschutz Intrusion Prevention System Network Access Control Antivirensystem (Server, Email, etc.)	Auf Grund der vom Bewerber bestätigten Datenschutz- und Zustimmungserklärung, sowie der von ihm erteilten Erlaubnis zur Speicherung seiner Daten für eine Dauer von 2 Jahren, respektive des Löschkonzeptes und des geringen Risikos, bewertet der Datenschutzverantwortliche der XY GmbH diese Verarbeitung, im Sinne der EUDSGVO, als datenschutzkonform.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

3.3 Datenschutzerklärungen

Datenschutzerklärungen werden immer dann benötigt, wenn ein Unternehmen über ein Onlinemedium in die „Öffentlichkeit“ tritt. Traditionell geschieht das bei Webseiten (Homepage) oder beim Versand von Newslettern.

Eine Datenschutzerklärung erfüllt einen Teil der Informationspflicht für Betroffene und hat zu beschreiben, welche personenbezogenen Daten (Kategorien) das Unternehmen bzw. die Webseite verarbeitet. Zusätzlich ist der Verantwortliche inkl. Vertretung, der legitime Verwendungszweck, die Betroffenen, ev. Empfänger, allfällige Datenübermittlungen und die Wahrung der Betroffenenrechte anzugeben. Dies gilt auch für ev. eingesetzte Cookies (z.B.: Google Analytics)!

Die Datenschutzerklärung ist auf der Webseite in klarer und verständlicher Formulierung und Schrift zu hinterlegen. Dies kann in einem eigenen Menüpunkt der Webseite geschehen oder im Impressum.

3.4 Zustimmungserklärungen

Falls bei der Verarbeitung von personenbezogenen Daten auch Datenarten verwendet werden, die über die benötigten Informationen zur Auftragserfüllung des Unternehmens hinausgehen, so wird dafür die Zustimmung des Betroffenen benötigt. Als Beispiel sind hier Fotos von Mitarbeitern oder die Anmeldung bzw. der Erhalt von Newslettern zu nennen.

Eine Zustimmungserklärung hat freiwillig zu erfolgen und ist nur bei völliger Kenntnis der Sachlage beim Betroffenen rechtsgültig. Daher ist der Betroffene **vor** Einholung der Zustimmung in vollem Umfang von der Verarbeitung dieser zusätzlichen Daten zu informieren, sodass er in der Lage ist, diese Verarbeitung zu beurteilen und ev. Risiken für sich selbst dabei zu bewerten. Der volle Informationsumfang kann als erfüllt betrachtet werden, wenn die Zustimmungserklärung die auch im Verfahrensverzeichnis bzw. in einer Datenschutzerklärung geforderten Inhalte enthält (siehe Kapitel 3.2 und 3.3).

Für die Anmeldung bei Newslettern ist die empfohlene und derzeit rechtssicherste Methode das sog. „Double Opt.In.“ Verfahren (https://de.wikipedia.org/wiki/Opt-in).

Die Erteilung der Zustimmung kann analog (Papierformular) oder digital (Onlineformular oder Email) erfolgen. Die Ablehnung einer Zustimmung zur Verarbeitung solcher Daten, z.B. Mitarbeiterfotos, darf für Mitarbeiter keine negativen Folgen haben (Freiwilligkeit). Jeder Betroffene kann eine einmal erteilte Zustimmung jederzeit und ohne Angabe von Gründen, widerrufen.

3.5 Auftragsverarbeitervereinbarungen

Die Verarbeitung von personenbezogenen Daten kann auch, im Auftrag des Verantwortlichen, extern bei einem Dienstleister, einem sog. Auftragsverarbeiter, erfolgen. Häufige Beispiele dafür sind Steuerberatung, externe Personalverrechnung, Cloud Services (z.B. Dropbox), IT Dienstleister oder Zahlungsdienstleister. In einem solchen Fall sind gewisse Rahmenbedingungen zu erfüllen, z.B. die gegenseitige Unterzeichnung einer Datenschutzvereinbarung bzw. einer sog. Auftragsverarbeiter-vereinbarung. Jeder Verantwortliche hat mit von ihm beauftragten externen Auftragsverarbeitern eine Vereinbarung zur Aufrechterhaltung des Datenschutzes abzuschließen.

Inhalte einer solchen Auftragsverarbeitervereinbarung sind:

- Art und Umfang des Auftrages bzw. der Verarbeitung
- Die Rechte und Pflichten jeweils des Auftraggebers (z.B. Kontrollrechte) und des Auftragsverarbeiters (z.B. Geheimhaltungsverpflichtung)
- Die technischen und organisatorischen Schutzmaßnahmen beim Auftragsverarbeiter

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

Zuerst ist zu ermitteln, welche Auftragsverarbeiter genutzt werden bzw. in Frage kommen. Daraufhin ist für jeden Verarbeitungszweck bzw. Auftragsverarbeiter eine Vereinbarung zu verfassen und mit dem Auftragsverarbeiter abzuschließen.

3.6 Regeln & Richtlinien

Die Wahrung des Datenschutzes ist auf Anforderung der Datenschutzbehörde jederzeit nachzuweisen. Ein solcher Nachweis kann über verabschiedete bzw. nachweislich zur Kenntnis gebrachte Regeln & Richtlinien für Mitarbeiter und den Nachweis deren Einhaltung (Monitoring, Protokollierung) erbracht werden.

Daher wird empfohlen, die Handhabung von personenbezogenen Daten möglichst exakt zu regeln. Sämtliche Mitarbeiter haben die verabschiedeten Regeln und Richtlinien genauestens zu befolgen. Die Einhaltung der Richtlinien ist zu überwachen und zu kontrollieren. Jeder Mitarbeiter ist über die grundsätzliche Überwachung der Richtlinien zu informieren. Geheimgehaltene Überwachungen sind unzulässig! Zu beachten ist, dass für eine rechtmäßige Überwachung die ausschließlich betriebliche Nutzung der IT Systeme Voraussetzung ist, d.h. von einer Privatnutzung der IT Systeme des Unternehmens ist abzusehen, da andernfalls unrechtmäßiger Zugriff auf private Daten der Mitarbeiter möglich wäre.

Zu diesen Regeln & Richtlinien sollten gehören:

- Internet Richtlinie
- Email Richtlinie
- Social Media Richtlinie
- Benutzer- und Passwortrichtlinie
- Richtlinie zur Datenentsorgung (Papier und digitale Daten)
- Richtlinie zur Einhaltung des Datenschutzes
- Richtlinie zur Handhabung von IT Systemen (PC, mobile Geräte, etc.)
- Geheimhaltungsverpflichtung

Zuerst ist festzulegen, welche Richtlinien, abhängig von den tatsächlichen Gegebenheiten, benötigt werden. Danach sind die entsprechenden Richtlinien zu verfassen und von allen Mitarbeitern zur nachweislich Kenntnis zu bringen.

3.7 Datenschutz durch Technik

Die EUDSGVO fordert den Einsatz aller technischen und organisatorischen Maßnahmen, entsprechend dem aktuellen Stand der Technik. Dies soll die Einhaltung und Wahrung des Datenschutzes unterstützen und gewährleisten. Allerdings sieht die EUDSGVO auch vor, den Einsatz dieser Maßnahmen auch unter wirtschaftlichen Gesichtspunkten zu bewerten und zu entscheiden, d.h. sollte der Einsatz gewisser Maßnahmen wirtschaftlich nicht zu rechtfertigen oder tragbar sein, so kann davon abgesehen werden. Zusätzlich zu wirtschaftlichen Gesichtspunkten dürfen auch die Höhe des Risikos für Betroffene und deren Eintrittswahrscheinlichkeit zur Bewertung herangezogen werden.

Zu diesen Maßnahmen gehören allgemein:

- Verschlüsselung
- Zugriffsrechte
- verpflichtende Richtlinien
- Firewalls
- Network Access Control

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

- Intrusion Prevention Systeme
- Überwachung und Kontrolle
- Berechtigungen
- etc.

Im Falle von Kaffeehäusern empfehlen wir folgende Maßnahmen (ohne Anspruch auf Vollständigkeit):

- personifizierte Berechtigungen für die Nutzung von IT Systemen
- Regeln und Richtlinien (siehe Kapitel 3.6)
- Firewall für den Internet Anschluss
- Überwachung der Einhaltung der Richtlinien (Monitoring, Protokollierung)
- Vertretungsregelungen
- Sicherheit und Datenschutz im Zahlungsverkehr
- Entsorgung von Daten über externe Dienstleister
- Privatnutzungsverbot
- Strenge Benutzer- und Passwortstruktur
- Datenschutzgerechte Bewerbung
- Verschlüsselung im Emailverkehr bei der Übermittlung sensibler Daten

3.8 Datenschutz Folgeabschätzung

Für Verarbeitungen personenbezogener Daten mit erkennbarem Risiko für Betroffene sieht die EUDSGVO vor, eine sog. Datenschutz Folgeabschätzung durchzuführen.

Die **Datenschutz Folgeabschätzung** ist eine Bewertung des bestehenden Risikos für Betroffene im Zuge der Verarbeitung seiner Daten und sie gehört zu den erweiterten Dokumentationspflichten. Dabei ist das Risiko für den Betroffenen nach Eintrittswahrscheinlichkeit und möglicher Schadenshöhe zu bewerten. Dazu werden mögliche Gefahren individuell erhoben (Gefahrenkatalog), die Höhe des möglichen Schadens bei Eintritt dieser Gefahren festgelegt, die Wahrscheinlichkeit des Eintritts dieser Gefahren ermittelt und aus diesen Kriterien das Risiko berechnet bzw. bewertet. Daraus sind für hohe und nicht tragbare Risiken entsprechende Gegen- bzw. Schutzmaßnahmen zu definieren. Der gesamte Vorgang ist zu dokumentieren und auf Verlangen einer Datenschutzbehörde vorzulegen.

Da jede Datenschutz Folgeabschätzung höchst individuell ist, sind Beispiele oder Vorlagen bis dato nicht verfügbar.

Als Verarbeitungen mit erkennbarem Risiko gelten beispielsweise Big Data, Profiling, RFID, Zahlungsverkehr, Verarbeitung sensibler Daten, Videoüberwachung oder Newsletter.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

4 Praxisbeispiele

Zum besseren Verständnis und zur erleichterten Interpretation der bisher beschriebenen Anforderungen und Aufgaben aus der EUDSGVO, nachfolgend einige Beispiele aus der Praxis.

4.1 Videoüberwachung

Der Einsatz von Videoüberwachungssystemen ist in den geltenden Datenschutzregularien streng geregelt. Grundsätzlich sind solche Anlagen nur dann datenschutzrelevant, wenn Daten aufgezeichnet werden und somit im Nachhinein auswertbar sind. Reine Live Bilder ohne Aufzeichnung sind (meist) nicht vom Datenschutzgesetz betroffen (Ausnahmen: sie überwachen fremde private oder öffentliche Bereiche und sie können zur Begehung von Straftaten herangezogen werden).

Ihre Verwendung ist zu bestimmten Zwecken erlaubt. Zu diesen Zwecken gehört der Schutz von Infrastruktur, dem persönlichen Eigentums, sowie von Gesundheit oder Leib und Leben.

Zulässige Zwecke einer Videoüberwachung sind:

- Schutz eines zu überwachenden Objektes oder einer Person
- Erfüllung rechtlicher Sorgfaltspflichten
- Lebenswichtige Interesse einer Person
- Ausdrückliche Zustimmung des Betroffenen (bzw. Betriebsratspflicht!)
- Echtzeitüberwachung ohne Speicherung
- Überwachung des Privatgrundstückes

Für andere Zwecke, wie z.B. die Verhaltensüberwachung, Profilerstellung oder Leistungskontrolle von Betroffenen (auch Mitarbeiter!), ist der Einsatz einer Videoüberwachung strengstens untersagt!

Unzulässige Zwecke einer Videoüberwachung sind:

- Mitarbeiterkontrolle (theoretische Möglichkeit genügt!)
- Automationsunterstützter Abgleich mit anderen Bilddaten
- Suche nach sensiblen Daten als Auswahlkriterium

Jedenfalls unzulässig ist eine Videoüberwachung ohne ausdrückliche Einwilligung im höchstpersönlichen Lebensbereich einer Person oder zum Zweck der Kontrolle von Arbeitnehmern.

Aufgezeichnete Videodaten sind zwar nicht per Definition sensibel (siehe Kapitel 2.1.1 und 2.1.2), werden aber als solche betrachtet, da ein erkennen sensibler Informationen von Betroffenen offensichtlich sein kann. Daher ist ein unrechtmäßiger Betrieb einer Videoüberwachungsanlage auch von sehr hohen Strafen bedroht.

Die maximale Aufbewahrungsdauer von Videodaten beträgt 72 Stunden. Danach sind diese Daten in jedem Fall zu löschen bzw. ist die Videoüberwachungsanlage so zu konfigurieren, dass Videodaten, die älter als 72 Stunden sind, automatisch gelöscht oder überschrieben werden. Die einzige Ausnahme von dieser Regel ist ein Auskunftsbegehren oder ein Sicherheitsvorfall. In diesem Fall müssen die Daten, zum Zwecke der Nachvollziehbarkeit bzw. Aufklärung, 4 Monate lang aufbewahrt werden.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

4.1.1 Empfehlung

Sollte eine Videoüberwachungsanlage zum Einsatz kommen, so ist auf folgendes zu achten:

- Der Verwendungszweck hat rechtmäßig zu sein. Eine unrechtmäßige Nutzung ist unter allen Umständen zu vermeiden.
- Die Verwendung der Anlage, deren Handhabung, der Zugriff auf aufgezeichnete Daten sowie deren Auswertung, ist mittels Richtlinie genauestens zu regeln. Die Richtlinie ist allen Beteiligten (Mitarbeitern) zur Kenntnis zu bringen.
- Es ist darauf zu achten, dass nur die Personen Zugriff auf das System bzw. aufgezeichnete Daten bekommen, die dies zur Erfüllung ihrer Aufgabe benötigen.
- Jeder Betroffene (Gäste) ist über den Einsatz der Anlage zu informieren. Dies ist mittels einer klaren und unübersehbaren Beschilderung durchzuführen.
- Der Aufnahmebereich der Kameras ist so zu wählen, dass keine fremden privaten oder öffentlichen Bereiche aufgezeichnet werden. Von Live Übertragungen aus dem Gästebereich raten wir ab.
- Die Löschung der Daten hat spätestens nach 72 Stunden zu erfolgen. Das kann auch automatisiert geschehen. Sollte eine längere Aufbewahrungszeit benötigt werden, so kann diese bei der Datenschutzbehörde beantragt werden.

4.2 Berechtigungen

Der Zugriff auf personenbezogene Daten ist so gut als möglich abzusichern. Dazu gehört, dass sicherzustellen ist, dass jeder Mitarbeiter nur auf die Daten Zugriff bekommt, die er für die Erfüllung seiner ihm zugewiesenen Aufgabe auch tatsächlich benötigt, und nicht mehr.

Die Vergabe von Benutzerrechten bzw. die Genehmigung von Zugriffsrechten ist zu regeln und möglichst restriktiv zu handhaben.

Dies kann über Benutzeraccounts mit Passwörtern und entsprechenden Berechtigungen erfolgen. Bei der Erstellung und Handhabung von Benutzeraccounts und der Erteilung von Berechtigungen ist folgendes zu beachten:

- Jeder Benutzer hat einen eigenen, personifizierten Benutzeraccount zu erhalten und zu verwenden
- Das Passwort sollte eine Mindestlänge von 16 Stellen haben und mindestens alle 6 Monate geändert werden. Das Passwort sollte aus unzusammenhängenden Wörtern mit Leerzeichen dazwischen bestehen.
- Die Weitergabe von Benutzerdaten (Benutzername und Passwort) im Vertretungsfall (Urlaub, Krankheit) ist unzulässig. Bei Email sollte der Abwesenheitsassistent aktiviert werden, mit dem Hinweis auf die Vertretung und der Bitte, das Mail an die Vertretung erneut zu senden.
- Verabschiedung eines Privatnutzungsverbotes.
- Der Zugriff auf Benutzerdaten aus einem anderen Benutzeraccount ist zu auszuschließen.
- Verabschieden einer Geheimhaltungsverpflichtung für Mitarbeiter, in der auch jedwede Meinungsäußerung des Mitarbeiters bei „Biertischgesprächen“ oder in Onlinemedien ausgeschlossen wird.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

4.3 Bewerbungen

Bewerbungen können auf unterschiedlichen Wegen und in unterschiedlichen Formaten im Unternehmen „eintreffen“. Einerseits in physikalischer Form per Post oder persönlich überbracht, oder in digitaler Form per Email oder über ein Portal. Meist enthalten Bewerbungen kritische (Fotos) oder sogar sensible (Religionsbekenntnis, Fotos) Daten. Daher ist die Handhabung von Bewerbungen und Bewerbungsunterlagen überaus datenschutzrelevant und sollte klar geregelt und datenschutzkonform organisiert werden.

Grundsätzlich ist die Verarbeitung von personenbezogenen Daten während und im Zuge einer Stellenbesetzung vom Datenschutzrecht gedeckt und auch zulässig.

Der Verwendungszweck für die Neubesetzung einer vakanten Stelle ist legitim. Das gilt zumindest so lange, bis der Kandidat ausgewählt und die Stelle besetzt ist. Danach erlischt der legitime Verwendungszeck zur weiteren Verarbeitung der Bewerbungsunterlagen.

Daraus folgt, dass nach Besetzen der freien Stelle sämtliche Bewerbungsunterlagen unverzüglich und unwiederbringlich zu vernichten sind. Das gilt vor allem für die Teile, die sensible Daten enthalten. Allerdings ist eine Aufbewahrung der Daten für 6 Monate geduldet, d.h. es gibt dafür keine Rechtsgrundlage, auf die man sich berufen könnte, aber eine Aufbewahrung von 6 Monaten wurde bis dato noch nie geahndet. Wird eine längere Aufbewahrungsdauer gewünscht oder benötigt, so ist vom Bewerber eine entsprechende Zustimmung einzuholen (siehe Kapitel 3.4), in der die gewünschten Bedingungen darzulegen sind.

Bei der Handhabung von Bewerbungsunterlagen ist auf folgendes zu achten:

- Vor Ausschreibung der Stelle sollten Überlegungen angestellt werden, welche Informationen für die Bewerbung tatsächlich benötigt werden. Jeder Bewerber sollte darauf hingewiesen wird, welche Daten von ihm gefordert werden und dass zusätzliche Daten gar nicht erst in den Unterlagen enthalten sein sollten.
- Nur die Personen, zu deren Aufgabenbereich es gehört, Bewerber auszuwählen, dürfen auf Bewerbungsunterlagen Zugriff bekommen.
- Zugriff und Aufbewahrung (Speicherung) sollten restriktiv gehandhabt werden, da es andernfalls bei der späteren Datenvernichtung zu ungewollten Aufwänden und Risiken kommen kann. Bewerbungsunterlagen sollten zentral gesammelt und gespeichert werden und keinesfalls verteilt werden.
- Bewerbungsunterlagen sollten, zum Zwecke der besseren Kontrolle und erleichterten Handhabung, möglichst auf elektronischem Weg übermittelt werden.
- Nach Besetzen der Stelle sollten alle Bewerbungsunterlagen unwiederbringlich vernichtet werden.
- Ist eine verlängerte Aufbewahrung der Bewerbungsunterlagen gewünscht, so ist vom Bewerber eine datenschutzgerechte Zustimmung einzuholen.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

5 Anhang A: Zusätzliche Anforderungen aus der EUDSGVO

5.1 Rechte für Betroffene

Die DSGVO definiert bestimmte Rechte für Betroffene, also alle die Personen, die eigentlich Eigentümer der Daten sind.

5.1.1 Auskunftsrecht

Der Auftraggeber hat jeder Person (Betroffener) auf Antrag innerhalb von 4 Wochen unentgeltlich Auskunft über die zu dieser Person verarbeiteten Daten zu geben (Löschungsverbot für 4 Monate!). Die Auskunft hat folgendes zu beinhalten:

- alle verarbeiteten Daten
- Herkunft der Daten
- allfällige Empfänger
- Zweck der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- allfällige Dienstleister

5.1.2 Datenlöschung und Richtigstellung

Der Auftraggeber hat unrichtige oder entgegen den Bestimmungen des Datenschutzgesetzes verarbeitete Daten innerhalb von 4 Wochen richtigzustellen oder zu löschen, und zwar aus eigenem Antrieb, wenn der Zweck nicht mehr gegeben ist oder auf Antrag eines Betroffenen. Es sei denn, es widerspricht anderen gesetzlichen Vorgaben (Archivierungsdauer). Der Antragsteller ist vom Auftraggeber aktiv über die durchgeführte Löschung bzw. Richtigstellung zu informieren. Zu beachten ist auch, dass bei der Löschung von Betroffenendaten auch ev. Datensicherungen zu beachten sind, d.h. auch Daten, die sich auf Datensicherungen befinden sind zu vernichten.

Weiters ist jeder Auftraggeber dazu verpflichtet, sämtliche Daten eines Betroffenen zu löschen, sobald der betreffende Verarbeitungszweck nicht mehr gegeben ist. Als Beispiel kann hier eine Bewerbung betrachtet werden. Sobald die offene Stelle besetzt worden ist, sind sämtliche personenbezogene Daten aller Bewerber, die die offene Stelle nicht bekommen haben, zu vernichten. Zur Löschung der Daten sind geeignete Verfahren zu wählen, die eine Wiederherstellung der Daten unmöglich machen.

Von der Verpflichtung zur Datenlöschung sind natürlich auch alle Daten auf Papier betroffen. Bei der Vernichtung von Papier sind spezielle Vorbedingungen zu beachten. Je nachdem, welche Daten auf Papier verzeichnet sind, ist auch hier eine Wiederherstellbarkeit zu verhindern. Dazu können Shredder oder Dienstleister, die sich auf die Vernichtung von Papier spezialisiert haben, genutzt werden. Bei Shreddern ist die jeweilige Schutzklasse zu beachten, d.h. bei personenbezogenen und sensiblen Daten ist ein alleiniger Längsschnitt nicht ausreichend, es wird auch ein Querschnitt benötigt.

5.1.3 Widerrufs- und Widerspruchsrecht

Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, Widerspruch einzulegen gegen die Verwendung seiner personenbezogenen oder sensiblen Daten (eigene bzw. freiwillige Veröffentlichung negiert nicht die Schutzwürdigkeit!!). Der Auftraggeber hat daraufhin die Verarbeitung der Daten unverzüglich einzustellen und binnen 4 Wochen aus der Datenanwendung zu löschen und umgehend allfällige Übermittlungen zu unterlassen. Jeder Betroffene hat jederzeit das Recht bereits erteilte Zustimmungen zur Verarbeitung seiner Daten ohne Angabe von Gründen zu widerrufen.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

5.1.4 Informationspflicht

Aus Anlass der Ermittlung von Daten sind Betroffene zu informieren, sowohl über den Zweck der Verarbeitung als auch über den Namen bzw. die Adresse des Auftraggebers. Dies kann mit einer datenschutzkonformen Datenschutzerklärung auf der Homepage erfüllt werden.

Zur Informationspflicht gehört auch die Data Breach Notification Duty. Diese verpflichtet Auftraggeber, im Zuge seiner Verarbeitung, zur sofortigen Meldung eventuell aufgetretener Datenverluste oder Verstöße gegen das Datenschutzgesetz bei der zuständigen Aufsichtsbehörde.

5.1.5 Beschwerderecht bei der Aufsichtsbehörde

Jeder Betroffene hat jederzeit das Recht, sich bei Unzufriedenheit, Unstimmigkeiten oder bei einem Verdacht auf Unregelmäßigkeiten direkt an die Datenschutzbehörde seines Heimatlandes zu richten, eventuell festgestellte Unregelmäßigkeiten zu melden und sich entsprechend an dieser Stelle zu beschweren.

© Prodinger Tourismusberatung
© ATRICON GROUP GmbH

6 Schlussbemerkungen

Dieser Leitfaden dient der Unterstützung bei der Erreichung einer ausreichenden Datenschutzkonformität und erhebt keinen Anspruch auf Vollständigkeit. Auch ist die Erreichung einer 100%igen Datenschutzkonformität nicht möglich. Letztendlich bleibt ein gewisses Restrisiko. Die Höhe dieses Restrisikos unterliegt der Bereitschaft, wirtschaftliche und personelle Ressourcen zu investieren und ist im Endeffekt eine Entscheidung der Geschäftsleitung.

Die Neuheit der Regelungen aus der EUDSGVO und die Tatsache, dass sie erst am 25.5.2018 in nationales Recht übergehen, lässt den Schluss zu, dass noch keine Judikaturen aus der Praxis existieren und in Zukunft noch einige Aspekte von Gerichten und Behörden präzisiert werden.

Daher stellen die Angaben in diesem Leitfaden keine (rechts-)verbindlichen Informationen dar, sondern spiegeln nur den aktuellen Wissens- und Erfahrungsstand wider. Der Leitfaden wird anhand von zukünftigen Entwicklungen kontinuierlich einer Überprüfung und Aktualisierung unterzogen, um Neuentwicklungen und zukünftige Rechtsprechungen ergänzen zu können.

Dieser Leitfaden ist keine abschließende Handlungsanweisung oder Rechtsberatung, d.h. eine Evaluierung konkreter Praxisfälle kann durch dieses Dokument nicht ersetzt werden.

ATRICON GROUP

ATRICON positioniert sich als IT- und Unternehmensberatung, die den Business Value seiner Kunden in den Mittelpunkt stellt. Unser Leitsatz „**inspired – designed – realized**“ betont die ganzheitliche Sichtweise, die uns leitet. Wir greifen auf jahrelange Praxis in großen, internationalen Unternehmen zurück. **ATRICON** analysiert die Situation, erarbeitet gemeinsam mit seinen Kunden Lösungen und begleitet die Umsetzung.

PRODINGER BERATUNGSGRUPPE

Als führende Wirtschaftsberatung unterstützt die **PRODINGER BERATUNGSGRUPPE** ihre Kunden in den Geschäftsfeldern **Steuerberatung, Unternehmensberatung, Tourismusmarketing und Tourismusberatung**. Die Firmengruppe hat Spezialisten in den Branchen Tourismus, Bau- und Baunebengewerbe, Immobilienwirtschaft, freiberufliche Tätigkeiten, Handel, Gewerbe und Dienstleistung. Die Beratungsgruppe hat Standorte in Bad Hofgastein, Bozen, Innsbruck, Lech am Arlberg, Linz, Mittersill, München, Saalfelden, Salzburg, St. Johann im Pongau, Velden, Wien und Zell am See.

Die Netzwerkgruppe betreut aktuell mehr als 6.000 Kunden, davon über 500 Hotelbetriebe, 30 Destinationen und 40 Bergbahnen. Derzeit sind 250 Mitarbeiterinnen und Mitarbeiter an 13 Standorten tätig.

Die PRODINGER BERATUNGSGRUPPE ist Mitglied in mehreren Netzwerken. Die Prodinger Steuerberatung ist unabhängiges Mitglied der GGI Geneva Group International. Die Prodinger Tourismusmarketing ist integriert in der Serviceplan Gruppe bei Saint Elmo´s Travel mit 26 Standorten weltweit.