Roter Hahn - Mitteilung 1 / 2018

Neue EU-Datenschutzbestimmungen

Am 25. Mai 2018 tritt die neue Europäische Datenschutzgrundverordnung (DSGVO – EU-Verordnung 2016/679) in Kraft. Mit diesem Rundschreiben informieren wir Sie über die wichtigsten Grundsätze und über die Änderungen, die auf Sie zukommen.

Allgemeines - Begriffsbestimmungen
Grundsätzlich mahnt die EU-Datenschutzgrundverordnung zu einem sorgsameren Umgang mit den Daten von Betroffenen, z.B. der Gäste, und nimmt den Dateninhaber - das ist der, der darüber entscheidet, was mit den Daten passiert - in die Verantwortung.
Die Daten der Gäste müssen rechtmäßig und in nachvollziehbarer Weise verarbeitet werden. Als Datenverarbeitung ist das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Abfragen, Verwenden, Übermitteln, Verbreiten, Abgleichen, Verknüpfen, Löschen und Vernichten von personenbezogenen Daten definiert, unabhängig davon, ob dies digital oder analog erfolgt.
Die Daten der Gäste werden für einen gewissen Zweck erhoben und die Erhebung soll für den jeweiligen Zweck angemessen sein. Das heißt konkret, dass nicht Daten erhoben werden sollen, die es für den jeweiligen Zweck nicht braucht. Zum Beispiel ist zum Versenden eines Angebotes an den Gast nur der Name des Betroffenen, eine E-Mail-Adresse und die Anzahl der Personen erforderlich. Es würde deshalb keinen Sinn machen, bereits bei der Angebotslegung Daten zu erheben, die erst später für die polizeiliche Meldung benötigt werden. Die Daten dürfen nicht für andere Zwecke, als für die sie erhoben wurden, verwendet werden. Weiters sollten die Daten der Gäste nur so lange verarbeitet und gespeichert werden, wie dies für den jeweiligen Zweck notwendig ist. Während der Verarbeitung und Speicherung der Daten ist darauf zu achten, dass die Daten vor unbefugtem Zugriff, Verlust oder Zerstörung geschützt sind.

Arten der personenbezogenen Daten
Als personenbezogene Daten werden alle Informationen verstanden, die sich auf eine natürliche Person (betroffene Person) beziehen bzw. zuordenbar sind (ehemals „gewöhnliche Daten“).
Besondere Daten (ehemals „sensible Daten“) sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Auch die Verarbeitung von genetischen Daten (z.B. Daten über genetisch bedingte Krankheiten), von biometrischen Daten (z.B. Fingerabdrücke), Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung zählen dazu. Weiters zählen auch indirekte Gesundheitsdaten der Gäste, wie beispielsweise Informationen über Allergien, Krankheiten (z.B. Diabetes) u.ä., dazu. Diese Daten unterliegen einem besonderen Schutz.

Aufklärung und Einholung der Zustimmung (Einwilligung)
Grundsätzlich müssen die Gäste als betroffene Personen über den Zweck der Datenverarbeitung und deren Rechtsgrundlage sowie über eventuelle Konsequenzen bei Verweigerung aufgeklärt werden **(siehe Anlage 1 - Muster eines Aufklärungsschreibens)**. Da der Betrieb im Zweifelsfalle nachweisen muss, dass der Gast transparent aufgeklärt wurde und gegebenenfalls der Datenverarbeitung zugestimmt hat, ist wie bisher eine schriftliche Dokumentation sinnvoll **(siehe Anlage 2 - Muster Zustimmung für Kommunikationszwecke)**.
In den Aufklärungsschreiben müssen den Gästen die Kontaktdaten des Dateninhabers (und ggf. seines Vertreters), eventuelle Empfänger oder Empfängerkategorien der Daten bei Übermittlung an Dritte (z.B die Polizeiorgane bei der polizeilichen Meldung), eine eventuelle Übermittlung in Drittländer (z.B Übermittlung der Gästedaten an eine ausländische Werbeagentur), die Speicherdauer und die Rechte der Gäste mitgeteilt werden. Sollte Profiling (z.B. Verwendung der Daten für personalisierte Anzeigen im Internet) genutzt werden, ist immer eine eigene Einwilligung notwendig. Die Einwilligung dürfen Personen ab 16 Jahren geben, bei Minderjährigen unter 16 Jahren müssen deren Erziehungsberechtigte der Datenverarbeitung zustimmen.
Die entsprechenden Schreiben sind in einer einfachen und verständlichen Sprache abzufassen. Falls nur Daten verarbeitet werden, die der Gast bereits vorher offensichtlich öffentlich gemacht hat (z.B. Daten in öffentlichen Registern, wie z.B. Adresse im Telefonbuch), ist keine weitere Informationspflicht notwendig.

Datenverarbeitung im Betrieb – Rechtsgrundlagen

Grundsätzlich sollten die Betriebe überlegen, welche Gästedaten im Betrieb verarbeitet werden **(siehe Anlage 3 - Muster Register der Datenverarbeitungen)**. Dieses Register der Datenverarbeitungen ist zwar nur für Betriebe mit mehr als 250 Angestellten verpflichtend vorgesehen, allerdings muss auch der UaB-Betrieb die Risiken und Schutzmaßnahmen definieren. Dies erfordert auf jeden Fall Überlegungen darüber, welche Gästedaten im Betrieb verarbeitet werden und welche Schutzmaßnahmen notwendig sind. Im Falle einer Kontrolle muss der UaB-Betrieb nachweisen, dass er ausreichend für den Schutz der Gästedaten gesorgt hat.

Wir haben in folgender Tabelle die wichtigsten Datenverarbeitungen in einem UaB-Betrieb aufgelistet. Außerdem haben wir aufgelistet, wann und wo eine Zustimmung des Gastes zur Datenverarbeitung notwendig ist.

Kategorie der Daten	Zweck der Verarbeitung	Art der Datenverarbeitung	Rechtsgrundlage	Art der Zustimmung, Konsequenz
Gästedaten bei der Buchung (Name, Adresse, E-Mail-Adresse)	Erstellung eines Angebotes, Abwicklung der Buchung	In der Regel telematisch, Daten werden in der Regel nicht an Dritte weitergeleitet	Vertrag mit dem Kunden	Keine zusätzliche Zustimmung notwendig, sofern die Daten nicht an Dritte weitergeleitet werden. Aufklärung des Gastes über die Datenverarbeitung ist ausreichend. Ein Angebot ist ansonsten nicht möglich.
Verpflichtende Gästedaten während des Aufenthaltes (Name, Adresse, Geburtsort, Geburtsdatum, Staats-angehörigkeit, auch von Familienmitgliedern bzw. Mitreisenden)	Polizeiliche Meldung, Ortstaxe, Rechnungslegung	Telematisch und/oder in Papierform, Daten werden auch an Dritte weitergeleitet	Gesetzliche Bestimmungen (z.B. Einheitstext für öffentliche Sicherheit, Steuerbestimmungen)	Aushändigung der Gästedaten zur Abwicklung der Beherbergung ist verpflichtend. Daher ist die Aufklärung darüber ausreichend, da die Beherbergung ansonsten nicht möglich ist.
Freiwillige Gästedaten während des Aufenthaltes (Name, Bankdaten, Vorlieben, Hobbys, Allergien, …)	Gästebetreuung	Telematisch und/oder in Papierform, Daten werden in der Regel nicht an Dritte weitergeleitet	Zustimmung des Gastes oder nachweislich berechtigtes Interesse	Aushändigung der Daten ist freiwillig, eine Aufklärung und ausdrückliche Zustimmung ist daher notwendig. Die Verarbeitung der Gästedaten ist ansonsten nicht möglich. (Achtung auf besondere Datenkategorien)
Gästedaten nach dem Aufenthalt (Name, Geburtsdaten, Vorlieben, Hobbys, Allergien, …)	Nachbearbeitung, Kommunikation	Telematisch und/oder in Papierform, Daten werden in der Regel nicht an Dritte weitergeleitet	Zustimmung des Gastes und berechtigtes Interesse (im Sinne von Erwägungsgrund 47 der EU-Datenschutz-grundverordnung)	Aushändigung der Daten ist freiwillig, eine Aufklärung und ausdrückliche Zustimmung ist daher notwendig. Die Verarbeitung der Gästedaten ist ansonsten nicht möglich.
Besucher auf der Webseite des UaB-Betriebes (Name, Adresse, IP-Adresse, E-Mail-Adresse)	Nachbearbeitung, Kommunikation	Telematisch, Daten werden in der Regel nicht an Dritte weitergeleitet	Zustimmung des Gastes, falls Daten weiterverarbeitet werden	Aushändigung der Daten ist freiwillig, eine Aufklärung und ausdrückliche Zustimmung ist daher notwendig. Die Verarbeitung der Gästedaten ist ansonsten nicht möglich.
Daten von Freiberuflern, Dienstleistern, Verbände usw.	Steuerberater, Internetagentur, …		Vertrag mit den Lieferanten und Dienstleistern, berechtigtes Interesse	Keine zusätzliche Zustimmung notwendig, sofern die Daten nicht an Dritte weitergeleitet werden. Aufklärung über die Verarbeitung der Daten ausreichend, Vertrag ansonsten nicht möglich.
Mitarbeiterdaten (Name Adresse, Bankdaten, Gesundheitsdaten)	Arbeitsverhältnis	Telematisch und/oder in Papierform, Daten werden in der Regel an Dritte weitergeleitet	Arbeitsvertrag, gesetzliche Bestimmungen (Arbeitsrecht)	Keine zusätzliche Zustimmung notwendig, sofern der Mitarbeiter über die Verarbeitung der Daten ausreichend aufgeklärt wird, Vertrag ansonsten nicht möglich.

Dauer der Datenspeicherung und -verwendung

Die Bestimmungen sehen vor, dass dem Gast die Dauer der Datenspeicherung bzw. die Kriterien, nach denen die Dauer festgelegt wird, mitgeteilt werden müssen. In diesem Zusammenhang muss eindeutig zwischen den Daten von Kunden (Gäste, die im Betrieb übernachtet haben) und anderen Personen (z.B. Newsletter-Abonnenten) unterschieden werden.

Es wird darauf verwiesen, dass Art. 2220 des Zivilgesetzbuches eine Verpflichtung vorsieht, dass Rechnungsunterlagen, Briefe und Telegramme zehn Jahre aufbewahrt werden müssen. Das heißt konkret, dass die Daten und die entsprechende Korrespondenz für jeden Geschäftsfall mindestens für 10 Jahre aufbewahrt werden müssen. Sie dürfen also nicht gelöscht werden.

Es könnte demnach aber auch sinnvoll sein, die neuen Bestimmungen zum Anlass zu nehmen, die Gästedatenbank zu überarbeiten. Es kann davon ausgegangen werden, dass ein Gast, der vor 10 Jahren das letzte Mal im Betrieb genächtigt hat und sich dann niemals mehr gemeldet hat, gelöscht werden kann.

Weiters könnte es sinnvoll sein, in einer Datenbank zu erfassen, wann und vor allem für welchen Zweck der Gast die Zustimmung für die Datenverarbeitung erteilt hat. Für Daten von potentiellen Kunden (nur Anfragen) muss überlegt werden, wie lange eine solche Speicherung Sinn macht.

Berechtigtes Interesse

Die europäischen Datenschutzbestimmungen sehen auch das „berechtigte Interesse" als Grundlage für die Datenverarbeitung vor. So kann die Verwendung von Gästedaten zum Zwecke der Direktwerbung ausdrücklich als eine „einem berechtigten Interesse dienende Verarbeitung betrachtet werden" (Erwägungsgrund 47 der EU-Datenschutzgrundverordnung). Auch der italienische Datenschutzkodex hat vorgesehen, dass die E-Mail-Adressen von Kunden, die der Dateninhaber anlässlich des Verkaufs eines Produktes oder einer Dienstleistung erhalten hat, zum Zwecke des Direktverkaufs der eigenen Produkte oder Dienstleistungen ohne weitere Zustimmung verwendet werden dürfen. Es muss sich allerdings um ähnliche Dienstleistungen handeln und die betroffene Person kann die weitere Verwendung ablehnen. Daraus kann abgeleitet werden, dass die Verwendung der E-Mail-Adressen von Kunden (wie z.B. der Gäste, die bereits im Betrieb übernachtet haben) auch weiterhin für die Zusendung von Newslettern verwendet werden dürfen, sofern sie darüber bei der Datenerhebung informiert worden sind und die Möglichkeit besteht, diese wieder abzubestellen. Im Zweifelsfall sollte eine Zustimmung eingeholt werden.

Die Rechte des Betroffenen

Der Gesetzgeber sieht für die Gäste bzw. für die Betroffenen verschiedene Rechte vor, die auch mitgeteilt werden müssen. Die meisten davon waren auch schon im italienischen Datenschutzkodex enthalten. Zu den Rechten zählen das Auskunftsrecht, das Recht, falsche Daten zu berichtigen, das Recht auf Löschung („Vergessen werden"), das Recht auf Einschränkung der Verarbeitung, das Recht auf Widerspruch der Datenverarbeitung und das Recht auf Beschwerde bei einer Aufsichtsbehörde. Ein Recht, das neu hinzugekommen ist, ist das Recht auf Datenübertragbarkeit. Das heißt, der Betroffene kann verlangen, die gesamten Daten an einen anderen Datenverarbeiter (z.B. an einen anderen Beherbergungsbetrieb) weiterzuleiten.

Aufklärung in Zukunft genauer

Aufgrund der neuen Rechte, die die EU-Datenschutzgrundverordnung vorsieht, und vor allem aufgrund der Bestimmung, dass die Zustimmung des Betroffenen für einen spezifischen Zweck vorliegen muss und dass nur unbedingt benötigte Daten verarbeitet werden sollen, müssen die Aufklärungen dem Gast gegenüber in Zukunft genauer formuliert werden.
Ein konkretes Beispiel: Soll die Zustimmung für die Zusendung eines Newsletters eingeholt werden, sind im Prinzip nur die E-Mail-Adresse und der Name notwendig. Die Adresse und das Geburtsdatum werden hierfür nicht benötigt. Sollte der Betrieb eine Geburtstags-Mail schicken wollen, ist demnach auch eine eigene Zustimmung für diesen Zweck notwendig.

Wir haben dazu ein Muster eines Aufklärungsschreibens vorbereitet, in denen mehrere solcher Zwecke aufgelistet sind (siehe Anlage 1 - Muster eines Aufklärungsschreibens).

Was geht in Zukunft nicht mehr?

Da die Zustimmung für freiwillige Nutzung der Daten eindeutig durch den Gast und vor allem aktiv gegeben werden muss (keine stillschweigende Zustimmung), ist in Zukunft darauf zu achten, dass die Nutzung nicht an andere Leistungen gebunden ist. So ist es beispielsweise nicht mehr zulässig, Preisausschreiben, Preisvergünstigungen usw. an die Zusendung von Direktwerbung zu koppeln.

Was passiert mit den alten Daten?

Die italienische Datenschutzbehörde hat festgestellt, dass die nach den alten Datenschutzbestimmungen rechtmäßig eingeholten Daten für Werbezwecke, für die eine ausdrückliche Einwilligung vorliegt und für die der Gast über den Verwendungszweck und seine Rechte informiert wurde, weiterhin verwendet werden dürfen.
Sie sollten also überprüfen, ob Sie für alle Gästedaten in Ihrer Datenbank ein unterschriebenes Aufklärungsschreiben bzw. eine Zustimmung bei den Internet-Formularen (Häkchen auf der Internetseite) für den verwendeten Zweck (z.B. Zusenden von Newsletter oder Werbematerial) vorliegen haben.

Sicherheitsmaßnahmen

Bereits die bestehenden italienischen Datenschutzbestimmungen sehen gewisse Mindestsicherungsmaßnahmen vor. Bisher galten folgende Mindestsicherungsmaßnahmen:

- Aufklärung und Schulung der Mitarbeiter (auch Familienmitglieder) über den Umgang mit den Daten.
- Aufklärung der Kunden (Gäste) über den Zweck und die Art der Datenverarbeitung.
- Schutz der Computer mit einem Kennwort mit 8 Zeichen. Die Kennwörter müssen alle 6 Monate ausgetauscht werden. Werden auch sensible Daten verarbeitet, muss der Austausch alle 3 Monate erfolgen.
- Erfolgt die Datenverarbeitung über mehrere Computer, werden ein Kennwort und ein Benutzername zur Pflicht.

- Im Zeitraum der Datenverarbeitung darf der Arbeitsplatz nicht unbeaufsichtigt, d.h. für Außenstehende frei zugänglich sein.
- Die Daten müssen mindestens einmal pro Woche gesichert werden.
- Sicherungskopien müssen in gesicherten und verschließbaren Schränken aufbewahrt werden.
- Die Computer müssen durch Virenschutzprogramme gesichert werden. Diese müssen mindestens halbjährlich aktualisiert werden.
- Alle Datenarchive in Papierform (Briefwechsel, Ausdrucke, Karteikarten, ...) müssen in verschließbaren Schränken aufbewahrt werden.

Die EU-Bestimmungen sind in diesem Punkt weniger konkret und verlangen nur geeignete technische und organisatorische Maßnahmen zum Datenschutz. In diesem Sinne sollte sich der Betreiber zusätzliche Gedanken über die Datensicherung machen und überprüfen, ob seine Maßnahmen dem Stand der Technik entsprechen. Eine Verschlüsselung des E-Mail-Verkehrs und der Internetseite (https statt http) zählt sicherlich dazu. Sollten aber diese Bedingungen eingehalten werden, sind eigentlich die wichtigsten Forderungen der EU-Bestimmungen bereits umgesetzt. Sollte dennoch eine Verletzung des Schutzes von personenbezogenen Daten von Gästen auftreten (z.B. Datenklau), so sind die betroffenen Gäste zu informieren.

Strafen

Die Sanktionen sind bis maximal 20. Mio. Euro festgelegt bzw. wenn höher, dann 4% des Jahresumsatzes, je nach Schwere der Übertretung. Dabei hat der Gesetzgeber sicherlich an die großen Player in der Datenverarbeitung gedacht (Google, Facebook & Co) und weniger an die kleinen Betriebe. Diese Sanktionen werden derzeit zur Panikmache genutzt. Wie hoch eventuelle Sanktionen dann definitiv ausfallen werden, muss erst die Erfahrung zeigen, die Betriebe sollten hier kühlen Kopf bewahren.

Fazit: Was ist nun bis zum 25. Mai 2018 konkret zu tun?

1) Überlegen Sie sich, welche Daten Sie in Ihrem Betrieb verarbeiten, und erstellen Sie dazu eine Tabelle (**siehe Anlage 3 - Muster Register der Datenverarbeitungen**).
2) Überprüfen Sie, ob die Daten ausreichend geschützt werden, definieren Sie gegebenenfalls Schutzmaßnahmen und setzen Sie diese in Ihrem Betrieb um. Beachten Sie die Mindestsicherungsmaßnahmen, die bereits bisher gültig waren und den Stand der Technik.
3) Aktualisieren Sie die Aufklärungsschreiben (**siehe Anlage 1 - Muster eines Aufklärungsschreibens**). Diese müssen auf der Internetseite aktualisiert werden. Ebenso sind diese ab 25. Mai 2018 bei der **ersten** Ankunft der Gäste zur Aufklärung zu verwenden. Jeder Gast muss die Zustimmung nur einmal geben. Also muss der Gast nicht bei jeder Ankunft unterschreiben. Informieren sie auch die Stammgäste über die neuen Bestimmungen.
4) Erstellen Sie eine Vorlage zum Einholen der Zustimmung für die Verwendung der Daten für Kommunikationszwecke (**siehe Anlage 2 - Muster Zustimmung für Kommunikationszwecke**). Diese sollte auch im Internet aktualisiert werden, sofern Sie dort eine Newsletter-Anfrage haben. Außerdem sollte der Gast bei der **ersten** Ankunft die Zustimmung unterzeichnen, sofern Sie die Daten für Kommunikationszwecke verwenden wollen. Auch bei dieser Erklärung gilt: Jeder Gast muss die Zustimmung nur einmal geben. Überprüfen Sie, ob Sie von Gästen, die bereits einmal im Betrieb übernachtet haben, eine Zustimmung vorliegen haben. Falls dies zutrifft, muss die Zustimmung dieser Gäste nicht noch einmal eingeholt werden, sofern sie bei der Datenerhebung informiert worden sind und die Möglichkeit besteht, sich aus der Datenbank löschen zu lassen. Für alle anderen Gäste, die in der Datenbank gespeichert sind und keine Zustimmung nachgewiesen werden kann, muss die Zustimmung erneut eingeholt werden. Eine Alternative wäre, diese Daten zu löschen.
5) Richten Sie eine Datenbank ein, in der Sie abspeichern, welche Gäste Ihnen die Zustimmung zur Datenverarbeitung gegeben haben, die über die gesetzlichen Verpflichtungen hinausgehen. Auch die unterschriebenen Zustimmungen sollten in einem Ordner abgelegt werden.
6) Versuchen Sie überflüssige Daten und Daten, die Sie nicht mehr brauchen, zu vermeiden und löschen Sie diese. Sofern Gäste dies wünschen, müssen alle Daten, für die es keine gesetzliche Aufbewahrungspflicht gibt, gelöscht werden.

Da Italien derzeit an weiteren Bestimmungen arbeitet, ist es möglich, dass in den nächsten Monaten noch Änderungen veröffentlicht werden. Für weitere Fragen können Sie sich gerne an Walter Rier (E-Mail: walter.rier@sbb.it, Tel 0471 999395) wenden.

Anlagen:

Anlage 1 - Muster eines Aufklärungsschreibens
Anlage 2 - Muster Zustimmung für Kommunikationszwecke
Anlage 3 - Muster Register der Datenverarbeitungen

Hinweis zu den Mustern: Trotz sorgfältiger Prüfung wird eine Haftung des Urhebers dieser Muster ausgeschlossen. Die Muster müssen an die jeweilige betriebliche Situation angepasst werden.