1 Zweck und Grundlagen

Diese Datenschutzweisung enthält Vorschriften zum Schutz von Personendaten, die für die GAIA Hotel AG Basel (nachfolgend **Unternehmen**) gelten. Die Weisung vermittelt den Mitarbeitenden die wichtigsten Grundlagen des Datenschutzes und ermöglicht ihnen, zusammen mit anderen Massnahmen und Dokumenten, ihre Tätigkeit im Einklang mit den anwendbaren datenschutzrechtlichen Vorgaben auszuüben.

Da das Unternehmen Hotellerie bezogene Dienstleistungen sowie gegebenenfalls weitere Dienstleistungen und Waren anbietet und in diesem Zusammenhang Personendaten bearbeitet und austauscht, sind die schweizerischen Datenschutzgesetze und ggf. auch andere datenschutzrechtliche Vorgaben (z.B. die europäischen) für das Unternehmen relevant.

1. Geltungsbereich

Diese Datenschutzweisung gilt für alle Mitarbeitenden des Unternehmens, die Personendaten bearbeiten. Die Mitarbeitenden werden im Rahmen ihres Arbeitsverhältnisses verpflichtet, die relevanten datenschutzrechtlichen Bestimmungen sowie diese Datenschutzweisung einzuhalten.

2. Gegenstand

Gegenstand dieser Datenschutzweisung ist die Bearbeitung von Personendaten, unabhängig von der Art und Form der Bearbeitung (d.h. auf Papier, digital, mündlich, ganz, teilweise oder nicht-automatisiert).

3. Begriffe

Das anwendbare Datenschutzrecht definiert einige wichtige Begriffe. Grundsätzlich haben die nachfolgenden Begriffe die gleiche Bedeutung, wie sie im Bundesgesetz über den Datenschutz (**DSG**) definiert werden. Die wichtigsten Begriffe haben folgende Bedeutung:

Personendaten: Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Beispiele: *Name, Anschrift, Standortdaten, Online-Identifikatoren wie z.B. Geräte-ID, Cookie-ID, IP-Adresse, RFID-Tags, etc.*

Merke: Es handelt sich um natürliche Personen und nicht um juristische Personen oder andere Einrichtungen. **Aber:** Informationen über eine Kontaktperson eines Lieferanten oder bei einer anderen B2B-Beziehung gelten ebenfalls als Personendaten.

Besonders schützenswerte Personendaten: Personendaten der folgenden Kategorien:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten

- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie

- genetische Daten;
- biometrische Daten, die eine natürliche Person eindeutig identifizieren;
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen;
- Daten über Massnahmen der sozialen Hilfe.

Beispiele: *Aufnahmen von Videoüberwachungssystemen, Daten über die Gesundheit von Mitarbeitern, Strafregisterauszüge von Mitarbeitern, etc.*

Betroffene Person: Jede natürliche Person, über die Personendaten bearbeitet werden.

Beispiele: *Gäste, Mitarbeiter, Partner, Lieferanten, etc.*

Bearbeiten/Verarbeiten: Die Bearbeitung von Personendaten umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren.

Beispiele: *das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.*

4. Grundsätze für die Bearbeitung von Personendaten

Das Unternehmen sowie alle Mitarbeitenden beachten bei der Bearbeitung von Personendaten folgende Grundsätze:

4.1 Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Transparenz

Personendaten müssen auf rechtmässige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die "Nachvollziehbarkeit" verlangt insbesondere, dass die Beschaffung von Personendaten sowie der Umfang und Zweck der Bearbeitung für die betroffene Person transparent ist (z.B. durch eine Datenschutzerklärung mit den notwendigen Informationen über die jeweilige Bearbeitung). Bei jedem Umgang mit Personendaten haben Mitarbeitende somit zu prüfen, ob die betroffenen Personen hierüber und über die weiteren Angaben nach Ziff. 7/8 informiert wurden.

Praktische Anweisung:

Vor der Bearbeitung von Personendaten haben sich die Mitarbeitenden zunächst zu vergewissern, ob Bearbeitung rechtmässig ist, d.h. ob die Grundsätze der Bearbeitung von Personendaten, wie sie in dieser Ziffer festgehalten sind, eingehalten werden und ob ggf. eine Einwilligung von der betroffenen Person eingeholt werden muss. Zudem müssen die Mitarbeitenden sicherstellen, dass die betroffenen Personen transparent über die Bearbeitung der Personendaten informiert wurden. Diese Information muss vor der Bearbeitung der Daten erfolgen.

Bestehen Zweifel, ob eine dieser Voraussetzungen erfüllt ist, hat die Bearbeitung zu unterbleiben, bis die Datenschutzkoordinationsstelle die Rechtmässigkeit bestätigt hat. Ausgenommen sind Bearbeitungen, die in anderen Weisungen explizit für rechtmässig erklärt werden.

4.2 Zweckbindung

Personendaten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen für diesen Zweck weiterbearbeitet werden. Die Bearbeitung von Daten, für welche, bspw. in einer Datenschutzerklärung, kein Zweck festgelegt wird, ist somit nicht zulässig. Sollen Daten zu einem anderen als dem festgelegten Zweck weiterverarbeitet werden, haben die Mitarbeitenden zu prüfen, ob dieser Zweck noch vom ursprünglichen Zweck erfasst wird.

Unter gewissen Umständen können Personendaten zu weiteren Zwecken, die über den ursprünglichen Bearbeitungszweck zum Zeitpunkt der Datenerhebung hinausgehen, bearbeitet werden. Um festzustellen, ob die Bearbeitung zu einem anderen Zweck als dem ursprünglichen vereinbar ist, berücksichtigt das Unternehmen unter anderem:

- jede Verbindung zwischen den Zwecken, für die die Personendaten erhoben wurden, und den Zwecken der beabsichtigten Weiterbearbeitung;
- den Zusammenhang, in dem die Personendaten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der Verantwortlichen;
- die Art der Personendaten, insbesondere ob besonders schützenswerte Personendaten bearbeitet werden;
- die möglichen Folgen der beabsichtigten Weiterbearbeitung für die betroffenen Personen;
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Praktische Anweisung:

Für die Beurteilung der Rechtmässigkeit einer solchen weitergehenden Bearbeitung ist vor Beginn der Datenerhebung die Datenschutzkoordinationsstelle hinzuzuziehen und deren Zustimmung für die Bearbeitung einzuholen.

Die Datenschutzkoordinationsstelle vermerkt die Grundlage für die Bearbeitung bei den betreffenden Personendaten.

4.3 Datenminimierung

Personendaten müssen für den festgelegten Zweck angemessen, erheblich und auf diesen beschränkt sein. Es dürfen deshalb nicht mehr Daten erhoben werden als es für den Bearbeitungszweck notwendig ist.

Praktische Anweisung:

Vor der Bearbeitung von Personendaten muss geprüft werden, ob diejenigen Daten, welche im Zusammenhang mit der Bearbeitung erhoben werden, auch zwingend für die Bearbeitung notwendig sind. Ist dies nicht der Fall dürfen diese Personendaten nicht zwingend, jedoch auf freiwilliger Basis erhoben werden.

Beispiele:

1. *Auf der Hotelwebseite besteht die Möglichkeit sich an den Newsletter anzumelden. Dabei werden die Anrede, der Name und die E-Mailadresse erhoben und als zwingende Angaben gekennzeichnet. Für den Versand eines Newsletters wäre es jedoch ausreichend, wenn der Gast die E-Mailadresse angibt. Um dem Grundsatz der Datenminimierung zu entsprechen, darf somit nur die E-Mailadresse als zwingende Angabe erhoben werden. Die Anrede und der Name dürften nur auf freiwilliger Basis erhoben werden.*

2. *Im Hotel muss der Gast einen Meldeschein ausfüllen. Dabei werden neben der Anrede, dem Namen, der Adresse und den weiteren gesetzlich vorgeschriebenen Angaben auch die Interessen des Gastes als zwingende Angaben gekennzeichnet. Für die Erfüllung der Meldepflicht wäre es jedoch ausreichend, wenn der Gast einzig die gesetzlich zwingend zu erhebenden Daten angibt. Um dem Grundsatz der Datenminimierung zu entsprechen, dürfen somit nur die gesetzlich vorgeschriebenen Angaben erhoben werden. Die anderen Informationen des Gastes dürften nur auf freiwilliger Basis erhoben werden.*

Bestehen Zweifel, ob gewisse Daten als zwingende Angaben erhoben werden dürfen, hat die Bearbeitung zu unterbleiben, bis die Datenschutzkoordinationsstelle den Einzelfall analysiert und darüber entschieden hat. Ausgenommen sind Bearbeitungen, die in anderen Weisungen explizit für rechtmässig erklärt werden.

4.4 Richtigkeit der Personendaten

Personendaten müssen sachlich richtig und auf dem neuesten Stand sein. Eine aktive Nachforschungspflicht bezüglich der Richtigkeit der Daten besteht allerdings nicht. Bestehen aber begründete Anhaltspunkte, dass Personendaten nicht mehr aktuell sind, muss diesem Verdacht nachgegangen werden und die betroffenen Daten müssen ggf. berichtigt werden.

Praktische Anweisung:

Mitarbeitende, die auf unrichtige Daten aufmerksam werden, teilen dies dem Vorgesetzten mit oder, sofern sie über die entsprechenden Bearbeitungsrechte verfügen und keine Zweifel bestehen, berichtigen diese selbständig.

4.5 Speicherbegrenzung

Personendaten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie bearbeitet werden, erforderlich ist. Daten, die nicht mehr benötigt werden, sind deshalb zu löschen oder zu anonymisieren. Die Frage, nach Ablauf welcher Dauer Daten nicht mehr benötigt werden, lässt sich nicht verallgemeinern und ist in bereichsspezifischen Weisungen festzulegen, oder im Einzelfall zu beurtei-

len. Das Unternehmen sowie alle Mitarbeitenden des Unternehmens speichern Personendaten nicht länger, als es für die Zwecke, zu denen sie ursprünglich erhoben oder später weiterverarbeitet wurden, notwendig ist.

Praktische Anweisung:

Was als notwendig gilt, hängt von den Umständen im Einzelfall ab und wird mit Unterstützung der Datenschutzkoordinationsstelle bestimmt.

4.6 Integrität und Vertraulichkeit ("Datensicherheit")

Personendaten müssen in einer Weise bearbeitet werden, die eine angemessene Sicherheit der Personendaten gewährleistet. Sie müssen daher durch geeignete technische und organisatorische Massnahmen vor unbefugter oder unrechtmässiger Bearbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt werden. Die Mitarbeitenden haben insbesondere sicherzustellen, dass andere Personen, inkl. andere Mitarbeitende, nicht auf Personendaten zugreifen oder diese bearbeiten können, solange deren Berechtigung nicht eindeutig feststeht.

Praktische Anweisung:

Jeder Mitarbeitende trägt dazu bei, dass die Datensicherheit für Personendaten von Gästen sichergestellt werden kann. Wird festgestellt, dass die Integrität oder Vertraulichkeit der Personendaten verletzt wurde (z.B. durch die Versendung einer E-Mail mit einer Gästeliste an einen falschen Empfänger oder besteht der Verdacht, dass eine Phishing-Mail vorliegt, etc.), muss die Datenschutzkoordinationsstelle umgehend benachrichtigt werden.

Die Datenschutzkoodinationsstelle entscheidet sodann über das weitere Vorgehen.

4.7 Dokumentationspflicht

Die Unternehmensleitung bzw. die Hoteldirektion sorgt dafür, dass die genannten Grundsätze für alle Personendaten eingehalten werden. Sie kann deren Einhaltung jederzeit in dokumentierter Art und Weise nachweisen.

4.8 Einwilligungen

Das Unternehmen holt die notwendigen Einwilligungen der betroffenen Personen rechtzeitig, d.h. bevor eine Bearbeitung vorgenommen wird, für welche eine Einwilligung notwendig ist, ein.

Sofern die Einwilligung ausdrücklich erfolgen muss, erfolgt die Einwilligung durch eine eindeutige bestätigende Handlung, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Bearbeitung der sie betreffenden Personendaten einverstanden ist.

Eine Einwilligungserklärung wird in verständlicher und leicht zugänglicher Form und in einer klaren, einfachen Sprache zur Verfügung gestellt. Sie ist von anderen Angelegenheiten klar unterscheidbar und beinhaltet keine missbräuchlichen Klauseln.

Zudem wird der betroffenen Person eine einfache Methode zur Verfügung gestellt, mit der sie ihre Einwilligung jederzeit widerrufen kann.

Praktische Anweisung:

Bei der Beurteilung, ob diese Anforderungen erfüllt sind, sind insbesondere die besonderen Weisungen zu beachten.

Bestehen Zweifel, so nehmen die Mitarbeitenden die Datenbearbeitung so lange nicht vor, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben bestätigt hat.

5. Besondere Bearbeitungstätigkeiten

5.1 Bearbeitung von besonders schützenswerten Personendaten

Besonders schützenswerte Personendaten werden nicht bearbeitet. Das Unternehmen sowie alle Mitarbeitenden bearbeiten besondere schützenswerte Personendaten ausschliesslich nach Rücksprache mit der Datenschutzkoordinationsstelle, unter folgenden Voraussetzungen und nur soweit der Bearbeitung keine gesetzlichen Regelungen entgegenstehen:

- Die betroffene Person hat in die Bearbeitung der Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt;

- die Bearbeitung ist erforderlich, damit das Unternehmen oder die betroffene Person, die ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann;

- die Bearbeitung bezieht sich auf Personendaten, die die betroffene Person offensichtlich öffentlich gemacht hat;

- die Bearbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte erforderlich.

Die Mitarbeitenden beachten, dass es sich bei solchen Daten um besonders schützenswerte Informationen handelt, und bearbeiten diese so lange nicht, bis die Datenschutzkoordinationsstelle die Rechtmässigkeit bestätigt hat.

Praktische Anweisung:

Vor der Bearbeitung besonders schützenswerten Personendaten wird jeweils die Datenschutzkoordinationsstelle beigezogen und deren Zustimmung zur Bearbeitung eingeholt sowie die Grundlage für die Bearbeitung bei den betreffenden Personendaten vermerkt.

Das Unternehmen wendet zur Bearbeitung von besonders schützenswerten Personendaten zusätzliche Sicherheitsmassnahmen an.

5.1.1 Bearbeitung von Personendaten eines Kindes

Personendaten eines Kindes werden grundsätzlich nur bearbeitet, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, werden dessen Personendaten nur bearbeitet, sofern und soweit die Einwilligung zur Bearbeitung durch den gesetzlichen Vertreter des Kindes erteilt wird.

Das Unternehmen sowie alle Mitarbeitenden unternehmen angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den gesetzlichen Vertreter des Kindes erteilt wurde.

Praktische Anweisung

Bestehen Zweifel, ob diese Anforderungen erfüllt sind, so nehmen die Mitarbeitenden die Datenbearbeitung so lange nicht vor, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben bestätigt hat.

5.1.2 Digitales Marketing

Es werden keine Mitteilungen zu Werbe- oder Marketingzwecken an Kontakte über digitale Medien wie Mobiltelefone, E-Mail oder Internet versandt, ohne vorher die Einwilligung der betroffenen Personen einzuholen. Wenn eine Einwilligung zur Bearbeitung von Personendaten zu digitalen Marketingzwecken vorliegt, wird die betroffene Person in jeder Mitteilung darüber informiert, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen.

Praktische Anweisung:

Bestehen Zweifel darüber, ob eine Mitteilung Werbecharakter hat, eine Einwilligung vorliegt oder eine Information über das Widerrufsrecht vorliegt, hat die Datenbearbeitung so lange zu unterbleiben, bis die Datenschutzkoordinationsstelle die Einhaltung der Vorgaben bestätigt hat.

Good Practice:

Folgendes ist nicht erlaubt:

- Vorangekreuzte Opt-in-Boxen.
- Auf Schweigen, Inaktivität, Standardeinstellungen oder ihre Allgemeinen Geschäftsbedingungen vertrauen.
- Nur eine "Opt-out"-Wahl (ohne explizites Opt-in zu verlangen).

Folgendes muss sichergestellt werden:

- Aufzeichnungen über das Einwilligungsverfahren werden geführt (z.B. Datum der Einwilligung, Art der Einwilligung, welche Informationen dem Einwilligen zur Verfügung gestellt wurden).

- Die Einwilligung zur Bearbeitung ist unterscheidbar, klar und nicht mit anderen schriftlichen Vereinbarungen oder Erklärungen verbunden.

- Einzelpersonen werden darüber informiert, dass sie das Recht haben, ihre Einwilligung jederzeit zu widerrufen.

- Es gibt einfache Methoden, um die Einwilligung zu widerrufen.

- Eine gesonderte Einwilligung wird für verschiedene Bearbeitungsvorgänge eingeholt (die Einwilligung zur Direktvermarktung muss immer von jeder anderen Einwilligung zur Bearbeitung getrennt sein).

Beachte: Für Bestandeskunden können gewisse Privilegierungen gelten, welche im Einzelfall gemeinsam mit der Rechtsabteilung geprüft werden müssen.

6. Verzeichnis über Bearbeitungstätigkeiten

Das Unternehmen und gegebenenfalls deren Vertreter führt ein Verzeichnis über alle Bearbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Dieses enthält mindestens folgende Angaben:

- Die Identität des Verantwortlichen, d.h. den Namen und die Kontaktdaten des Unternehmens und gegebenenfalls der gemeinsam mit ihm Verantwortlichen, gegebenenfalls ihres Vertreters sowie gegebenenfalls des Datenschutzbeauftragten;

- die Zwecke der Bearbeitung;

- eine Beschreibung der Kategorien betroffener Personen und der Kategorien der bearbeiteten Personendaten;

- die Kategorien von Empfängern, gegenüber denen die Personendaten offengelegt worden sind oder noch offengelegt werden (einschliesslich Empfänger in Drittländern oder internationale Organisationen);

- wenn möglich, die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen;

- falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates und die implementierten Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus.

Praktische Anweisung:

Damit das Verzeichnis über die Bearbeitungstätigkeiten stets aktuell bleibt, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, bevor diese aufgenommen werden inkl. der oben aufgeführten Informationen, sofern möglich.

7. Informationspflichten bei der Erhebung von Personendaten direkt bei der betroffenen Person

Zum Zeitpunkt der Erhebung der Personendaten müssen den betroffenen Personen insbesondere folgende Informationen vom Unternehmen mitgeteilt werden:

- die Identität und die Kontaktdaten;
- den bzw. die Bearbeitungszwecke;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der Personendaten;
- werden die Personendaten ins Ausland bekanntgegeben: den Staat oder das internationale Organ und gegebenenfalls die Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus oder die Anwendung einer Ausnahme zur Sicherstellung eines angemessenen Datenschutzniveaus;
- bei der Vornahme von sog. automatisierten Einzelentscheidungen: Über die Entscheidung, welche ohne menschlichen Einfluss gefällt wird, die Möglichkeit der betroffenen Person ihren Standpunkt dazulegen sowie die Möglichkeit zur Überprüfung der automatisierten Einzelentscheidung durch eine natürliche Person.

Ggf. kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen, so z.B. das europäische Datenschutzrecht, welches zusätzlich vorsieht, dass folgende Angaben in den Informationen enthalten sein müssen:

- die Rechtsgrundlage für die Verarbeitung;
- gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland zu übermitteln sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der EU-Kommission, einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

- ggf. das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmässigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Diese Informationen werden den betroffenen Personen z.B. über eine Datenschutzerklärung zur Verfügung gestellt.

Praxis Anweisung:

Damit die Informationen gegenüber den betroffenen Personen stets aktuell bleiben, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, bevor diese aufgenommen werden inkl. der oben aufgeführten Informationen, sofern möglich.

8. Informationspflichten bei der indirekten Erhebung von Personendaten

Personendaten über betroffene Personen können auch indirekt, d.h. bei Dritten, erhoben werden. Diese entbindet das Unternehmen jedoch nicht davon, die betroffene Person über die Bearbeitung zu informieren. Zusätzlich zu den unter Ziffer 7 aufgelisteten Informationen, teilt das Unternehmen der betroffenen Person die Kategorien der bearbeiteten Personendaten mit. Die Information muss der betroffenen Person spätestens einen Monat nach dem das Unternehmen die Personendaten vom Dritten erhalten hat, mitteilen bzw. spätestens im Zeitpunkt der Bekanntgabe an einen Dritten.

Ggf. kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen, so z.B. das europäische Datenschutzrecht, welches zusätzlich vorsieht, dass folgende Angaben in den Informationen enthalten sein müssen (zusätzlich zu Ziffer 7 oben):

- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

Praktische Anweisung:

Damit die Informationen gegenüber den betroffenen Personen stets aktuell bleiben, melden die Mitarbeitenden der Datenschutzkoordinationsstelle neue Bearbeitungstätigkeiten, bevor diese aufgenommen werden inkl. der oben aufgeführten Informationen, sofern möglich.

9. Rechte der betroffenen Personen

Das Unternehmen sowie alle Mitarbeitenden beachten folgende Rechte der betroffenen Personen:

9.1.1 Auskunftsrecht

Jede betroffene Person, deren Personendaten das Unternehmen bearbeitet, hat das Recht, vom Unternehmen eine Bestätigung darüber zu verlangen, ob Personendaten über die anfragende betroffene Person bearbeitet werden. Dazu muss die betroffene Person eine schriftliche Anfrage via E-Mail, an die für die für Datenschutz verantwortliche Stelle beim Unternehmen stellen. Vor der Beantwortung der Anfrage muss, die die Identität der betroffenen Person überprüft werden.

Konnte die Identität zweifelsfrei festgestellt werden, hat die betroffene Person das Recht, die folgenden Informationen bezüglich ihrer eigenen Personendaten zu erhalten:

- die Identität und die Kontaktdaten des Verantwortlichen;
- die bearbeiteten Personendaten als solche;
- die Bearbeitungszwecke;
- die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Aufbewahrungsdauer;
- die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;
- gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;
- gegebenenfalls die Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden, sowie den Staat oder das internationale Organ und gegebenenfalls die Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus oder die Anwendung einer Ausnahme zur Sicherstellung eines angemessenen Datenschutzniveaus.

Ggf. kann das anwendbare Datenschutzrecht darüberhinausgehende Inhalte vorsehen, so z.B. das europäische Datenschutzrecht, welches zusätzlich vorsieht, dass der betroffenen Person folgende Informationen mitgeteilt werden müssen:

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling nach und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Das Unternehmen stellt eine Kopie der Personendaten, die Gegenstand der Bearbeitung sind, zur Verfügung.

Durch die Weitergabe der angefragten Informationen an die betroffene Person könnten unter gewissen Umständen Personendaten einer anderen betroffenen Person offengelegt werden. In solchen Fällen müssen die betreffenden Informationen redigiert oder zurückbehalten werden, je nachdem, was notwendig oder angemessen erscheint, um die Rechte dieser Person zu schützen.

Praktische Anweisung:

Auskunftsgesuche von betroffenen Personen sind umgehend an die Datenschutzkoordinationsstelle weiterzuleiten.

9.1.2 Recht auf Berichtigung

Die betroffene Person hat das Recht, vom Unternehmen unverzüglich die Berichtigung sie betreffender unrichtiger Personendaten zu verlangen. Unter Berücksichtigung der Zwecke der Bearbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger Personendaten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Berichtigung sind umgehend der Datenschutzkoordinationsstelle weiterzuleiten. Anfragen von betroffenen Personen auf Berichtigung von Mitarbeiterdaten sind an die Personalabteilung des Unternehmens zu richten.

9.1.3 Recht auf Löschung ("Recht auf Vergessenwerden")

Die betroffene Person hat das Recht unter gewissen Voraussetzungen, vom Unternehmen zu verlangen, dass sie betreffende Personendaten unverzüglich gelöscht werden, und das Unternehmen ist verpflichtet, Personendaten unverzüglich zu löschen.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Löschung sind umgehend der Datenschutzkoordinationsstelle weiterzuleiten. Anfragen von betroffenen Personen auf Löschung von Mitarbeiterdaten sind an die Personalabteilung des Unternehmens zu richten.

9.1.4 Recht auf Einschränkung der Bearbeitung

Die betroffene Person hat das Recht, die Einschränkung der Bearbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- die Richtigkeit der Personendaten wird von der betroffenen Person bestritten (inkl. Eintragung eines Bestreitungsvermerks). Die Einschränkung der Bearbeitung erfolgt, für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der Personendaten zu überprüfen;

- die Bearbeitung ist unrechtmässig und die betroffene Person lehnt die Löschung der Personendaten ab und verlangt stattdessen die Einschränkung der Nutzung der Personendaten;

- das Unternehmen benötigt die Personendaten für die Zwecke der Verarbeitung nicht länger. Die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;

- die betroffene Person hat Widerspruch gegen die Bearbeitung gemäss dem Widerspruchsrecht eingelegt. Die Einschränkung erfolgt so lange noch nicht feststeht, ob die berechtigten Gründe des Unternehmens gegenüber denen der betroffenen Person überwiegen.

Wurde die Bearbeitung eingeschränkt, so dürfen diese Personendaten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses bearbeitet werden.

Eine betroffene Person, die eine Einschränkung der Bearbeitung erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Einschränkung sind umgehend der Datenschutzkoordinationsstelle weiterzuleiten.

9.1.5 Datenübertragbarkeit ("Datenportabilität")

Die betroffene Person hat das Recht, die sie betreffenden Personendaten, die sie dem Unternehmen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat ferner das Recht, diese Daten einer anderen Gesellschaft ohne Behinderung zu übermitteln, sofern die:

- Bearbeitung auf einer Einwilligung der betroffenen Person beruht;

- Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Unternehmen und der betroffenen Person bearbeitet werden; oder

- die Bearbeitung mithilfe automatisierter Verfahren erfolgt.

Praktische Anweisung:

Anfragen von betroffenen Personen auf Übertragung ihrer Daten sind stets an die Datenschutzkoordinationsstelle weiterzuleiten.

9.1.6 Widerspruchsrecht

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Bearbeitung sie betreffender Personendaten Widerspruch einzulegen.

In solchen Fällen bearbeitet das Unternehmen die Personendaten nicht mehr, es sei denn, es kann zwingende schutzwürdige Gründe für die Bearbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Bearbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Praktische Anweisung:

Bei der Geltendmachung des Widerspruchrechts durch die betroffene Person ist die Datenschutzkoordinationsstelle zu involvieren, sofern Unklarheiten bestehen.

9.1.7 Rechte bei automatisierten Einzelentscheidungen

Die betroffene Person hat das Recht, dass Entscheidung, die ihr gegenüber rechtlichen Wirkungen entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen nicht ausschliesslich auf einer automatisierten Bearbeitung beruhen. Ausnahmen sind zulässig, soweit sie das Gesetz vorsieht.

Das Unternehmen wendet automatisierte Einzelentscheidungen, die ihm gegenüber rechtlicher Wirkung entfalten nur an, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Unternehmen erforderlich ist, aufgrund von anwendbaren gesetzlichen Vorschriften notwendig ist oder mit der ausdrücklichen Einwilligung der betroffenen Person.

Als Entscheidungen in diesem Sinn gelten solche, die auf einer rein automatisierten Datenbearbeitung basieren und entweder rechtliche Wirkungen gegenüber der betroffenen Person haben oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigen. Somit sind beispielsweise bei einer automatisierten Bonitätsprüfung, gestützt auf welche ein Vertragsschluss mit einer Person gegebenenfalls abgelehnt wird, die Vorgaben dieser Ziffer zu beachten.

Als Profiling gilt jede Art der automatisierten Bearbeitung Personendaten, die darin besteht, dass diese Personendaten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Soweit das Profiling mit einer automatisierten Einzelentscheidung verbunden wird, welche entweder rechtliche Wirkung gegenüber der betroffenen Person hat oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigt, sind die Vorgaben dieser Ziffer ebenfalls zu beachten.

Das Unternehmen sorgt dafür, dass Profiling und automatisierte Einzelentscheidungen im Einzelfall auf korrekten Daten beruht.

Praktische Anweisung:

Die Mitarbeitenden verzichten so lange auf automatisierte Einzelentscheidungen bis die Datenschutzkoordinationsstelle den Einsatz sowie die Modalitäten derselben für rechtmässig erklärt hat.

9.1.8 Vorgehen bei Gesuchen von betroffenen Personen

In der Regel werden Auskunfts-, Löschungs- und Berichtigungsgesuche sowie Anträge auf Datenübertragbarkeit, Widerruf von Einwilligungen und Widersprüche gegen die Datenbearbeitung aufgrund berechtigter Interessen automatisch an die Datenschutzkoordinationsstelle weitergeleitet. Für den Fall, dass eine solche Mitteilung der betroffenen Personen dennoch an einen Mitarbeitenden weitergeleitet werden sollten, leitet dieser die Mitteilung unverzüglich an die Datenschutzkoordinationsstelle weiter.

Den Mitarbeitenden ist es untersagt, Anfragen von Betroffenen zu bearbeiten oder mit Betroffenen ohne Abstimmung mit der Datenschutzkoordinationsstelle zu kommunizieren.

10. Übermittlung Personendaten an Dritte

10.1 Grundsatz

Jedwede Übermittlung von Personendaten ins Ausland ist nur zulässig, wenn für das betreffende Drittland oder für die betreffende internationale Organisation ein angemessenes Datenschutzniveau sichergestellt werden kann. Ein angemessenes Datenschutzniveau eines Staates liegt dann vor, wenn dies durch die zuständige Behörde festgestellt wurde (in der Schweiz durch den EDÖB bzw. den Bundesrat; in der EU durch die EU-Kommission).

Sollten Personendaten dereinst in Drittländer ohne Angemessenheitsbeschluss übermittelt werden, sind entsprechende geeignete Garantien einzusetzen. Ein Entscheid hierzu ist nur mit Zustimmung der Datenschutzkoordinationsstelle zulässig.

10.2 Übermittlungen zwischen Gruppengesellschaften

Sämtliche Gruppengesellschaften des Unternehmens stellen datenschutzrechtlich untereinander sogenannte Dritte dar. Als Grundlage für ein gruppenweit einheitliches Vorgehen schliessen die Gesellschaften einen Intercompany-Vertrag ab, wobei alle Gruppengesellschaften sowohl als "Verantwortlicher" (Controller) als auch als "Auftragsbearbeiter" (Processor) eingesetzt werden. Der Intercompany-Vertrag regelt die Verpflichtungen der Vertragsparteien entsprechend ihrer Rolle als Verantwortlicher wie auch ihrer Rolle als Auftragsbearbeiter.

10.3 Übermittlungen an sonstige Dritte

Das Unternehmen übermittelt Personendaten ausschliesslich dann an Dritte und gewährt Dritten Zugang zu Personendaten, wenn garantiert ist, dass die Daten vom Empfänger rechtmässig bearbeitet und angemessen geschützt werden:

- Wenn der Dritte als Verantwortlicher gilt, schliesst das Unternehmen einen Vertrag mit dem Verantwortlichen ab, in dem die Verantwortlichkeiten bezüglich der übermittelten Personendaten jeder Partei definiert werden.

- Wenn der **Dritte als Auftragsbearbeiter** gilt, schliesst das Unternehmen einen entsprechenden Auftragsdatenbearbeitungsvertrag mit dem Auftragsbearbeiter ab, mit dem der Auftragsbearbeiter verpflichtet wird, die datenschutzrechtlichen Grundsätze einzuhalten. Insbesondere wird er verpflichtet, die Daten vor einer weiteren Offenlegung zu schützen, diese nur gemäss den Weisungen des Unternehmens zu bearbeiten sowie angemessene technische und organisatorische Massnahmen zum Schutz der Personendaten zu implementieren und Verletzungen der Datensicherheit zu melden.

11. Technische und organisatorische Massnahmen

Das Unternehmen trifft angemessene technischen und organisatorischen Massnahmen, um die Sicherheit der Personendaten gemäss den anwendbaren datenschutzrechtlichen Vorschriften zu gewährleisten. Verletzungen der Datensicherheit (z.B. bei einem Hackerangriff) werden gemäss einer gesonderten Weisung an die Datenschutzkoordinationsstelle gemeldet.

12. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Das Unternehmen stellt sicher, dass die datenschutzrechtlichen Grundsätze bereits frühzeitig in neuen Projekten berücksichtigt werden und jeweils in die technische Umsetzung einfliessen ("Privacy by Design").

Das Unternehmen trifft zudem geeignete technische und organisatorische Massnahmen, damit durch Voreinstellungen sichergestellt werden kann, dass nur Personendaten, deren Bearbeitung für den jeweiligen Bearbeitungszweck erforderlich sind, bearbeitet werden. Dazu wird insbesondere sichergestellt, dass die jeweiligen Voreinstellungen datenschutzfreundlich sind ("Privacy by Default").

Praktische Anweisung:

Ist es geplant, dass neue Prozesse oder Tools eingeführt werden, wird die Datenschutzkoordinationsstelle möglichst früh in die Planung mit einbezogen, sodass die Grundsätze des "Privacy by Design" und "Privacy by Default" angemessen in das Projekt einfliessen können.

13. Datenschutz-Folgenabschätzung (DSFA)

Das Unternehmen führt vorab eine Abschätzung der Folgen von vorgesehenen Bearbeitungsvorgängen durch, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.

Die Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, hat insbesondere bei der Verwendung neuer Technologien oder bei neuartigen Datenverarbeitungsvorgängen, sowie aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung zu erfolgen (z.B. bei umfangreichen Bearbeitungen von besonders schützenswerten Daten oder bei der systematischen und umfangreichen Überwachung von öffentlichen Bereichen [z.B. Videoüberwachungsanlagen]).

Das Unternehmen holt vorab bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat der Datenschutzkoordinationsstelle ein. Die Durchführung von Datenschutz-Folgenabschätzungen erfolgt nach der gesonderten internen Richtlinie.

14. Meldung von Verletzungen der Datensicherheit ("Data Breach")

Eine Verletzung der Datensicherheit liegt dann vor, wenn eine Verletzung der Sicherheit dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Im Falle einer Verletzung der Datensicherheit meldet das Unternehmen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, sobald die Verletzung des Schutzes der Personendaten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Das Unternehmen informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder die zuständige Aufsichtsbehörde dies verlangt.

Der Prozess zur internen Meldung einer Verletzung der Datensicherheit richtet sich nach einer gesonderten Richtlinie.

Praktische Anweisung:

Wenn Mitarbeitende eine Verletzung der Datensicherheit (z.B. einen Hackerangriff oder die Offenlegung von Daten an unberechtigte Dritte, etc.) erkennen oder vermuten, können sie dies umgehend telefonisch der Direktion (intern 370) mitteilen.

15. Verantwortlichkeiten

15.1 Geschäftsleitung bzw. der Hoteldirektion

Die Geschäftsleitung bzw. der Hoteldirektion definiert die übergeordneten Grundsätze für die Gewährleistung des Datenschutzes im Unternehmen. Sie ernennt eine datenschutzverantwortliche Person – die Datenschutzkoordinationsstelle –, die mit der Durchsetzung der datenschutzrechtlichen Vorgaben beauftragt wird.

15.2 Vorgesetzte

Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Sie sorgen in Zusammenarbeit mit der Datenschutzkoordinationsstelle für Schulung und Sensibilisierung ihrer Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz einzuhalten.

15.3 Die Datenschutzkoordinationsstelle

Das Unternehmen hat eine Datenschutzkoordinationsstelle benannt. Die Datenschutzkoordinationsstelle ist die zentrale Anlaufstelle für Fragen des Datenschutzes und kann via management@gaiahotel.ch.

Die Datenschutzkoordinationsstelle hat insbesondere folgende Aufgaben:

- Sie trägt die Dokumentenverantwortung für diese Datenschutzweisung.
- Sie unterstützt das Unternehmen bei der Durchsetzung und Umsetzung des Datenschutzes.
- Sie beobachtet und berücksichtigt die Entwicklung der gesetzlichen Vorgaben im Bereich des Datenschutzes.

Die Durchsetzung dieser Weisung obliegt nicht der Datenschutzkoordinationsstelle sondern ausschliesslich den Vorgesetzten.

Weitere Aufgaben sind im Pflichtenheft der Datenschutzkoordinationsstelle definiert.

16. Sanktionen

Verletzungen dieser Datenschutzweisung können disziplinarische Massnahmen und/oder zivil- und/oder strafrechtliche Massnahmen nach sich ziehen.

17. Schlussbestimmungen

17.1 Änderungen und Ergänzungen

Diese Datenschutzweisung kann nur schriftlich durch einen Beschluss der Geschäftsleitung bzw. der Hoteldirektion abgeändert, ergänzt oder aufgehoben werden. Als Änderung oder Ergänzung ist jegliche Hinzufügung, Streichung oder Modifikation einzelner Bestimmungen zu qualifizieren. Ausgenommen hiervon sind Berichtigungen formeller Art.

17.2 Ergänzende Dokumente

Diese Datenschutzweisung stellt die Grundlage für die datenschutzrechtlichen Vorgaben des Unternehmens dar. Abgeleitet von dieser können weitere Dokumente, Weisungen und Prozesse erarbeitet werden, die im Zusammenhang mit der Bearbeitung von Personendaten notwendig sind.

17.3 Zugang zu dieser Weisung und Änderungen

Diese Datenschutzweisung ist allen Mitarbeitenden über das bestehende Weisungswesen des Unternehmens oder über andere Medien gemäss Entscheidung der Datenschutzkoordinationsstelle zugänglich.

Änderungen oder Ergänzungen zu dieser Datenschutzweisung treten im Moment der Publizierung auf www.gaiahotel.ch/ma (Code wird durch die Direktion laufend gewechselt – Infos erhalten Sie von der Direktion) in Kraft.

17.4 Inkrafttreten

Diese Datenschutzweisung tritt am 01.09.2023 in Kraft.

Basel, 1. September 2023 l ad