



HOTELS VIVA & RESORTS
FUN BEGINS HERE!

ETHIK-RICHTLINIE UND VERHALTENSKODEX VON HOTELS VIVA

Veröffentlicht und aktualisiert im Mitarbeiterportal: www.portalpersonas.hotelsviva.com

Die Geschäftsleitung von Hotels Viva hat diese interne Richtlinie erstellt, um eine Reihe von Vorschriften zusammenzufassen, die Ihnen helfen sollen, Ihre Rechte und Pflichten am Arbeitsplatz besser zu verstehen. Insbesondere behandelt dieses Regelwerk die folgenden Punkte:

- **Richtlinie und Protokoll zur Prävention von sexueller und moralischer Belästigung am Arbeitsplatz.**
- **Spezifische Verhaltensregeln während der Arbeitszeit.**
- **Richtlinie zu Bestechung und Vergütungen.**
- **Regelungen zur Arbeitszeit und deren Erfassung.**
- **Regeln, Informationen, Rechte und Pflichten im Zusammenhang mit personenbezogenen Daten.**
- **Nutzung von Computern, Internet, sozialen Netzwerken und E-Mail.**

Protokoll zur Prävention von sexueller und moralischer Belästigung

Einleitung

Zunächst möchten wir Sie darauf hinweisen, dass Hotels Viva besonderen Wert auf die Prävention und Beseitigung jeglicher Form von sexueller oder geschlechtsbezogener Belästigung legt, ebenso wie auf Belästigung aufgrund von ethnischer oder rassistischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung oder Geschlecht. Zu diesem Zweck wurde die folgende Regelung festgelegt.

Dieses Protokoll umfasst sowohl einen Verhaltenskodex als auch ein Handlungsprotokoll. Der Verhaltenskodex verfolgt das Ziel, Richtlinien und Maßnahmen zu fördern, die eine belästigungsfreie Arbeitsumgebung gewährleisten. Das Handlungsprotokoll legt die Verfahren fest, die in Fällen von sexueller oder moralischer Belästigung anzuwenden sind.

Definition von sexueller Belästigung

Gemäß dem Organgesetz 3/2007 liegt sexuelle Belästigung vor, wenn jedes verbale oder körperliche Verhalten sexueller Natur darauf abzielt oder zur Folge hat, die Würde einer Person zu verletzen, insbesondere wenn dadurch eine einschüchternde, erniedrigende oder feindselige Arbeitsumgebung geschaffen wird.

Definition von moralischer Belästigung

Psychologischer Druck am Arbeitsplatz, unabhängig davon, ob er zwischen Kollegen oder zwischen Vorgesetzten und Untergebenen auftritt. Dies besteht aus systematischen und anhaltenden Angriffen auf eine Person, mit dem Ziel, diese zu demütigen oder sie in Situationen zu bringen, die eine schwere Verletzung der persönlichen Würde darstellen.

1. Verhaltenskodex

Die Geschäftsleitung des Unternehmens bekräftigt ihr Engagement für die Vermeidung und Bekämpfung von Belästigungsfällen und legt großen Wert darauf, dass alle Mitarbeiter mit Würde behandelt werden. Daher wird sexuelle und moralische Belästigung am Arbeitsplatz weder geduldet noch toleriert.

Alle Mitarbeiter haben die Verantwortung, eine Arbeitsumgebung zu schaffen, in der die Würde jedes Einzelnen geachtet wird. **Es ist die unverzichtbare Pflicht aller Führungskräfte, proaktiv gegen Belästigung vorzugehen, indem sie deren Prävention, Aufdeckung und Bekämpfung sicherstellen. Die Geschäftsleitung verpflichtet sich, solche Verhaltensweisen konsequent zu sanktionieren, sofern sie einen Angriff auf die persönliche Würde und Privatsphäre von Frauen oder Männern darstellen.**

Alle Mitarbeiter haben das Recht, eine Beschwerde einzureichen, wenn sie Belästigung erfahren. Jede Meldung wird ernsthaft, zügig und unter Wahrung der Vertraulichkeit behandelt. Die Beschwerde muss eine detaillierte Beschreibung der Vorfälle enthalten und kann nach Wahl des Mitarbeiters an ein Mitglied der Personalabteilung, den Abteilungsleiter oder den Hoteldirektor gerichtet werden. Auf Wunsch des Mitarbeiters können die gesetzlichen Arbeitnehmervertretungen über den Vorfall informiert werden, damit sie im Rahmen des Informationsverfahrens tätig werden.

Gemäß Artikel 54.2 Buchstabe g) des spanischen Arbeitnehmerstatuts stellt Belästigung aus Gründen der ethnischen oder rassistischen Herkunft, Religion oder Weltanschauung, Behinderung, des Alters oder der sexuellen Orientierung

sowie sexuelle oder geschlechtsbezogene Belästigung gegenüber dem Arbeitgeber oder anderen Mitarbeitern eine schwerwiegende Vertragsverletzung dar. Darüber hinaus wird diese Vertragsverletzung als Grund für eine fristlose Kündigung gewertet.

Auch Artikel 40.12 des staatlichen Tarifvertrags für das Hotel- und Gastgewerbe stuft das zuvor beschriebene Verhalten als sehr schwerwiegend ein. Mögliche Sanktionen umfassen eine Suspendierung ohne Gehalt für einen Zeitraum von sechzehn bis sechzig Tagen oder eine fristlose Kündigung.

Artikel 40.13 desselben Tarifvertrags definiert zudem Folgendes als sehr schwerwiegendes Fehlverhalten: Moralische Belästigung, sexuelle Belästigung oder geschlechtsbezogene Belästigung sowie Belästigung aufgrund der ethnischen oder rassischen Herkunft, Religion oder Weltanschauung, Behinderung, des Alters, der sexuellen Orientierung oder des Geschlechts gegenüber anderen Mitarbeitern.

2. Handlungsprotokoll

A) Informelles Verfahren

Da es in den meisten Fällen lediglich darum geht, das unerwünschte Verhalten zu beenden, wird zunächst geprüft, ob ein informelles Verfahren angemessen ist. Dieses ermöglicht es, der betreffenden Person auf nicht offiziellem Weg klar und deutlich mitzuteilen, dass ihr Verhalten unerwünscht, unangemessen oder störend ist und die Arbeitsausführung beeinträchtigt. Ziel ist es, dass die betreffende Person das Verhalten unverzüglich einstellt. Diese Erklärung kann entweder unter vier Augen zwischen den betroffenen Mitarbeitern erfolgen oder – nach Wahl des betroffenen Mitarbeiters – in Anwesenheit eines Dritten. Dies kann der Abteilungsleiter, der Hoteldirektor, eine Person aus der Personalabteilung oder ein Vertreter der Arbeitnehmervertretung sein.

Falls der betroffene Mitarbeiter es wünscht, kann dieser nicht offizielle Schritt auch ohne seine persönliche Anwesenheit erfolgen. In diesem Fall kann die Mitteilung an die betroffene Person durch einen Vertreter der Arbeitnehmervertretung, den Abteilungsleiter, den Hoteldirektor oder eine Person aus der Personalabteilung übermittelt werden.

B) Formelles Verfahren

Das formelle Verfahren wird durch die Einreichung einer schriftlichen Beschwerde eingeleitet, die eine möglichst detaillierte Auflistung der Vorfälle enthält, die von der betroffenen Person als sexuelle oder moralische Belästigung wahrgenommen wurden. Die Beschwerde kann nach Wahl des Mitarbeiters an ein Mitglied der Personalabteilung oder den Hoteldirektor gerichtet werden. Auf Wunsch des Mitarbeiters kann zudem eine Kopie der Beschwerde an die gesetzlichen Arbeitnehmervertretungen weitergeleitet werden.

Die Einreichung der Beschwerde führt zur sofortigen Eröffnung eines Informationsverfahrens, das darauf abzielt, die Sachlage aufzuklären. Dabei wird allen beteiligten Parteien Gehör gewährt, einschließlich der gesetzlichen Arbeitnehmervertretungen, sofern diese im Betrieb vorhanden sind.

Anschließend werden die erforderlichen Untersuchungsschritte eingeleitet, um die Glaubwürdigkeit und Wahrhaftigkeit der geschilderten Vorfälle zu prüfen.

Während der Bearbeitung des Verfahrens wird dem Beschwerdeführer oder der beschuldigten Person, sofern diese es wünschen, die Möglichkeit eines Arbeitsplatzwechsels eingeräumt – sofern dies organisatorisch umsetzbar ist – bis eine endgültige Entscheidung getroffen wird.

Die gesetzlichen Arbeitnehmervertretungen, mögliche Zeugen sowie alle weiteren Beteiligten sind zur vertraulichen Behandlung des gesamten Verfahrens verpflichtet, da die Vorgänge die Privatsphäre und Würde der betroffenen Personen direkt betreffen. Sowohl der Beschwerdeführer als auch die beschuldigte Person sind mit dem gebotenen Respekt zu behandeln.

Falls sich der Vorwurf der sexuellen Belästigung bestätigt, werden die im Artikel 40.12 und Artikel 40.13 des staatlichen Tarifvertrags für das Hotel- und Gastgewerbe vorgesehenen Sanktionen angewendet.

Wenn sich die gemeldeten Vorfälle nicht eindeutig bestätigen lassen und daher keine disziplinarischen Maßnahmen ergriffen werden, wird der hinweisgebende Mitarbeiter keinesfalls benachteiligt oder sanktioniert. Im Gegenteil: Die Situation wird besonders aufmerksam überwacht, um sicherzustellen, dass kein Belästigungsverhalten vorliegt.

Zudem wird, sofern möglich, auf eine Arbeitsorganisation hingewirkt, die einen dauerhaften Kontakt zwischen den betroffenen Mitarbeitern vermeidet.

Spezifische Verhaltensregeln

Der Mitarbeiter hat die Anweisungen der Unternehmensleitung oder der von dieser beauftragten Person zu befolgen und muss insbesondere:

- Auf persönliche Hygiene achten und die Arbeitsuniform in einwandfreiem Zustand halten, insbesondere bei kundenorientierten Tätigkeiten. Die Namensplakette muss stets sichtbar getragen werden.
- Die Einrichtungen des Hotels pfleglich behandeln und zu deren vollkommenen Sauberkeit und Hygiene beitragen.
- Einen respektvollen Umgang mit allen Kolleginnen und Kollegen pflegen und stets einen angemessenen Ton und Ausdrucksweise wahren. Es ist verboten, in den Hotelbereichen laut zu sprechen.
- Das Hotel darf nur mit der von dem Unternehmen bereitgestellten Handtasche betreten und verlassen werden.
- Es ist ausdrücklich untersagt, sich Getränke, Lebensmittel, Reinigungsmittel oder andere Gegenstände, unabhängig davon, ob sie dem Hotel oder den Gästen gehören, anzueignen.
- Wenn ein Mitarbeiter einen verlorenen Gegenstand findet, muss er diesen dem Abteilungsleiter übergeben.
- Rauchen ist nur in den ausgewiesenen Bereichen erlaubt und ausschließlich während der mit den jeweiligen Abteilungen abgestimmten Pausen, **wobei dies im Zeiterfassungssystem registriert werden muss**. Während eines gesundheitlichen Notstands aufgrund von COVID-19 oder einer ähnlichen Situation ist das Rauchen auf dem gesamten Betriebsgelände untersagt. Ebenso ist das Rauchen im Außenbereich untersagt.
- Die Maßnahmen zur Verhütung von Arbeitsrisiken sind einzuhalten.
- Im Falle eines Notstands sind sämtliche zur Prävention von COVID-19 erlassenen Maßnahmen zu befolgen.
- Es ist untersagt, auf dem Betriebsgelände Alkohol zu konsumieren, sowohl während der Arbeitszeit als auch außerhalb dieser, es sei denn, es liegt eine ausdrückliche Genehmigung der Geschäftsleitung vor. Ebenso ist es verboten, illegale Drogen aufzubewahren, zu besitzen oder zu beschaffen, sei es innerhalb der Räumlichkeiten des Unternehmens oder in deren Umgebung.
- Die Benutzung von Mobiltelefonen während des Dienstes ist untersagt, außer mit ausdrücklicher Genehmigung der Geschäftsleitung.
- Es ist untersagt, in sozialen Netzwerken Kommentare oder Bilder zu veröffentlichen, die die Wahrnehmung, das Ansehen oder den Ruf des Unternehmens, seiner Mitarbeiter oder Kunden beeinträchtigen könnten.

Richtlinie zu Bestechung und Vergütungen

Wir halten uns an alle Gesetze, die Bestechung verbieten, und versprechen oder gewähren keine Gefälligkeiten im Austausch für geschäftliche Vorteile.

Da Hotels Viva im Falle rechtswidriger Handlungen durch Dritte, die in unserem Namen handeln, zur Verantwortung gezogen werden kann, handeln wir mit größter Sorgfalt bei der Auswahl und Überwachung dieser Dritten.

Verwenden Sie niemals Gelder, Vermögenswerte, Dienstleistungen oder Einrichtungen von Hotels Viva, um unangemessen Einfluss auf eine geschäftliche Entscheidung zu nehmen, und bieten Sie diese niemals an.

- Wir bieten keine Leistungen über den aktuellen Arbeitsbereich hinaus an, in der Hoffnung, dadurch zusätzliche Aufträge zu erhalten.
- Wenn wir im Auftrag Dritter handeln, stellen wir sicher, dass diese mit den Antibe­stechungsrichtlinien von Hotels Viva vertraut sind und überwachen ihr Verhalten sorgfältig.
- Zahlungen und Transaktionen werden von uns wahrheitsgemäß und korrekt durchgeführt und dokumentiert; wir versuchen niemals, den tatsächlichen Zweck eines Aufwands zu verschleiern.
- Wir konkurrieren fair und bieten unseren Gästen das bestmögliche Erlebnis.

- Wir halten die Wettbewerbsgesetze ein, die zum Schutz der Verbraucher und zur Gewährleistung eines freien Marktes dienen. Wir halten uns an diese Gesetze und versuchen niemals, den Wettbewerb einzuschränken oder zu verzerren.
- Wir schließen keine Absprachen (weder persönlich noch schriftlich, weder formell noch informell) mit Wettbewerbern, die den Wettbewerb beeinträchtigen könnten.
- Wir handeln fair gegenüber allen Lieferanten von Hotels Viva.
- Wir stellen keine falschen Tatsachen dar, wenn wir im Namen von Hotels Viva verhandeln.

Arbeitszeit und deren Erfassung

In den Betrieben, in denen ein elektronisches Zeiterfassungssystem vorhanden ist, gelten folgende Regeln:

- Es muss das nächstgelegene Gerät zum Arbeitsplatz verwendet werden.
- Der Beginn/Das Ende der Arbeitszeit oder von Pausen muss unmittelbar vor bzw. nach der tatsächlichen Arbeitsaufnahme oder -beendigung erfasst werden.

Das bedeutet, dass der Arbeitsbeginn NICHT beim Betreten des Hotels und das Arbeitsende nicht beim Verlassen des Hotels erfasst werden darf. Die Erfassung muss am nächstgelegenen Zeiterfassungsgerät unmittelbar vor Beginn und direkt nach Ende der tatsächlichen Arbeit erfolgen.

- Die Nutzung des Zeiterfassungsgeräts ist verpflichtend. Eine Nichtnutzung oder unsachgemäße Nutzung kann als arbeitsrechtlicher Verstoß gewertet werden.
- Jede Unregelmäßigkeit (z. B. Vergessen, nicht erkannter Mitarbeiter, technischer Fehler usw.) muss dem zuständigen Abteilungsleiter gemeldet werden.
- Die vom System erfassten Daten können als Nachweis für Abwesenheiten, Verspätungen oder vorzeitiges Arbeitsende verwendet werden.

In jedem Fall gilt: Die bloße Zeiterfassung über die planmäßige Arbeitszeit hinaus stellt keinen Nachweis für die tatsächliche Leistung von Überstunden dar. Überstunden dürfen nur mit vorheriger Genehmigung durch den Direktor des Hotels/Arbeitsplatzes geleistet werden.

Schutz personenbezogener Daten

1. Information.

Diese Datenschutzerklärung gilt für die Datenverarbeitung im Personalwesen von HOTELS VIVA & RESORTS. Bitte lesen Sie sie sorgfältig durch. Sie enthält wichtige Informationen über die Verarbeitung Ihrer personenbezogenen Daten, die Rechte, die Ihnen gemäß den geltenden Vorschriften zustehen, sowie Ihre Pflichten.

Wir behalten uns das Recht vor, diese Informationen jederzeit zu aktualisieren, sei es aus geschäftlichen Gründen oder zur Einhaltung gesetzlicher oder gerichtlicher Änderungen. Wenn Sie Fragen oder Klarstellungen bezüglich des Datenschutzes oder Ihrer Rechte benötigen, können Sie sich über die unten angegebenen Kanäle an uns wenden.

1. Wer ist für die Verarbeitung Ihrer Daten verantwortlich?

Verantwortlich für die Verarbeitung Ihrer Daten ist das Unternehmen von HOTELS VIVA & RESORTS, mit dem Sie ein Arbeits- oder Vertragsverhältnis haben (im Folgenden das „UNTERNEHMEN“). Die Daten aus dem Personalwesen aller Unternehmen von HOTELS VIVA & RESORTS werden auf Konzernebene konsolidiert, um die in dieser Richtlinie angegebenen Zwecke zu erfüllen. Die für die Verarbeitung dieser konsolidierten Daten verantwortliche Stelle ist

INVERSIONES PASCUAL, S.L. mit Sitz in Calle Agustín Argüelles, 1, 07400 Alcudia, Illes Balears, Spanien (im Folgenden HOTELS VIVA & RESORTS).

Bei Fragen zum Datenschutz können Sie sich an den Datenschutzbeauftragten wenden: Calle Agustín Argüelles, 1, 07400 Alcudia, Illes Balears, Spanien, oder per E-Mail an: dpd@hotelsviva.com.

2. Zu welchem Zweck verarbeiten wir Ihre Daten und auf welcher Rechtsgrundlage?

Die personenbezogenen Daten der Mitarbeiter werden zu folgenden Zwecken verarbeitet:

- 2.1. Personalverwaltung
- 2.2. Arbeitszeiterfassung
- 2.3. Umsetzung von Kontroll- und Überwachungsmaßnahmen am Arbeitsplatz
- 2.4. Erhebung und Nutzung von Bildmaterial
- 2.5. Konsolidierung von Personaldaten
 - INTERNE VERWALTUNGSZWECKE
 - GEHALTSABRECHNUNG
 - INTERNE UNTERNEHMENSVERTRÄGE
 - MANAGEMENTKONTROLLE UND GESCHÄFTSDATENANALYSE

Im Folgenden finden Sie detaillierte Informationen zu jedem dieser Zwecke.

2.1. Personalverwaltung

DAS UNTERNEHMEN verarbeitet Ihre Daten zur Verwaltung, Organisation, Planung, Administration und Schulung seines Personalwesens.

Die Kategorien von Daten, die zu diesem Zweck verarbeitet werden, sind:

- Identifikations- und Kontaktdaten, wie z. B. Personalausweisnummer, Vor- und Nachname, Aufenthaltserlaubnis (falls zutreffend), Anschrift, Telefonnummer, E-Mail, Unterschrift, Bild/Ton, Sozialversicherungsnummer/Versorgungswerk. Die von Ihnen angegebene Mobilnummer wird für den gegenseitigen Austausch betrieblicher Mitteilungen über WhatsApp oder eine andere vereinbarte Messaging-App verwendet.
- Daten zu persönlichen Merkmalen, wie Familienstand, Geburtsdatum, Nationalität oder Sprachkenntnisse.
- Ausbildungs- und Berufsdaten.
- Beschäftigungsbezogene Daten.
- Finanz-, Bank- und Versicherungsdaten, einschließlich Gehalts- und Bankverbindungen.
- Transaktionsdaten über Waren und Dienstleistungen.
- Daten, die aus dem Arbeitsverhältnis entstehen, darunter der Arbeitsvertrag, sonstige Regelungen zur Überlassung oder zu Praktikumsverhältnissen sowie Arbeitszeitaufzeichnungen.
- Besondere Kategorien personenbezogener Daten: Wir verarbeiten Gesundheitsdaten, soweit dies zur Erfüllung unserer Pflichten im Bereich des Arbeitsrechts, der Arbeitssicherheit, der Sozialversicherung oder der Integration von Menschen mit Behinderung erforderlich ist – z. B. Informationen zu Krankschreibungen, dem Vorliegen einer Behinderung oder dem Grad der Behinderung. Wir können auch Daten zur Gewerkschaftszugehörigkeit verarbeiten, wenn Sie uns ausdrücklich darum gebeten haben, z. B. zur Abwicklung des Gewerkschaftsbeitrags. In diesem Fall erfolgt die Verarbeitung Ihrer Gewerkschaftszugehörigkeit auf der Grundlage Ihrer Einwilligung, die Sie dem Personalwesen erteilt haben. Diese Einwilligung können Sie jederzeit widerrufen, indem Sie sich an die Personalabteilung wenden.

Die Verarbeitung dieser Daten ist erforderlich zur Durchführung Ihres Arbeitsvertrags oder des Vertrags, der Ihre Einsatzüberlassung oder Ihren Status als Praktikant oder Trainee regelt, sowie zur Erfüllung der gesetzlichen Verpflichtungen des UNTERNEHMENS in den Bereichen Arbeitsrecht, Arbeitsschutz, Sozialversicherung oder Integration von Menschen mit Behinderungen.

Die im Rahmen des Arbeitsverhältnisses entstehenden wirtschaftlichen Daten und Transaktionsdaten über Waren und Dienstleistungen werden zum Zweck der Buchhaltungs- und Verwaltungsorganisation sowie zur Erfüllung gesetzlicher Verpflichtungen des UNTERNEHMENS in den Bereichen Buchhaltung und Steuern verarbeitet.

Alle genannten Daten werden entweder direkt von Ihnen erhoben oder im Verlauf des Arbeitsverhältnisses generiert. Das UNTERNEHMEN kann vergünstigte Konditionen für den Erwerb von Produkten oder Dienstleistungen bei

Drittunternehmen aushandeln. Bitte beachten Sie, dass jegliche vertraglichen Beziehungen, die Sie mit diesen Drittunternehmen eingehen, außerhalb unseres Einflussbereichs liegen.

2.2. Arbeitszeiterfassung

Das UNTERNEHMEN verarbeitet die in der Arbeitszeiterfassung erfassten Daten zum Zweck der Kontrolle Ihrer täglichen Arbeitszeit, gemäß Artikel 34.9 des Arbeitnehmerstatuts.

Das Unternehmen verarbeitet das aus Ihrem Gesichtsmuster errechnete mathematische Modell, um Ihre Identität im Rahmen des Arbeitszeiterfassungssystems zu verifizieren. Die Verwendung eines biometrischen Verifizierungssystems beruht auf unserem berechtigten Interesse, eine schnelle und effiziente Authentifizierung der Personen sicherzustellen, die ihre Arbeitszeit erfassen.

Wie wurde dieses berechnete Interesse gegenüber Ihren Rechten und Freiheiten abgewogen? Folgende Aspekte wurden bei der Abwägung berücksichtigt:

- Artikel 20.3 des Arbeitnehmerstatuts gewährt dem Arbeitgeber das Recht, Überwachungs- und Kontrollmaßnahmen zu ergreifen, um die Einhaltung der arbeitsvertraglichen Pflichten der Mitarbeiter zu überprüfen.
- Die Verarbeitung ist mit den berechtigten Erwartungen der betroffenen Personen vereinbar, da es sich um eine gängige Praxis in Unternehmen handelt.
- Der Eingriff in die Privatsphäre der Betroffenen ist gering, da das Gesichtsmuster ausschließlich zur Verifizierung dient und nicht zur biometrischen Identifikation verwendet wird. Zudem speichert das biometrische System kein Gesichtsbild, und aus dem gespeicherten mathematischen Muster kann kein Bild rekonstruiert werden.

2.3. Umsetzung von Kontroll- und Überwachungsmaßnahmen am Arbeitsplatz

Das UNTERNEHMEN ergreift Maßnahmen, um die Sicherheit der Einrichtungen, Vermögenswerte, Ressourcen oder Systeme zu gewährleisten. In diesem Zusammenhang und gemäß Artikel 89.1 des Organisationsgesetzes 3/2018 über den Schutz personenbezogener Daten und die Gewährleistung digitaler Rechte weisen wir Sie ausdrücklich darauf hin, dass Bildaufnahmen durch Videoüberwachungskameras, die sich in den Einrichtungen des Unternehmens befinden – ob sichtbar oder verdeckt –, auch zum Zweck der Kontrolle der Mitarbeiter verarbeitet werden. Dies gilt sowohl im Hinblick auf die Ausführung ihrer Aufgaben als auch auf die Einhaltung interner Unternehmensvorgaben sowie zur Untersuchung und Verfolgung von Straftaten. Diese Verarbeitung erfolgt auf Grundlage der dem Arbeitgeber im Arbeitsrecht ausdrücklich zugestandenen Rechte und unterliegt stets den Grundsätzen der Verhältnismäßigkeit und Transparenz.

2.4. Erhebung und Nutzung von Bildmaterial

Das UNTERNEHMEN ist Teil von HOTELS VIVA & RESORTS, das über eine unternehmenseigene Website verfügt: <https://www.hotelsviva.com/> sowie über Social-Media-Kanäle wie Instagram, Twitter, Facebook und YouTube. Im Rahmen von Veranstaltungen oder zur Präsentation der Einrichtungen des Unternehmens können Video- oder Fotoaufnahmen innerhalb der Betriebsräume gemacht werden, auf denen Sie als Mitarbeiter zu sehen sein könnten. Diese Aufnahmen werden über die genannten Kanäle veröffentlicht, um die Öffentlichkeit über Dienstleistungen, Aktivitäten oder Einrichtungen des UNTERNEHMENS zu informieren. Die Verarbeitung und Verbreitung Ihrer Bild- und/oder Tonaufnahmen über die Website oder soziale Netzwerke erfolgt gemäß dem Organisationsgesetz 1/1982 vom 5. Mai über das Recht auf Ehre, Privatsphäre und das eigene Bild und auf Grundlage Ihrer Einwilligung, die in jedem Fall gesondert eingeholt wird.

2.5. Konsolidierung von Personaldaten

Die Unternehmen übermitteln die Daten ihres Personalwesens an HOTELS VIVA & RESORTS zur Datenkonsolidierung. Die von HOTELS VIVA & RESORTS durchgeführten Verarbeitungen dieser Daten sind wie folgt:

INTERNE VERWALTUNGSZWECKE

Ihre Identifikationsdaten, Positionsdaten und beruflichen Kontaktdaten werden im unternehmensweiten Verzeichnis erfasst, das allen Mitarbeitern zugänglich ist. Diese Daten werden auch verarbeitet, um Sie in die entsprechenden Systeme aufzunehmen, z. B. um Ihnen den Zugang zum Mitarbeiterportal zu ermöglichen.

HOTELS VIVA & RESORTS verarbeitet diese Daten auch, um Sie in den Verteiler für interne Unternehmenskommunikation aufzunehmen.

Diese Konsolidierung stützt sich auf das berechtigte Interesse, das im Erwägungsgrund 48 der DSGVO anerkannt wird und die Übermittlung personenbezogener Daten aus dem Personalwesen zwischen Unternehmen erlaubt, wenn diese Teil einer Unternehmensgruppe mit zentraler Verwaltung sind.

Wie wurde dieses berechtigte Interesse gegenüber Ihren Rechten und Freiheiten abgewogen? Für die Abwägung dieses Interesses in Bezug auf Ihre Rechte und Freiheiten wurde Folgendes festgestellt:

- Die Verarbeitung ist mit den berechtigten Erwartungen der betroffenen Personen vereinbar, da es sich um Mitarbeiter der Unternehmen von HOTELS VIVA & RESORTS handelt, die Datenverarbeitung im Rahmen eines laufenden Beschäftigungsverhältnisses erfolgt und sie für dessen Abwicklung notwendig ist.
- Die Auswirkungen der Verarbeitung auf die Privatsphäre der Betroffenen sind begrenzt, da es sich um nicht sensible Daten handelt und die Zwecke rein verwaltungsbezogen sind.

GEHALTSABRECHNUNG

Ihre Bankdaten und Informationen zu Ihrer Gehaltsabrechnung werden verarbeitet, um die Lohnzahlungen an unsere Mitarbeiter durchzuführen. Diese Verarbeitung erfolgt auf Grundlage der Erfüllung Ihres Arbeitsvertrags sowie unseres berechtigten Interesses an einer effizienten Abwicklung von Gehaltszahlungen. Für die Abwägung dieses Interesses gegenüber Ihren Rechten und Freiheiten wurde festgestellt, dass die Verarbeitung nur einen begrenzten Einfluss auf die Privatsphäre der betroffenen Personen hat, den berechtigten Erwartungen der Betroffenen entspricht und keine erheblichen Risiken oder Gefährdungen mit sich bringt.

INTERNE UNTERNEHMENSVERTRÄGE

Sofern Sie zustimmen, bewahrt HOTELS VIVA & RESORTS Ihre Personalunterlagen auf, um Sie für zukünftige Arbeitsverhältnisse in Unternehmen unter seiner Leitung berücksichtigen zu können.

Konkret verarbeitet HOTELS VIVA & RESORTS folgende Daten:

- Identifikations- und Kontaktdaten, wie Personalausweisnummer, Vor- und Nachname, Aufenthaltserlaubnis (falls zutreffend), Adresse, Telefonnummer und E-Mail.
- Daten zu persönlichen Merkmalen, wie Familienstand, Geburtsdatum, Nationalität oder Sprachkenntnisse.
- Ausbildungs- und Berufsdaten.
- Daten zum Beschäftigungsverlauf: Ihre bisherige Laufbahn im Unternehmen.
- Besondere Kategorien personenbezogener Daten: insbesondere Informationen über eine bestehende Behinderung und den Grad der Einschränkung. Diese Daten werden verarbeitet, um unseren gesetzlichen Verpflichtungen zur Integration von Menschen mit Behinderungen nachzukommen.

Die Verarbeitung dieser Daten erfolgt auf Grundlage Ihrer Einwilligung, die im Mitarbeiter-Anmeldeformular eingeholt wird. Die Verweigerung oder der Widerruf dieser Einwilligung hat keine Auswirkungen auf Ihr aktuelles Beschäftigungsverhältnis mit dem UNTERNEHMEN. Allerdings können wir Sie dann nicht direkt kontaktieren, sollte zukünftig eine passende Stelle frei werden.

Sie können Ihre Einwilligung jederzeit widerrufen, indem Sie sich an die Personalabteilung wenden.

MANAGEMENTKONTROLLE UND GESCHÄFTSDATENANALYSE

HOTELS VIVA & RESORTS verarbeitet Daten zu persönlichen Merkmalen, sozialen Umständen, Ausbildung und Beruf, Beschäftigungsdetails, wirtschaftlichen, finanziellen und versicherungsbezogenen Aspekten sowie Transaktionsdaten über Waren und Dienstleistungen, die aus der Konsolidierung der Personaldaten stammen. Diese Daten dienen der Erstellung von Berichten und der Analyse von Geschäftsdaten zu Zwecken der Business Intelligence und der Managementkontrolle. Die Analysen und Berichte liefern aggregierte Ergebnisse und werden für statistische Auswertungen sowie zur Erstellung von Prognosen verwendet. Ziel ist es, unternehmerische Entscheidungen zu unterstützen und Prozesse und Kosten zu optimieren.

Diese Verarbeitungen beruhen auf dem berechtigten Interesse von HOTELS VIVA & RESORTS, eine konsolidierte Sicht auf sein Personalwesen für interne Verwaltungszwecke und strategische Entscheidungsfindung zu erhalten.

Wie wurde dieses berechnigte Interesse gegenüber Ihren Rechten und Freiheiten abgewogen? Für die Abwägung dieses Interesses in Bezug auf Ihre Rechte und Freiheiten wurde Folgendes festgestellt:

- Erwägungsgrund 48 der DSGVO erkennt das berechnigte Interesse an der Übermittlung personenbezogener Daten aus dem Personalwesen zwischen Unternehmen an, wenn diese Teil einer gemeinsamen Organisation mit zentraler Verwaltung sind.
- Die Verarbeitung entspricht den berechnigten Erwartungen der Betroffenen, da es sich um Mitarbeiter von Unternehmen handelt, die von HOTELS VIVA & RESORTS geführt werden, und die Verarbeitung im Rahmen aktiver Verhältnisse erfolgt.
- Die Auswirkungen auf die Privatsphäre der Betroffenen sind begrenzt, da technische und organisatorische Maßnahmen getroffen wurden, um eine Identifizierung der einzelnen Personen durch die Berichtsnutzer auszuschließen. Zu diesen Maßnahmen gehört die Trennung der für Managementkontrolle und Business Intelligence eingesetzten Systeme von den übrigen operativen Systemen, ebenso wie die funktionale Trennung zwischen den Nutzern der Business-Intelligence-Werkzeuge und den für die Systemadministration zuständigen Personen.

3. An wen können Ihre Daten übermittelt werden?

Grundsätzlich werden Ihre Daten nur innerhalb der Unternehmen von HOTELS VIVA & RESORTS weitergegeben, und zwar in den in den vorstehenden Abschnitten beschriebenen Fällen, an Dritte auf Grundlage gesetzlicher Verpflichtungen, mit Ihrer vorherigen Einwilligung oder wenn dies zur Erfüllung des Vertrags erforderlich ist.

Die für Zahlungen im Bereich Personalwesen erforderlichen personenbezogenen Daten werden an das mit der Abwicklung der entsprechenden Überweisungen beauftragte Finanzinstitut übermittelt. Die Gehaltsüberweisung basiert auf dem berechnigten Interesse, die Zahlungsabwicklung effizient zu organisieren. Für die Abwägung dieses Interesses gegenüber Ihren Rechten und Freiheiten wurde festgestellt, dass die Verarbeitung nur einen begrenzten Einfluss auf die Privatsphäre der betroffenen Personen hat, den berechnigten Erwartungen der Betroffenen entspricht, da dies gängige Praxis ist und keine erheblichen Risiken oder Gefährdungen mit sich bringt.

Zur Erfüllung unserer gesetzlichen Verpflichtungen können Ihre personenbezogenen Daten an öffentliche Verwaltungen oder Behörden übermittelt werden, wie z. B. die Arbeitsaufsichtsbehörde, die Gesundheitsbehörden, die Sozialversicherung oder das Finanzamt, sowie gegebenenfalls auch an den Sicherheits- und Gesundheitsausschuss des Unternehmens, die Sicherheitsbeauftragten, den Betriebsrat oder die Personalvertretung – dies nicht abschließend.

4. Wie lange bewahren wir Ihre Daten auf?

Grundsätzlich werden Ihre Daten für die Dauer des bestehenden Beschäftigungsverhältnisses mit uns gespeichert – und in jedem Fall so lange, wie es die geltenden gesetzlichen Bestimmungen vorschreiben – sowie für den Zeitraum, der erforderlich ist, um etwaige aus der Verarbeitung resultierende Verpflichtungen oder Verantwortlichkeiten zu erfüllen. Ihre Daten werden gelöscht, sobald sie für die Zwecke, zu denen sie erhoben wurden, nicht mehr erforderlich oder relevant sind.

Die Daten aus Ihrer Personalakte werden mindestens für die gesetzlich vorgeschriebenen Fristen gemäß dem Arbeitsrecht aufbewahrt. Die Personalakten ausgeschiedener Mitarbeiter werden für einen Zeitraum von 6 Jahren ab Austrittsdatum gespeichert. Ab diesem Zeitpunkt wird alle drei Jahre eine Überprüfung durchgeführt, um festzustellen, welche Dokumente nicht mehr aufbewahrungspflichtig sind – diese werden anschließend gelöscht. Die Zeiterfassungsdaten werden für die Dauer der Verjährungsfrist arbeitsrechtlicher Verstöße gemäß dem anzuwendenden Tarifvertrag oder der geltenden arbeitsrechtlichen Gesetzgebung gespeichert, in jedem Fall jedoch für mindestens vier Jahre.

Die Daten, die für Veröffentlichungen auf der Unternehmenswebsite oder in sozialen Netzwerken von HOTELS VIVA & RESORTS verarbeitet werden, werden für die Dauer der erteilten Einwilligung aufbewahrt und in jedem Fall so lange, wie das UNTERNEHMEN sie für notwendig hält, um die Zwecke zu erfüllen, für die die Fotos und/oder Videos erstellt wurden.

Die Aufzeichnungen der Videoüberwachungskameras werden spätestens einen Monat nach ihrer Erfassung gelöscht, sofern keine gesetzlich vorgesehene längere Aufbewahrungsfrist greift – beispielsweise zum Nachweis von Vorfällen, die die Sicherheit oder Unversehrtheit von Personen, Eigentum oder Einrichtungen gefährden könnten.

Die von HOTELS VIVA & RESORTS zu Zwecken der Managementkontrolle und Geschäftsdatenanalyse verarbeiteten Daten werden zeitlich unbegrenzt aufbewahrt, da die Informationen nach Ablauf der Aufbewahrungsfrist der Personalakten anonymisiert werden.

Nachweise Ihrer Einwilligung zur Datenverarbeitung – z. B. unterzeichnete Formulare oder das vorliegende Regelwerk – werden während der gesamten Dauer der Verarbeitung sowie während der geltenden Verjährungsfristen aufbewahrt.

5. Welche Rechte haben Sie?

Sie haben das Recht, eine Bestätigung darüber zu erhalten, ob wir Ihre personenbezogenen Daten verarbeiten oder nicht, und – falls dies der Fall ist – auf Auskunft über diese Daten. Sie können außerdem verlangen, dass unrichtige Daten berichtigt oder unvollständige Daten ergänzt werden, sowie deren Löschung, wenn z. B. die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Unter bestimmten Umständen können Sie die Einschränkung der Verarbeitung Ihrer Daten verlangen. In diesem Fall werden die betroffenen Daten nur zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer Personen verarbeitet. Unter bestimmten Bedingungen und aus Gründen, die sich aus Ihrer besonderen Situation ergeben, können Sie auch der Verarbeitung Ihrer Daten widersprechen. In einem solchen Fall werden wir die Daten nicht weiterverarbeiten, es sei denn, es bestehen zwingende schutzwürdige Gründe, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Daten dienen der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Unter bestimmten Voraussetzungen haben Sie außerdem das Recht, die Übertragbarkeit Ihrer Daten zu verlangen, sodass diese an einen anderen Verantwortlichen übermittelt werden.

Sie können Ihre Einwilligung jederzeit widerrufen, ohne dass dies die Rechtmäßigkeit der Verarbeitung vor dem Widerruf beeinträchtigt. Sie haben zudem das Recht, nicht Gegenstand einer ausschließlich automatisierten Entscheidung zu sein, die Ihnen gegenüber rechtliche Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt, sofern dieses Recht gemäß Artikel 22 der Verordnung (EU) 2016/679 zur Anwendung kommt.

Darüber hinaus haben Sie das Recht, Beschwerde bei der spanischen Datenschutzbehörde (Agencia Española de Protección de Datos) oder einer anderen zuständigen Datenschutzaufsichtsbehörde einzulegen. Sie können die Liste und Kontaktdaten der europäischen Datenschutzbehörden auf der Website der Europäischen Kommission einsehen unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

Um Ihre Rechte auszuüben, senden Sie bitte einen Antrag per Post oder E-Mail an die in dem Abschnitt „Wer ist für die Verarbeitung Ihrer Daten verantwortlich?“ angegebenen Adressen.

Weitere Informationen über Ihre Rechte und deren Ausübung finden Sie auf der Website der Spanischen Datenschutzbehörde (<https://www.aepd.es>).

6. Welche Pflichten haben Sie?

Sie versichern, dass die Daten, die Sie uns jetzt oder in Zukunft zur Verfügung stellen, richtig und wahrheitsgemäß sind, und verpflichten sich, uns jede Änderung dieser Daten mitzuteilen.

Im Rahmen Ihrer Aufgaben können Sie Zugang zu personenbezogenen Daten erhalten, die von dem UNTERNEHMEN oder von Unternehmen der HOTELS VIVA & RESORTS verarbeitet werden, sowie zu anderen Informationen, die durch deren Tätigkeit entstehen. Diese Datenverarbeitungen unterliegen der geltenden Datenschutzgesetzgebung.

Die Daten stellen einen Vermögenswert des Unternehmens dar. Daher hat das Unternehmen Maßnahmen eingeführt, um deren Qualität, Sicherheit, Vertraulichkeit, Verfügbarkeit und die Einhaltung der geltenden gesetzlichen Vorschriften sicherzustellen.

Um dieses Ziel zu erreichen, wird Ihnen Zugang zu den notwendigen Ressourcen gewährt, um Ihre Arbeit ausführen zu können – unter Wahrung eines angemessenen Sicherheitsniveaus, das die Integrität, Vertraulichkeit und Verfügbarkeit der Informationen schützt. Diese Sicherheitsmaßnahmen gelten unabhängig vom verwendeten Medium, d. h. unabhängig davon, ob die Informationen auf Papier oder elektronisch gespeichert, manuell oder digital verarbeitet oder über Sprache, Telefon, Fax, E-Mail oder ein anderes automatisiertes Mittel übertragen werden.

Die internen Verfahren des Unternehmens, deren Definition und Umsetzung, ebenso wie Arbeitsmethoden, Schemata, Vorlagen und allgemein alles, was zum „Know-how“ des Unternehmens gehört, sind Eigentum des Unternehmens. In diesem Zusammenhang verpflichtet sich der Mitarbeiter, keine dieser Informationen – weder ganz noch teilweise – zu reproduzieren, zu kopieren, zu verbreiten, zu veröffentlichen oder an Dritte weiterzugeben, noch sie für eigene Zwecke

zu verwenden. Darüber hinaus verzichtet der Mitarbeiter ausdrücklich auf jegliche Rechte an sämtlicher Dokumentation, die im Rahmen seiner Tätigkeit für das Unternehmen erstellt wurde, zugunsten des Unternehmens.

Daher verpflichtet er sich, die Sicherheitsmaßnahmen in Bezug auf die Verarbeitungssysteme einzuhalten und durchzusetzen sowie die Nutzungsrichtlinien für die bereitgestellten IT-Systeme zu respektieren. Die Systeme dürfen ausschließlich entsprechend den von dem UNTERNEHMEN erteilten Anweisungen genutzt werden. Im Allgemeinen ist die private Nutzung der IT- und Kommunikationssysteme des Unternehmens untersagt, ebenso wie jede anderweitige Verwendung, die nicht unmittelbar mit der beruflichen Tätigkeit zusammenhängt. Mitarbeiter dürfen diese Mittel nicht zur Speicherung, Verarbeitung oder Übertragung von Inhalten verwenden, bei denen eine Erwartung an Privatsphäre besteht. Informationen, die sich auf betrieblichen Ressourcen befinden, gelten unter keinen Umständen als privat oder persönlich, sodass das UNTERNEHMEN Zugriff darauf nehmen darf, um notwendige oder zweckmäßige Kontrollmaßnahmen durchzuführen.

Sie verpflichten sich, absolute Vertraulichkeit über alle personenbezogenen Daten, auf die Sie zugreifen oder zu denen Sie Zugang hatten, zu wahren – auch nach Beendigung des Arbeitsverhältnisses. Diese Verschwiegenheitspflicht und Geheimhaltungspflicht erstreckt sich auf alle Unternehmen, die unter der Marke HOTELS VIVA & RESORTS tätig sind.

Im Mitarbeiterportal finden Sie die geltenden Datenschutzrichtlinien, -vorschriften und -verfahren für die von HOTELS VIVA & RESORTS verwalteten Unternehmen. Falls Sie keinen Zugang zu diesem Portal haben, können Sie beim Personalwesen des UNTERNEHMENS Zugangsdaten anfordern.

Die Datenschutzrichtlinien, -vorschriften und -verfahren sind verbindlich einzuhalten. Sie verpflichten sich, die für Ihre Tätigkeit geltenden Regeln und Verfahren, die in dieser INTERNEN RICHTLINIE oder in anderen vom UNTERNEHMEN jetzt oder zukünftig bereitgestellten Regelungen enthalten sind, zu lesen, zu beachten und einzuhalten.

2. Richtlinie für saubere Schreibtische und Bildschirme

Angesichts der von dem Unternehmen verwalteten Informationen und der damit verbundenen Vertraulichkeitsanforderungen gelten die folgenden Verhaltensregeln:

- **Richtlinie für saubere Schreibtische:**
 - Bei vorübergehendem Verlassen des Arbeitsplatzes dürfen keine vertraulichen Informationen offen auf dem Schreibtisch liegen bleiben.
 - Wenn sich eine Person dem Arbeitsplatz eines Mitarbeiters nähert, muss dieser besonders darauf achten, dass keine vertraulichen Unterlagen einsehbar sind.
 - Am Ende des Arbeitstages wird empfohlen, den Schreibtisch frei von zugänglicher Information zu hinterlassen (da Dritte darauf Zugriff erhalten könnten). Informationen, die personenbezogene Daten enthalten, sind in einem sicheren Behälter aufzubewahren (z. B. abschließbare Schublade oder Schrank).
- **Richtlinie für saubere Bildschirme:**
 - Wenn sich eine Person dem Arbeitsplatz nähert und direkten Blick auf den Bildschirm hat, ist darauf zu achten, dass keine vertraulichen Informationen sichtbar sind (z. B. durch Minimieren der entsprechenden Anwendung).
 - Am Ende des Arbeitstages oder bei kurzzeitiger Abwesenheit vom Arbeitsplatz ist die Benutzersitzung zu beenden oder der Bildschirm zu sperren.
- **Weitere Hinweise:** Es ist besonders darauf zu achten, dass keine vertraulichen Unterlagen unbeaufsichtigt in Kopierern, Faxgeräten, Druckern usw. verbleiben. Dokumente oder Ausdrücke mit sensiblen Informationen dürfen nicht in öffentlichen Bereichen liegen gelassen werden.

3. Nutzung von IT-Ressourcen.

3.1 Allgemeine Bedingungen.

Der Mitarbeiter ist verantwortlich für die Sicherheit und den Schutz der IT-Ressourcen, die ihm vom Unternehmen zur Verfügung gestellt werden. Diese Verantwortung umfasst auch den Schutz vor Bedrohungen wie unbefugtem Zugriff, Missbrauch, Fehlern oder Unterlassungen.

Ebenso müssen die im vorliegenden Dokument sowie im Sicherheitskonzept des Unternehmens beschriebenen Maßnahmen zur Verwendung und Verwaltung von Daten im Rahmen der beruflichen Tätigkeit beachtet werden.

Dazu erklärt der Mitarbeiter, dass er:

- die geltenden Richtlinien kennt und sich verpflichtet, diese einzuhalten,
- die ihm zugewiesenen Ressourcen schützt,
- die Vertraulichkeit und Integrität der Daten bewahrt, auf die er Zugriff hat, die er lokal verarbeitet oder in Papierform verwaltet.

Das Unternehmen stellt den Mitarbeitern IT-Ressourcen bereit, die je nach den betrieblichen Anforderungen der jeweiligen Position als angemessen erachtet werden.

Diese Ressourcen sind Eigentum des Unternehmens und dürfen ausschließlich zur Ausübung der dem Mitarbeiter durch die Geschäftsleitung zugewiesenen Aufgaben verwendet werden. Das Unternehmen behält sich das Recht vor, jegliche Ressourcen ohne vorherige Ankündigung zu ersetzen, zurückzunehmen, zu ändern oder unbrauchbar zu machen, je nach den aktuellen Anforderungen und Prioritäten.

Sie nehmen hiermit zur Kenntnis, dass folgende Handlungen ausdrücklich untersagt sind – sofern keine schriftliche Genehmigung durch die Geschäftsleitung oder deren bevollmächtigte Vertreter vorliegt:

- Nutzung der Computer und IT-Ausstattung des Unternehmens zu anderen als den durch die Geschäftsleitung bestimmten Zwecken.
- Verwendung von Browsern und E-Mail-Systemen für andere als die von der Geschäftsleitung festgelegten Zwecke.
- Installation oder Änderung des Betriebssystems oder jeglicher Software auf diesen Geräten.
- Anschluss persönlicher Geräte (USB-Sticks, andere digitale Speichermedien, Laptops, Tablets usw.) an Unternehmensressourcen, wie Server, Rechner oder das Firmennetzwerk.

Falls Ihnen eine Genehmigung zum Zugriff auf das Firmennetzwerk mit einem privaten Gerät erteilt wird, darf dieser Zugriff nur von außerhalb des internen Netzwerks erfolgen. Der Zugang ist nur zulässig nach Akzeptanz der spezifischen Nutzungsbedingungen des Dienstes. Die Annahme dieser Bedingungen umfasst auch die Möglichkeit, die Nutzung der Daten zu protokollieren, sowie die Option, im Falle von Geräteverlust oder Beendigung des Arbeitsverhältnisses die Unternehmensdaten aus der Ferne zu löschen.

3.2 Internetnutzung.

Bezüglich der Nutzung des Internets, das durch INVERSIONES PASCUAL S.L. oder eine der unter der Marke HOTELS VIVA geführten Gesellschaften bereitgestellt wird, muss sich der Mitarbeitende darüber im Klaren sein, dass er im Rahmen seiner beruflichen Tätigkeit das Unternehmen repräsentiert. Dementsprechend verpflichtet er sich, durch sein Verhalten die Ethik, Professionalität, Höflichkeit und Verantwortungsbereitschaft widerzuspiegeln, die von den Mitarbeitern erwartet werden.

Darüber hinaus verpflichtet sich der Mitarbeiter zu Folgendem:

- Die Internetnutzung ausschließlich auf jene Websites zu beschränken, die für die Ausübung der ihm übertragenen Aufgaben erforderlich sind.
- Keine Programme zu verwenden, um nicht autorisierte Downloads von digitalen Dateien (Software, Videos, Musik usw.) von öffentlich zugänglichen Servern im Internet durchzuführen.
- Keine Multimedia-Player zu nutzen, die Bandbreitenressourcen des Unternehmens beanspruchen (z. B. für Video, Radio oder Fernsehen).
- Keine Internetseiten aufzurufen, die eine Gefährdung der IT-Ressourcen des Unternehmens darstellen könnten, wie z. B. P2P-Websites.
- Keinen Zugriff auf Internetseiten mit pornografischen, beleidigenden oder menschenunwürdigen Inhalten zu nehmen – dies ist unter allen Umständen untersagt.
- Die Vorschriften des Urheberrechts und gewerblichen Rechtsschutzes sind strikt einzuhalten; daher müssen die Benutzer vor Nutzung von Informationen aus dem Internet sorgfältig prüfen, ob diese durch entsprechende Gesetze geschützt sind.
- Das Unternehmen behält sich das Recht vor, den Zugriff auf Webseiten mit verbotenen Inhalten oder solche, die die Leistung oder Sicherheit des Systems beeinträchtigen könnten, durch technische Maßnahmen (z. B. Proxys) zu blockieren. Daher wird der Internetverkehr überwacht, und die dabei gewonnenen Daten können im Falle eines Missbrauchs als Beweismittel für einen arbeitsrechtlichen Verstoß verwendet werden.

3.3 E-Mail-Nutzung.

E-Mails sind ein zentrales Arbeitsmittel im täglichen Betrieb des Unternehmens. Daher sind alle Praktiken zu vermeiden, die das ordnungsgemäße Funktionieren und die sichere Nutzung des Systems gefährden könnten.

Zudem machen die organisatorischen Abläufe des Unternehmens die Nutzung gemeinsamer E-Mail-Konten unter Mitarbeitenden **sowie den Zugriff auf unternehmensinterne E-Mail-Konten aus folgenden Gründen erforderlich:**

- Durch vorgesetzte Personen, um eine höhere Servicequalität im Unternehmen zu gewährleisten.
- Im Falle eines krankheitsbedingten Ausfalls des Kontoinhabers.
- Während des Urlaubszeitraums des Kontoinhabers.
- Während inaktiver Zeiträume von Saisonkräften mit unregelmäßiger Beschäftigung.

In keinem Fall dient dieser Zugriff dem Zweck, in die Privatsphäre des Mitarbeiter einzugreifen – vielmehr wird betont, dass E-Mails ausschließlich beruflich zu nutzen sind.

Im Zusammenhang mit der E-Mail-Nutzung ist Folgendes ausdrücklich verboten:

- Das Lesen, Löschen, Kopieren oder Verändern von E-Mails oder Dateien, die an andere Benutzer gerichtet sind.
- Das Anhängen oder Versenden von Massen-E-Mails oder großen Dateien, insbesondere in Kettenbriefen oder an viele Empfänger gleichzeitig.
- Das Versenden von Nachrichten zu kommerziellen oder werblichen Zwecken, ohne die entsprechende Datenschutzklausel einzufügen.

Das Öffnen von E-Mails, deren Betreff oder Absender auf Unsicherheit hinweist (z. B. Virusverdacht).

Die private Nutzung des E-Mail-Kontos ist unter keinen Umständen gestattet, ebenso wenig darf die E-Mail-Adresse für private Zwecke weitergegeben werden.

Die Mitarbeiter werden darüber informiert, dass bei Beendigung ihres Arbeitsverhältnisses, einem Abteilungswechsel oder einer Funktionsänderung im Unternehmen der Zugriff auf das E-Mail-Postfach – sowohl auf personenbezogene als auch auf allgemeine Konten – an den Nachfolger übergeht, um den Service weiterhin in bestmöglicher Qualität zu gewährleisten.

3.4 Gute E-Mail-Praxis

- Vermeiden Sie unnötige Antworten auf E-Mails: Es ist nicht erforderlich, sich für jede Nachricht mit „Danke“, „OK“ o. Ä. zu bedanken – es wird davon ausgegangen, dass Mitteilungen gewürdigt und verstanden werden. Antworten Sie nur, wenn eine Bestätigung verlangt, eine konkrete Frage gestellt oder ein Kommentar Ihrerseits notwendig ist.
- Verzichten Sie auf die Vorschaufunktion. Diese Funktion erhöht das Risiko, dass sich Viren verbreiten.
- Öffnen Sie keine verdächtigen E-Mails. Informieren Sie in einem solchen Fall umgehend die IT-Abteilung.
- Sensible Daten dürfen ohne vorherige Genehmigung durch die Hoteldirektion oder – im Fall der Zentrale – durch die Abteilungsleitung nicht versendet, weitergeleitet oder beantwortet werden.
- Verwenden Sie die Funktion „BCC“ (Blindkopie), wenn eine E-Mail an mehrere externe Empfänger (außerhalb des Unternehmens) gesendet wird.
- Leiten Sie E-Mails nur weiter, wenn sichergestellt ist, dass der Empfänger Zugriffsrecht auf den ursprünglichen Absender, den Inhalt sowie die gesamte E-Mail-Kette hat.
- Löschen Sie die Signatur, wenn Sie eine private Nachricht über das geschäftliche E-Mail-Konto senden.
- Geben Sie einen klaren und prägnanten Betreff an.
- Vermeiden Sie dabei die Angabe personenbezogener Daten im Betreff.
- Vermeiden Sie Wörter oder Formulierungen, die Spam-Filter auslösen könnten.
- Denken Sie daran: Wenn Sie eine Antwort auf eine E-Mail erwarten, erhalten Sie diese von den Empfängern im Feld „An“. Die Empfänger im Feld „CC“ (Kopie) dienen der Information oder Aufsicht – außer wenn zur Wahrung der Privatsphäre die Option „BCC“ (Blindkopie) genutzt wurde.

3.5 Nutzung interner und externer Kommunikationsprogramme:

- **Intranet, Microsoft Teams, Skype und jegliche andere interne Kommunikationssoftware, die das Unternehmen dem Mitarbeitenden zur Verfügung stellt.**
- **Online-Bewertungsportale, in denen Hotels Viva ein eigenes Profil besitzt, wie z. B. Booking, Expedia, Google+, Holidaycheck, Tripadvisor, Trivago.**
- **Soziale Netzwerke, in denen Hotels Viva über offizielle Unternehmensprofile verfügt, wie Facebook, Twitter, Instagram, Pinterest, LinkedIn, YouTube.**

Der Zugriff auf diese digitalen Tools ist ohne ausdrückliche Genehmigung der Unternehmensleitung strengstens untersagt.

Die Nutzung dieser Tools ist ausschließlich für berufliche Zwecke zulässig.

Die Unternehmensleitung überwacht die ordnungsgemäße Nutzung dieser Kommunikationsmittel – insbesondere in folgenden Fällen:

- Weitergabe von Informationen mit eingeschränktem Zugriff an nicht autorisierte Personen, unabhängig davon, ob sie Mitarbeiter von Hotels Viva sind.
- Veröffentlichung von Kommentaren, die die Würde von Personen verletzen oder dem guten Ruf von Hotels Viva schaden.
- Äußerung persönlicher Meinungen im Namen von Hotels Viva, einschließlich politischer oder religiöser Inhalte.
- Unhöfliche Antworten auf Kundenkommentare sowie jegliche Beiträge, die nicht mit der Kommunikationspolitik des Unternehmens vereinbar sind.
- Werbung oder Verkaufsförderung für Dritte, die nicht zu Hotels Viva gehören.

3.6 Audit und Wartung der IT-Ressourcen.

Hotels Viva behält sich das Recht vor – und der Nutzer (Mitarbeiter) erkennt dies als Voraussetzung für die Nutzung der IT-Ressourcen ausdrücklich an –, geeignete technische Mittel zu installieren, um sämtliche im E-Mail-System des Unternehmens erstellten, empfangenen, gesendeten oder gespeicherten Nachrichten sowie alle sonstigen Datenverarbeitungs- oder Speichermedien einschließlich der Internetnutzung zu überprüfen, zu auditieren, darauf zuzugreifen, sie zu löschen oder zu sperren. Ziel ist es, die Sicherheit des Systems zu wahren und die ordnungsgemäße Nutzung der Ressourcen sicherzustellen.

Zur Durchführung von Audits und Wartungsarbeiten an den IT-Systemen sowie der darauf installierten Software kann die Leitung der IT-Abteilung den Technikern der Abteilung oder extern beauftragten Personen den Zugriff auf Benutzerprofile gestatten – entweder durch direkte Anfrage beim Nutzer oder, im Falle seiner Abwesenheit, durch die Nutzung administrativer Superuser-Zugänge oder durch Änderung des Passworts.

4. Zugangssicherheit.

Das Sicherheitssystem ist direkt mit der Verwendung von Passwörtern verbunden. Die Zugangsprofile und zugewiesenen Passwörter sind daher vertraulich, persönlich und nicht übertragbar. Die Identifikation des Mitarbeitenden besteht aus einem Benutzercode (öffentlich) und einem Passwort, das ausschließlich dem jeweiligen Nutzer bekannt sein darf.

Die Zugangsdaten, die zur Identifikation und Freischaltung des Zugangs zu Unternehmensräumen, IT-Anwendungen, E-Mail, Alarmanlagen oder anderen Diensten dienen, sind nur für den persönlichen Gebrauch bestimmt und sind nicht übertragbar. Der Nutzer trägt die Verantwortung für jede missbräuchliche Nutzung, die mit seinen Zugangsdaten erfolgt.

Sie sind verpflichtet, die Vertraulichkeit Ihres Passworts zu wahren und dieses niemals in lesbarer Form – weder digital noch auf Papier oder anderen Speichermedien – aufzubewahren, auf die Dritte zugreifen könnten.

- Falls der Mitarbeiter den Verdacht hat, dass sein Passwort unbeabsichtigt oder auf betrügerische Weise durch unbefugte Personen aufgedeckt wurde, muss er dieses unverzüglich ändern und den Vorfall der IT-Abteilung melden.
- Ebenso ist bei Kenntnis eines Sicherheitsvorfalls eine sofortige Meldung erforderlich.
- Die Kenntnis eines Vorfalls ohne dessen Meldung wird als Verstoß gegen die Sicherheit gewertet und stellt dementsprechend eine arbeitsrechtliche Pflichtverletzung dar.
- Der Mitarbeiter ist verpflichtet, sein Passwort regelmäßig zu ändern, wobei sichere Zugangscodes gemäß den in den unternehmensinternen Sicherheitsrichtlinien festgelegten Vorgaben verwendet werden müssen.
- Während der Abwesenheit vom Arbeitsplatz sind die vorgesehenen Maßnahmen anzuwenden, um unbefugten Zugriff auf Daten zu verhindern – etwa durch Sperren oder Ausschalten des Computers.

Wird ein missbräuchlicher Gebrauch festgestellt, der die Sicherheit des Unternehmens gefährdet oder gegen die Sicherheitsrichtlinie im Einklang mit dem Organgesetz zum Schutz personenbezogener Daten (Ley Orgánica de Protección de Datos) verstößt, ist das Unternehmen berechtigt, geeignete Korrekturmaßnahmen oder disziplinarische Sanktionen zu ergreifen sowie den Inhalt der betroffenen Geräte zu protokollieren.

5. Datenschutzvorfälle.

Als Datenschutzvorfall gilt jede Unregelmäßigkeit, die die Sicherheit von Informationen beeinträchtigt oder beeinträchtigen könnte, insbesondere wenn sie die Verfügbarkeit, Integrität oder Vertraulichkeit dieser Daten verändert. Beispiele für Datenschutz- bzw. Informationssicherheitsvorfälle:

- Verstöße gegen Datenschutzrichtlinien oder -verfahren.
- Unbefugter Zugang zu gesperrten Bereichen.
- Verlust der Vertraulichkeit von Kunden- oder Mitarbeiterdaten.
- Unrechtmäßige Weitergabe von Daten an Dritte.
- Jeder Vorfall, der Unternehmenswerte betrifft (z. B. Verlust von USB-Sticks oder Papierunterlagen mit sensiblen Informationen).
- Zugriffsanfragen auf Kundendaten durch nicht betroffene Personen.
- Versand von Kundendaten an nicht autorisierte Unternehmen.

Jeder Mitarbeiter ist verpflichtet, jede Anomalie oder jeden Verdacht, der eine Bedrohung für die Sicherheit personenbezogener Daten darstellen könnte oder darstellt, so schnell wie möglich dem Sicherheitsverantwortlichen zu melden. Dazu ist eine E-Mail an gdpr@hotelsviva.com mit den Einzelheiten des festgestellten Vorfalls zu senden. Diese Mitteilung muss unverzüglich ab dem Zeitpunkt erfolgen, an dem der Vorfall entdeckt oder bekannt wurde. Kenntnis eines Vorfalls ohne entsprechende Meldung durch Mitarbeiter wird als schwerwiegender Verstoß gegen die Datensicherheit und damit als arbeitsrechtlicher Verstoß gewertet.

Dieses Dokument ist Anhang zu Ihrem Arbeitsvertrag und enthält verbindliche Verhaltensregeln. Ein Verstoß gegen die hierin enthaltenen Vorschriften kann von der Unternehmensleitung gemäß Artikel 39.5 des 5. Staatlichen Arbeitsabkommens für das Hotel- und Gaststättengewerbe (ALEH V) als arbeitsrechtlicher Verstoß gewertet werden. Dort wird festgelegt, dass schwere Verstöße Folgendes umfassen:

„Die Missachtung von Anordnungen und Anweisungen des Unternehmens oder der von ihm beauftragten Personen im Rahmen der Ausübung ihrer rechtmäßigen Leitungsbefugnisse, einschließlich solcher, die sich auf die Prävention von Arbeitsrisiken beziehen und gemäß der erteilten Schulung und Information erfolgen. Wird ein solcher Verstoß wiederholt, beeinträchtigt er offensichtlich die Arbeit oder verursacht er einen spürbaren Schaden für das Unternehmen oder andere Mitarbeitende, kann er als sehr schwerwiegender Verstoß eingestuft werden.“