Datenschutz-Richtlinie
Jungfrau Region Tourismus AG

Jungfrau Region Tourismus AG
Kammistrasse 13, CH-3800 Interlaken

Jungfrau Region

Inhaltsverzeichnis

Ziel der Datenschutzrichtlinie

Die Jungfrau Region Tourismus AG (JRT), führt die Geschäftstätigkeit der REGION[1] Sie verpflichtet sich und ihre Mandatsnehmerinnen im Rahmen zur Einhaltung von Datenschutzrechten und erlässt hierfür vorliegende Datenschutzrichtlinie. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der JRT als attraktiver Arbeitgeber.
Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für die Datenübermittlungen zwischen den beteiligten Unternehmen. Sie gewährleistet die Einhaltung des schweizerischen Bundesgesetzes über den Datenschutz (DSG, SR 235.1), der Europäischen Datenschutzrichtlinie (DSGVO) und das nach nationalen Gesetzen verlangte angemessene Datenschutzniveau für den grenzüberschreitenden Datenverkehr auch in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

1 Geltungsbereich und Änderung der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für alle Unternehmen der JRT und deren Mitarbeiter. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen, unabhängig ob es sich um natürliche oder juristische Personen handelt.
Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.
Die Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite https://jungfrauregion.swiss, abgerufen werden.

2 Prinzipien für die Verarbeitung personenbezogener Daten

2.1 Fairness und Rechtmässigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmässige und transparente Weise erhoben und verarbeitet werden.

2.2 Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur möglich, wenn die betroffenen Personen der Zweckänderung zustimmen.

2.3 Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- Die Identität der verantwortlichen Stelle und den Weg zur Kontaktaufnahme
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

2.4 Datenvermeidung und Datensparsamkeit

Vor einer Erhebung und Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den angestrebten Zweck zu erreichen. Es sind, wenn immer möglich anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nur dann auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, wenn staatliches Recht dies vorschreibt oder erlaubt.

2.5 Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall schutzwürdige Interessen namentlich im Zusammenhang mit strafbaren Handlungen oder haben die Daten nachgewiesenermassen eine historische Bedeutung, können sie weiter gespeichert bleiben. Die entsprechenden Datenbestände sind als "historisch" oder "von besonderem Interesse" zu kennzeichnen und im Archiv zu lagern.

---

[1] Grindelwald Tourismus, Wengen Tourismus, Lauterbrunnen Tourismus, Mürren Tourismus, Haslital Tourismus

2.6 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Massnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

2.7 Vertraulichkeit und Datensicherheit

Personenbezogene Daten müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Massnahmen gegen unberechtigten Zugriff, unrechtmässige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

3 Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

3.1 Kunden- und Partnerdaten

3.1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Verträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuelle vom Interessenten geäusserte Einschränkungen sind zu beachten. Für darüberhinausgehende Werbemassnahmen müssen die folgenden Voraussetzungen unter Ziff. 4.1.2 beachtet werden.

3.1.2 Datenverarbeitung aufgrund persönlicher Einwilligung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäss Ziff. 3.3. dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.
Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen der JRT (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.
Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren.
Sofern Daten ausschliesslich für Werbezwecke erhoben werden, kann dies nur unter zustimmender Kenntnisnahme des Betroffenen erfolgen. Für bereits vor Inkrafttreten dieser Richtlinie erhobene Daten kann im Rahmen einer Kommunikation mit den Betroffenen die notwendige Einwilligung eingeholt werden. Für neue Erhebungen muss der Betroffene über die Freiwilligkeit der Angabe informiert werden. Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden. Falls sie ausschliesslich zu Werbezwecken gespeichert sind, müssen sie gelöscht werden.

3.1.3 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

3.1.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der JRT erforderlich ist. Dies sind in der Regel rechtliche oder wirtschaftliche Interessen. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

3.1.5 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schützenswerte Personendaten nach Art. 3 des DSG oder besonderen Kategorien personenbezogener Daten nach Art. 9 der DSGVO darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

3.1.6 Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschliessliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.

3.1.7 Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.
Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).
Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

3.2 Mitarbeiterdaten

3.2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren erforderlich.
Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.
Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen bei einem Dritten erforderlich, sind die gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.
Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

3.2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

3.2.3 Kollektivregelungen für Datenverarbeitungen

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des schweizerischen Datenschutzrechts gestaltbar.

3.2.4 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäss dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden. Vor der Einwilligung muss der Betroffene gemäss Ziff. 3.3. über diese Datenschutzrichtlinie informiert werden.

3.2.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der JRT erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich oder wirtschaftlich begründet.
Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.
Kontrollmassnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismässigkeit der Kontrollmassnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmassnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Massnahme betroffenen Mitarbeiters am Ausschluss der Massnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Massnahme festgestellt und dokumentiert werden.

3.2.6 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schützenswerte Personendaten nach Art. 3 des DSG oder besonderen Kategorien personenbezogener Daten nach Art. 9 der DSGVO dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund des Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.

3.2.7 Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschliessliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss ausserdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

3.2.8 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.
Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmassnahmen an den Übergängen in das JRT-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstosses gegen Gesetze oder Richtlinien der JRT erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismässigkeitsprinzips erfolgen. Die nationalen Gesetze sind zu beachten.

4 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger ausserhalb der JRT unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 6. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

5 Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschliessen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmassnahmen auszuwählen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmässig zu wiederholen.
    a. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die schweizerischen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen.

6 Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind.
2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

7 Vertraulichkeit der Verarbeitung

Eine unbefugte Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.
Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetze müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

8 Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmässige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Massnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Massnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Die technisch-organisatorischen Massnahmen zum Schutz personenbezogener Daten sind Teil des Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

9 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmässig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem betrieblichen Datenschutzbeauftragten oder beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen sind der Geschäftsleitung der JRT mitzuteilen.

10 Datenschutzvorfälle

Jeder Mitarbeiter muss seinem jeweiligen Vorgesetzten oder dem betrieblichen Datenschutzbeauftragten unverzüglich Fälle von Verstössen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden. Der Linienverantwortliche ist verpflichtet, den betrieblichen Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten.
In Fällen von

- unrechtmässiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmässigem Zugriff durch Dritte auf personenbezogene Daten, oder
- bei Verlust personenbezogener Daten

11 Verantwortlichkeiten und Sanktionen

Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Massnahmen eine ordnungsgemässe Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der betriebliche Datenschutzbeauftragte umgehend zu informieren.
Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstösse gegen das Datenschutzrecht werden auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

12 Der Betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Er wird durch die Geschäftsleitung der JRT beauftragt.
Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den betrieblichen Datenschutzbeauftragten wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.
Der betriebliche Datenschutzbeauftragte kann wie folgt erreicht werden:

Jungfrau Region Tourismus AG
Datenschutz
Kammistrasse 13
CH-3800 Interlaken
E-Mail: datenschutz@jungfrauregion.swiss