INHALTSVERZEICHNIS

1.	ZIEL DER DATENSCHUTZLEITLINIE	2
2.	GELTUNGSBEREICH UND ÄNDERUNG DER DATENSCHUTZLEITLINIE	2
3.	PRINZIPIEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN	2
3.1.	RECHTMÄßIGKEIT	2
3.2.	TRANSPARENZ	2
3.3.	ZWECKBINDUNG	2
3.4.	DATENMINIMIERUNG	2
3.5.	RICHTIGKEIT DER DATEN	3
3.6.	VERTRAULICHKEIT UND INTEGRITÄT	3
3.7.	LÖSCHUNG	3
4.	ZULÄSSIGKEIT DER DATENVERARBEITUNG	3
4.1.	KUNDEN- UND PARTNERDATEN	3
4.1.1.	DATENVERARBEITUNG FÜR EINE VERTRAGLICHE BEZIEHUNG	3
4.1.2.	EINWILLIGUNG IN DIE DATENVERARBEITUNG	3
4.1.3.	DATENVERARBEITUNG AUFGRUND GESETZLICHER REGELUNGEN	3
4.1.4.	DATENVERARBEITUNG AUFGRUND BERECHTIGTEN INTERESSES	4
4.1.5.	VERARBEITUNG BESONDERS SCHUTZWÜRDIGER DATEN	4
4.1.6.	AUTOMATISIERTE EINZELENTSCHEIDUNGEN	4
4.1.7.	HOMEPAGE-NUTZERDATEN UND INTERNET	4
4.2.	MITARBEITERDATEN	4
4.2.1	DATENVERARBEITUNG FÜR DAS BESCHÄFTIGUNGSVERHÄLTNIS	4
4.2.2.	DATENVERARBEITUNG AUFGRUND GESETZLICHER ERLAUBNIS	4
4.2.3.	KOLLEKTIVREGELUNGEN FÜR DATENVERARBEITUNGEN	5
4.2.4.	EINWILLIGUNG IN DIE DATENVERARBEITUNG	5
4.2.5.	DATENVERARBEITUNG AUFGRUND BERECHTIGTEN INTERESSES	5
4.2.6.	VERARBEITUNG BESONDERS SCHUTZWÜRDIGER DATEN	5
4.2.7.	AUTOMATISIERTE EINZELENTSCHEIDUNGEN	5
4.2.8.	TELEKOMMUNIKATION UND INTERNET	5
5.	ÜBERMITTLUNG PERSONENBEZOGENER DATEN	6
6.	AUFTRAGSVERARBEITUNG	6
7.	RECHTE DES BETROFFENEN	7
8.	VERTRAULICHKEIT DER VERARBEITUNG	7
9.	SICHERHEIT DER VERARBEITUNG	7
10.	DATENSCHUTZKONTROLLE	7
11	DATENSCHUTZVORFÄLLE	8
12.	DER DATENSCHUTZBEAUFTRAGTE	8
13.	VERANTWORTLICHKEITEN UND SANKTIONEN	8
14.	INKRAFTSETZUNG	9

Verantwortlicher im Sinne der DSGVO, sonstiger in den Mitgliedstaaten der EU geltenden Datenschutzgesetze und anderer Bestimmungen mit datenschutz-rechtlichem Charakter ist:

Kay Fenneberg
Bahnhofstrasse 14
48143 Münster
Telefon: 0251 - 41780
E-Mail: kayfenneberg@kaiserhof-muenster.de

Datenschutzbeauftragte ist

Karin Schröer
Höltenweg 51
48155 Münster
Telefon: 0173 246 84 53
E-Mail: karin.schroeer@arbeitsicherheit-ms.de

1. ZIEL DER DATENSCHUTZLEITLINIE

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn sie Fragen zu unserer Datenschutzpraxis haben. Das Hotel Kaiserhof Münster verpflichtet sich zur Einhaltung der DSGVO und des BDSG. Mit der Einhaltung dieser Datenschutzleitlinie schafft das Hotel Kaiserhof ein Fundament für vertrauensvolle Geschäftsbeziehungen. Gleichzeitig ist diese Leitlinie eine Verpflichtung gegenüber unseren Mitarbeitern.
Die Datenschutzleitlinie gewährleistet das von der DSGVO und dem BDSG geforderte Niveau für den Datenschutz in unserem Unternehmen sowie bei unseren beauftragten Verarbeitern. Diese Datenschutzrichtlinie gilt für alle Unternehmensbereiche des Hotel Kaiserhof Münster und beruht auf akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen.

2. GELTUNGSBEREICH UND ÄNDERUNG DER DATENSCHUTZLEITLINIE

Diese Datenschutzleitlinie gilt für alle Mitarbeiter des Hotels Kaiserhof. Sie berücksichtigt sämtliche Verarbeitungen personenbezogener Daten. Eine Änderung dieser Datenschutzleitlinie findet ausschließlich in Abstimmung mit der Datenschutzbeauftragten statt. Die aktuellste Version der Datenschutzleitlinie kann auf der Internetseite abgerufen werden.

3. PRINZIPIEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

3.1. RECHTMÄßIGKEIT

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte gewahrt werden. Die Daten werden fair und rechtmäßig erhoben und verarbeitet.

3.2. TRANSPARENZ

Grundsätzlich werden Daten direkt beim Betroffenen erfasst. Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- die Identität der verantwortlichen Stelle (Hotel Kaiserhof)
- den Zweck der Datenverarbeitung (z.B. Vertragserstellung, Stammdaten, …)
- die hinterlegten Aufbewahrungsfristen
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

3.3. ZWECKBINDUNG

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3.4. DATENMINIMIERUNG

Das Verhältnis von Zweck und erhobenen Daten muss angemessen sein. Es werden nur ausdrücklich für den Zweck benötigte Daten erhoben. Es erfolgt keine Vorratsdatenspeicherung. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

3.5. RICHTIGKEIT DER DATEN

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

3.6. VERTRAULICHKEIT UND INTEGRITÄT

Einem unberechtigten Zugriff, einer unberechtigten Verarbeitung und Weitergabe, einem versehentlichen Verlust, einer versehentlichen Veränderung und/ oder Zerstörung ist mittels technischer und organisatorischer Maßnahmen vorzubeugen.

3.7. LÖSCHUNG

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen dieser Daten, müssen die Daten gespeichert bleiben, bis das schutzwürdige Interesse – rechtlich geklärt durch das Hotel Kaiserhof – geprüft werden konnte. Daten dürfen nur solange gespeichert werden wie es der Zweck erfordert. Aufbewahrungsfristen werden dennoch eingehalten.

4. ZULÄSSIGKEIT DER DATENVERARBEITUNG

Die Verarbeitung von Daten ist nur dann zulässig, wenn einer der folgenden Erlaubnistatbestände eintritt. Die Änderung des Zwecks der Datenerhebung erfordert ebenso einen der folgenden Erlaubnistatbestände.

4.1. KUNDEN- UND PARTNERDATEN

4.1.1. DATENVERARBEITUNG FÜR EINE VERTRAGLICHE BEZIEHUNG

Personenbezogene Daten des betroffenen Interessenten oder Kunden 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 z.B. Angeboten zulässig. Äußert ein Betroffener Verarbeitungsbeschränkungen, sind diese ausnahmslos zu berücksichtigen.

4.1.2. EINWILLIGUNG IN DIE DATENVERARBEITUNG

Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden, dann muss jedoch ihre Erteilung dokumentiert werden.

4.1.3. DATENVERARBEITUNG AUFGRUND GESETZLICHER REGELUNGEN

Ist die Verarbeitung der Daten durch das Gesetz vorgeschrieben oder gestattet ist sie zulässig. Die Verarbeitung wird dabei durch das entsprechende Gesetz geregelt.

4.1.4. DATENVERARBEITUNG AUFGRUND BERECHTIGTEN INTERESSES

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des Hotel Kaiserhof erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen) Tatbestände. 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.

4.1.5. VERARBEITUNG BESONDERS SCHUTZWÜRDIGER DATEN

Ist die Datenverarbeitung besonders schutzwürdiger Daten notwendig, darf dies nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene der Verarbeitung ausdrücklich zugestimmt 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. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

4.1.6. 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.

4.1.7. HOMEPAGE-NUTZERDATEN UND INTERNET

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzerklärungen 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 Datenschutzerklärungen informiert werden. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzerklärungen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).

4.2. MITARBEITERDATEN

4.2.1. DATENVERARBEITUNG FÜR DAS BESCHÄFTIGUNGSVERHÄLTNIS

Personenbezogene Daten die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages notwendig sind dürfen verarbeitet werden. Die Datenverarbeitung ist dabei grundsätzlich dem Zweck des Arbeitsvertrages untergeordnet und kann nur durch Erlaubnistatbestände 4.2.2ff erweitert werden. Bei vorvertraglichen Maßnahmen dürfen die Daten des Bewerbers verarbeitet werden. Kommt kein Arbeitsvertrag zustande dürfen die Daten bis zu sechs Monate gespeichert werden. Darüber hinaus ist eine Datenspeicherung und Datenverarbeitung nur mit Einwilligung des Bewerbers z.B. für spätere Auswahlverfahren oder andere Bewerbungsverfahren zulässig. 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 oder eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

4.2.2. DATENVERARBEITUNG AUFGRUND GESETZLICHER ERLAUBNIS

Ist die Verarbeitung der Daten durch das Gesetz vorgeschrieben oder gestattet, ist sie zulässig. Die Verarbeitung wird dabei durch das entsprechende Gesetz geregelt. Die schutzwürdigen Interessen des Mitarbeiters müssen gewahrt werden.

4.2.3. KOLLEKTIVREGELUNGEN FÜR DATENVERARBEITUNGEN

Liegen dem Beschäftigungsverhältnis Tarifregelungen oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen zugrunde, ist eine Verarbeitung über den Zweck der Vertragsabwicklung zulässig, sofern sie durch die jeweilige Grundlage geregelt wird. Die Kollektivregelungen müssen sich dabei auf den geplanten Zweck erstrecken.

4.2.4. EINWILLIGUNG IN DIE DATENVERARBEITUNG

Erteilt der Betroffene eine freiwillige, eindeutige Einwilligung zur Datenverarbeitung, ist die Datenverarbeitung zulässig. Der Betroffene muss darüber hinaus über die Einzelheiten der Verarbeitung im Vorwege informiert werden. Die Erklärung zur Einwilligung muss schriftlich erfolgen.

4.2.5. DATENVERARBEITUNG AUFGRUND BERECHTIGTEN INTERESSES

Hat das Hotel Kaiserhof ein berechtigtes Interesse an der Datenverarbeitung, ist diese zulässig. Berechtigte Interessen sind rechtliche oder wirtschaftliche z.B. Einhaltung von gesetzlichen Bestimmungen oder Vertragsverletzungen. Dabei ist zu berücksichtigen, dass die schutzwürdigen Interessen des Mitarbeiters ggf. schwerer wiegen als die berechtigen Interessen des Hotel Kaiserhof. Besteht eine gesetzliche Verpflichtung oder ein begründeter Anlass dürfen Mitarbeiterdaten zu Kontrollmaßnahmen verarbeitet werden. Auch bei einem begründeten Anlass wiegt das schutzwürdige Interesse des Mitarbeiters mehr als das berechtigte Interesse des Hotel Kaiserhof.

4.2.6. VERARBEITUNG BESONDERS SCHUTZWÜRDIGER DATEN

Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Ist die Datenverarbeitung besonders schutzwürdiger Daten notwendig, darf dies nur erfolgen, wenn dies aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben ist oder der Betroffene der Verarbeitung ausdrücklich zugestimmt hat. 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. Bei einer geplanten Verarbeitung schutzwürdiger Daten ist die/der Datenschutzbeauftragte im Vorwege zu informieren.

4.2.7. AUTOMATISIERTE EINZELENTSCHEIDUNGEN

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.

4.2.8. 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 geltenden 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 sind Schutzmaßnahmen an den Übergängen in das Hotel Kaiserhof-Netzwerk implementiert worden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und

Internets sowie der internen sozialen Netzwerke protokolliert. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Hotel Kaiserhof erfolgen. Diese Kontrollen dürfen nur unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Unternehmensregeln. Die Auswertungen dienen nicht der Leistungserfassung.

5. ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Eine Übermittlung von Daten erfolgt nur unter den bereits unter 4. genannten Erlaubnistatbeständen. Empfänger abseitig des Hotel Kaiserhof werden durch einen Vertrag zur Auftragsdatenverarbeitung verpflichtet, die Datenschutzverordnung einzuhalten. Im Falle einer Datenübermittlung an einen Empfänger außerhalb des Hotel Kaiserhof in einem Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Im Falle einer Datenübermittlung von Dritten an das Hotel Kaiserhof muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

6. AUFTRAGSVERARBEITUNG

Eine Auftragsverarbeitung 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 Auftragsverarbeitung 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. Die für den Datenschutz bereitgestellten Vertragsstandards müssen beachtet werden.
4. 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.

Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:

a) Vereinbarung der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
b) Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.
c) Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz Aufsichtsbehörden.

Unbefugte Verarbeitung von personenbezogenen Daten ist den Mitarbeitern des Hotel Kaiserhof untersagt. Dies gilt für eine Verarbeitung außerhalb seiner übertragenen Aufgaben ebenso wie die Nutzung für private oder wirtschaftliche Zwecke. Unsere Mitarbeiter werden zu Beginn eines Beschäftigungsverhältnisses über die Wahrung des Datengeheimnisses unterrichtet und verpflichten sich zur Einhaltung der DSGVO. Diese Einschränkung gilt auch über die Beendigung des Beschäftigungsverhältnisses hinaus.

7. 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. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
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.

Im Falle des Eintreffens eines Betroffenenrechts ist unverzüglich der Zuständige für Betroffenenrechte – siehe Zuständigkeiten – im vollen Umfang zu informieren.

8. VERTRAULICHKEIT DER VERARBEITUNG

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung 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. 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.

9. 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.

10. DATENSCHUTZKONTROLLE

Zur Sicherstellung des Datenschutzes nach DSGVO und BDSG und der Umsetzung der Datenschutzleitlinie werden regelmäßig, aber mindestens einmal im Jahr, Schulungen zum Thema Datenschutz durchgeführt. Die Durchführung obliegt dem Datenschutzbeauftragten und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen. Weitere Kontrollen sind möglich und werden stichprobenhaft durchgeführt. Die Ergebnisse der Kontrollen sind der/dem Datenschutzbeauftragen

vorzulegen. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt.

11. DATENSCHUTZVORFÄLLE

Jeder Mitarbeiter soll dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzleitlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den zuständigen 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

sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

12. DER DATENSCHUTZBEAUFTRAGTE

Der 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. Der Datenschutzbeauftragte wurde von der Direktion des Hotel Kaiserhof bestellt. Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Kann der zuständige Datenschutzbeauftragte einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzleitlinien nicht abstellen, muss zur Abhilfe der Datenschutzverletzung die Geschäftsführung berücksichtigt werden. Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen. Der Datenschutzbeauftragte kann wie folgt erreicht werden:

AS Münsterland
Datenschutzbeauftragter
Karin Schröer
Höltenweg 51 , 48155 Münster
Tel.: +49 251 703 9997
Karin.schroeer@arbeitssicherheit-ms.de

13. VERANTWORTLICHKEITEN UND SANKTIONEN

Die Geschäftsführung ist verantwortlich für die Datenverarbeitung. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzleitlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskraft, 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 Datenschutzbeauftragte umgehend zu informieren. Die Geschäftsführung ist verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. 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 in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

14. INKRAFTSETZUNG

Dieses Dokument wird einmal jährlich sowie bei Bedarf auf Vollständigkeit und Aktualität überprüft. Änderungen dieses Dokuments liegen in der Verantwortung des Zuständigen für Datenschutz-Vorgaben. Dieses Dokument ist allen Mitarbeitern zugänglich zu halten.

Münster, 26.11.2018