

zuständigen Aufsichtsbehörden können im Einzelfall oder auch im Hinblick auf das vorliegende Datenschutzkonzept von denen des Landesamtes für Datenschutzaufsicht Bayern abweichen.

## **DATENSCHUTZKONZEPT**

### **DES BUNDESVERBANDES DER SYSTEMGASTRONOMIE E.V. (BDS)**

#### **Präambel**

Die Systemgastronomie in Deutschland ist eine innovative und dynamische Branche, in der qualitativ sehr hochwertige Speisen und Getränke mithilfe optimierter und standardisierter Prozesse hergestellt und angeboten werden. Die hohen Ansprüche an die Qualität dieser Prozesse sowie der Produkte gelten in gleichem Maße für die Einhaltung der Bestimmungen des Datenschutzes. Aufgrund der besonderen Bedeutung und Schutzwürdigkeit personenbezogener Daten besteht hier eine besondere Verantwortung, zu der sich die systemgastronomischen Unternehmen in vollem Umfang bekennen.

Ein funktionierender und durchdachter Datenschutz ist für die gesamte Branche unerlässlich, vor allem auch im Hinblick auf das berechnete Vertrauen der Mitarbeiter, Kunden, Franchisenehmer und Geschäftspartner in den Schutz ihrer personenbezogenen Daten.

Mit diesem Datenschutzkonzept gibt der BdS als zuständiger Branchenverband Empfehlungen und Orientierungspunkte für die Systemgastronomie im Bereich des Datenschutzes. Es soll die Grundsätze für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten darstellen bzw. erläutern und als Ratgeber und Hilfsmittel bei Fragen rund um den Datenschutz dienen. Darüber hinaus werden in diesem Konzept auch Vorschläge zur Organisation und Handhabung des betrieblichen Datenschutzes und der Datensicherheit vorgestellt.

Grundlage dieses Datenschutzkonzepts ist das Bundesdatenschutzgesetz (BDSG) in seiner jeweils gültigen Fassung, alle sonstigen rechtlichen Bestimmungen hierzu und die zum Datenschutz ergangene Rechtsprechung.

Unser besonderer Dank gilt dem Landesamt für Datenschutzaufsicht Bayern als der für den Sitz des Bundesverbandes der Systemgastronomie e.V. zuständigen Datenschutzaufsichtsbehörde für die Unterstützung und die vielen hilfreichen Anregungen bei der Erstellung des vorliegenden Datenschutzkonzepts.

Hinweis: Für die datenschutzrechtliche Aufsicht über Unternehmen mit Sitz außerhalb von Bayern ist jeweils die Datenschutzaufsichtsbehörde des Bundeslandes zuständig, in dem das Unternehmen seinen Sitz hat. Datenschutzrechtliche Bewertungen der örtlich jeweils

### Übersicht:

- I. Grundsätze des Datenschutzes
- II. Verantwortlichkeit für den Datenschutz und Datenschutzbeauftragter
- III. Technische und organisatorische Schutzmaßnahmen
- IV. Erhebung, Verarbeitung und Nutzung bei allen Arten von personenbezogenen Daten
- V. Umgang mit Beschäftigtendaten
- VI. Schutz von sonstigen personenbezogenen Daten (Kunden, Franchisenehmer und Geschäftspartner)
- VII. Rechte der Betroffenen
- VIII. Auftrags-Datenverarbeitung und Zusammenarbeit mit externen Dienstleistern
- IX. Sicherheitskameras

## I. Grundsätze des Datenschutzes

### 1. Verbot mit Erlaubnisvorbehalt

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dies durch eine Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat (§ 4 Absatz 1 BDSG).

### 2. Grundsatz der Direkterhebung

Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben (§ 4 Absatz 2 BDSG). Dies soll sicherstellen, dass jeder Betroffene selbst entscheiden kann, welche Daten von ihm wem bekannt werden. Außerdem soll dies die Richtigkeit der Daten sicherstellen.

### 3. Grundsatz der Zweckbindung

Bei der Erhebung von personenbezogenen Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (§ 28 Absatz 1 Satz 2 BDSG). Die Daten dürfen dann grundsätzlich auch nur für diesen Zweck verwendet werden. Eine nachträgliche Verwendung der Daten für andere Zwecke ist nur ausnahmsweise zulässig, wenn die gesetzlichen Vorgaben erfüllt sind (§ 28 Absatz 2 und 3 BDSG) oder der Betroffene eingewilligt hat.

### 4. Grundsatz der Datenvermeidung und Datensparsamkeit

Grundsätzlich sollen so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Dieser Grundsatz entspricht auch der effektiven Ausrichtung der Systemgastronomie, die sich durch optimierte und gestraffte Prozesse auszeichnet. Bei allen Prozessen, insbesondere auch bei der Erstellung von Formblättern, z.B. bei Bewerbungsbögen, sollte daher immer hinterfragt werden, ob ein konkret abgefragter Aspekt tatsächlich für das Ziel notwendig ist. Soweit es möglich und nicht unverhältnismäßig ist,

sollen personenbezogene Daten anonymisiert oder pseudonymisiert werden. Dies wird bei rein statistischen Erhebungen regelmäßig der Fall sein, dagegen kommt eine Anonymisierung von Personalakten nicht in Betracht.

### 5. Verbot automatisierter Einzelfallentscheidungen

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Dieser Grundsatz ist besonders dann zu beachten, wenn es um die Beurteilung der beruflichen Leistungsfähigkeit eines Beschäftigten oder Bewerbers geht.

## II. Verantwortlichkeit für den Datenschutz und Datenschutzbeauftragter

### 1. Allgemeine Verantwortlichkeit

Verantwortlich für die Einhaltung und Gewährleistung des Datenschutzes sind die einzelnen Rechtsträger der systemgastronomischen Unternehmen, dies sind in den meisten Fällen die Betriebsgesellschaften der Restaurants. In der Regel tragen somit die Inhaber bzw. Geschäftsführer der einzelnen juristischen Personen (z.B. GmbHs) eine unmittelbare persönliche Verantwortung.

Innerhalb des Unternehmens haben alle Mitarbeiter, sobald sie personenbezogene Daten erheben, verarbeiten oder nutzen die Regelungen zum Datenschutz zu beachten und zwar unabhängig von ihrer Hierarchiestufe. Konkretisiert werden diese Regelungen durch die im jeweiligen Unternehmen allgemein gültigen Datenschutzstandards sowie Weisungen der Vorgesetzten.

Es wird empfohlen, im Unternehmen klare (möglichst schriftliche) Regelungen zu treffen und zu kommunizieren, wer für welche Daten und deren Schutz in welcher Form verantwortlich ist. Beispielsweise können verschiedene Berechtigungsstufen für den Einblick in Mitarbeiterdaten vergeben werden, die von der Dienstplangestaltung bis hin zur vollständigen Personalakte reichen können.

### 2. Verpflichtung auf das Datengeheimnis

Beschäftigte, die mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten befasst sind müssen nach § 5 BDSG explizit (schriftlich) auf das Datengeheimnis verpflichtet werden. Bei neu eintretenden Mitarbeitern kann dieser „Verpflichtungspflicht“ mittels eines Formulars oder Anhangs zum Arbeitsvertrag nachgekommen werden. Dieses Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort; auch dies ist in die Verpflichtung aufzunehmen.

### 3. Datenschutzbeauftragter

Der Datenschutzbeauftragte wirkt auf die Einhaltung des Datenschutzes im jeweiligen Unternehmen hin. Hierzu gehören u.a. die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme (bzgl. personenbezogener Daten) sowie die Durchführung von Trainings, um die entsprechenden Mitarbeiter mit den Anforderungen des Datenschutzes vertraut zu machen.

Ein Datenschutzbeauftragter muss (verpflichtend!) bestellt werden, sobald in der Regel zehn Personen oder mehr ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind. Der Datenschutzbeauftragte ist schriftlich zu bestellen. Er ist direkt der Geschäftsführung unterstellt. Es wird empfohlen, dass alle systemgastronomischen Unternehmen regelmäßig prüfen, ob die Bestellung eines Datenschutzbeauftragten notwendig ist. Insbesondere wenn Zugriffsrechte auf Daten neu vergeben werden, empfiehlt es sich, den o.g. Schwellenwert von zehn Personen erneut zu prüfen. Bei Nichtbestellung eines notwendigen Datenschutzbeauftragten droht ein Bußgeld bis zu 50.000 €.

Datenschutzbeauftragter kann eine betriebsangehörige oder auch eine externe Person sein. Der Arbeitgeber muss sicherstellen, dass der Datenschutzbeauftragte die erforderliche Fachkunde und Zuverlässigkeit besitzt. Der Datenschutzbeauftragte kann hierfür auf Kosten des Arbeitgebers entsprechende Schulungen in Anspruch nehmen. Sollte ein externer Datenschutzbeauftragter bestellt werden, sollte mit diesem vertraglich geklärt werden, ob und in welcher Höhe Schulungskosten zu zahlen sind. Außerdem muss der Datenschutzbeauftragte seine Funktion unabhängig ausführen können, d.h. er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes vom Arbeitgeber weisungsfrei. Die Bestellung zum Datenschutzbeauftragten kann nur aus wichtigem Grund oder einvernehmlich widerrufen werden. Der Datenschutzbeauftragte besitzt daneben einen arbeitsrechtlichen Sonderkündigungsschutz, der auch ein Jahr nach Beendigung der Funktion nachwirkt.

### III. Technische und organisatorische Schutzmaßnahmen

Jedes Unternehmen muss die technischen und organisatorischen Maßnahmen treffen, die für den Datenschutz erforderlich sind, soweit diese nicht unverhältnismäßig sind. Nach dem Gesetz (vgl. Anlage zu § 9 Satz 1 BDSG) sind insbesondere Maßnahmen zu treffen, um:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und

festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Jedes Unternehmen trifft dazu die erforderlichen Maßnahmen, insbesondere sollten:

- die Zugangsberechtigungen zu PCs und Datenverarbeitungsprogrammen sparsam verteilt und auf den notwendigen Personenkreis beschränkt werden,
- Passwörter sicher gewählt und periodisch geändert werden. Eine gemeinsame Nutzung von Passwörtern sollte untersagt werden,
- stets ein aktuelles Virenschutzprogramm und eine Firewall verwendet werden. Diese müssen regelmäßig upgedatet werden,
- Daten in regelmäßigen Abständen gesichert werden,
- Netzwerke gesichert werden. Dies gilt insbesondere für drahtlose Netzwerke. Der Server als Kommandozentrale des Netzwerks bedarf eines besonderen Schutzes,
- Papierakten und Datenträger fachmännisch entsorgt und datenschutzgerecht vernichtet werden.

Diese aufgelisteten Punkte fallen in Unternehmen üblicherweise in die Verantwortlichkeit unterschiedlicher Abteilungen, z.B. EDV-Abteilung, Personalabteilung und Haussicherheit. Mit jeder betroffenen Abteilung sollte die jeweilige Zuständigkeit ausdrücklich geklärt werden, damit es keine Kompetenzüberschneidungen oder Lücken gibt. Unternehmen können sich als technische Hilfestellung an den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik ([www.bsi.bund.de](http://www.bsi.bund.de)) orientieren.

#### IV. Erhebung, Verarbeitung und Nutzung bei allen Arten von personenbezogenen Daten

Umfasst sind alle personenbezogenen Daten, mit denen die Unternehmen in Berührung kommen, insbesondere die Daten von:

- Mitarbeitern
- Kunden
- Franchisenehmern
- Sonstigen Geschäftspartnern

Personenbezogene Daten sind nach der gesetzlichen Definition des § 3 Absatz 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Beispiele sind: Name, Adresse, Geburtstag und -ort, Telefonnummer, Kontodaten.

Einen zusätzlichen Schutz genießen die in § 3 Absatz 9 BDSG aufgelisteten besonderen Arten von personenbezogenen Daten: rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftzugehörigkeit, Gesundheit oder Sexualleben. Diese Daten dürfen nur in ganz besonderen Ausnahmefällen erhoben oder verwendet werden.

Die Begriffe Erhebung, Verarbeitung und Nutzung werden gem. § 3 BDSG wie folgt verstanden:

- Erheben ist das Beschaffen von personenbezogenen Daten.
- Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
- Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um eine Verarbeitung handelt.

#### V. Umgang mit Beschäftigtendaten

##### 1. Erhebung, Verarbeitung oder Nutzung von Mitarbeiterdaten

Mit den Daten von Beschäftigten und Bewerbern muss besonders verantwortungsvoll umgegangen werden. Dies ergibt sich schon aus der Wertschätzung, die die Systemgastronomie ihren Beschäftigten entgegen bringt. Für den Umgang mit den Daten der

Beschäftigten sind die maßgeblichen rechtlichen Vorgaben, insbesondere § 32 BDSG, zu beachten. Nach § 32 BDSG dürfen personenbezogene Daten eines Beschäftigten nur dann:

- erhoben
- verarbeitet
- oder genutzt

werden, wenn dies

- für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses
- für die Durchführung des Beschäftigungsverhältnisses
- oder dessen Beendigung

erforderlich ist.

##### 2. Personalaktenführung

Es muss auf Richtigkeit, Aktualität und Vollständigkeit der personenbezogenen Daten in Personalakten geachtet werden. Es darf keine geheimen Personalakten geben. Jeder Beschäftigte darf seine Personalakte einsehen und muss damit wissen, welche Daten der Arbeitgeber über ihn aufbewahrt. Um dies sicherzustellen, darf es nur eine Personalakte über jeden Beschäftigten geben. Er kann das Einfügen einer Gegendarstellung und bei falschen Angaben die Berichtigung der Personalakte verlangen.

##### 3. Bewerber

Bei Bewerbungsgesprächen dürfen (auch in Form von Fragebögen) nur Beschäftigtendaten erhoben werden, soweit dies erforderlich ist, um die Eignung des Beschäftigten für die vorgesehene Tätigkeit festzustellen oder um über die Begründung des Beschäftigungsverhältnisses zu entscheiden. Unzulässige Fragen verstoßen gegen den Datenschutz und der Bewerber darf darüber hinaus „ungestraft“ eine falsche Antwort geben bzw. die Antwort verweigern. Mitarbeiter, die Bewerbungsgespräche führen, sollten daher stets mit der aktuellen Rechtsprechung hierzu vertraut sein bzw. in Zweifelsfragen zuvor Rücksprache halten.

Bewerbungsunterlagen müssen nach einer angemessenen Frist gelöscht bzw. vernichtet werden. Als angemessene Frist sind in der Regel drei Monate anzusehen, es sei denn, ein Gerichtsverfahren ist anhängig oder ein Solches droht. Auf Wunsch des Bewerbers darf der Arbeitgeber dessen Daten länger speichern, wenn er diesen z.B. bei zukünftigen freien Stellen berücksichtigen möchte. Das Einverständnis hierzu kann der Bewerber jederzeit widerrufen.

#### 4. Aufklärung von Straftaten

Aufgrund der strengen gesetzlichen Vorgaben dürfen personenbezogene Daten nur in absoluten Ausnahmefällen zur Aufdeckung von Straftaten erhoben, verarbeitet oder genutzt werden. Es müssen hierfür tatsächliche Anhaltspunkte vorliegen, die der Arbeitgeber im Vorfeld dokumentieren muss. Die Nutzung der Daten muss außerdem erforderlich und verhältnismäßig sein. In Zweifelsfällen sollte unbedingt zuvor Rücksprache mit dem Datenschutzbeauftragten bzw. einem Rechtsanwalt gehalten werden.

#### **VI. Schutz von sonstigen personenbezogenen Daten (Kunden, Franchisenehmer und Geschäftspartner)**

Der Schutz von personenbezogenen Daten von Kunden, Franchisenehmern und sonstigen Geschäftspartnern ist der Branche ein wichtiges Anliegen. Deshalb ist mit allen personenbezogenen Daten von Kunden, Franchisenehmern und sonstigen Geschäftspartnern vertraulich umzugehen. Die oben genannten Grundsätze des Datenschutzrechts sind auch hier einzuhalten. Eine Erhebung, Verarbeitung und Nutzung ist nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke zulässig:

- wenn es für die Begründung, Durchführung oder Beendigung eines (rechtsgeschäftlichen oder rechtsgeschäftsähnlichen) Schuldverhältnisses mit dem Betroffenen erforderlich ist
- soweit es zur Wahrung der berechtigten Interessen der verantwortlichen Stelle erforderlich ist und das schutzwürdige Interesse des Betroffenen nicht überwiegt
- wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen durfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

#### **VII. Rechte der Betroffenen**

Die von der Datenverarbeitung betroffenen Personen haben im Rahmen der §§ 33 bis 35 BDSG Anspruch auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung ihrer Daten. Alle Anfragen sollen zügig bearbeitet werden. Beim Umgang mit personenbezogenen Daten muss auf ausreichende Transparenz geachtet werden, damit jeder Betroffene eine Vorstellung davon hat, wie mit seinen Daten umgegangen wird.

#### 1. Auskunftsrecht

Jeder Betroffene kann Auskunft verlangen über:

- die zu seiner Person gespeicherten Daten und deren Herkunft
- Empfänger und Kategorien von Empfängern, an die die Daten weitergegeben werden, und
- den Zweck der Speicherung

#### 2. Berichtigungsrecht

Jeder Betroffene kann die Berichtigung der zu seiner Person unrichtig oder unvollständig gespeicherten Daten verlangen.

#### 3. Maßregelungsverbot

Niemand darf wegen der Ausübung seiner Rechte benachteiligt werden.

#### 4. Löschung und Sperrung von Daten

Personenbezogene Daten sind insbesondere dann zu **löschen**:

- wenn ihre Speicherung unzulässig ist  
oder
- sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist

Personenbezogene Daten sind insbesondere dann zu **sperr**en:

- soweit die Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, einer Löschung jedoch gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten entgegenstehen
- eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist  
oder
- wenn Grund zur Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden

## 5. Widerspruchsrecht bei Werbemaßnahmen

Die Betroffenen haben das Recht, Werbemaßnahmen zu widersprechen. Bei einem Widerspruch gegen Werbung oder Maßnahmen der Markt- oder Meinungsforschung ist die Verarbeitung oder Nutzung von personenbezogenen Daten für diese Zwecke unzulässig. Über das Widerspruchsrecht sowie über die Stelle gegenüber der dieses ausgeübt werden muss, ist der Betroffene schon bei Vertragsabschluss und bei der Ansprache zu unterrichten.

## **VIII. Auftrags-Datenverarbeitung und Zusammenarbeit mit externen Dienstleistern**

Häufig wird die Datenverwaltung oder Bearbeitung im Wege der Auftragsdatenverarbeitung ausgelagert. Eine Auftrags-Datenverarbeitung kann z. B. vorliegen, wenn die Lohnabrechnung auf ein externes Lohnbüro ausgelagert wird. In diesen Fällen sind die Vorgaben des § 11 BDSG einzuhalten:

- Der Auftragnehmer ist unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.
- Der Auftrag ist schriftlich zu erteilen, wobei insbesondere die in § 11 Absatz 2 BDSG genannten Punkte schriftlich festzuhalten sind.
- Vor Beginn der Datenverarbeitung und sodann regelmäßig muss die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überprüft werden. Das Ergebnis muss dokumentiert werden.

Der Arbeitgeber bzw. Auftraggeber muss beachten, dass er selbst für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich bleibt. Ein Muster zur Auftragsdatenverarbeitung kann im Mitgliederbereich der BdS-Homepage heruntergeladen werden.

## **IX. Sicherheitskameras**

Unter bestimmten (engen) Voraussetzungen können Sicherheitskameras installiert und betrieben werden. Dabei ist eine strenge Interessenabwägung in jedem Einzelfall vorzunehmen, da das Grundrecht auf informationelle Selbstbestimmung aufgezeichneter Personen betroffen ist. Sicherheitskameras dürfen auf keinen Fall der dauerhaften und generellen Überwachung der Mitarbeiter dienen. Den Unternehmen wird empfohlen, den Einsatz von Sicherheitskameras durch eine unternehmensspezifische bzw.

betriebsspezifische Regelung zu präzisieren und in Zweifelsfällen Rechtsrat einzuholen. Es sollte außerdem der Personenkreis, der Zugriff auf die aufgezeichneten Daten haben kann, bestimmt werden.

Bei Sicherheitskameras ist zwischen der Beobachtung in öffentlich zugänglichen Räumen und nicht öffentlich zugänglichen Räumen zu unterscheiden.

### 1. Öffentlich zugängliche Räume

Die Beobachtung in öffentlich zugänglichen Räumen richtet sich nach § 6b BDSG. Demnach ist eine Beobachtung zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte vorliegen, dass schutzwürdige Interessen der Betroffenen überwiegen. Kameras dürfen nicht speziell auf die Arbeitsbereiche der Mitarbeiter gerichtet werden. Besonders in den Sitzbereichen sind bei der Interessenabwägung die Persönlichkeitsrechte der Gäste speziell zu beachten. Aufgrund der besonderen Schutzbedürftigkeit sollte grundsätzlich auf die Überwachung der Sitzbereiche verzichtet werden, soweit keine überwiegenden berechtigten Interessen ausnahmsweise für eine Beobachtung, etwa bei einer besonderen Gefährdung, sprechen. Der Umstand der Beobachtung und die verantwortliche Stelle (der Arbeitgeber) sind durch geeignete Maßnahmen erkennbar zu machen. Dies kann z.B. durch das Anbringen von Hinweisschildern erfolgen.

### 2. Nicht öffentlich zugängliche Räume

Eine Beobachtung in öffentlich nicht zugänglichen Räumen ist nur im Ausnahmefall möglich, wenn sie zur Wahrnehmung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Überwachung überwiegt. Zulässig ist sie z.B. in einem abgegrenzten Bereich, wenn alle anderen Sicherheitsmaßnahmen ausgeschöpft worden sind. Vor jeder Maßnahme sollte Rechtsrat eingeholt werden. Generell als zulässig erachtet wird in der Systemgastronomie eine Kamera, die auf den Tresor gerichtet ist. Diese muss derart ausgerichtet werden, dass möglichst keine Arbeitsbereiche der Mitarbeiter mit gefilmt werden.

\*\*\*\*\*