

RICHTLINIE ZUR SPEICHERUNG UND VERNICHTUNG PERSONENBEZOGENER DATEN

1. Zweck

Diese Richtlinie legt die Grundsätze fest, die vom Verantwortlichen TT HOTELS TURKEY OTEL HİZ. TUR. VE TİC. A.Ş. („TT HOTELS“) für die Speicherung und Vernichtung personenbezogener Daten gemäß dem Gesetz Nr. 6698 zum Schutz personenbezogener Daten („KVKK“) und den einschlägigen Rechtsvorschriften zu befolgen sind. Zweck ist es, die Rechte der betroffenen Personen zu schützen, unsere Verpflichtungen durch einen transparenten Ansatz zu erfüllen und Verarbeitungstätigkeiten zu regeln.

2. Geltungsbereich

Diese Richtlinie gilt für die personenbezogenen Daten der Gäste, Mitarbeiter, Bewerber, Mitarbeiter von Lieferanten und Besucher unseres Unternehmens. Sie umfasst alle elektronischen und nicht-elektronischen Umgebungen.

3. Definitionen

Empfängergruppe: Die Kategorie der natürlichen oder juristischen Person, an die der Datenverantwortliche personenbezogene Daten übermittelt.

Ausdrückliche Einwilligung: Einwilligung zu einem bestimmten Thema, basierend auf Informationen und im freien Willen ausgedrückt.

Anonymisierung: Es ist unmöglich, personenbezogene Daten in irgendeiner Weise einer identifizierten oder identifizierbaren natürlichen Person zuzuordnen, auch nicht durch den Abgleich mit anderen Daten.

Mitarbeiter: TT HOTELS Mitarbeiter

Mitarbeiterkandidat: Echte Person, die sich für die Arbeit in unserem Unternehmen bewirbt.

EBYS: Elektronisches Dokumentenmanagementsystem

Elektronische Umgebung: Umgebungen, in denen personenbezogene Daten mit elektronischen Geräten erstellt, gelesen, geändert und geschrieben werden können.

Nicht-elektronische Medien: Alle schriftlichen, gedruckten, visuellen usw. außer elektronischen Medien. andere Umgebungen.

Dienstleister: Natürliche oder juristische Person, die Dienstleistungen im Rahmen eines bestimmten Vertrags zwischen TT HOTELS und KVKK erbringt.

Relevante Person: Natürliche Person, deren personenbezogene Daten verarbeitet werden.

Relevanter Benutzer: Personen, die personenbezogene Daten innerhalb der Organisation des Datenverantwortlichen oder gemäß der vom Datenverantwortlichen erhaltenen Genehmigung und Anweisungen verarbeiten, mit Ausnahme der Person oder Einheit, die für die technische Speicherung, den Schutz und die Sicherung der Daten verantwortlich ist.

Vernichtung: Löschung, Vernichtung oder Anonymisierung personenbezogener Daten.

Gesetz: Gesetz zum Schutz personenbezogener Daten Nr. 6698.

Aufzeichnungsumgebung: Jede Umgebung, in der personenbezogene Daten mit ganz oder teilweise automatischen oder nichtautomatischen Mitteln verarbeitet werden, sofern sie Teil eines Datenaufzeichnungssystems sind.

Personenbezogene Daten: Alle Informationen über eine identifizierte oder identifizierbare natürliche Person.

Inventar der Verarbeitung personenbezogener Daten: Verarbeitungsaktivitäten personenbezogener Daten, die von Datenverantwortlichen in Abhängigkeit von ihren Geschäftsprozessen durchgeführt werden; Sie erstellen ein Inventar, indem sie die personenbezogenen Daten mit den Zwecken und dem rechtlichen Grund für die Verarbeitung personenbezogener Daten, der Datenkategorie, dem übermittelten Empfängerkreis und der Gruppe der betroffenen Personen in Verbindung bringen und die maximale Aufbewahrungsdauer angeben, die für die Zwecke, für die personenbezogene Daten verarbeitet werden, erforderlich sind, die für die Übermittlung ins Ausland vorgesehenen personenbezogenen Daten und die getroffenen Maßnahmen zur Datensicherheit.

Verarbeitung personenbezogener Daten: Alle Arten von Vorgängen, die mit Daten durchgeführt werden, wie z. B. das Erhalten, Aufzeichnen, Speichern, Bewahren, Ändern, Umordnen, Offenlegen, Übertragen, Übernehmen, Bereitstellen, Klassifizieren oder Verhindern der Nutzung personenbezogener Daten durch ganz oder teilweise automatische oder nichtautomatische Mittel, sofern sie Teil eines Datenaufzeichnungssystems sind.

Vorstand: Ausschuss für den Schutz personenbezogener Daten

KVKK: Behörde für den Schutz personenbezogener Daten

Gast: Echte Person, die in unserem Hotel übernachtet

Besondere personenbezogene Daten: Daten über Rasse, ethnische Herkunft, politische Meinung, philosophische Überzeugung, Religion, Sekte oder andere Überzeugungen, Aussehen und Kleidung, Vereins-, Stiftungs- oder Gewerkschaftsmitgliedschaft, Gesundheit, Sexualleben, strafrechtliche Verurteilung und Sicherheitsmaßnahmen sowie biometrische und genetische Daten.

Regelmäßige Vernichtung: Der Prozess der Löschung, Vernichtung oder Anonymisierung personenbezogener Daten, der in der Richtlinie zur Speicherung und Vernichtung personenbezogener Daten festgelegt ist und von Amts wegen in wiederkehrenden Abständen durchgeführt wird, sofern alle im Gesetz festgelegten Bedingungen für die Verarbeitung personenbezogener Daten entfallen.

Richtlinie: Richtlinie zur Speicherung und Vernichtung personenbezogener Daten

Mitarbeiter des Lieferanten: Beamter/Mitarbeiter des Unternehmens im Rahmen eines bestimmten Produkt- oder Dienstleistungsvertrags.

Datenverarbeiter: Natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet, basierend auf der vom Datenverantwortlichen erteilten Befugnis.

Datenaufzeichnungssystem: Ein Aufzeichnungssystem, in dem personenbezogene Daten nach bestimmten Kriterien strukturiert und verarbeitet werden.

Datenverantwortlicher: Die natürliche oder juristische Person, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt und für die Einrichtung und Verwaltung des Datenaufzeichnungssystems verantwortlich ist.

Registerinformationssystem für Datenverantwortliche: Das von der Präsidenschaft erstellte und verwaltete Informationssystem, das über das Internet zugänglich ist und das Datenverantwortliche bei der Beantragung des Registers und anderen damit zusammenhängenden Transaktionen im Zusammenhang mit dem Register verwenden.

VERBIS: Registerinformationssystem für Datenverantwortliche

Verordnung: Verordnung über die Löschung, Vernichtung oder Anonymisierung personenbezogener Daten, veröffentlicht im Amtsblatt vom 28. Oktober 2017.

4. Autorität und Verantwortlichkeiten

ROLLE	JOBDESCREIBUNG
Ansprechpartner für den Datenverantwortlichen	Im Rahmen von TT HOTELS, sowohl im Rahmen von EU GDPR als auch von KVKK, Harmonisierung des Betriebs der gesamten Gruppe mit der Gesetzgebung, Erstellung allgemeiner Richtlinien, Überprüfung der Prozesse, Planung und Vorbereitung von Schulungen, Prüfung und Abschluss der gemäß der Gesetzgebung einzureichenden Anträge und Beschwerden, Sicherstellung der Kommunikation und Koordination mit dem TUI-Zentrum und anderen Unternehmen von TUI, durch TUI Center. Die Erfüllung der übertragenen Aufgaben ist die Hauptaufgabe dieser Kommission. Es übernimmt auch die Pflichten der Registrierung bei VERBIS, der Benachrichtigung und Beantwortung der Korrespondenz mit der KVK-Behörde im Namen des Datenverantwortlichen.
KVKK-Kommission	Lokaler Experte für Datenschutz-Compliance-Themen • Berücksichtigung der Verpflichtungen von Unternehmen und relevanten Mitarbeitern gemäß den geltenden Datenschutzgesetzen, einschließlich der EU-Datenschutzgrundverordnung. • Überwachen, bewerten, analysieren und überprüfen Sie die Einhaltung der geltenden Datenschutzgesetze, einschließlich behördlicher und interner Datenschutzrichtlinien. • Unterstützung bei der Untersuchung und Bearbeitung von Datenschutzbeschwerden und Datensicherheitsvorfällen. • Schlagen Sie Datenschutz-Folgenabschätzungen vor und überwachen Sie deren Durchführung • Entwicklung, Durchführung und Überwachung von Mitarbeiterschulungen und -bewusstsein. • Die geltenden Aufzeichnungsanforderungen einhalten und einhalten. • Als Ansprechpartner fungieren und mit der örtlichen Aufsichtsbehörde zusammenarbeiten. • Zusammenarbeit mit dem Datenschutz- und Datenschutznetzwerk der TUI-Gruppe.

Datenschutzkommission	Identifizieren von Lücken in der IT und der physischen Infrastruktur und Informieren des Managements darüber, wie und zu welchen Kosten diese Lücken und Mängel geschlossen werden können, Ergreifen der erforderlichen Maßnahmen mit Zustimmung des Managements, Durchführen der erforderlichen Kontrollen und Inspektionen sowohl in der Einrichtung als auch in der Zentrale.
Datenschutzbeauftragter der Einrichtung	Als TT HOTELS sicherstellen, dass alle im Rahmen von KVKK/GDPR getroffenen Entscheidungen und Umsetzungsanweisungen in der zuständigen Einrichtung umgesetzt und überwacht werden, und den Prozess durch die Teilnahme an der Schulung des KVKK/GDPR-Trainers der Einrichtung unterstützen, Ermittlung der Probleme und Bedürfnisse in den Einrichtungen und Meldung dieser sowohl an die Kommission KVKK als auch an die Kommission für Datensicherheit sowie Erfüllung anderer von der Kommission KVKK/GDPR zugewiesener Aufgaben.
Hotel KVKK Schulungsbeauftragter	Pläne für die Durchführung von KVKK-Sensibilisierungsschulungen für das gesamte Personal zu erstellen, Schulungen anzubieten und/oder sicherzustellen, dass die Schulungen durchgeführt werden.

5. Rechtliche Gründe und Zwecke der Speicherung

Personenbezogene Daten werden aus den in den Artikeln 5 und 6 von KVKK genannten rechtlichen Gründen und zu folgenden Zwecken verarbeitet:

5.1. Rechtliche Gründe

- ALLGEMEINE HYGIENEGESETZ NR. 1593
- LANDVERKEHRSVERORDNUNG NR. 30295
- ARBEITSGESETZ NR. 4857
- BEVÖLKERUNGSDIENSTLEISTUNGSGESETZ NR. 5490
- SOZIALVERSICHERUNG UND ALLGEMEINE KRANKENVERSICHERUNG GESETZ NR. 5510,
- GESETZ NUMMER 5651 ÜBER DIE REGELUNG VON VERÖFFENTLICHUNGEN IM INTERNET UND DIE BEKÄMPFUNG VON VERBRECHEN, DIE DURCH DIESE VERÖFFENTLICHUNGEN BEGEBEN WERDEN,
- TÜRKISCHES PFLICHTENRECHT NR. 6098,
- ARBEITSGESUNDHEITS- UND SICHERHEITSGESETZ NR. 6361,
- GESETZ ZUM SCHUTZ PERSÖNLICHER DATEN NR. 6698,

5.2. Zwecke

Datenkategorie	Zweck der Verarbeitung personenbezogener Daten
1-ID	-Ausführung von Notfallmanagementprozessen -Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten -Durchführung von Prozessen zur Mitarbeiterzufriedenheit und -bindung - Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer -Durchführung von Bildungsaktivitäten -Durchführung von Aktivitäten im Einklang mit der Gesetzgebung -Durchführung von Commitment-Prozessen für das Unternehmen / Produkt / Dienstleistungen -Gewährleistung der physischen Raumsicherheit -Verfolgung und Ausführung von Rechtsangelegenheiten

	-Durchführung von Kommunikationsaktivitäten -Ausführung/Prüfung von Geschäftsaktivitäten -Durchführung von Aktivitäten im Bereich Gesundheit und Sicherheit am Arbeitsplatz -Ausführung von Logistikaktivitäten -Durchführung von Waren-/Dienstleistungseinkaufsprozessen -Ausführung von Waren-/Dienstleistungsverkaufsprozessen -Durchführung von Leistungsbewertungsprozessen -Durchführung von Vertragsprozessen -Bearbeitung von Anfragen/Beschwerden -Arbeits- und Aufenthaltsgenehmigungsverfahren für ausländisches Personal -Durchführung von Aktivitäten zur Talent-/Karriereentwicklung -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen -Erstellung und Verfolgung von Besucherdatensätzen
2-Kontakt	-Ausführung von Notfallmanagementprozessen -Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten - Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer -Durchführung von Aktivitäten im Einklang mit der Gesetzgebung -Durchführung von Commitment-Prozessen für das Unternehmen / Produkt / Dienstleistungen -Gewährleistung der physischen Raumsicherheit -Verfolgung und Ausführung von Rechtsangelegenheiten -Durchführung von Kommunikationsaktivitäten -Ausführung von Logistikaktivitäten -Durchführung von Waren-/Dienstleistungseinkaufsprozessen -Bearbeitung von Anfragen/Beschwerden -Arbeits- und Aufenthaltsgenehmigungsverfahren für ausländisches Personal -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen -Erstellung und Verfolgung von Besucherdatensätzen

4-Grundlagen	- Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer -Durchführung von Bildungsaktivitäten -Durchführung von Leistungsbewertungsprozessen -Durchführung von Aktivitäten zur Talent-/Karriereentwicklung -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
5-Rechtliche Schritte	-Verfolgung und Ausführung von Rechtsangelegenheiten
6-Kundentransaktion	-Ausführung von Notfallmanagementprozessen -Durchführung von Aktivitäten im Einklang mit der Gesetzgebung -Gewährleistung der physischen Raumsicherheit -Verfolgung und Ausführung von Rechtsangelegenheiten -Durchführung von Kommunikationsaktivitäten -Ausführung/Prüfung von Geschäftsaktivitäten -Durchführung von Aktivitäten im Bereich Gesundheit und Sicherheit am Arbeitsplatz -Durchführung von Waren-/Dienstleistungseinkaufsprozessen -Ausführung von Waren-/Dienstleistungsverkaufsprozessen -Bearbeitung von Anfragen/Beschwerden -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen -Durchführung von Managementaktivitäten -Erstellung und Verfolgung von Besucherdatensätzen
7-Physische Weltraumsicherheit	-Gewährleistung der physischen Raumsicherheit -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen -Erstellung und Verfolgung von Besucherdatensätzen
8-Transaktionssicherheit	-Ausführung von Informationssicherheitsprozessen -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
10-Financen	-Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten - Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer -Verfolgung und Ausführung von Rechtsangelegenheiten -Arbeits- und Aufenthaltsgenehmigungsverfahren für ausländisches Personal -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
11-Berufserfahrung	-Ausführung von Notfallmanagementprozessen -Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten - Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für

	Arbeitnehmer -Durchführung von Bildungsaktivitäten -Durchführung von Aktivitäten im Einklang mit der Gesetzgebung -Gewährleistung der physischen Raumsicherheit -Durchführung von Kommunikationsaktivitäten -Durchführung von Aktivitäten im Bereich Gesundheit und Sicherheit am Arbeitsplatz -Durchführung von Waren-/Dienstleistungseinkaufsprozessen -Durchführung von Leistungsbewertungsprozessen -Durchführung von Vertragsprozessen -Arbeits- und Aufenthaltsgenehmigungsverfahren für ausländisches Personal -Durchführung von Aktivitäten zur Talent-/Karriereentwicklung -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
13-Bild- und Audioaufzeichnungen	-Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten -Durchführung von Kommunikationsaktivitäten -Arbeits- und Aufenthaltsgenehmigungsverfahren für ausländisches Personal -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
16-Philosophische Überzeugungen, Religion, Sekten und Überzeugungen	- Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer
21-Gesundheitsinformationen	-Ausführung von Notfallmanagementprozessen -Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten - Erfüllung arbeitsvertraglicher und gesetzlicher Verpflichtungen für Arbeitnehmer -Durchführung von Aktivitäten im Bereich Gesundheit und Sicherheit am Arbeitsplatz -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen -Sonstiges (Schutz der öffentlichen Gesundheit)
23-Strafrechtliche Verurteilung und Sicherheitsmaßnahmen	-Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten -Gewährleistung der physischen Raumsicherheit -Durchführung von Leistungsbewertungsprozessen -Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
24-Biometrische Daten	-Gewährleistung der physischen Raumsicherheit
26-Sonstige Informationen – Körperinformationen	-Sonstiges (Bereitstellung von Kleidung für das Personal)

6. Maßnahmen zum Schutz personenbezogener Daten

Technische und administrative Maßnahmen

Um die Sicherheit personenbezogener Daten zu gewährleisten, werden folgende technische und administrative Maßnahmen ergriffen:

Die Schlüsselverwaltung ist implementiert.

Netzwerksicherheit und Anwendungssicherheit sind gewährleistet.

Für die Übermittlung personenbezogener Daten über das Netzwerk wird ein geschlossenes Systemnetzwerk genutzt.

Im Rahmen der Bereitstellung, Entwicklung und Wartung informationstechnischer Systeme werden

Sicherheitsmaßnahmen ergriffen.

Die Sicherheit der in der Cloud gespeicherten personenbezogenen Daten ist gewährleistet.

Zugriffsprotokolle werden regelmäßig geführt.

Unternehmensrichtlinien zu Zugriff, Informationssicherheit, Nutzung, Speicherung und Vernichtung wurden erstellt und umgesetzt.

Es werden Vertraulichkeitsverpflichtungen eingegangen.

Die Befugnisse von Mitarbeitern, die in diesem Bereich ihren Aufgabenbereich wechseln oder ihren Arbeitsplatz aufgeben, werden aufgehoben.

Es kommen aktuelle Antivirensysteme zum Einsatz.

Es kommen Firewalls zum Einsatz.

Es wurden Richtlinien und Verfahren zur Sicherheit personenbezogener Daten festgelegt.

Probleme mit der Sicherheit personenbezogener Daten werden schnell gemeldet.

Die Sicherheit personenbezogener Daten wird überwacht.

Beim Betreten und Verlassen physischer Umgebungen, die personenbezogene Daten enthalten, werden die erforderlichen Sicherheitsmaßnahmen ergriffen.

Die Sicherheit physischer Umgebungen, die personenbezogene Daten enthalten, vor externen Risiken (Feuer, Überschwemmung usw.) ist gewährleistet.

Die Sicherheit von Umgebungen, die personenbezogene Daten enthalten, ist gewährleistet.

Personenbezogene Daten werden so weit wie möglich reduziert.

Es werden personenbezogene Daten gesichert und die Sicherheit der gesicherten personenbezogenen Daten gewährleistet.

Es ist ein Benutzerkontenverwaltungs- und Berechtigungskontrollsystem implementiert, das auch überwacht wird.

Innerhalb der Einrichtung werden regelmäßige und/oder stichprobenartige Audits durchgeführt.

Protokollaufzeichnungen werden ohne Benutzereingriff gespeichert.

Aktuelle Risiken und Bedrohungen wurden identifiziert.

Es wurden Maßnahmen zur Cybersicherheit getroffen und deren Umsetzung wird laufend überwacht.

Es werden Penetrationstests angewendet.

Datenverarbeitungsdienstleister werden regelmäßig hinsichtlich der Datensicherheit überprüft.

Datenverarbeitungsdienstleister werden auf die Datensicherheit hingewiesen.

Es bestehen Disziplinarregelungen für Mitarbeiter, die Bestimmungen zum Datenschutz enthalten.

Für die Mitarbeiter werden in regelmäßigen Abständen Schulungen und Sensibilisierungsmaßnahmen zum Thema Datensicherheit durchgeführt.

Für Mitarbeiter wurde eine Autoritätsmatrix erstellt.

Protokolle und Verfahren zur Sicherheit besonderer personenbezogener Daten wurden festgelegt und umgesetzt.

Sollen sensible personenbezogene Daten per E-Mail versendet werden, muss diese verschlüsselt über einen Firmenmail-Account versendet werden.

Die unterzeichneten Verträge enthalten Datenschutzbestimmungen.

Die Verschlüsselung ist abgeschlossen.

7. Maßnahmen zur Speicherung und Vernichtung besonderer personenbezogener Daten

Besondere Kategorien personenbezogener Daten werden gemäß Artikel 6 von KVKK streng geschützt. Ihre Daten, die mit der Einwilligung der betroffenen Person verarbeitet und gespeichert werden, werden durch die erforderlichen Maßnahmen im gesetzlich vorgegebenen Rahmen geschützt. Mit der gleichen Sensibilität geht unser Unternehmen bei der Verarbeitung und Speicherung dieser sensiblen Daten vor.

Für besondere personenbezogene Daten müssen angemessene Vorkehrungen getroffen werden, sowohl aufgrund ihrer Natur als auch aufgrund der Tatsache, dass sie zu Viktimisierung oder Diskriminierung führen können. Diese Daten; Daten über Rasse, ethnische Herkunft, politisches Denken, philosophische Überzeugung, Religion, Sekte oder andere Überzeugungen, Aussehen und Kleidung, Vereins-, Stiftungs- oder Gewerkschaftsmitgliedschaft, Gesundheit, Sexualleben, strafrechtliche Verurteilung und Sicherheitsmaßnahmen sowie biometrische und genetische Daten.

TT HOTELS ergreift die erforderlichen Maßnahmen, um besondere personenbezogene Daten zu schützen, die gesetzlich als „besondere Daten“ eingestuft sind und in Übereinstimmung mit dem Gesetz verarbeitet werden. Bei den technischen und administrativen Maßnahmen zum Schutz personenbezogener Daten wird die Sensibilität für besondere personenbezogene Daten deutlich.

8. Bestandsaufnahme und Aufbewahrungsfristen für personenbezogene Daten

8.1. Aufnahmeumgebungen

ELEKTRONISCHE MEDIEN	NICHTELEKTRONISCHE MEDIEN
Server (Domäne, Backup, E-Mail, Datenbank, Web, Dateifreigabe usw.) Software (Office-Software, PMS usw.) Informationssicherheitsgeräte (Firewall, Protokolldatei,	Papier Schriftliche, gedruckte und visuelle Medien

Antivirenprogramm usw.) Arbeitsplätze (Desktop, Laptop usw.) Cloud-Umgebungen Mobile Geräte (Telefon, Tablet usw.) Optische Datenträger (CD, DVD usw.) Wechselspeicher (USB, Speicherkarte usw.)	
---	--

Die Aufbewahrungsfristen der Daten sind in der Tabelle „Aufbewahrungsfristen“ des Dokuments „Richtlinie zur Speicherung und Vernichtung personenbezogener Daten“ festgelegt. Unter Bezugnahme auf die angegebene Tabelle sind die allgemeinen Aufbewahrungsfristen wie folgt.

8.2. Aufbewahrungsfristen

Datenkategorie	Datenaufbewahrungsfrist
1-ID	10 Jahre
2-Kontakt	10 Jahre
4-Grundlagen	10 Jahre
5-Rechtliche Schritte	10 Jahre
6-Kundentransaktion	10 Jahre
7-Physische Weltraumsicherheit	1 Monat
8-Transaktionssicherheit	Unbestimmt
10-Finanzen	10 Jahre
11-Berufserfahrung	10 Jahre
13-Bild- und Audioaufzeichnungen	10 Jahre
16-Philosophische Überzeugungen, Religion, Sekte und andere Überzeugungen	10 Jahre
21-Gesundheitsinformationen	15 Jahre
23-Strafrechtliche Verurteilung und Sicherheitsmaßnahmen	10 Jahre
24-Biometrische Daten	Während der Arbeit
26-Sonstige Informationen – Körperinformationen	1 Jahr

* Eine längere Dauer muss gesetzlich geregelt sein, andernfalls kann es zu Verjährungsfristen, Verjährungsfristen, Aufbewahrungsfristen etc. kommen. Sofern für die Speicherung eine längere Frist vorgesehen ist, gelten als maximale Speicherdauer die in der Gesetzgebung vorgesehenen Fristen.

9. Gründe, die eine Vernichtung erfordern

Persönliche Daten;

- Änderung oder Aufhebung der einschlägigen Rechtsvorschriften, die die Grundlage für die Verarbeitung bilden,
- Der Zweck, der eine Verarbeitung oder Speicherung erfordert, entfällt,
- In Fällen, in denen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Einwilligung verarbeitet werden, widerruft die betroffene Person ihre ausdrückliche Einwilligung.
- TT HOTELS akzeptiert den Antrag der betreffenden Person auf Löschung und Vernichtung ihrer personenbezogenen Daten im Rahmen ihrer Rechte gemäß Artikel 11 des Gesetzes.

- In Fällen, in denen TT HOTELS den Antrag der betreffenden Person auf Löschung, Vernichtung oder Anonymisierung ihrer personenbezogenen Daten ablehnt, die gegebene Antwort für unzureichend hält oder nicht innerhalb der im Gesetz vorgesehenen Frist antwortet; Beschwerde beim Personal Data Protection Board und Genehmigung dieses Antrags durch das Board,
- Die maximale Aufbewahrungsfrist für personenbezogene Daten ist abgelaufen und es liegen keine Bedingungen vor, die die Speicherung personenbezogener Daten über einen längeren Zeitraum rechtfertigen.

In solchen Fällen werden sie von unserer Organisation auf Wunsch der betreffenden Person gelöscht, vernichtet oder von Amts wegen gelöscht, vernichtet oder anonymisiert.

Darüber hinaus sind im Folgenden einige Gesetze aufgeführt, die die Verarbeitung und Speicherung von Daten vorschreiben:

- Türkisches Obligationenrecht Nr. 6098,
- Gesetz zum Schutz personenbezogener Daten Nr. 6698,
- Arbeitsgesetz Nr. 4857
- Sozialversicherungs- und allgemeines Krankenversicherungsgesetz Nr. 5510,
- Arbeitsschutzgesetz Nr. 6331
- Türkisches Handelsgesetzbuch Nr. 6102
- Steuerverfahrensgesetz Nr. 213
- Allgemeines Hygienegesetz Nr. 1593
- Straßenverkehrsverordnung Nr. 30295

und alle weiteren zwingenden gesetzlichen Bestimmungen.

10. Techniken zur Vernichtung personenbezogener Daten

Nach Ablauf der in den einschlägigen Rechtsvorschriften vorgesehenen Frist oder der für den Verarbeitungszweck erforderlichen Aufbewahrungsfrist werden personenbezogene Daten von unserer Organisation von Amts wegen oder auf Antrag der betreffenden Person unter Verwendung der unten aufgeführten Techniken gemäß den Bestimmungen der einschlägigen Rechtsvorschriften vernichtet.

10.1. Löschmethoden

Persönliche Daten auf Servern

Für personenbezogene Daten auf den Servern, deren Aufbewahrungsfrist abgelaufen ist, entzieht der Systemadministrator den betreffenden Benutzern die Zugriffsberechtigung und löscht sie.

Personenbezogene Daten in elektronischen Medien

Unter den personenbezogenen Daten im elektronischen Umfeld sind diejenigen, deren Aufbewahrungsfrist abgelaufen ist, für andere Mitarbeiter (relevante Benutzer) außer dem Datenbankadministrator unzugänglich und unbrauchbar gemacht.

Persönliche Daten in physischer Umgebung

Personenbezogene Daten, die auf physischen Datenträgern aufbewahrt werden und deren Aufbewahrungsfrist abgelaufen ist, werden für andere Mitarbeiter, mit Ausnahme des für das Dokumentenarchiv zuständigen Abteilungsleiters, unzugänglich und in irgendeiner Weise unbrauchbar gemacht. Darüber hinaus wird die Oberfläche auch durch Zeichnen/Malen/Radieren geschwärzt, so dass sie nicht mehr lesbar ist.

In tragbaren Medien enthaltene personenbezogene Daten

Von den auf Flash-basierten Speichermedien gespeicherten personenbezogenen Daten werden diejenigen, die abgelaufen sind, in sicheren Umgebungen mit Verschlüsselungsschlüsseln gespeichert, indem sie vom Systemadministrator verschlüsselt werden und die Zugriffsberechtigung nur dem Systemadministrator erteilt wird.

10.2. Zerstörungsmethoden

Persönliche Daten in physischer Umgebung

Auf Papier gespeicherte und abgelaufene personenbezogene Daten werden in Papiervernichtungsmaschinen unwiderruflich vernichtet.

Persönliche Daten auf optischen/magnetischen Datenträgern

Personenbezogene Daten auf optischen und magnetischen Datenträgern, deren Aufbewahrungsfrist abgelaufen ist, werden physisch zerstört, beispielsweise durch Schmelzen, Verbrennen oder Pulverisieren. Darüber hinaus werden die

Daten auf den magnetischen Medien unlesbar gemacht, indem sie durch ein spezielles Gerät geleitet und einem hohen Magnetfeld ausgesetzt werden.

10.3. Anonymisierungsverfahren

Unter Anonymisierung versteht man den Vorgang, bei dem personenbezogene Daten nicht mehr einer bestimmten Person zugeordnet werden können. Folgende Methoden kommen zum Einsatz:

Maskierung: Verstecken direkt identifizierender Informationen.

Verallgemeinerung: Organisieren von Daten zur Darstellung einer bestimmten Gruppe.

Datenaustausch: Verstecken von Identitätsinformationen durch zufälliges Ändern von Daten.

Diese Methoden werden insbesondere in statistischen Analyse- und Reportingprozessen eingesetzt.

11. Periodische Zerstörung

Die Daten werden regelmäßig vernichtet, wenn die Zwecke der Verarbeitung nicht mehr bestehen und ihre Aufbewahrungsfrist abläuft:

Zerstörungszeitraum	Frequenz
Elektronische Daten	1 Mal in 6 Monaten
Physische Daten	1 Mal in 6 Monaten

12. Veröffentlichung und Speicherung der Richtlinie

Die Richtlinie wird elektronisch veröffentlicht und auf der Website der Öffentlichkeit zugänglich gemacht.

13. Aktualisierung und Einhaltung der Richtlinien

Unser Unternehmen behält sich das Recht vor, diese jederzeit im Rahmen von Änderungen der Gesetzgebung und des Zwecks der Speicherung/Vernichtung personenbezogener Daten innerhalb des Unternehmens zu aktualisieren.

14. Durchsetzung der Richtlinie

Diese Richtlinie gilt mit ihrer Veröffentlichung auf der Website des Unternehmens als in Kraft getreten.