GAIA HOTEL
COME AS A GUEST, LEAVE AS A FRIEND

Neues Datenschutzgesetz

nach nCH-DSG und DSGVO

nCH-DSG = neues Schweizer Datenschutzgesetz
DSGVO = Datenschutzgesetzverordnung der Europäischen Union

Sie als Mitarbeitende sind mitverantwortlich für die Einhaltung des neuen Datenschutzgesetzes!

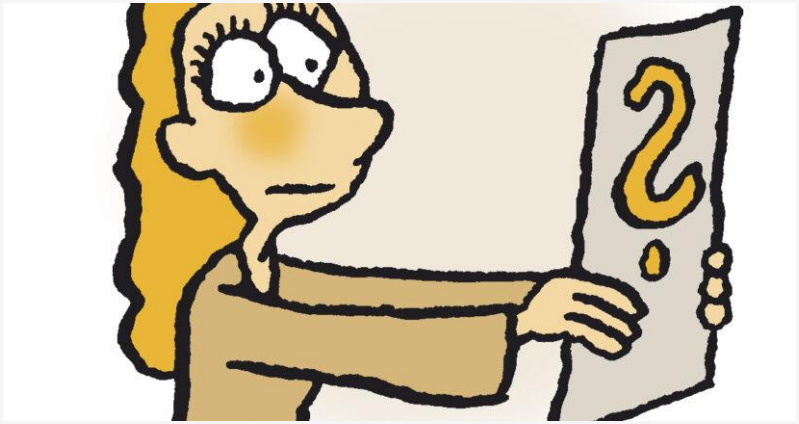
RESPONSIBLE HOTELS OF SWITZERLAND

Recommended by Switzerland Tourism. Typically Swiss Hotel

ibex platinum sustainability label

Swisstainable leading

Datenschutz – was wie wo?



Warum muss ich über Datenschutz im GAIA Hotel Bescheid wissen?

Was verstehe ich unter Datenschutz?

An welche Daten muss ich denken?

- Front Office
- Hauswirtschaft/Frühstück
- Sales
- Management/Mitarbeiterwesen

Welche Risiken/Verletzungen können im Unternehmen auftreten?

Ziel des DSG

Was?		Wie/Warum?
Schutz der Persönlichkeit und Grundrechte von **natürlichen Personen** (Schutz von juristischen Personen entfällt)	→	Verbesserung der Transparenz der Daten-bearbeitung und Stärkung der persönlichen Selbstbestimmung über Personendaten.
Angleichung an die EU-Gesetzgebung	→	Formlose grenzüberschreitende Datenbekanntgabe soll weiterhin möglich sein
Datenschutz wurde an die veränderten **technologischen** und **gesellschaftlichen** Verhältnisse angepasst		

Folgen …

Erhöhung der gesetzlichen Bestimmungen (Compliance)-**Anforderungen**

- Ausdehnung der Informations- und Auskunfts-pflicht
- Dokumentationsanforderungen
- Datensicherheitsvorschriften
- Meldepflicht von Datensicherheitsverletzungen

Verschärfung der Strafbestimmungen

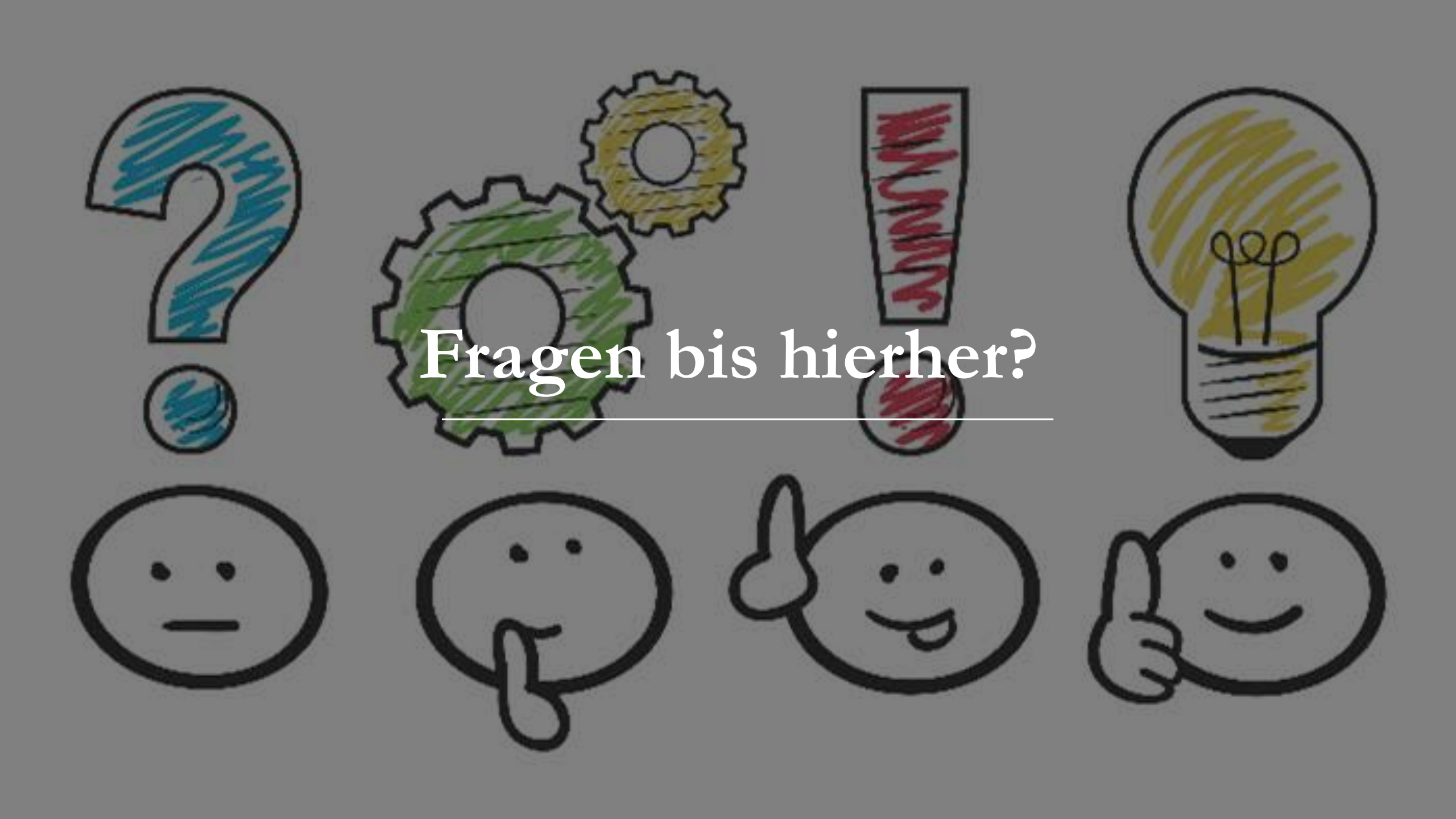
- Höhere Bussen bis max. 250‘000 CHF
- **Persönliche Haftung** (nicht Unternehmen!)
- Verwaltungsverfahren infolge Stärkung der Kompetenzen der Aufsichtsbehörde mit Kostenfolgen

Wichtige Begriffe

Begriffe:

- Personendaten
- Verantwortliche/r
- Betroffene Personen
- Auftragsbearbeiter
- Bearbeitung
- Besonders schützenswerte Personendaten
- DSGVO = Datenschutz Grundverordnung der EU
- TOM = Technische und organisatorische Mass-nahmen
- DSFA = Datenschutz-Folgeabschätzung
- EDÖB = Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter in der CH

Compliance =
Einhalten gesetzliche Bestimmungen


Fragen bis hierher?

Pflichten des Verantwortlichen

Anwendbarkeit DSG (Datenschutzgesetz)

- Das Bearbeiten von Personendaten unterliegt dem DSG – ob auf Papier oder per Software.
- Nur geschäftlich – nicht für den privaten Gebrauch wie z.B. privates Adressbüchlein

Wann braucht es einen Rechtfertigungsgrund?

nur notwendig, wenn entweder:

- die Bearbeitungsgrundsätze nicht eingehalten werden
- die betroffenen Personen der Bearbeitung widersprechen
- besonders schützenswerte Personendaten mitgeteilt werden sollen

Pflichten des Verantwortlichen

Empfehlung: Datencheck

Datencheck		Beispiele
1) **Wo** werden…	→	Mews, Outlook, SharePoint
2) **welche Personendaten**…	→	Mailadresse, Namen, Vorname
3) **für welchen Zweck** bearbeitet?	→	Newsletterversand

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
1	Einhaltung der Bearbeitungsgrundsätze bzw. Vorliegen eines Rechtfertigungsgrundes
2	Informationspflicht: Das Unternehmen informiert die betroffenen Personen vorgängig, was mit den Personendaten wozu gemacht wird.
3	Einhaltung der Betroffenenrechte
4	Meldepflicht bei einem Datensicherheitsvorfall beim EDÖB
5	Datenschutz-Folgeabschätzung (DSFA) bei hohem Risiko für die betroffenen Personen
6	Führen eines Bearbeitungsverzeichnisses – jeder Vorfall muss dokumentiert werden

Pflichten des Verantwortlichen

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
1	Einhaltung der Bearbeitungsgrundsätze bzw. Vorliegen eines Rechtfertigungsgrundes

Ein Unternehmen hat die folgenden **Bearbeitungsgrundsätze** einzuhalten	
Rechtmässigkeit	Zweckbindung
Treue, Glauben & Transparenz	Verhältnismässigkeit
Datenrichtigkeit & Datensicherheit	Privacy by Design & Privacy by Default

Hält ein Unternehmen einen Bearbeitungsgrundsatz nicht ein, ist dafür einer der folgenden **Rechtfertigungsgründe** notwendig:

Einwilligung
oder
Grundlage im Schweizer Recht

Pflichten des Verantwortlichen

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
2	Informationspflichten

Bei jeder Beschaffung von Personendaten muss ein Unternehmen die betroffenen Personen angemessen informieren, dabei ist zwischen dem Mindestinhalt und erweiterter Informationspflicht im Einzelfall zu unterscheiden.

-> Ausnahmen

-> Umsetzung

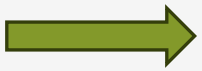
Pflichten des Verantwortlichen

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
3	Einhaltung der Betroffenenrechte

Bestehendes Recht

- Recht auf Berichtigung
- Recht auf Löschung/Vergessen werden
- Berichtigungsvermerk
- Anzeigerecht



Neue oder erweiterte Recht

- Auskunftsrecht
  - Was, wie, Ausnahmen
- Recht auf menschliches Gehör
  - Was, wie?

Pflichten des Verantwortlichen

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
4	Meldepflichten bei Datensicherheitsvorfällen

Datensicherheitsvorfall – was ist zu tun?

- Meldung an die Aufsichtsbehörde EDÖB
- Information der betroffenen Personen

Voraussetzung und Umsetzung

Eine **Datensicherheitsverletzung** liegt vor, wenn im Rahmen einer Datenbearbeitung in unvorhergesehener Weise die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten beeinträchtigt wird und diese dazu führt, **dass Personendaten unbeaufsichtigt sind, verlorengehen, gelöscht, vernichtet, verändert, Unbefugten offengelegt oder zugänglich gemacht werden.**

Aktuelle **technische** und **organisatorische** Massnahmen (TOM) sind ein guter Schutz gegen Datensicherheitsverletzungen.

technische Beispiele:

- Zugang „need to know“, Authentifizierung
- persönliches Konto, Firewall

organisatorische Beispiele:

- Weisungen, Regelungen
- Schulungen

Pflichten des Verantwortlichen

Ein Unternehmen hat folgende Pflichten

	Pflicht des Unternehmens
5	Datenschutz Folgeabschätzung (DSFA)
6	Bearbeitungsverzeichnis

Voraussetzung für die DSFA

Wenn hohes Risiko für die Persönlichkeit oder die Grundrechte der betr. Person entsteht

Ausnahmen

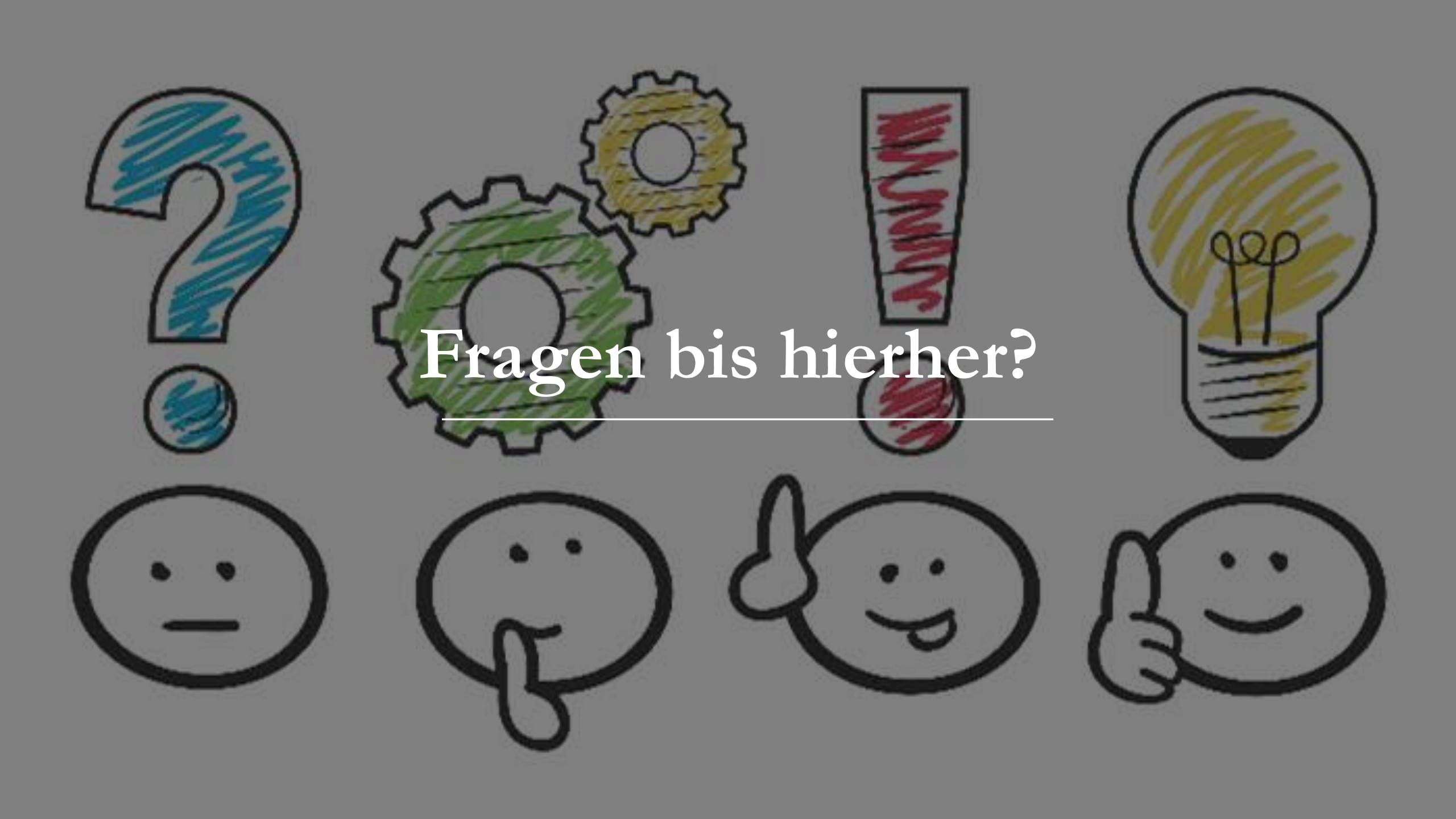
- gesetzlich verpflichtet
- Produkt, System, Dienstleistung neue Regelung zertifiziert
- geprüfter Verhaltenskodex enthält

Vorteile eines Bearbeitungsverzeichnisses

Das Wissen, welche Personendaten wie und wofür bearbeitet werden, ist die Basis für einen verantwortungsvollen Datenschutz.

Pflicht, Ausnahme und Mindestinhalt

- Unternehmen sind verpflichtet
- schriftlich geführt (Excel online ok)
- Unternehmen als Verantwortlicher oder Auftragsbearbeiter (je nach dem…)


Fragen bis hierher?

Auftragsdatenbearbeitungsvertrag & Geheimhaltungspflicht

Eigenes Unternehmen gibt Daten an einen Dritten weiter…

Dies ist wenn ein Unternehmen seine Daten durch einen Dritten in seinem Auftrag ausführen lässt, handelt es sich um eine Auftragsdatenbearbeitung.

Hierfür wird ein Vertrag abgeschlossen.

Welche Drittanbieter haben wir?

Geheimhaltungspflicht

Eine Zusammenarbeit mit Dritten kann auch in der Form stattfinden z.B. Personendaten und Fabrikations-Geschäftsgeheimnisse.

Mit der Geheimhaltungspflicht kann sichergestellt werden, dass die betroffenen Daten geschützt bleiben.

Was passiert wenn die Mitarbeitenden das nicht machen?

Datenbekanntgabe ins Ausland

Grundsatz

Unternehmen dürfen Personendaten ins Ausland bekannt geben, solange diese Daten im Empfängerland angemessen, also mindestens in einem vergleichbaren Umfang wie in der Schweiz, geschützt sind (z.B. EU).

Der Bundesrat sagt welche Länder einen angemessenen Datenschutz aufweisen.

Garantien und Ausnahmen

Gilt ein Land nicht als sicher, so muss durch hinreichende Garantien ein geeigneter Datenschutz gewährleistet werden.

Umsetzung

In der Praxis sind wir insbesondere bei der IT-Struktur an grosse Softwareanbieter wie Microsoft Office 365 gebunden.

Dies führt zu einem Datenabfluss.

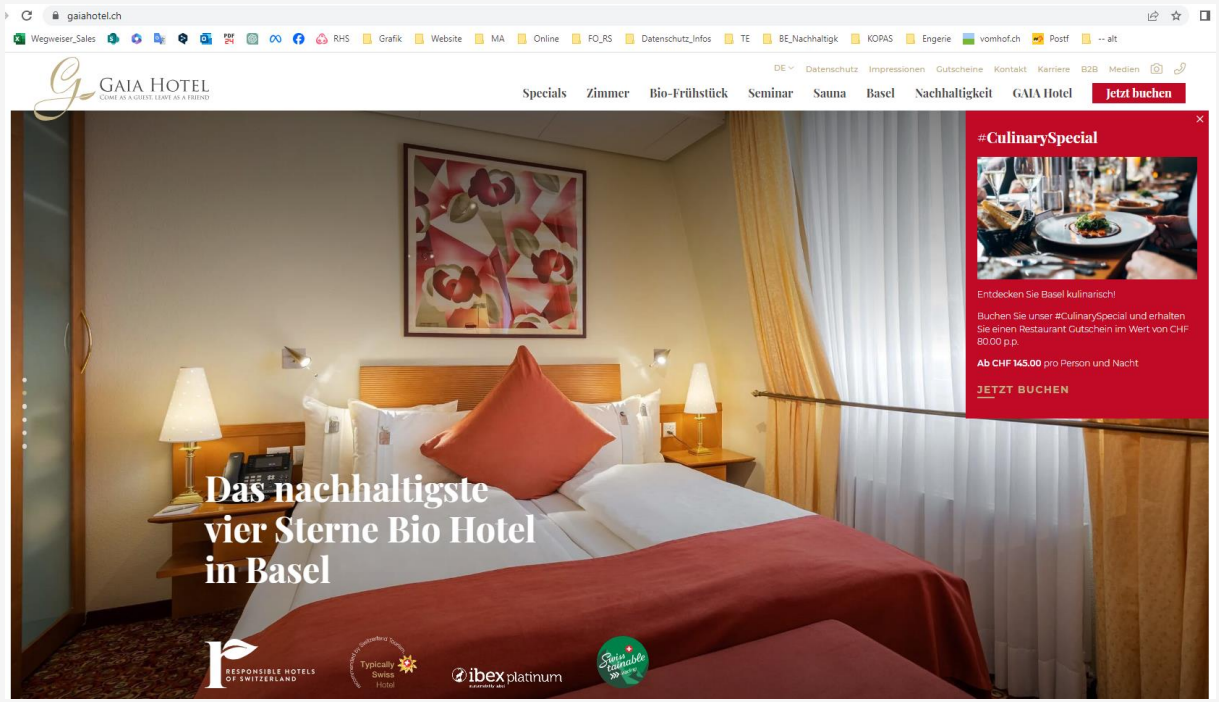
Die Daten werden besser in der Schweiz oder EU gespeichert.

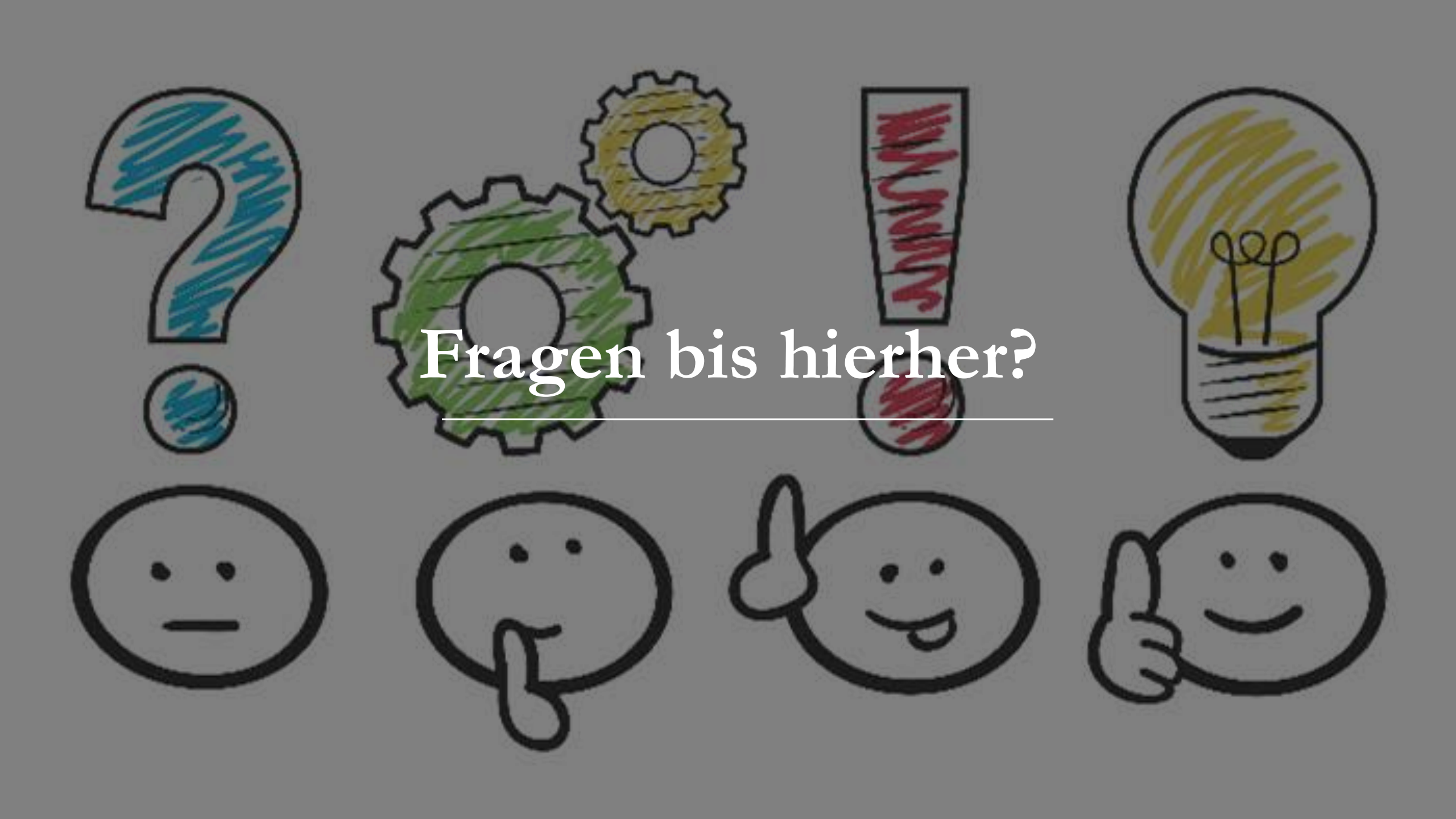
Internetauftritt

Internetauftritt

Jedes Unternehmen nutzt das Internet für mind. seine Firmenwebseite. Aus **datenschutzrechtlichen Überlegungen** sind dabei folgende Punkte zu beachten. Mögliche Inhalte:

- reine Informationsseite
- Ware, Werke oder Leistungen werden angeboten
- Mitarbeiterfotos und deren Kontaktdaten
- Kontaktformular/Onlineanmeldung
- Newsletter
- Impressum
- Datenschutzerklärung
- Analytic Tools und Cookies




Fragen bis hierher?

Mitarbeiterinformationen & Vertraulichkeitsverpflichtung

Mitarbeiterinformationen

Jedes Unternehmen bearbeitet HR Daten, ob vor dem Eintritt oder bis zum Austritt und u.a. auch schützenswerte Daten. **Diese Daten gilt es zu schützen.**

Das Unternehmen muss die Mitarbeitenden entsprechend informieren.

Der Bearbeitungszweck und die sich daraus ergebende Informationspflicht ist abhängig vom Status der betreffenden Person. Dabei gilt im Arbeitsbereich generell die **Datenminimierungs-pflicht!**

Grundsatz: „Nur so viel wie nötig und so wenig wie möglich".

Wo? Job-Interessierte, Stellensuchende, Mitarbeitende, ausgetretene Mitarbeitende

Vertraulichkeitsverpflichtung & Einwilligung

Die Mitarbeitenden im Personalbüro sind verpflichtet zur Einhaltung der Vorschriften.

Die Verwendung und Veröffentlichung von **fotografischen und/oder Bild- und Tonaufnahmen** sowie Kontaktdaten von Mitarbeitenden – soweit sie nicht in Erfüllung der arbeitsvertraglichen Pflicht offengelegt werden dürfen – bedürfen **einer Einwilligung. -> Diese haben Sie mit dem Zusatz zum Arbeitsvertrag bei uns im GAIA Hotel visiert.**

Sie können die Einwilligung jederzeit **widerrufen. Wichtig dabei ist,** dass die Nutzung von bereits gedruckten z.B. Broschüren weiter möglich sein muss und dass bei Veröffentlichung im Internet durch die Nutzung von Dritten eine generelle Löschung nicht möglich ist.

Datenschutzbehörde der Schweiz

Der **EDÖB** als Aufsichtsbehörde ist zuständig bei Datenbearbeitungen durch Bundesorgane und Private.

-> Datenbearbeitungen durch kantonale und kommunale Behörden fallen **nicht** in seinen Zuständigkeitsbereich.

Hauptaufgaben:

- **Beaufsichtigung** der Bundesbehörde und privaten Personen
- **Beratung** von Bundes-, kantonalen Behörden und private Personen
- **Stellungsnahme** zu Rechtssetzungsprojekten des Bundes
- **Schulungen** von **Informationen** an Bundesorgane und private Organisationen
- **Sensibilisierung** von Personen & **Auskunft** an betroffene Personen
- Stellt **Arbeitsinstrumente** als Empfehlung zur Verfügung
- **Zusammenarbeit** mit in-/ausl. Datenschutz-behörden

Bussen und weitere Sanktionen

Ablauf

➔ Anzeige/Amtes wegen -> Untersuchung

➔ Mitwirkungspflicht des Unternehmens

➔ Datenschutzbestimmungen verletzt

- ➔ Nein -> keine Folgen ☺
- ➔ Ja -> Folgen: Datenbearbeitung anpassen, Daten löschen/vernichten, Auslandstransfert verbieten/ unterbrechen -> Verwarnung

Strafrechtliche Massnahmen – Verletzungsbestand

- Verletzung der Informationspflicht
- Verletzung der Auskunftspflicht
- Verletzung der Mitwirkungspflicht
- Verletzung der Bestimmungen zum Datenexport
- Nicht konforme Beauftragung von Auftragsbearbeitern
- Verletzung der Massnahmen zur Datensicherheit
- Verletzung der beruflichen Schweigepflicht
- Missachtung von Verfügungen des EDÖB oder der Beschwerdebehörde

→ Bussen bis 250’000 CHF – Privatperson

Videoüberwachung

Warum wird Video überwacht?

Schutz vor Diebstahl, Plünderei, unerlaubten Personen im Hause, Eindringlinge, Angriffen von Fremden, unbeliebten Gästen etc.

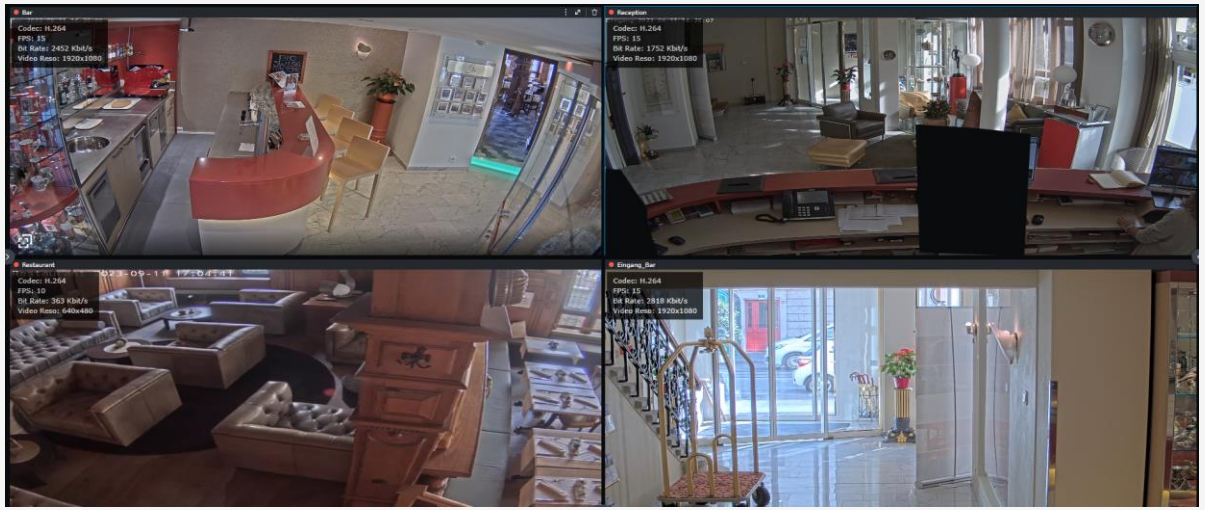
Schutz für unsere Mitarbeitenden

Wo wird Video überwacht?

1. Barbereich mit Blick zum Eingang Frühstück
2. Lounge im Restaurant
3. Von oberhalb der Reception zum Hoteleingang
   (die Mitarbeitenden hinter der Reception sind ausgepixelt)
4. Hoteleingang nach draussen auf die Strasse zum Bahnhof

Aufzeichnung: 16 Tage 24h / 7 Tage die Woche

Einsicht in die Daten: jederzeit beim Front Office




Fragen zum
Datenschutz?