Leitfaden

Umsetzung der Datenschutzgrundverordnung in Seilbahnunternehmen

Impressum

Hersteller:
Fachgruppe Seilbahnen der Wirtschaftskammer Tirol
Wilhelm-Greil-Straße 7, 6020 Innsbruck

1. Auflage, April 2018

Text und Konzeption:
Dr. Werner Pilgermair, Mag. Florian Brutter

Soweit im Text personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen oder Männer in gleicher Weise. Bei der Anwendung auf bestimmte Personen wird die jeweils geschlechtsspezifische Form verwendet.

Es wird darauf hingewiesen, dass alle Angaben trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen. Eine Haftung der Verfasser wird ebenso wie eine Haftung der Fachgruppe Seilbahnen der Wirtschaftskammer Tirol ausgeschlossen.

Inhaltsverzeichnis

1 Einführung ... 2
1.1 Die neue Rechtslage im Datenschutz ... 2
1.2 Auswirkungen auf die Seilbahnwirtschaft ... 3
1.3 Personenbezogene Daten ... 3
1.3.1 Ohne Personenbezug ... 4
1.3.2 Softwaresysteme, Excel-Listen oder Papierakte ... 6
1.4 Datenschutzrechtliche Rollen ... 6
1.5 Zusammengefasst ... 7
2 Relevante Bereiche in der Seilbahnwirtschaft ... 8
2.1 Pisten ... 8
2.1.1 Trainingsgruppen ... 8
2.1.2 Flotten- und Pistenmanagement ... 9
2.2 Pistenrettung ... 9
2.3 Bahnen und Lifte ... 10
2.3.1 Tagesberichte ... 10
2.3.2 Betriebstagebuch ... 10
2.4 Verwaltung ... 11
2.4.1 Abwicklung von Schadensfällen ... 11
2.4.2 Beschwerdemanagement ... 11
2.4.3 Krisenhandbuch ... 12
2.4.4 Lost and Found ... 12
2.4.5 Adressverwaltungen ... 12
2.5 Gastronomie ... 13
2.5.1 Bonier- und Bezahlsysteme ... 13
2.5.2 Reservierungen und Veranstaltungen ... 13
2.6 Handel ... 13
2.6.1 Merchandising- und Sportartikel ... 13
2.6.2 Online-Shop ... 14
2.6.3 Verleih ... 14
2.7 Kassa ... 14
2.7.1 Verkauf vor Ort ... 14
2.7.2 Online-Verkauf ... 15
2.7.3 Dezentrale Kassensysteme ... 15
2.7.4 Poolkarten ... 15
2.9 Personal ... 16
2.9.1 Bewerber ... 16
2.9.2 Personalverwaltung ... 17
2.9.3 Verpflichtung zum Datengeheimnis ... 20
2.9.4 Privatnutzung von Internet (Social Media) und Handy ... 21
2.9.5 Schulung und Sensibilisierung von Mitarbeitern, Datenschutzrichtlinie ... 21
2.9.6 Ausgeschiedene Mitarbeiter ... 22
2.9.7 Datenverarbeitung durch den Betriebsrat ... 22
2.10 Direktwerbung ... 22
2.11 Bildverarbeitung ... 23
2.11.1 Definition „Bildaufnahme“ ... 24
2.11.2 Zulässigkeit der Bildaufnahme ... 24
2.11.3 Informations- und Kennzeichnungspflicht ... 27
2.11.4 Aufbewahrungsfrist/ Löschungspflicht ... 27
2.11.5 Besondere Datensicherheitsmaßnahmen und Protokollierungspflicht ... 28
2.11.6 Auswertung von durch Bildaufnahmen gewonnener personenbezogener Daten ... 28
2.11.7 Übermittlung und Veröffentlichung ... 28
2.11.8 Unzulässige Bildaufnahme ... 29
2.11.9 Strafbestimmungen ... 29
2.12 Übersicht ... 29
2.13 Zusammengefasst ... 30
3 Keine Datenverarbeitung ohne Rechtsgrundlage ... 30
3.1 Unterscheidung von Datenkategorien ... 31
3.1.1 Nichtsensible personenbezogene Daten ... 31
3.1.2 Beispiel: IP-Adressen ... 32
3.1.3 Besondere Kategorien personenbezogener Daten („Sensible Daten“) ... 32
3.1.4 Strafrechtsrelevante Daten ... 33
3.2 Unter welchen Voraussetzungen ist die Verarbeitung rechtmäßig? ... 33
3.2.1 Einwilligung des Betroffenen ... 33
3.2.2 Vertrag und vorvertragliche Maßnahmen ... 36
3.2.3 Rechtliche Verpflichtung ... 36
3.2.4 Schutz lebenswichtiger Interessen ... 37
3.2.5 Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt ... 37
3.2.6 Wahrung berechtigter Interessen ... 37
3.2.7 Weiterverarbeitung von Daten ... 39
3.2.8 Verarbeitung besonderer Kategorien personenbezogener Daten („Sensible Daten“) ... 40
3.2.9 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten ... 41
3.3 Zusammenfassung ... 41
4 Aufgaben und Pflichten ... 42
4.1 Grundsätze der Datenverarbeitung ... 42
4.1.1 Rechtmäßigkeit ... 42
4.1.2 Zweckbindung ... 43
4.1.3 Datenminimierung ... 43
4.1.4 Richtigkeit ... 43
4.1.5 Speicherbegrenzung ... 44
4.1.6 Integrität und Vertraulichkeit ... 44
4.2 Erstellung eines Verarbeitungsverzeichnisses ... 44
4.2.1 Sinn und Zweck des Verzeichnisses ... 44
4.2.2 Notwendige Angaben ... 45
4.2.3 Relevante Datenverarbeitungen ... 45
4.2.4 Umsetzung in der Praxis ... 46
4.2.5 Bildung von Clustern ... 46
4.3 Auswahl und Implementierung geeigneter TOMs ... 46
4.3.1 Beispiele für technische Maßnahmen: ... 47
4.3.2 Beispiele für organisatorische Maßnahmen: ... 47
4.4 Datensicherheitsmaßnahmen ... 48
4.4.1 Beispiele für Datensicherheitsmaßnahmen: ... 48
4.4.2 Broschüren der Wirtschaftskammern zur Datensicherheit ... 49
4.5 Durchführung von Folgenabschätzungen ... 49
4.5.1 Vorherige Konsultation ... 50
4.6 Benennung eines Datenschutzbeauftragten ... 51
4.7 Meldung von Datenschutz-Vorfällen ... 52
4.8 Informierung der Betroffenen ... 53
4.8.1 Datenerhebung bei der betroffenen Person ... 53
4.8.2 Datenerhebung bei einer anderen als der betroffenen Person ... 54
4.9 Datenschutzerklärung ... 54
4.10 Datenübermittlung ins Ausland ... 56
4.11 Ausarbeitung interner Datenschutzstrategien ... 56
4.12 Zusammenfassung ... 57
5 Hilfreiches ... 57
5.1 Checkliste ... 57
5.2 Muster ... 58
5.2.1 Datenschutzerklärung für Mitarbeiter ... 58
5.2.2 Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen ... 62
5.2.3 Beispiele für Datenverarbeitungen ... 65
5.3 Nützliche Links ... 68

1 Einführung

Mit Geltung der **Datenschutz-Grundverordnung ab 25. Mai 2018** wird ein neues Datenschutzzeitalter eingeläutet, das auch Auswirkungen auf Seilbahnunternehmen hat.

Gäste erwarten reibungslose Abläufe, mit kurzen Wartezeiten, sicheren Pisten und vielfältigen Angeboten. Wintersportler wollen die gesamte touristische Bandbreite, bestehend aus Bergbahnen, Hotellerie, Nahverkehr, Sportausrüster und Gastronomie komfortabel nutzen, was einen hohen Vernetzungsgrad zwischen den Systempartnern bedingt. Dass damit weit verzweigte Datenflüsse einhergehen, liegt auf der Hand. Gäste wollen darüber informiert werden, was mit ihren personenbezogenen Daten geschieht, welche Rechte sie im Datenschutz haben und wie sie diese geltend machen können. Für Seilbahnbetriebe, die im Alpintourismus eine Schlüsselrolle spielen, können diese unterschiedlichen Erwartungshaltungen zur Herausforderung werden.

Dieser Leitfaden dient dazu, datenschutzrechtliche Aspekte im Beziehungsgefüge zwischen dem Bergbahnunternehmen und seinen Kunden praxisnah und verständlich aufzuarbeiten und das erforderliche Niveau im Datenschutz, die von der (medialen) Öffentlichkeit zunehmend als Qualitätsmerkmal wahrgenommen wird, nachhaltig im Betrieb zu verankern.

Im Folgenden werden typische Strukturen von Seilbahnen skizziert, die sich im Einzelfall naturgemäß auch ganz anders darstellen können. Insofern soll der Leitfaden auch ein Baukasten sein, aus dem der einzelne Betrieb die für ihn relevanten Aspekte und Punkte übernehmen kann.

1.1 Die neue Rechtslage im Datenschutz

Unterschiedliche Datenschutzgesetze in den Mitgliedstaaten der Europäischen Union haben während der letzten Jahre zum Phänomen des **„Datenschutz-Hoppings“** geführt. Internationale Konzerne haben sich demnach in Ländern mit vergleichsweise „sanften“ Datenschutzbestimmungen niedergelassen, was zu Wettbewerbsverzerrungen geführt hat.

Durch die Datenschutz-Grundverordnung der EU (DSGVO)[1] werden die unterschiedlichen Datenschutzniveaus weitestgehend angeglichen (ein Regelwerk für alle Mitgliedstaaten) und damit die gewünschte Wettbewerbsneutralität erreicht. Ab 25. Mai 2018 werden damit für alle europäischen Bergbahn- und Tourismusbetriebe einheitliche Standards gelten.

---

[1] Vollständiger Text der DSGVO abrufbar unter http://eur-lex.europa.eu .

Das novellierte österreichische Datenschutzgesetz, das ebenfalls am 25. Mai 2018 in Kraft tritt, regelt nur mehr vereinzelte Bereiche, wird aber für österreichische Seilbahnunternehmen speziell im Hinblick auf die Bildverarbeitung (Videoüberwachung und Fotos) von großer praktischer Relevanz bleiben.

1.2 Auswirkungen auf die Seilbahnwirtschaft

Das neue europäische Datenschutzrecht ist von einer starken Tendenz zur **Eigenverantwortlichkeit** von Unternehmen geprägt. Wirtschaftsbetriebe – und damit auch Bergbahnunternehmen – sollen die Pflichten und Aufgaben der DSGVO selbständig und eigenverantwortlich umsetzen, während sich die Aufsichtsbehörden (in Österreich die **Datenschutzbehörde**[2]) auf ihre Überwachungs- und Kontrollfunktion zurückziehen.

Bei Verstößen gegen die DSGVO können künftig exorbitant hohe **Geldbußen** verhängt werden. Die Strafandrohungen reichen bis zu maximal 20 Mio. Euro oder bis zu 4% des gesamten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist. Hinsichtlich der Strafhöhen verlangt die DSGO, dass die Bemessung der Geldbußen im Einzelfall „*wirksam, verhältnismäßig und abschreckend*“ sein muss.

In welchem Ausmaß von der Datenschutzbehörde Geldbußen ausgesprochen werden, ist nicht vorhersagbar, wird aber auch davon abhängen, wie oft Datenschutzvorfälle künftig von ehemaligen Mitarbeitern und von Gästen (aus welchen Gründen immer) aufgegriffen und vor die Datenschutzbehörde getragen werden.

Unabhängig von den Geldbußen drohen auch Klagen auf **Unterlassung** und auf **Schadenersatz** durch betroffene Personen sowie wettbewerbsrechtliche Maßnahmen, die von Mitbewerbern ergriffen werden.

Neben diesem Sanktionenrisiko können Verstöße gegen den Datenschutz schnell zu **Vertrauensverlusten** bei Kunden und generell zu einem negativen Imagetransfer in der (medialen) Öffentlichkeit führen. Für Bergbahnunternehmen, die im Internet und speziell in Social Media Networks entsprechend präsent sind, gilt dies umso mehr.

1.3 Personenbezogene Daten

Personenbezogene Daten sind nach Artikel 4 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“.

---

[2] Webseiten der österreichischen Datenschutzbehörde: https://www.dsb.gv.at/.

Identifizierbar kann eine Person bereits durch indirekte Zuordnung zu einer Kennung, einer Kennnummer oder zu bestimmten Merkmalen sein, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

EMPFEHLUNG: Das der Begriff der personenbezogenen Daten sehr weit gefasst ist, sollte im Zweifel immer von personenbezogenen Daten ausgegangen werden.

Beispiele für personenbezogene Daten: Name, Geburtsdatum, Staatsbürgerschaft, Sozialversicherungsnummer, Reisepassnummer, Führerscheinnummer, Schipassnummer, Kreditkartennummer, KFZ-Kennzeichen, IP-Adresse, Telefonnummer, E-Mail-Adresse, Ausbildung, Qualifikation, Beruf, Einkommen, Vermögen, Wohnort, Urlaubsort, Arbeitszeiten, Familienstand, Lebensgeschichte, Beziehungen, Talente, Vorlieben, Wünsche, Erwartungen, Abneigungen, Beschwerden.

1.3.1 Ohne Personenbezug

Daten, die von vornherein keinen Personenbezug aufweisen, sind datenschutzrechtlich nicht relevant und müssen nicht weiter beachtet werden.

Beispiele:
Das Seilbahnunternehmen bestellt Ersatzteile für einen Schlepplift.
Gäste bezahlen ihr Mittagessen im Selbstbedienungsrestaurant bar.
Ein Gast bewertet die Bergbahn anonym im Internet.

Wird der Personenbezug nachträglich entfernt, ist die Weiterverarbeitung zu statistischen Zwecken zulässig.

Beispiel:
Der Geschäftsführer eines Seilbahnunternehmens lässt auswerten, wie viele Saisonkarten in der abgelaufenen Wintersaison an den Kassen verkauft wurden. Insbesondere interessiert ihn, das Verhältnis zwischen vergünstigten Karten im Vorverkauf und regulären Karten im normalen Verkauf. Dafür benötigt er nur die Verkaufszahlen und nicht auch die Namen der einzelnen Käufer. Die rein statistische Auswertung dieser Verkaufszahlen hat daher keinen Personenbezug und ist ohne Weiteres zulässig.

Bestimmte personenbezogene Daten werden vom Gesetzgeber besonders geschützt. Diese „*besonderen Kategorien personenbezogener Daten*“ werden nach der alten Rechtslage im Datenschutz als **„sensible Daten“** bezeichnet, wobei davon auszugehen ist, dass diese Bezeichnung im Alltag weiterhin gebräuchlich bleiben wird.[3] Es handelt sich um folgende Daten **(vollständige Aufzählung)**:

[3] Auch in diesem Leitfaden wird aus Gründen der besseren Lesbarkeit gelegentlich noch von „sensiblen Daten“ gesprochen. Gemeint sind damit „Besondere Kategorien personenbezogener Daten“ im Sinn der DSGVO.

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrischen Daten
- Gesundheitsdaten
- Daten zum Sexualleben

Im Bergbahnbetrieb sind Gesundheitsdaten von zentraler Bedeutung, andere besondere Kategorien personenbezogener Daten werden in der Regel nicht verarbeitet.

Beispiel:
Im Rahmen der Pistenrettung werden vor Ort sensible Gesundheitsdaten der verunfallten Gäste (Art und Ausmaß der Verletzung) sowie andere relevante Daten erhoben und in internen Dokumentationssystemen verarbeitet.

„Gesundheitsdaten“ sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

EMPFEHLUNG: So wie der Begriff der personenbezogenen Daten ist auch der Begriff der Gesundheitsdaten weit gefasst. Im Zweifel sollte daher immer von gesundheitsrelevanten Informationen ausgegangen werden.

Gesundheitsdaten sind demnach nicht nur „handfeste“ Informationen zur Krankengeschichte (Vorverletzungen, Operationen, etc.) und aktuelle Untersuchungsergebnisse, sondern z.B. auch subjektive Beschwerden.

Im Ergebnis sind besondere Kategorien personenbezogener Daten eine **Teilmenge** der personenbezogenen Daten, die vom Gesetzgeber besonders geschützt werden:

1.3.2 Softwaresysteme, Excel-Listen oder Papierakte

Nicht von Bedeutung ist, ob personenbezogene Daten in einer EDV-Applikation (angekaufte oder selbst programmierte Software) oder z.B. in einer „selbstgebastelten“ Excel-Lösung verarbeitet werden. Auch strukturierte Papierordner sind datenschutzrelevant.

Beispiel:
Besondere Vorkommnisse, z.B. Unfälle bei der Benutzung von Liftanlagen, werden in den Tagesberichten (ausgedruckte Formblätter) handschriftlich dokumentiert und chronologisch in einem Papierordner abgelegt.

1.4 Datenschutzrechtliche Rollen

Im datenschutzrechtlichen Beziehungsgefüge zwischen Systempartnern im Alpintourismus sind unterschiedliche Rollen zu beachten.

„Verantwortlicher“ ist derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

In der Praxis ist in der Regel der **Rechtsträger** des Seilbahnunternehmens (z.B. GmbH, AG oder GmbH & Co KG) Verantwortlicher im Sinn des Datenschutzrechtes und damit auch primärer Adressat der Aufgaben und Pflichten nach der DSGVO.

Beispiel:
Vom Seilbahndirektor und dem Abteilungsleiter Personal einer Seilbahn-AG wird entschieden, eine neue Personalverwaltungssoftware einzusetzen. In dieser Software soll auch das neue Zutrittskontrollsystem integriert sein. Auch wenn diese Entscheidung von den Führungskräften des Unternehmens getroffen wird, bleibt der Rechtsträger des Unternehmens (AG) für die entsprechenden Datenverarbeitungen, die künftig im Rahmen der Software erfolgen, datenschutzrechtlich verantwortlich.

MERKE: In Bezug auf die Verarbeitung der Daten seiner Gäste und Kunden ist das Seilbahnunternehmen grundsätzlich immer Verantwortlicher.

„Auftragsverarbeiter“ ist derjenige, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Beispiele:
Das Seilbahnunternehmen beauftragt einen Marketingdienstleister mit der Versendung eines News-Letters und stellt im dafür die E-Mail Adressen seiner Kunden zur Verfügung.
Ein externer EDV-Dienstleister wird mit der Administration und Wartung der Kundendatenbank des Seilbahnunternehmens betraut. Zur Erbringung seiner Leistung muss der EDV-Dienstleister Zugriff auf die Datenbank und damit auch auf die Kundendaten haben.

Nahegelegene Hotels verkaufen im Namen und auf Rechnung des Seilbahnunternehmens Schipässe. Die entsprechenden Kundendaten werden damit im Hotel (im Auftrag des Seilbahnunternehmens) erhoben.

Der Verantwortliche hat mit den von ihm beigezogenen Auftragsverarbeitern eine **Vereinbarung über die Auftragsverarbeitung** abzuschließen.

Diese Vereinbarung regelt die datenschutzrelevanten Pflichten des Auftragsverarbeiters (insbesondere die Pflicht zur Geheimhaltung der im Auftrag verarbeiteten personenbezogenen Daten des Verantwortlichen und zur Gewährleistung ausreichender Datensicherheitsmaßnahmen) und besteht neben dem zivilrechtlichen Vertragsverhältnis zwischen Auftraggeber und Dienstleister (in der Praxis häufig Werkvertrag oder Auftragsvertrag nach § 1002 ABGB).

EMPFEHLUNG: Die Wirtschaftskammern haben ein Muster für eine Vereinbarung über die Auftragsverarbeitung erstellt, das für den konkreten Anlassfall angepasst werden kann[4].

1.5 Zusammengefasst

- Mit der DSGVO wird ab 25. Mai 2018 ein einheitliches Datenschutzniveau in allen Mitgliedstaaten eingeführt (Wettbewerbsneutralität).
- Das novellierte österreichische DSG, das ebenfalls am 25. Mai 2018 in Kraft tritt, wird insbesondere für die Bildverarbeitung (Videoüberwachung, Fotos) Bedeutung haben.
- Neben hohen Geldbußen (verhängt durch die Datenschutzbehörde) sowie Klagen auf Unterlassung und Schadenersatz vor dem Zivilgericht droht bei Verstößen gegen den Datenschutz auch Vertrauens- und Imageverluste bei Kunden und generell in der öffentlichen Wahrnehmung.
- Im Zweifel sollte immer von „personenbezogenen Daten“ ausgegangen werden. Auch der Begriff der „Gesundheitsdaten“ (besondere Kategorie personenbezogener Daten) ist weit auszulegen. Daten ohne Personenbezug (z.B. statistische Auswertungen) sind nicht von Belang.
- Es spielt keine Rolle, ob personenbezogene Daten in komplexen EDV-Applikationen, einfachen Excel-Lösungen oder strukturierten Papierordnern verarbeitet werden.
- Das Seilbahnunternehmen (konkret der Rechtsträger des Unternehmens, z.B. eine GmbH oder AG) ist in Bezug auf die Verarbeitung von Daten seiner Kunden und Mitarbeitern in der Regel „Verantwortlicher“ und primärer Adressat der Aufgaben und Pflichten nach der DSGVO. Beauftragt der

[4] Die Muster-Vereinbarung wird auf den Webseiten der Wirtschaftskammern zum Download zur Verfügung gestellt: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html .

Verantwortliche externe Dienstleister mit der Verarbeitung von Daten, hat er mit diesen eine Vereinbarung über die Auftragsverarbeitung abzuschließen.

2 Relevante Bereiche in der Seilbahnwirtschaft

Im Folgenden werden typische Verarbeitungstätigkeiten eines Seilbahnunternehmens dargestellt. Im Einzelfall können aufgrund der individuellen Rahmenbedingungen und spezifischen Voraussetzungen eines jeden Unternehmens noch (viele) andere Verarbeitungstätigkeiten hinzukommen. An den Grundsätzen der datenschutzrechtlichen Beurteilung ändern diese zusätzlichen Verarbeitungstätigkeiten jedoch nichts, insbesondere gilt auch für sie der Grundsatz, wonach jede Datenverarbeitung rechtmäßig sein muss (keine Datenverarbeitung ohne Rechtsgrundlage, siehe dazu unten Kapitel 3).

2.1 Pisten

Im Rahmen der Organisation des Schi- und Pistenbetriebs können unterschiedliche Datenverarbeitungen stattfinden, die bei der Erfüllung der Aufgaben und Pflichten nach der DSGVO zu beachten sind, beispielsweise:

2.1.1 Trainingsgruppen

Trainingsgruppen werden häufig in einer eigenen Datenbank verwaltet. Verarbeitet werden darin alle Daten, die zur Planung, Organisation und reibungslosen Abwicklung der Trainingseinheiten während einer Schisaison notwendig sind.

Im Hinblick auf personenbezogene Daten betrifft dies insbesondere Daten von Ansprechpartnern (Trainern, Trainingsgruppenleitern, etc.) und den Teilnehmern (Sportler), die in allen möglichen Formen verarbeitet werden.

Beispiel:
Im Rahmen von Anmeldeformularen und schriftlichen Vereinbarungen (Regelung der zivilrechtlichen Rahmenbedingungen für die Abwicklung der Trainingseinheiten) werden personenbezogene Daten, wie Name, Funktion und Kontaktdaten der Ansprechpartner und Teilnehmer verarbeitet. Im Zuge der Durchführung der Trainingseinheiten am Berg kann es auch sein, dass personenbezogene Daten (z.B. Name, Funktion und Einsatzgebiet von Trainern) auf Bildschirmen angezeigt werden, um den verschiedenen Trainingsgruppen die Orientierung zu ermöglichen. Diese Orientierungshilfen können auch im Wege von Flipcharts, White-Boards oder sonstigen analogen Darstellungen erfolgen.

2.1.2 Flotten- und Pistenmanagement

In Rahmen des Flotten- und Pistenmanagements wird üblicherweise festgehalten, welche Mitarbeiter (Name, Funktion) sich zu welchen Zeiten mit welchen Geräten auf welchen Pisten aufhalten und bewegen. Auch technische Nachweise, z.B. ob vom Mitarbeiter Lichter oder Warnleuchten ordnungsgemäß eingeschaltet sind, werden erfasst.

Der damit einhergehenden Verarbeitung personenbezogener Daten liegen betriebliche Planungs- und Steuerungsmomente zu Grunde. Einerseits sollen dadurch Unfälle vermieden werden, andererseits wird die nachträgliche Absicherung des Seilbahnunternehmens im Schadensfall gewährleistet.

2.2 Pistenrettung

Datenverarbeitungen im Rahmen der Pistenrettung sind von datenschutzrechtlich höchster Relevanz, da praktisch in allen Abläufen und Prozessen Gesundheitsdaten (und damit besonders geschützte Kategorien von Daten) betroffen sind.

Passiert auf einer Piste oder im Bereich einer Seilbahn- oder Liftanlage ein Unfall mit Personenschaden, wird nach der Sicherung der Unglücksstelle die möglichst rasche Bergung mit der gebotenen Ersten Hilfe geleistet. Nach der unverzüglichen Kommunikation mit Leiteinrichtungen zur Organisation der jeweils indizierten fachmedizinischen Versorgung kommt es bereits am Einsatzort– durch Ausfüllen eines **Patientendatenblattes** – zur Dokumentation von personenbezogenen Daten und von sensiblen Gesundheitsdaten.

Bei Verweigerung der gebotenen ersten Hilfe wird vor Ort allenfalls auch ein **Revers** unterfertigt, der typischerweise folgende Inhalte aufweist:

- Aufklärungen, z.B. über die möglichen Folgen der Verweigerung angeratener Hilfeleistungen,
- Aufforderungen, z.B. zum unverzüglichen Aufsuchen eines Arztes oder Krankenhauses) und
- Bestätigungen, z.B. betreffend die Verweigerung des Mitflugs in dem vor Ort befindlichen Notarzthubschrauber.

Zur Dokumentation und Nachbereitung des Unfallgeschehens wird ein **internes Unfallprotokoll** angelegt, in dem wiederum personenbezogene Daten zum Verunfallten und den Versorgern (Mitarbeiter der Pistenrettung, externe Sanitäter, Freiwillige, Abtransport, Übergabe an welches Rettungsmittel etc.) verarbeitet werden. Auch dieses Unfallprotokoll enthält regelmäßig sensible Gesundheitsdaten der betroffenen Person. Typischerweise werden folgende personenbezogene Daten verarbeitet:

- Daten des Verletzten (Name, Geschlecht, Geburtsdatum, Adresse, Herkunftsland, Urlaubsadresse, Kontaktdaten, bei Kindern die Körpergröße)
- Art der Verletzung
- Erfolgte Erstversorgung

Relevante Bereiche in der Seilbahnwirtschaft

- Unfallhergang
- Unfallursache
- Weitere beteiligte Personen
- Zeugen

Unfallmeldungen werden bei strafrechtlich relevanten Tatbeständen an die zuständige Sicherheitsbehörde weitergeleitet und allenfalls auch an Versicherungen.

Bei Unfällen und Störungen in Verbindung mit Liftanlagen müssen Seilbahnbetreiber unter gewissen Voraussetzungen (Schwere Verletzungen und Tötungen im Zusammenhang mit der Betriebsabwicklung oder der Instandhaltung etc.) unverzüglich Meldung an die jeweils zuständige Behörde je nach Bahntyp vornehmen (§ 104 Abs 2 SeilbG 2003 iVm Melde-VO Seilb 2006).

2.3 Bahnen und Lifte

Im Umfeld von Bahnen und Liften werden personenbezogene Daten – neben Videoüberwachungen - insbesondere im Rahmen von Tagesberichten und dem Betriebstagebuch verarbeitet.

2.3.1 Tagesberichte

Werden in Tagesberichten von Bahnen und Liften personenbezogene Daten von Mitarbeitern verarbeitet, sind diese dienstbezogen und beschreiben relevante betriebliche Abläufe des betreffenden Tages.

Werden in den Berichten Gäste namentlich erwähnt, sind in der Regel gesundheitsbezogenen Daten (und damit besonders geschützte Kategorien von Daten) betroffen und zwar insbesondere dann, wenn Unfallereignisse beschrieben oder ausgefüllte Formulare und Berichte der Pistenrettung beigelegt werden.

Beispiel:
In einem Tagesbericht wird in der Rubrik „Besondere Vorkommnisse“ folgendes vermerkt: „Max Muster aus Deutschland wurde beim Auslauf des Schlepplift X/Y durch einen noch ausgezogenen Bügel am Kopf verletzt. Der Vorfall wurde auf dem Überwachungsmonitor beobachtet und der Not-Stopp aktiviert. Die Erstversorgung ist durch die Pistenrettung erfolgt.“

2.3.2 Betriebstagebuch

Im Betriebstagebuch können ebenfalls personenbezogene Daten von Mitarbeitern und Gästen angeführt werden, in der Regel in Form von Berichten und Verweisen auf Unfälle.

Auch wenn das Betriebstagebuch nur in Form eines strukturierten Papierordners geführt wird, ist es datenschutzrechtlich relevant (siehe oben Punkt 1.3.3.)

2.4 Verwaltung

Im Verwaltungsbereich des Seilbahnunternehmens finden verschiedenste Datenverarbeitungen statt, die bei der Erfüllung der Aufgaben und Pflichten nach der DSGVO zu beachten sind. Die wichtigen sind:

2.4.1 Abwicklung von Schadensfällen

Bei der Abwicklung von Sachschäden wird vom Geschädigten in der Regel ein **Schadenerhebungsblatt** ausgefüllt, in dem neben Informationen zum Schaden (Art des Schadens, Schadensort und Schadensdatum) und den Kontaktdaten des Betroffenen auch Hinweise zum Schadensablauf und zum möglichen Verschulden aufgenommen werden.

Wird in diesem Zusammenhang abgefragt, ob sich der Geschädigte im Zuge des Schadensvorfalles verletzt hat, sind von der Datenverarbeitung auch besonders geschützte Kategorien von Daten (Gesundheitsdaten) betroffen.

Im nächsten Schritt ergeht eine **Schadensmeldung** des Seilbahnunternehmens an die Haftpflichtversicherung, in der ebenfalls personenbezogene Daten zum Geschädigten verarbeitet werden. Sind Zeugen bekannt, werden diese in der Meldung angeführt.

Gibt es im Unternehmen ein spezielles Verfahren zur Behandlung von Kleinschadensbeträgen, werden diese häufig im Wege von **Kleinschadensrechnungen** abgewickelt, in der neben den zentralen Informationen zum Schadensereignis auch eine Erklärung des Geschädigten zum pauschalen Entschädigungsbetrag unterfertigt wird.

2.4.2 Beschwerdemanagement

Werden Kundenbeschwerden nicht **anonym** eingebracht (was datenschutzrechtlich nicht relevant wäre), müssen für die Bearbeitung von Beschwerden und Anregungen personenbezogene Daten der betreffenden Personen erfasst werden. Üblicherweise betrifft dies neben Stammdaten wie Name, Anschrift und Kontaktdaten (Telefonnummer, E-Mail Adresse), den Inhalt bzw. Gegenstand der Beschwerde oder Anregung und die vom Seilbahnunternehmen getroffene Entscheidung (z.B. Antwortscheiben per E-Mail).

Beispiel:
Ein Kunde beschwert sich, dass er an der Kasse nicht über kostengünstigere Alternativen (z.B. Umtausch des Schipasses) aufgeklärt wurde. Im Kulanzwege wird dem Kunden eine Tagesfreikarte gewährt. Die Abwicklung dieser Beschwerde (vom Einlagen der Beschwerde des Kunden bis zur Entscheidung des zuständigen Mitarbeiters) wird dokumentiert.

In der Praxis kann das Beschwerdemanagement digital (z.B. im Excel) oder analog durch ein Formularsystem geführt werden.

2.4.3 Krisenhandbuch

Zur Gewährleistung standardisierter Abläufe in Krisensituationen (Lawinenabgänge, Unwetter, Brandfälle, etc.) wird von Bergbahnunternehmen ein Krisenhandbuch geführt, in dem auch personenbezogene Daten wie z.B. Namen, Funktionen und Kontaktdaten verarbeitet werden. Davon sind auch private Telefonnummern (z.B. von Ersthelfern im Betrieb) sowie Name und Erreichbarkeit von nahe Angehörige erfasst, die im Notfall zu kontaktieren sind.

Auch Einsatzpläne, die im Krisenhandbuch dargestellt werden, können personenbezogene Daten enthalten.

2.4.4 Lost and Found

In größeren Bergbahnunternehmen ist häufig ein Fundbüro eingerichtet. Bei der Abwicklung entsprechender Vorfälle kommt es zur Verarbeitung personenbezogener Daten.

In der Regel wird im ersten Schritt eine **Verlustmeldung** erstattet, in der Stammdaten des betroffenen Kunden (Name, Anschrift, Kontaktdaten) sowie nähere Informationen zum Vorfall (verlorener Gegenstand, Ort und Zeit des Verlusts) erfasst werden.

Im Fall der Abgabe oder der Abholung eines Fundgegenstandes wird im zweiten Schritt vom Finder und vom Abholer eine entsprechende **Bestätigung** ausgefüllt und unterfertigt. Auch im Rahmen dieses Formulars werden personenbezogene Daten verarbeitet.

Beispiel:
Der Finder einer Armbanduhr beschreibt in der Abgabebestätigung zunächst den Gegenstand des Fundes (Marke, Zustand, etc.) und führt seinen Namen und seine Kontaktdaten an. Weiters wählt er durch Ankreuzen (Ja/Nein) aus, ob seine Daten – im Fall der Abholung – an den Besitzer des Fundgegenstandes weitergegeben werden sollen.

2.4.5 Adressverwaltungen

In praktisch allen Seilbahnunternehmen werden Systeme zur Adressverwaltung geführt, um mit verschiedenen Personengruppen mehr oder weniger regelmäßig in Kontakt treten zu können.

Beispiele:
Vom Bergbahnunternehmen wird eine Liste von Stammgästen geführt, an die Rabattaktionen versendet werden.
Verunfallten Kunden wird ein kleines Präsent mit Genesungswünschen an den Wohnort gesendet.
In einer Liste werden alle pensionierten Mitarbeiter geführt, um sie zu den wichtigsten Betriebsfesten (z.B. Weihnachtsfeier) einzuladen.

2.5 Gastronomie

Führen Bergbahnen eigene Gastronomiebetriebe (z.B. Après-Ski Bar, Restaurant), sind sie in Bezug auf mögliche Datenverarbeitungen selbst „Verantwortlicher“ im Sinn der DSGVO.

Werden entsprechende Betriebe hingegen ausgelagert, so ist in der Regel der Pächter datenschutzrechtlich verantwortlich für die Verarbeitung von Gäste- und Mitarbeiterdaten.

2.5.1 Bonier- und Bezahlsysteme

Beim Einsatz von Boniersystemen werden in der Regel auch personenbezogene Daten von Mitarbeitern verarbeitet, insbesondere wird erfasst wie viele und welche Getränke und Speisen vom Mitarbeiter verkauft und abgerechnet wurden.

Außerhalb der Barbezahlung (anonymes Zug um Zug Geschäft) werden in der Gastronomie auch personenbezogene Daten der Gäste (insbesondere Bankomat- oder Kreditkartendaten) verarbeitet.

2.5.2 Reservierungen und Veranstaltungen

Je größer und qualitativer die gastronomischen Angebote eines Bergbahnunternehmens sind, desto häufiger werden diese Angebote in der Praxis auch für Tischreservierungen und private Feiern und Veranstaltungen genutzt.

Zur Abwicklung solcher Reservierungen und Veranstaltungen werden zwangsläufig personenbezogene Daten verarbeitet. Dies gilt einerseits für die Personen, die das Angebot in Anspruch nehmen (von ihnen werden z.B. Name, Kontaktdaten und nähere Details zur Reservierung oder Veranstaltung erfasst), andererseits auch für hinzugezogene Dienstleister wie Musikanten (von diesen Personen werden z.B. Name, Kontaktdaten, nähere Informationen zu ihrer Dienstleistung und Honorarhöhen) verarbeitet.

2.6 Handel

Führen Bergbahnen selbst Handelsbetriebe (z.B. Merchandising- und Sportartikelhandel, Onlineshop), sind sie in Bezug auf mögliche Datenverarbeitungen selbst „Verantwortlicher“ im Sinn der DSGVO.

Werden entsprechende Betriebe ausgelagert, so ist in der Regel der Pächter datenschutzrechtlich verantwortlich in Bezug auf die Verarbeitung von Kundendaten.

2.6.1 Merchandising- und Sportartikel

Werden vom Seilbahnunternehmen Merchandising- und Sportartikel verkauft, so werden außerhalb der Barbezahlung (anonymes Zug um Zug Geschäft) – so wie in der Gastronomie –personenbezogene Daten der Kunden (insbesondere Bankomat- oder Kreditkartendaten) verarbeitet.

2.6.2 Online-Shop

Beim Bezug von Artikeln über einen Online-Shop des Seilbahnunternehmens kommt es in jedem Fall zur Erfassung von personenbezogenen Daten der Kunden im Rahmen der Bankomat- oder Kreditkartenzahlung.

Darüber hinaus können bei Online-Shops auch **Cookies** eingesetzt werden, mit denen IP-Daten des Kunden (personenbezogene Daten) gespeichert werden.

2.6.3 Verleih

Beim Verleih von Sportgeräten und -ausrüstung wird neben Stammdaten und Kontaktdaten des Kunden in der Regel auch die Kopie eines amtlichen Lichtbildausweises (Pass, Personalausweis, Führerschein) abgelegt bzw. eingescannt gespeichert.

Werden in Kooperation mit Schiherstellern und Sporthäusern **Testtage** durchgeführt, ist entscheidend mit welchem Unternehmen das Verleihgeschäft zustande kommt. In der Praxis ist dies oftmals der Schihersteller oder das Sporthaus, dieses Unternehmen trifft dann in der Regel auch die wesentlichen Entscheidungen zur Datenverarbeitung. Es wird damit zum „Verantwortlichen“ im Sinn der DSGVO.

Wird das Seilbahnunternehmen vom Schihersteller oder Sporthaus mit dem Verleih und der Datenerhebung vor Ort beauftragt, kann es zum Auftragsverarbeiter des Verantwortlichen werden (siehe dazu oben Punkt 1.4).

2.7 Kassa

Beim Verkauf von Schikarten und -pässen werden unterschiedlichste Systeme, zumeist auch parallel, eingesetzt. Wichtige Bezugssysteme sind:

2.7.1 Verkauf vor Ort

Der direkte Verkauf von Schikarten und –pässen an den Kassen des Seilbahnunternehmens geht regelmäßig mit der Verarbeitung personenbezogener Daten von Kunden einher.

Zunächst kann es bei Bankomat- oder Kreditkartenzahlungen zur Erfassung von personenbezogenen Daten kommen. Jedenfalls aber dann, wenn Saison- und Jahreskarten erworben werden. In diesen Fällen werden zumindest Name, Anschrift und Bankverbindung des Kunden erfasst, auch ein Foto des Kunden wird gespeichert.

Bei **Saison- und Jahreskarten** kommt darüber hinaus eine Verarbeitung sensibler Gesundheitsdaten in Betracht, und zwar dann, wenn verunfallte bzw. verletzte Kunden unter Nachweis entsprechender Atteste ihre Karten vorzeitig zurückgeben können.

2.7.2 Online-Verkauf

Im Wege des Online-Bezugs von Schikarten und –pässen kommt es bei Bankomat- oder Kreditkartenzahlungen zur Erfassung von personenbezogenen Daten der Kunden.

2.7.3 Dezentrale Kassensysteme

Werden Schikarten- und –pässe in umliegenden Hotels zum Kauf angeboten, werden zum Zweck der Zahlungsabwicklung wiederum personenbezogene Daten der Gäste verarbeitet. Anderes würde nur gelten, wenn im Hotel Tageskarten bar erworben werden können (anonymes Zug um Zug Geschäft) und keine personenbezogenen Daten an das Seilbahnunternehmen weitergegeben werden.

2.7.4 Poolkarten

Beim Erwerb von regionalen und überregionalen Poolkarten kommt es zunächst zur üblichen Datenverarbeitung, wie sie auch beim Kauf von Saison- und Jahreskarten stattfindet, die örtlich auf das betreffende Seilbahnunternehmen begrenzt sind.

Zusätzlich zu dieser Datenverarbeitung wird das Fotos des Kunden an alle anderen Poolteilnehmer übermittelt.

Auch bei regionalen und überregionalen Poolkarten können im Verletzungsfall (vorzeitiges Rückgabe der Karte) sensible Gesundheitsdaten verarbeitet werden.

2.8 Marketing

Zielgerichtete Marketingmaßnahmen sind auch für Bergbahnunternehmen unerlässlich. Dass dabei personenbezogene Daten verarbeitet werden, liegt in der Natur der Sache, wenn das Unternehmen seine Stammkunden und potentielle neue Kunden persönlich ansprechen will. Praxisrelevante Werbemaßnahmen sind:

2.8.1 Newsletter

Werden an Kunden Newsletter gesendet, werden zumindest die E-Mail Adressen und häufig auch die Namen der Kunden verarbeitet. Werden diese Werbemaßnahmen an einen professionellen Dienstleister ausgelagert, so wird dieser als Auftragsverarbeiter des Bergbahnunternehmens tätig.

Unter bestimmten Voraussetzungen können Newsletter im Rahmen der Direktwerbung ohne Einwilligung der Empfänger versendet werden (siehe 2.10).

2.8.2 Drucksorten und Internetwerbung

In Broschüren, Flyern, Magazinen oder Inseraten werden oftmals auch Fotos von Kunden veröffentlicht. Damit liegt eine Bildverarbeitung vor, die sich an potentielle Leser oder – im Fall der Internetwerbung – sogar an einen unbeschränkten Personenkreis (Internetnutzer) richten.

Der Verwendung von Fotos zu Werbe- und Repräsentationszwecken und dem damit einhergehenden **„Recht am eigenen Bild“** der betroffenen Person muss dabei **besondere Beachtung** geschenkt werden, da diese Form der Datenverarbeitung eine Einwilligung der betroffenen Gäste voraussetzt (siehe 3). Verstöße dagegen können nicht nur urheberrechtliche Konsequenzen nach sich ziehen, sondern sind – wegen Verletzung der Privatsphäre - auch mit Geldbußen nach der DSGVO bedroht.

Besuchen Kunden und Interessierte die Webseiten oder Social Media Plattformen des Seilbahnunternehmens, werden in der Regel auch **Cookies** und **Webtracking-Tools** eingesetzt. In der Regel werden dabei automatisch personenbezogene Daten der Internetnutzer (konkret IP-Daten) verarbeitet. Die betroffenen Personen müssen in diese Datenverarbeitung einwilligen.

2.8.3 Gewinnspiele

Werden Gewinnspiele veranstaltet (in der Praxis häufig in Sozialen Medien), werden zumindest die E-Mail Adressen und gegebenenfalls weitere personenbezogene Daten der Teilnehmer verarbeitet. Für diese Datenverarbeitung wird – so wie für jede andere Datenverarbeitung – eine Rechtsgrundlage benötigt (siehe 3).

Wird zur Durchführung der Gewinnspiele ein externer Dienstleister herangezogen, wird dieser als Auftragsverarbeitet des Seilbahnunternehmens tätig.

2.9 Personal

Mitarbeiter spielen im Datenschutz gleich eine doppelte Rolle. Einerseits verarbeiten Seilbahnunternehmen personenbezogene Daten ihrer Mitarbeiter, andererseits sind es gerade die Mitarbeiter, die im Auftrag des Seilbahnunternehmens Daten verarbeiten. Aus diesem Blickwinkel ergeben sich gleich mehrere Ansatzpunkte für den Datenschutz.

Es gibt kein eigenständiges österreichisches Mitarbeiterdatenschutzrecht. In der Personalverwaltung werden Daten von potenziellen, bestehenden und auch ehemaligen Mitarbeitern verarbeitet. Sämtliche in diesem Leitfaden beschriebene Grundsätze sind daher auch im Personalbereich anzuwenden. Seilbahnunternehmen mit **Betriebsrat** müssen zusätzlich das Arbeitsverfassungsgesetz (ArbVG) beachten. Unerheblich ist, ob die Mitarbeiterdaten EDV-mäßig oder in Papierform verarbeitet werden.

Zur Analyse der Rechtmäßigkeit der Mitarbeiterdatenverarbeitung (siehe auch 3.2) macht es einen Unterschied, ob es sich um **Bewerber**, um **aktuelle** oder **ausgeschiedene Mitarbeiter** handelt.

2.9.1 Bewerber

Personenbezogene Daten von Bewerbern dürfen im Unternehmen nur denjenigen Personen **zugänglich** gemacht werden, die mit dem Bewerbungsverfahren beauftragt sind. In der Regel ist der Arbeitgeber, die/der zukünftige Vorgesetzte beispielsweise als Abteilungsleiter der Bewerber und die Personalabteilung für Aufnahmeprozesse von neuen Mitarbeitern zuständig.

Mit der Besetzung einer **ausgeschriebenen Stelle** ist der Zweck der Verarbeitung personenbezogener Daten der abgewiesenen Stellenbewerber erfüllt. Schadenersatzansprüche wegen behaupteter Diskriminierung im Rahmen des Bewerbungsverfahrens können innerhalb von 6 Monaten ab Absage geltend gemacht werden, weshalb die Aufbewahrung sämtlicher Bewerbungsunterlagen für diesen Zeitraum (zuzüglich einer angemessenen Zeit für den Postlauf) jedenfalls zulässig ist. Auch bei **Initiativbewerbungen** erscheint diese Speicherdauer legitim.

Eine Aufbewahrung der Eckdaten der Bewerbung (Stammdaten des Bewerbers, Stelle, Bewerbungszeitpunkt) wird wohl mit dem ursprünglichen Zweck vereinbar sein und damit im berechtigten Interesse des Seilbahnunternehmens liegen.

Soll der Bewerber in **Evidenz für zukünftige Stellenbesetzungen** gehalten oder überhaupt die Bewerbung innerhalb des Konzerns oder gar an andere Seilbahnunternehmen **weitergeleitet** werden, so ist jeweils eine Einwilligung des Betroffenen einzuholen.

Problematisch scheinen **Background-Checks** des Bewerbers zu sein. Allgemeine Internetrecherchen („Googeln“) sind generell zulässig. Dies gilt auch für **vom Bewerber offensichtlich selbst veröffentlichte Daten** im Rahmen „privater“ sozialer Medien (siehe auch 3.2.8). Die Weiterverarbeitung (Speicherung) und Nutzung muss aber wohl für das Dienstverhältnis und seine Begründung notwendig sein. Im Detail sind allerdings viele Abgrenzungsfragen zu beachten.

2.9.2 Personalverwaltung

Zulässig ist die Verarbeitung sämtlicher Daten, soweit dies zur Durchführung der Lohn- und Gehaltsabrechnung, Mitarbeiterführung, Personalplanung, Personalentwicklung usw. notwendig ist.

2.9.2.1 Personalakten

Eine **Personalakte** ist eine in Papierform abgelegte oder in elektronischer Form gespeicherte Sammlung von Unterlagen („digitale Personalakte“), die das Seilbahnunternehmen über einen Mitarbeiter führt und die Angaben zur Person und zum Arbeitsverhältnis im Betrieb enthält. Weder die Form noch der Inhalt von Personalakten sind gesetzlich geregelt.

Typische Arten von **Dokumenten**, die sich in Personalakten befinden, sind beispielsweise: Bewerbungen, Zeugnisse, Dienstverträge, Vereinbarungen, Ausweise, Meldezettel, Kursbestätigungen/Zertifikate, Pendlerpauschale, AV/AE-Formulare, (Versicherungs-)Polizzen, Pensionskassa, Protokolle (Mitarbeitergespräch, Personalmeetings), Lohnzettel (L16), Arbeitsbescheinigungen, Nettozettel, Lohnkonto, Reisekostenabrechnungen.

Festzustellen ist, dass in der Praxis oft viele Dokumente in Personalakten archiviert sind, die in diesen gar nicht aufgehoben werden sollten, etwa veraltete Strafregisterauszüge, Gesundheitszeugnisse, Dokumente über familiäre Anlässe, sogar alte Pläne über private Bauvorhaben von Arbeitnehmern wurden schon gesichtet. Daher sollten nicht benötigte Dokumente aus dem Personalakt entfernt werden.

Grundsätzlich könnte man die **Register** des Aktes (auch in elektronischer Form) z.B. in folgende Bereiche **gliedern:** Bewerbungsunterlagen, Aus- & Weiterbildung, Vertragsunterlagen, Beurteilungen, (gesetzlich vorgeschriebene) Aufzeichnungen, Kopien von Urkunden, Dokumente (sofern für Entgelt oder arbeitsvertragliche Regelungen von Bedeutung), weitere Unterlagen für Steuer und Sozialversicherung. Weitere jeweils spezifisch notwendige Kategorien sind natürlich denkbar.

Der **Zugriff** auf Personalakten ist auf einen möglichst kleinen Kreis an Personen zu beschränken. Papierakten sind sicher zu verwahren. Ebenso sind digitale Personalakten abzusichern.

2.9.2.2 Zeiterfassung

Das Seilbahnunternehmen ist verpflichtet, die geleistete Arbeitszeit seiner Mitarbeiter aufzuzeichnen. Es handelt sich um die Erfüllung gesetzlicher Verpflichtungen, weshalb dies grundsätzlich (z.B. mittels Chip) unproblematisch ist. Werden jedoch Systeme benutzt, die die Menschenwürde berühren (z.B. Erfassung biometrischer Daten anhand Fingerprint- oder Iris-Scanner) handelt es sich um eine zustimmungspflichtige Maßnahme (Einwilligung des einzelnen Mitarbeiters oder durch Betriebsvereinbarung).

2.9.2.3 Lohn- / Gehaltsabrechnung

Bei der **Weitergabe von Gehaltsdaten an externe Stellen** ist zu unterscheiden, ob diese notwendig ist, ob es gesetzliche Vorschriften gibt oder ob andere Gründe für die Weitergabe vorliegen.

Gehaltsdaten müssen an die Bank, die die Gehaltsüberweisung durchführt, weitergegeben werden, ebenso wie an die Sozialversicherungsträger zur Bestimmung der Sozialversicherungshöhe. Im ersten Fall liegt die Weitergabe im Interesse des Betroffenen, im zweiten Fall bestehen gesetzliche Vorschriften.

Zusätzlich darf das Seilbahnunternehmen zur Erfüllung seiner Aufgaben oder auch zu Controllingzwecken interne und externe Stellen (Steuerberater, Rechtsanwälte...) heranziehen. Diese dürfen Daten nur in Hinblick auf den übertragenen Verwendungszweck verwenden und unterliegen der Verschwiegenheitspflicht. Werden die Daten im Auftrag des Seilbahnunternehmens verarbeitet ist eine Auftragsverarbeitervereinbarung abzuschließen.

2.9.2.4 Lohn-/Gehaltszettel

Dem Mitarbeiter ist bei Fälligkeit des Entgelts eine schriftliche, übersichtliche, nachvollziehbare und vollständige Abrechnung von Entgelt und Aufwandsentschädigungen zu übermitteln. Die Abrechnung kann auch auf elektronischem Weg zur Verfügung gestellt werden.

Lohn- bzw. Gehaltszettel können im Einzelfall eine Reihe von Informationen enthalten, an denen nach allgemeiner Lebenserfahrung ein erhebliches Geheimhaltungsinteresse des Betroffenen anzunehmen ist. Das Seilbahnunternehmen hat darauf zu achten, dass der Lohn- bzw. Gehaltszettel nur demjenigen übermittelt wird, den er betrifft.

2.9.2.5 Mitarbeiterausweise, Mitarbeiterfotos

Das Veröffentlichen von Namens- und Kontaktdaten z.B. auf der Firmenwebsite ist anhand der Aufgabe des Mitarbeiters am Vorliegen eines berechtigten Interesses zu messen. Ebenso ist bei anderen Veröffentlichungen vorzugehen, wie z.B. bei verpflichtenden Namensschildern. Ob die Veröffentlichung von Fotos bzw. Videos von Mitarbeitern auf ein berechtigtes Interesse gestützt werden kann, ist fraglich. Im Zweifel ist die Einwilligung des Betroffenen einzuholen.

2.9.2.6 Überwachungs- und Kontrollmaßnahmen, Mitwirkung des Betriebsrates

Aus dem Arbeitsvertrag ergibt sich das Recht des Seilbahnunternehmens, die Einhaltung der arbeitsrechtlichen Pflichten durch den Mitarbeiter zu kontrollieren. Die **Kontrolle von Leistung und Verhalten des Mitarbeiters** ist dementsprechend legitim.

Das Seilbahnunternehmen muss dem Betriebsrat mitteilen, welche Arten von personenbezogenen **Mitarbeiterdaten** er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht. Da gegenüber den Mitarbeitern selbst eine **Datenschutzerklärung** abgegeben werden muss (siehe Muster 5.2.1), verursacht diese Pflicht dem Seilbahnunternehmen keinen großen Mehraufwand.

Zusätzlich zu den Informationen über die Datenkategorien kann der Betriebsrat verlangen, dass ihm die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung der Arbeitnehmerdaten ermöglicht wird.

Der Betriebsrat ist berechtigt, in die vom Betrieb geführten **Aufzeichnungen** über die Bezüge der Arbeitnehmer und die zur Berechnung dieser Bezüge erforderlichen Unterlagen **Einsicht zu nehmen**, sie zu überprüfen und die Auszahlung zu kontrollieren. Dies gilt auch für andere die Arbeitnehmer betreffenden gesetzlich vorgeschriebenen Aufzeichnungen. Sofern sich ein unbeschränktes Einsichtsrecht des Betriebsrates nicht aus Rechtsvorschriften ergibt, ist zur Einsicht in die Daten einzelner Arbeitnehmer deren **Zustimmung** erforderlich.

Zur **Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren**, ist eine Betriebsvereinbarung notwendig. Für Betriebe, in denen kein Betriebsrat eingerichtet ist, muss hingegen (im Rahmen des Dienstvertrages bzw. Sideletters des Dienstvertrages) die Zustimmung jedes einzelnen Mitarbeiters eingeholt werden.

Ein Beispiel einer Kontrollmaßnahme, die die Menschenwürde berühren kann, ist die Videoüberwachung (siehe 2.11). Ob die Menschenwürde im Einzelfall berührt wird, hängt ab von:

- **Kontrolldichte/Häufigkeit** der durchgeführten Maßnahmen hinsichtlich Zeit, Ort und Umfang (stichprobenartige Kontrolle des Internetverhaltens ist unbedenklich)
- **Eingriffsidentität** (eine unzulässige Videoüberwachung besteht beispielsweise, wenn neben dem Eingang auch der gesamte Eingangsbereich mit den dort befindlichen Arbeitsplätzen permanent überwacht würde)
- **Objektive Eignung** zur Berührung der Menschenwürde (z.B. Navigationsgeräte in Firmenfahrzeugen lassen Rückschlüsse auf das Verhalten der Mitarbeiter während Außendienste zu)

Unzulässig ist eine Videoüberwachung (nur) zum Zweck der Mitarbeiterkontrolle, also die gezielte Überwachung von Mitarbeitern in Arbeitsstätten. Dieses Verbot schließt allerdings die Überwachung von Kassenräumen, die Überwachung gefährlicher Maschinen usw. nicht ein, da derartige Überwachungen nicht auf die Leistungskontrolle der Beschäftigten gerichtet ist. Die Überwachung der Mitarbeiter stellt nur einen nicht vermeidbaren, unbedeutenden Nebeneffekt dar bzw. kommt übergeordneten Interessen (z.B. Arbeitnehmerschutzbelangen) zugute.

2.9.3 Verpflichtung zum Datengeheimnis

Mitarbeiter sind verpflichtet, Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, geheim zu halten, außer es besteht ein zulässiger Grund zur Weitergabe der Daten (Datengeheimnis).

Seilbahnunternehmen haben ihre Mitarbeiter, sofern eine solche Verpflichtung nicht schon kraft Gesetzes besteht (z.B. bei Ärzten), **vertraglich zu verpflichten**, personenbezogene Daten aus Datenverarbeitungen nur **aufgrund von Anordnungen** zu übermitteln und das **Datengeheimnis** auch nach Beendigung des Arbeitsverhältnisses einzuhalten.

Die einfachste Form ist, die Mitarbeiter eine **Kopie des § 6 DSG 2018** unterschreiben zu lassen und diese zu Dokumentationszwecken entweder im Personalakt oder in der datenschutzrechtlichen Dokumentation abzulegen. Der Gesetzestext ist allerdings ungeeignet, Mitarbeiter darüber zu informieren, was im Zusammenhang mit der betrieblichen Datenverarbeitung zulässig und erwünscht ist, bzw. welche Handlungen – vor allem in datenschutzrechtlicher Hinsicht - zu unterlassen sind. Die mit der Datenverarbeitung betrauten Mitarbeiter sind über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu **belehren**.

Wesentlich tauglicher geschieht dies im Rahmen einer **Klausel im Arbeitsvertrag** oder einer vom Mitarbeiter gegenzuzeichnenden **Verpflichtungsvereinbarung**. (siehe auch Muster 5.2.2)

Unabhängig von dieser Belehrung bzw. auch ohne diese Belehrung können jedoch Verletzungen des Datengeheimnisses den Tatbestand arbeitsrechtlicher **Entlassungsgründe** erfüllen.

2.9.4 Privatnutzung von Internet (Social Media) und Handy

Die Privatnutzung von Betriebsmitteln, wie etwa von Firmen-PC, Internet, Firmen-WLAN mit einem Privatgerät, Telefon und Kopierer, kann ausdrücklich genehmigt, schlüssig vereinbart oder verboten sein. Es kann eine entsprechende, erzwingbare Betriebsvereinbarung über Maßnahmen zur zweckentsprechenden Benützung von Betriebseinrichtungen und Betriebsmitteln abgeschlossen werden.

Auch bei durch das Seilbahnunternehmen **erlaubter Privatnutzung**, hat der Mitarbeiter darauf zu achten, dass dadurch

- seine Arbeit nicht beeinträchtigt,
- die für betriebliche Zwecke vorgesehenen Speichermöglichkeiten nicht unzumutbar stark belastet werden,
- keine Sicherheitsrisiken (z.B. Gefahr eines Virenimports) und
- keine finanziellen Belastungen für den Betrieb geschaffen werden dürfen.

Hat das Seilbahnunternehmen die Privatnutzung **ausdrücklich verboten**, muss gemäß bestehender Rechtsprechung dennoch eine solche in geringem Umfang für kurze, unbedingt erforderliche Mitteilungen geduldet werden.

Die übermäßige Privatnutzung kann jedenfalls einen Entlassungsgrund darstellen („täglich mind. 1,5h Internetznutzung, privates Surfen und Download umfangreicher Film- und Musikdateien“.

Überwachung der Internet- und E-Mail-Nutzung durch das Seilbahnunternehmen

Die Überwachung ist in Österreich ohne Betriebsvereinbarung oder (in Betrieben ohne BR) ohne Zustimmung des einzelnen Mitarbeiters grundsätzlich nicht möglich, außer es liegt ein **konkreter Verdacht auf eine strafbare Handlung** bzw. sonstige mögliche Schädigungen (Viren, extremes Datenvolumen, Versand von Kundendaten etc.) vor. Das „Mit-Lesen“ privater E-Mails ist grundsätzlich nicht erlaubt. In begründeten Einzelfällen ist eine individuelle, spontane Kontrolle zulässig.

Bring your own device

Damit ist der Einsatz privater Geräte von Mitarbeitern für berufliche Tätigkeiten gemeint. Neben datenschutzrechtlicher Probleme wirft dies vor allem Fragen der Datensicherheit auf.

2.9.5 Schulung und Sensibilisierung von Mitarbeitern, Datenschutzrichtlinie

Das Seilbahnunternehmen ist für die nachweisliche Einhaltung der Datenschutz- und Datensicherheitsmaßnahmen verantwortlich. Da Mitarbeiter diejenigen sind, die tatsächlich Daten verarbeiten, dürfen diese Daten nur auf Anordnung verarbeiten. Grundsätzlich ist diese Weisung bereits im Arbeitsvertrag vereinbarten Tätigkeit bzw. Stellenbeschreibung enthalten.

Um die Einhaltung dieser Verpflichtung gewährleisten zu können, hat das Seilbahnunternehmen seine Mitarbeiter tätigkeitsbezogen zu schulen und zu sensibilisieren. Es empfiehlt sich die Entwicklung einer

generellen Dienstanweisung (Datenschutzrichtlinie) auf Basis der im Verarbeitungsverzeichnis enthaltenen Datenverarbeitungen. Wie diese Belehrung auszusehen hat, bzw. welche Schulungsmaßnahmen sinnvoll sind, ergibt sich aus dem jeweiligen Unternehmen selbst. Tipps und Vergleiche finden sich unter www.it-safe.at.

2.9.6 Ausgeschiedene Mitarbeiter

Mit dem Ausscheiden des Mitarbeiters ist der Zweck der Verarbeitung der Mitarbeiterdaten erfüllt. Geregelt sollte die Dauer der Speicherung der Personalakten werden. Es gibt keine generelle gesetzliche Vorschrift, weshalb sich das Seilbahnunternehmen am besten an den gesetzlichen Aufbewahrungs- und Verjährungsfristen orientieren kann. Zweckmäßig erscheint, jedenfalls nicht mehr benötigte Teile des Aktes auszuscheiden und zu vernichten.

Fragen wirft auch der Umgang mit **e-mail-Accounts** und auf den firmeneigenen Geräten gespeicherte private Dateien nach Beendigung des Arbeitsverhältnisses auf. Mangels gesetzlicher Vorgaben ist die Vereinbarung einer Vorgangsweise (individuell oder mittels Betriebsvereinbarung) zu empfehlen.

2.9.7 Datenverarbeitung durch den Betriebsrat

Für Datenverarbeitungen die vom Betriebsrat betrieben werden ist dieser selbst und nicht das Seilbahnunternehmen verantwortlich.

2.10 Direktwerbung

Als Direktwerbung wird jede Äußerung des Seilbahnunternehmens an ausgewählte Personen oder Personengruppen bezeichnet, die den Absatz von Waren oder die Erbringung von Dienstleistungen des eigenen Unternehmens fördern soll. Darunter fallen auch Marketingtätigkeiten und solche Maßnahmen, welche die Inanspruchnahme einer Leistung lediglich anregen, wie beispielsweise Informations-Mails, telefonische Zufriedenheitsumfragen oder *Newsletter*.

Grundsätzlich darf jedes Unternehmen zum Zwecke der Direktwerbung personenbezogene Daten von betroffenen Personen, mit denen sie in einer maßgeblichen und angemessenen Beziehung stehen, **ohne deren Einwilligung**, gesetzlicher Ermächtigung o.ä. verarbeiten. Eine solche Beziehung besteht u.a. dann, wenn die betroffene Person schon **Kunde** ist oder in den Diensten des Unternehmens steht. Der Betroffene muss jedoch im Zeitpunkt der Erhebung der personenbezogenen Daten angesichts der dabei vorliegenden Umstände vernünftigerweise vorhersehen können, dass künftig eine Verarbeitung zu diesem bestimmten Zweck erfolgen könnte. Sensible Daten dürfen in der Regel nicht für Direktwerbung genutzt werden.

Der Betroffene hat das Recht, jederzeit unentgeltlich **Widerspruch** gegen die Verarbeitung der personenbezogenen Daten zum Zwecke der Direktwerbung zu erheben. Das gilt auch für das Profiling, soweit es mit einer Direktwerbung in Verbindung steht. Auf das Widerspruchsrecht ist der Betroffene in verständlicher und von anderen Informationen getrennter Form zum Zeitpunkt der ersten Kommunikation

ausdrücklich hinzuweisen. Wenn ein Widerspruch erfolgt, dürfen die Daten nicht mehr zum Zweck der Direktwerbung verarbeitet werden bzw. müssen gelöscht werden, wenn ansonsten keine Rechtmäßigkeit der Datenverarbeitung mehr besteht.

Bei Direktwerbungen mittels elektronischer Post (E-Mail, Newsletter, SMS, Social Media) müssen auch die Voraussetzungen des Telekommunikationsgesetzes eingehalten werden.

Danach ist eine solche Direktwerbung ohne vorherige Zustimmung des Empfängers nur dann zulässig, wenn der Absender die personenbezogenen Daten (insb. die E-Mail-Adresse) im Zusammenhang mit dem Verkauf einer Ware oder der Erbringung einer Dienstleistung an seine Kunden erhalten hat und die Werbemaßnahme sich auf eigene ähnliche Produkte oder Dienstleistungen bezieht. Gleiches gilt für bereits bestehende Lieferantenbeziehungen, da zwischen den Verhältnissen „B2C“ und „B2B“ grundsätzlich keine unterschiedlichen Zulässigkeitsvoraussetzungen für Direktwerbung bestehen.

Kunden dürfen die Zusendung auch nicht im Vorhinein abgelehnt haben (insb. durch Eintragung in der sog. „ECG-Liste“). Weiters muss die betroffene Person sowohl bei der Erhebung als auch bei jeder erneuten Zusendung die Möglichkeit erhalten, den künftigen Empfang solcher Werbungen kostenfrei und problemlos abzulehnen.

Werbung durch elektronische Kommunikation (Werbe-E-Mail) muss als solche – im Betreff – gekennzeichnet und die Identität des Absenders ersichtlich sein. Falls keine aufrechte Kundenbeziehung oder Lieferantenbeziehung besteht, ist vor der erstmaligen Zusendung einer Direktwerbung vom Empfänger dessen Einwilligung einzuholen (z.B. schriftlich oder durch Ankreuzen einer Check-Box).

Jeder Newsletter, sofern dieser mindestens viermal im Kalenderjahr in vergleichbarer Gestaltung elektronisch verbreitet wird, hat überdies ein Impressum zu enthalten. In diesem sind Name bzw. Firma sowie Anschrift des Medieninhabers und des Herausgebers (sofern dieser vom Medieninhaber verschieden ist) anzuführen. Zudem sind folgende Angaben (falls vorhanden) seitens des Unternehmens offenzulegen: Firma, Sitz, Unternehmensgegenstand, grundlegende Richtung des Newsletters, vertretungsbefugte Organe und Mitglieder des Aufsichtsrates, Beteiligungsverhältnisse der Gesellschafter inkl. deren Beteiligungshöhe, Treuhandverhältnisse bzw. stille Beteiligungen, Vereinszweck, Stifter und Begünstigte.

2.11 Bildverarbeitung

Teile der bisherigen Bestimmungen des DSG 2000 zur „Videoüberwachung“, nämlich im Wesentlichen die Protokollierungspflicht, die grundsätzliche Löschungspflicht nach 72 Stunden sowie die Kennzeichnungspflicht, wurden inhaltsähnlich in das neue DSG 2018 (unter der Überschrift „Bildverarbeitung“) übernommen. Sowohl die Meldepflicht an das Datenverarbeitungsregister, als auch die Vorabkontrolle durch die Datenschutzbehörde und die Möglichkeit der Hinterlegung eines Schlüssels bei der Daten-

schutzbehörde sind entfallen. Da das DSG 2018 der Durchführung der DSGVO dient, sind die dort enthaltenden Bestimmungen (insb. Verarbeitungsverzeichnis, Datenschutz-Folgenabschätzung, Rechte der betroffenen Person und Pflichten des Verantwortlichen) auch bei der Bildverarbeitung unmittelbar anwendbar. Zudem sind die Bestimmungen des österreichischen Arbeitsrechtes (insb. die Verpflichtung zum Abschluss einer Betriebsvereinbarung/ individuelle Zustimmung aller Arbeitnehmer, wenn durch Bildaufnahmen eine Kontrolle von Arbeitnehmern *abstrakt möglich* ist) einzuhalten.

Unter „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, zu verstehen (Seilbahnunternehmen).

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“, also alle natürlichen Personen, die in Bildaufnahmen unmittelbar oder mittelbar erfasst werden).

2.11.1 Definition „Bildaufnahme“

Unter einer "Bildaufnahme“ ist „die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nichtöffentlichen Raum zu privaten Zwecken“ zu verstehen.

Darunter fallen grundsätzlich **alle Bildaufnahmen durch Verantwortliche des privaten Bereichs**. Das bedeutet, dass nicht wie bisher nur Videoaufnahmen, sondern auch das Herstellen von Lichtbildern (z.B. das Anfertigen von Fotografien zu beruflichen Zwecken) vom Geltungsbereich des DSG 2018 mitumfasst sind. Dazu zählen auch im Rahmen der Bildaufnahme „mitverarbeitete akustische Informationen“, also mit Videoaufzeichnung allenfalls verbundene Tonaufnahmen. Bereits Aufzeichnungen, welche nicht auf eine Überwachung abzielen, sondern bloß ein **bestimmtes Objekt oder eine bestimmte Person** zum Inhalt haben, fallen in den Anwendungsbereich des DSG 2018.

Es ist ferner unbeachtlich, ob die Bildaufnahme im öffentlichen oder nichtöffentlichen Raum erfolgt. Bildaufnahmen, die ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgen (Freizeit, Urlaub ect.) sowie die damit zusammenhängende Nutzung von sozialen Netzwerken und Onlinetätigkeiten, sind davon klarerweise ausgenommen. Unter dem Begriff “Ereignis“ wird das Festhalten von einer zu erwartenden und beobachtbaren Veränderung in der Außenwelt (= Geschehen) verstanden. Diese weitgefasste Wortauslegung umfasst beispielsweise bereits mobile Videoaufzeichnungen, wie das Filmen einer Ski-Abfahrt mit einer Action-Cam.

2.11.2 Zulässigkeit der Bildaufnahme

Eine Bildaufnahme ist zulässig, wenn

- sie im lebenswichtigen Interesse einer Person erforderlich ist,

- die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
- sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist,

oder (die für Seilbahnunternehmen relevante Zulässigkeitsvoraussetzung)

- im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

Ein überwiegendes berechtigtes Interesse des Verantwortlichen besteht u.a. dann, wenn die Bildaufnahme ein **privates Dokumentationsinteresse** verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

Zudem liegt ein überwiegendes berechtigtes Interesse des Verantwortlichen vor, wenn die Bildaufnahme für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, erforderlich ist. Die Erforderlichkeit liegt bei bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotentials vor, wenn kein gelinderes geeignetes Mittel zur Verfügung steht.

Damit werden insbesondere auch die bisherigen geltenden Standardanwendungen zur Videoüberwachung (SA 032 der Standard- und Musterverordnung 2004, u.a. **Parkgaragen und –plätze**) sowie Bildaufnahmen **in öffentlichen Verkehrsmitteln** (zu welchen auch Seilbahnen zählen) erfasst.

Die Zulässigkeit aller anderen Bildaufnahmen durch Seilbahnunternehmen ist **im Einzelfall** anhand der o.a. gesetzlichen Bestimmungen zu überprüfen. Hierbei kommt es u.a. auf die genaue technische Ausgestaltung jeder einzelnen (Video-)Kamera, den genauen Bildausschnitt sowie die Erkennbarkeit von Einzelpersonen an. Ratsam ist die Einholung bisheriger eigener DVR-Meldungen via DVR-Online um der Verpflichtung zur Führung eines Verarbeitungsverzeichnisses nachzukommen, sofern alle bisherigen Video- und Kameraüberwachungsanlagen rechtmäßige Datenverarbeitungen i.S.d. DSGVO bzw. DSG darstellen.

Durch den Kauf eines Skipasses kommt es zwischen dem Kunden und dem Seilbahnunternehmen zum Abschluss eines Beförderungsvertrages. Das Seilbahnunternehmen treffen gewisse vertragliche Nebenpflichten wie u.a. die Sicherheit und den Schutz des körperlichen Wohlbefindens seiner Fahrgäste bereits durch das gefahrlose Ein- und Aussteigen der Fahrgäste zu gewähren. Im Rahmen des Verantwortungsschutzes und zum allfälligen Zweck des Eigenschutzes (des Eigentums oder der Mitarbeiter des Seilbahnunternehmens) sowie zum allfälligen Zweck der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens könnten **Bildaufnahmen an den Zu- bzw. Abgängen der Seilbahnen** als zulässig erachtet werden.

Bildaufnahmen an den Kassen, die den Kauf eines Skipasses aufzeichnen, könnten zum Schutz des Eigentums des Seilbahnunternehmens, sohin also zum Eigenschutz, sowie zum allfälligen Zweck der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens als zulässig erachtet werden.

Auch **Echtzeitübertragungen** und **Bildaufnahmen mittels Webcams, bei denen keine Aufzeichnung der gesendeten Bilder erfolgt** könnten durch das Bestehen eines überwiegenden berechtigen Interesses des Seilbahnunternehmens zur Erfüllung seines Verantwortungsschutzes (Wegehalterhaftung betreffend Pisten) sowie eines überwiegenden berechtigten Interesses Dritter, nämlich potentieller Kunden von Skipässen sowie zum allfälligen Zweck der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens als zulässig erachtet werden. Jedenfalls empfehlenswert ist hierbei der Einsatz technischer Maßnahmen, durch welche die Identifizierung von Personen ausgeschlossen wird (z.B. „Verpixelung“ oder niedrige Bildschärfe).

Zutrittskontrollen mit Bildvergleich, also Bildaufnahmen, die beim Passieren des Drehkreuzes erfolgen (=Kontrollfoto) und mit dem jeweiligen Referenzfoto, welches beim Kauf des Skipasses aufgenommen wird, auf Übereinstimmung verglichen werden, sind laut rechtlicher Beurteilung der Datenschutzbehörde (allerdings an Hand der alten Rechtslage des DSG 2000) unter Einhaltung nachfolgender Voraussetzungen zulässig:

- Einsatz nicht bei allen Liftanlagen des Skigebietes, sondern nur an einigen speziellen Einstiegsstellen (z.B. Talstation)
- Verschlüsselung aller Bilddaten
- Keine Tonaufzeichnungen
- Kein automationsunterstützter Bilddatenabgleich (sondern nur durch den nächst dem Drehkreuz in einem abgeschlossenen Raum befindlichen Mitarbeiter durch persönliche Wahrnehmung am Bildschirm)
- Löschung der Referenzfotos unmittelbar nach Ende der Gültigkeitsdauer des Skipasses
- Automatische Löschung des Kontrollfotos innerhalb weniger Minuten nach Passieren des Drehkreuzes, spätestens jedoch nach 30 Minuten
- Speicherung der Zugangszeitpunkte und –orte der Liftkarte ausschließlich für Verrechnungszwecke mit anderen Skigebieten (keine Erstellung von Bewegungsprofilen der Liftkartenbenutzer)
- Alternative Möglichkeit für den Erwerb einer Liftkarte, diese technisch so zu konfigurieren, dass beim Durchschreiten des Drehkreuzes kein Foto angefertigt wird (das Referenzfoto wird bei der Kassa erstellt und wird auf der Liftkarte, nicht jedoch im Photocompare-System, gespeichert; in diesem Fall ist mit stichprobenartigen Kontrollen durch das Liftpersonal zu rechnen)

Nur wenn Zweifel an der Übereinstimmung des Referenzfotos mit dem gerade angefertigten Kontrollfoto bestehen, darf die automatische Löschung der Bilddaten verhindert werden. Wenn sich in einem solchen Anlassfall ein Verdacht nicht erhärtet, sind die Bilddaten sofort zu löschen.

2.11.3 Informations- und Kennzeichnungspflicht

Die Informationspflicht zählt zu den allgemeinen Pflichten des Verantwortlichen. Diese Informationen sind der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln und zwar in schriftlich, elektronisch oder in einer anderen Form.

Für die Informationserteilung von Zutrittskontrollen mit Bildvergleich wurde von der Datenschutzbehörde ein entsprechender Text ausgearbeitet (https://www.wko.at/branchen/transport-verkehr/seilbahnen/Rahmenbedingungen-Zutrittskontrolle.pdf).

Zudem hat der Verantwortliche die Bildaufnahme geeignet zu kennzeichnen und zwar so, dass daraus der Verantwortliche eindeutig hervorgeht, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

Die Kennzeichnung für Zutrittskontrollen mit Bildvergleich und Videoüberwachungen mittels **Hinweisschildern oder Aufklebern**, welche auf Kopfhöhe des Lesers in der Größe von mindestens 6,5 x 9 cm angebracht werden, werden als ausreichend erachtet. Darin muss noch vor dem Betreten des überwachten Bereichs und sofort erkennbar auf die Zutrittskontrolle mit Bildvergleich bzw. die Videoüberwachung hingewiesen werden. Zudem hat der Aushang eines Hinweises zu erfolgen, welcher die Identität des Verantwortlichen offenlegt und erläutert, wie detaillierte Informationen zur Zutrittskontrolle mit Bildvergleich bzw. Videoüberwachung erlangt werden können (z.B. *„Diese Seilbahnanlage wird videoüberwacht. Bei Fragen wenden Sie sich bitte an die Geschäftsleitung. Seilbahngesellschaft XY.“*).

Diese Kennzeichnungspflicht gilt nicht für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer verdeckten Ermittlung erreicht werden kann. Voraussetzung dafür ist jedoch, dass der Verantwortliche ausreichende Garantien zur Wahrung der betroffenen Interessen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

Die unbegründete Nichtkennzeichnung bzw. die mangelnde Erteilung näherer Auskünfte stellt eine Verweigerung der DSGVO-Auskunftsrechte dar, die mit einer empfindlichen Geldbuße geahndet werden kann.

2.11.4 Aufbewahrungsfrist/ Löschungspflicht

Abgesehen von den o.a. Bildaufnahmen im Rahmen von Zutrittskontrollen mit Bildvergleich dürfen Foto- und Videoaufnahmen grundsätzlich **72 Stunden** lang aufbewahrt werden. Aufgenommene personenbezogene Daten sind immer dann zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden,

nicht mehr benötigt werden und keine andere gesetzliche Aufbewahrungspflicht besteht. Eine längere Speicherung ist nur dann zulässig, wenn sie für den Verarbeitungszweck erforderlich ist, verhältnismäßig ist und gesondert protokolliert und begründet wird. Eine längere Speicherung ist außerdem dann zulässig, wenn innerhalb der regulären Speicherfrist festgestellt wird, dass die Bildaufnahme eine strafbare Handlung dokumentiert hat (z.B. Sachbeschädigung oder Diebstahl) oder wenn die Bildaufnahme zum Zweck der Aufklärung von Straftaten erfolgt, derartige Straftaten typischerweise aber erst nach mehr als 3 Tagen entdeckt werden.

2.11.5 Besondere Datensicherheitsmaßnahmen und Protokollierungspflicht

Der Verantwortliche hat *geeignete* Datensicherheitsmaßnahmen zu ergreifen und dafür sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung durch Unbefugte ausgeschlossen ist. Dieser Auflage wird man am besten durch technische Maßnahmen, wie z.B. Verschlüsselung, entsprechen können.

Zudem sind alle Verarbeitungsvorgänge (außer im Falle von Echtzeitüberwachungen bzw. Webcams, bei denen keine Aufzeichnung der gesendeten Bilder erfolgt) zu protokollieren, also festzuhalten, wann und in welcher Form die Bilddaten genutzt (etwa kopiert oder veröffentlicht) werden.

2.11.6 Auswertung von durch Bildaufnahmen gewonnener personenbezogener Daten

Eine Auswertung von Bildaufnahmen zum Schutz von Personen oder Sachen darf nur vorgenommen werden, wenn der **begründete Verdacht** besteht, dass es zu einem Angriff auf Personen oder Sachen gekommen ist. Des Weiteren darf eine Auswertung nur dann erfolgen, wenn der dafür ausschlaggebende Anlassfall vom ursprünglichen Zweck der Bildaufnahmen erfasst ist.

Es ist daher unzulässig, Bildaufnahmen ohne besonderen Grund durchzusehen oder gar auszuwerten.

2.11.7 Übermittlung und Veröffentlichung

Jedenfalls zulässig ist die **Übermittlung** von mittels Bildaufnahmen gewonnener personenbezogener Daten an eine zuständige Behörde oder ein zuständiges Gericht, wenn beim Verantwortlichen der **begründete Verdacht** besteht, die personenbezogenen Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren sowie an Sicherheitsbehörden zur Ausübung der ihnen durch das Sicherheitspolizeigesetz eingeräumten Befugnisse.

Die **Veröffentlichung** von Bildaufnahmen oder die Zugänglichmachung mittels eines Dienstes der Informationsgesellschaft (z.B. in sozialen Netzwerken im Internet) ist eingeschränkt möglich. Voraussetzend hierfür ist, dass die erfolgte Bildaufnahme nach den Bestimmungen des DSG 2018 zulässig war und die Veröffentlichung oder Zugänglichmachung im Einzelfall verhältnismäßig erscheint. (Hierbei können insbesondere die Abwägungskriterien der gesetzlichen Bestimmungen zum Bildnisschutz nach dem Urhebergesetz herangezogen werden, nämlich: Betrifft ein Beitrag oder ein Foto eine Debatte von allgemeinem Interesse? Welche Rolle oder Funktion kommt der betroffenen Person zu? Wie ist das

Verhalten der betroffenen Person vor der Veröffentlichung zu beurteilen? Wie wurde die Information beschafft? Wie ist die Art und Weise der Darstellung der betroffenen Person?). Gegebenenfalls müssen Maßnahmen zum Ausschluss der Identifizierbarkeit der betroffenen Person, beispielsweise durch „verpixeln“, erfolgen.

2.11.8 Unzulässige Bildaufnahme

Jedenfalls unzulässig ist

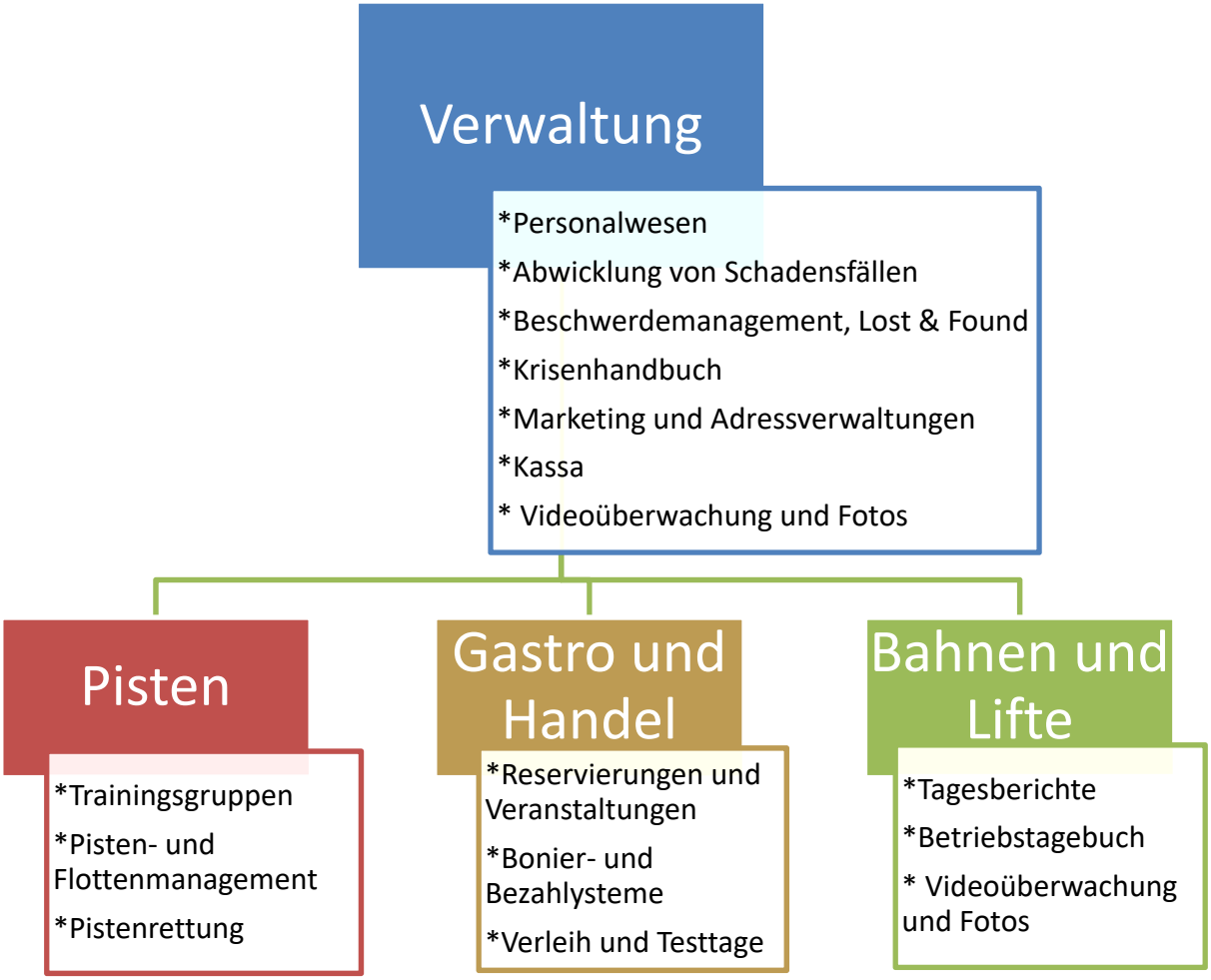
- eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichem Lebensbereich,
- eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,
- der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnen personenbezogenen Daten mit anderen personenbezogenen Daten (Achtung: Zutrittskontrollen mit Bildvergleich) oder
- die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten als Auswahlkriterium.

2.11.9 Strafbestimmungen

Wer eine Bildverarbeitung entgegen den genannten Bestimmungen betreibt, ist mit Geldstrafe bis zu € 50.000,- zu bestrafen, sofern die Tat nicht unter die Strafbestimmungen der DSGVO fällt oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

2.12 Übersicht

In der Übersicht lassen sich die aufgezeigten Datenverarbeitungen wie folgt darstellen:



2.13 Zusammengefasst

- In Seilbahnunternehmen werden in den zentralen Bereichen Verwaltung, Pisten, Bahnen und Lifte sowie Gastronomie und Handel zu unterschiedlichen Zwecken personenbezogene Daten von Gästen und Mitarbeitern verarbeitet.
- Speziell im Rahmen der Pistenrettung und bei der Abwicklung von Schadensfällen werden sensible Gesundheitsdaten (besondere Kategorien personenbezogener Daten) verarbeitet.
- Videoüberwachung wird vor allem bei Lift- und Bahnanlagen sowie in Verwaltungsgebäuden und im Kassabereich eingesetzt.
- In der Personalverwaltung finden – von der Prüfung der Bewerbung bis hin zur Durchführung von Überwachungs- und Kontrollmaßnahmen - vielfältige Datenverarbeitungen statt.

3 Keine Datenverarbeitung ohne Rechtsgrundlage

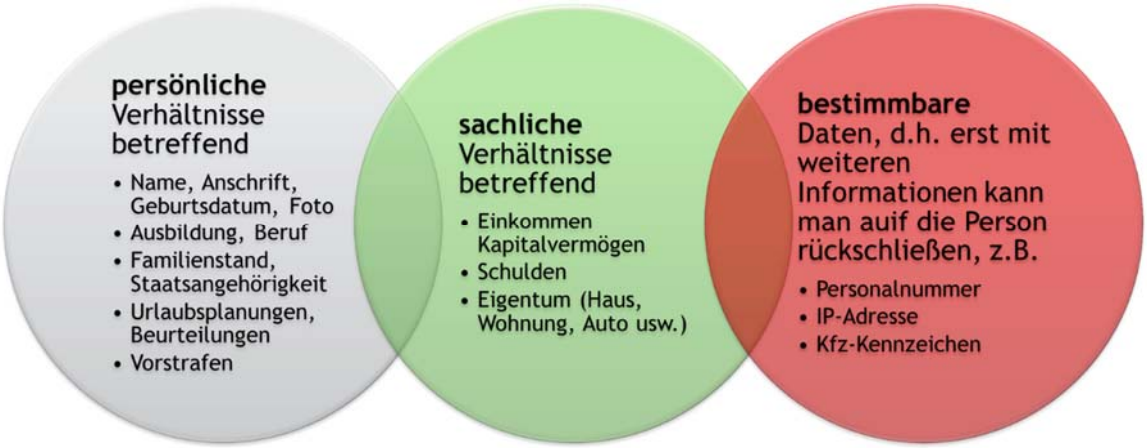
Jede Verarbeitung personenbezogener Daten durch das Seilbahnunternehmen bedarf einer Rechtfertigung. Datenverarbeitung ist verboten, außer sie ist erlaubt. Der Begriff Rechtsgrundlage bedeutet

dabei, dass ein **Erlaubnistatbestand** vorliegen muss. Man unterscheidet zwischen **„normalen", „sensiblen" (besonders geschützten) und strafrechtsrelevanten Daten**.

3.1 Unterscheidung von Datenkategorien

3.1.1 Nichtsensible personenbezogene Daten

Unter personenbezogene Daten sind alle Informationen zu verstehen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** („betroffene Person") beziehen. Darunter fallen Angaben über persönliche und sachliche Verhältnisse aber auch bloß individualisierbare Daten, also solche, die erst über Zusatzinformationen Rückschlüsse auf eine bestimmte Person ermöglichen. Die DSGVO schützt weder personenbezogene Daten juristischer Personen, noch jene bereits Verstorbener. Kein Fall für den Datenschutz sind **anonymisierte Daten** (die betroffene Person kann nicht oder nicht mehr identifiziert werden). Informationen müssen nicht unbedingt wahr oder bewiesen zu sein, damit sie als personenbezogen gelten.



„Identifiziert" ist eine Person, wenn die Daten direkt mit der betroffenen Person verbunden sind oder wenn sich ein solcher Bezug unmittelbar herstellen lässt: „Herr Max Mustermann ist unser Kunde" oder „Der Seilbahndirektor fährt einen BMW".

„Identifizierbar" ist eine Person, wenn sie mit Hilfe von „Zusatzinformationen" ausfindig gemacht werden kann. Beispiel für eine identifizierbare Person: „Der Gast mit der Jahreskarte Nummer 1234 hat heuer 25 Schitage erlebt". Zumindest für Mitarbeiter der Kundenverwaltung ist es möglich, die Kartennummer und einer Person zuzuordnen. Dabei ist es nicht ausschlaggebend, dass das Seilbahnunternehmen selbst über diese Zusatzinformationen verfügt.

Laut Europäischem Gerichtshof gilt ein Datum als personenbezogen, wenn eine Stelle „über rechtliche Mittel verfügt, die es [ihr] erlauben, die betreffende Person anhand der Zusatzinformationen […] bestimmen zu lassen" (EuGH, Urteil vom 19.10.2016, Rs. C-582/14, Rn. 49). Die „rechtlichen Mittel" sind auch gegeben, wenn man Dritte einschalten kann und diese rechtlich gezwungen sind, Auskünfte zur Identität zu geben. Um festzustellen, ob eine natürliche Person direkt oder indirekt **identifizierbar**

ist, müssen alle Mittel berücksichtigt werden, die vom Seilbahnunternehmen oder einer anderen Person **nach allgemeinem Ermessen** wahrscheinlich genutzt werden. Dabei sind alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Damit liegt ein Personenbezug nur dann nicht vor, wenn die Identifizierung der betreffenden Person praktisch nicht durchführbar oder gesetzlich verboten ist. Im Zweifel ist von personenbezogenen Daten auszugehen.

Personen werden zwar in der Praxis überwiegend anhand ihres **Namens** identifiziert, ein Name ist zur Identifizierung aber nicht immer notwendig. So ordnen rechnergestützte Dateien zur Erfassung personenbezogener Daten den erfassten Personen gewöhnlich ein eindeutiges Kennzeichen zu, um Verwechslungen zwischen zwei Personen in der Datei auszuschließen. Auch im Internet kann das Verhalten eines Geräts und somit des Gerätenutzers mit Hilfe von Überwachungswerkzeugen für den Internetverkehr problemlos identifiziert werden. Dadurch entsteht Stück für Stück ein Bild von der Persönlichkeit der Person, der bestimmte Entscheidungen zugeschrieben werden können. Die Person kann also ohne Kenntnis ihres Namens und ihrer Adresse anhand sozioökonomischer, psychologischer, philosophischer oder sonstiger Kriterien kategorisiert und mit bestimmten Entscheidungen in Zusammenhang gebracht werden, da der Kontaktpunkt der Person (Computer) die Offenlegung ihrer Identität im engeren Sinn nicht mehr zwingend erfordert.

3.1.2 Beispiel: IP-Adressen

Beispiel IP-Adresse:
Ein Internetprovider kann Daten der IP-Adresse einer im Internet surfenden Person mit deren Kontaktdaten verknüpfen. Dadurch wird diese Person für den Internetprovider identifizierbar und die Daten personenbezogen.
Für das Seilbahnunternehmen als Webseitenbetreiber ist es technisch möglich, durch Trackingdaten ebenfalls an die IP-Adresse seiner Besucher zu gelangen. Allerdings wird das Seilbahnunternehmen in der Regel nicht über die Kontaktdaten des Surfers verfügen und ist damit die surfende Person nicht ohne weiteres identifizierbar.

3.1.3 Besondere Kategorien personenbezogener Daten („Sensible Daten“)

Sensible Daten sind besonders verarbeitungsgeschützte personenbezogene Daten, aus denen rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie biometrische und genetische Daten, Daten zum Sexualleben oder zur sexuellen Orientierung und **Gesundheitsdaten** (wozu nicht nur die Beschreibung krankheitsbedingter Beeinträchtigungen in der Krankengeschichte zählen, sondern bereits die Erwähnung von Allergien, Unverträglichkeiten oder Abhängigkeiten).

Die Verarbeitung dieser Datenkategorien ist für die betroffene Person mit **besonders hohen Risiken** verbunden, weshalb dies nur unter ganz engen Voraussetzungen erlaubt ist.

3.1.4 Strafrechtsrelevante Daten

Das sind personenbezogene Daten über **strafrechtliche Verurteilungen** und **Straftaten** einschließlich des begründeten Verdachts oder damit zusammenhängende **Sicherungsmaßregeln** wie z.B. die Unterbringung in einer Anstalt für geistig abnorme Rechtsbrecher.

3.2 Unter welchen Voraussetzungen ist die Verarbeitung rechtmäßig?

Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.Die Verarbeitung personenbezogener Daten ist rechtmäßig:

- wenn eine **Einwilligung** der betroffenen Person vorliegt,
- zur **Erfüllung eines Vertrages** oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung
- zum Schutze lebenswichtiger Interessen,
- zur Wahrnehmung einer Aufgabe, die im **öffentlichen Interesse** liegt oder in Ausübung öf**fentlicher Gewalt** oder
- aufgrund einer **Interessenabwägung** erforderlich ist.

Die Datenverarbeitung ist bereits dann rechtmäßig, wenn **einer dieser Tatbestände** vorliegt. Im Grundsatz bleibt daher alles verboten, was nicht ausdrücklich erlaubt ist.

3.2.1 Einwilligung des Betroffenen

An erster Stelle der Erlaubnistatbestände steht die **Einwilligung** (vormals Zustimmung) des Betroffenen. Sie verkörpert das **informationelle Selbstbestimmungsrecht** oder anders die direkte Kontrolle des Einzelnen über die Verarbeitung ihn betreffender Daten.

Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen.

Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.

Voraussetzung einer wirksamen Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten personenbezogener Daten ist, dass der Betroffene diese **für einen oder mehrere bestimmte Zwecke** gegeben hat. Die Einwilligung muss durch eine **eindeutige bestätigende Handlung** erfolgen, mit der **freiwillig**, für den **konkreten Fall**, in **informierter Weise** und **unmissverständlich** bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung muss vom Seilbahnunternehmen **nachgewiesen** und vom Betroffenen **jederzeit widerrufen** werden können.

Freiwillig bedeutet ohne Zwang und nach freier Entscheidungsmöglichkeit. Das ist zweifelhaft, wenn:

- Einwilligungen zu verschiedenen Verarbeitungsvorgängen nicht gesondert erteilt (oder eben nicht erteilt) werden können, obwohl es im Einzelfall angebracht ist,
- die Erfüllung eines Vertrages von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung des Vertrages nicht erforderlich ist (**Koppelungsverbot**),
- wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht (z.B. wenn es sich bei dem Verantwortlichen um eine Behörde handelt).

Die **eindeutige bestätigende Handlung** kann durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der der Betroffene im jeweiligen Kontext eindeutig sein Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen keine Einwilligung dar.

In informierter Weise und für **bestimmte Zwecke** bedeuten, dass der Betroffene im Rahmen der Einwilligungserklärung in Kenntnis gesetzt werden muss, welche Datenarten für welche konkreten Zwecke verarbeitet werden sollen. Der Einwilligende muss Kenntnis der Sachlage haben., d.h. ihm muss klar sein, wer welche Daten zu welchem Zweck verarbeitet. Dazu gehört die Information über eventuelle Weitergaben an Dritte und/oder Übermittlungen in ein Drittland. Eine Blankoeinwilligung ist unwirksam, sie muss sich auf eine konkrete Verarbeitung beziehen.

Die **Nachweispflicht** dient der Steigerung der Transparenz und wird wohl dazu führen, dass vermehrt schriftliche oder elektronische Einwilligungen eingeholt werden.

Die betroffene Person hat jederzeit das Recht, ihre abgegebene Einwilligungserklärung zu **widerrufen**. Auf diese Möglichkeit ist die betroffene Person vor Abgabe der Einwilligung hinzuweisen.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Ist die Einwilligungserklärung z.B. in AGB eingebettet, die noch andere Sachverhalte mitumfassen (z.B. Regelungen über die Gewährleistung oder Zahlungsbedingungen) so muss die Einwilligungserklärung sich von den anderen Sachverhalten klar „unterscheiden". Das kann entweder durch eine Separierung erfolgen oder – weniger empfehlenswert (u.a. wegen des „Koppelungsverbots") - durch eine optische Hervorhebung innerhalb der AGB (z.B. durch Fettdruck und dicke schwarze oder sonstige farbliche Umrahmung). Wird gegen dieses Transparenzgebot verstoßen, sind jene als intransparent zu wertenden Teile einer datenschutzrechtlichen Einwilligungserklärung nicht verbindlich.

Hinweis:
Für die Zulässigkeit der Verarbeitung **„sensibler Daten"** ist eine **„ausdrückliche Einwilligung"** erforderlich.

Besonderheiten bei Einwilligungserklärungen von Kindern

Die **Einwilligung eines Kindes**, die sich auf ein Angebot von **Diensten der Informationsgesellschaft**, die **einem Kind direkt** gemacht werden, bezieht, ist in Österreich nur rechtmäßig, wenn das Kind das **14. Lebensjahr vollendet** hat. Sonst hat die Einwilligung durch den Erziehungsberechtigten oder mit dessen Zustimmung zu erfolgen. Solche **Dienste der Informationsgesellschaft** sind z.B. der Online-Verkauf von Waren, Online-Informationsdienste, soziale Netzwerke oder Kommunikationsnetzwerke. An ein Kind gerichtet ist ein Angebot, wenn Darstellung und Ansprache auf Kinder zugeschnitten sind. Das reine Anbieten von Waren für Kinder bedeutet noch nicht, dass sich das Angebot an Kinder richtet.

Musterformulierung:
„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich … (die Datenarten genau aufzählen, z.B. „Name", „Adresse" etc.) zum Zweck der … (genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma …") bei der Firma NN verarbeitet werden und die Daten … (die Datenarten genau aufzählen, z.B. „Name", „Adresse" etc.) zum Zweck der … (genaue Zweckangabe, z.B. „zur zentralen Abwicklung des Kunden-Beschwerdemanagements") an … (genaue Angabe des Übermittlungsempfängers, z.B. Name der Konzernmutter mit Anschrift) weitergegeben werden.
Diese Einwilligung kann jederzeit bei … (Angabe der entsprechenden Kontaktdaten*)* widerrufen werden.*"*

Bestehende Einwilligungserklärungen

Zustimmungserklärungen gelten nur dann weiter, wenn sie die Voraussetzungen einer Einwilligung erfüllen. Fehlt allerdings eines der beschriebenen Elemente (wenn z.B. das neue Koppelungsverbot nicht

eingehalten oder nicht auf die Widerrufsmöglichkeit hingewiesen wurde) muss die Einwilligung neu eingeholt werden.

3.2.2 Vertrag und vorvertragliche Maßnahmen

Datenschutz soll die Vertragsabwicklung nicht behindern. Die Verarbeitung von Daten ist grundsätzlich rechtmäßig, wenn sie für die **Erfüllung** (z.B. Arbeitsvertrag) oder den **zur Durchführung vorvertraglicher Maßnahmen** (z.B. Stellenbewerbung), die auf Anfrage der betroffenen Person (z.B. des Stellenwerbers) erfolgen, **objektiv erforderlich** ist. Die betroffene Person muss **Vertragspartei** des Vertrages sein. Im Rahmen abgeschlossener Verträge ist es beispielsweise nahezu unumgänglich die Vertrags-, Stammdaten und Abrechnungsdaten des Vertragspartners, wie etwa seinen Name und seine Adresse zu verarbeiten, um die Rechnung oder die Lieferung adressieren zu können.

Auch die Datenverarbeitung zur Abwicklung von Trainingsgruppen, zur Durchführung von Reservierungen, Veranstaltungen und Bezahlvorgängen im Gastronomiebereich, zur Abwicklung der Datenverarbeitung in Handelsbetrieben, zur Durchführung der unterschiedlichen Bezahlsysteme beim Erwerb von Schikarten und -pässen (Kassa) und die Erledigung von Sachschadensfällen, können auf dieser Rechtsgrundlage erfolgen.

Das Seilbahnunternehmen muss dabei die Daten allerdings nicht unbedingt selbst verarbeiten. Auch Datenverarbeitungen zu fremden Geschäftszwecken sind erlaubt, wie z.B. die Verarbeitung von Daten durch einen Zusteller.

Beispiel:
Ein Onlineshop-Anbieter darf auf Kontaktformularanfragen antworten und dem Warenspediteur die Adressen der Käufer übermitteln.

Achtung! Die bloße Tatsache, dass die Datenverarbeitung mit einem Vertrag in Zusammenhang steht oder irgendwo in den Bestimmungen und Klauseln des Vertrags vorgesehen ist, bedeutet nicht zwangsläufig, dass dieser Erlaubnistatbestand anwendbar ist.

3.2.3 Rechtliche Verpflichtung

Dieser Erlaubnistatbestand betrifft Verarbeitungen, die durch oder aufgrund von **Rechtsvorschriften** erforderlich ist. Die Rechtsgrundlage wird dabei durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt.

Man unterscheidet zwischen gesetzlicher Ermächtigung und Verpflichtung. Solche begründen etwa die zahlreichen gesetzlichen Verjährungs- und Aufbewahrungsfristen. Man denke allein an **Gewährleistungsansprüche** (2 Jahre (bewegliche Sachen), 3 Jahre (unbewegliche Sachen), **allgemeiner Schadenersatz** (Entschädigungsklagen) 3 Jahre (wenn Schaden und Schädiger bekannt) /ansonsten 30 Jahre

(betrifft insb auch Arbeitsunfälle!) oder die **steuerrechtliche Aufbewahrungspflicht** 7 Jahre (darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind). Viele Vorschriften sehen Übermittlungen personenbezogener Daten an Ämter (z.B. Finanzamt), Behörden (z.B. Bezirkshauptmannschaft), Gerichte (z.B. Drittschuldnererklärung) oder sonstige Stellen (z.B. Offenlegung des Gästeblattverzeichnisses) vor.

In den Erwägungsgründen wird klargestellt, dass nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt wird, sondern dass ein Gesetz auch die Grundlage für mehrere Verarbeitungen bilden kann.

3.2.4 Schutz lebenswichtiger Interessen

Dieser Tatbestand wird für das Seilbahnunternehmen hoffentlich nie eine Rolle spielen! Nur wenn keine andere Rechtsgrundlage gefunden werden kann, ist die erforderliche Datenverarbeitung aufgrund eines lebenswichtigen Interesses des Betroffenen oder eines Dritten erlaubt. Gemeint sind Fälle, die das Leben oder die Gesundheit betreffen, beispielsweise Pistenunfälle mit Schwerstverletzten, Lawinenabgänge und andere Naturkatastrophen oder vom Menschen verursachte Katastrophen.

3.2.5 Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt

Dieser Tatbestand betrifft Verantwortliche, denen eine **öffentliche Aufgabe** übertragen wurde. Konkret betrifft dies die im Datenschutzgesetz geregelten im öffentlichen Interesse gelegenen Archivzwecke, wissenschaftliche historische Forschungszwecke oder statistische Zwecke, die Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung Betroffener, Freiheit der Meinungsäußerung und Informationsfreiheit (Medienprivileg) und Verarbeitung im Katastrophenfall.

3.2.6 Wahrung berechtigter Interessen

Dieser Erlaubnistatbestand ist neben der Einwilligung wohl der wichtigste. Die Datenverarbeitung ist rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Seilbahnunternehmens oder eines Dritten erforderlich ist, dabei aber die schutzwürdigen Interessen der betroffenen Person nicht überwiegen. Berechtigt sind insbesondere auch wirtschaftliche Interessen.

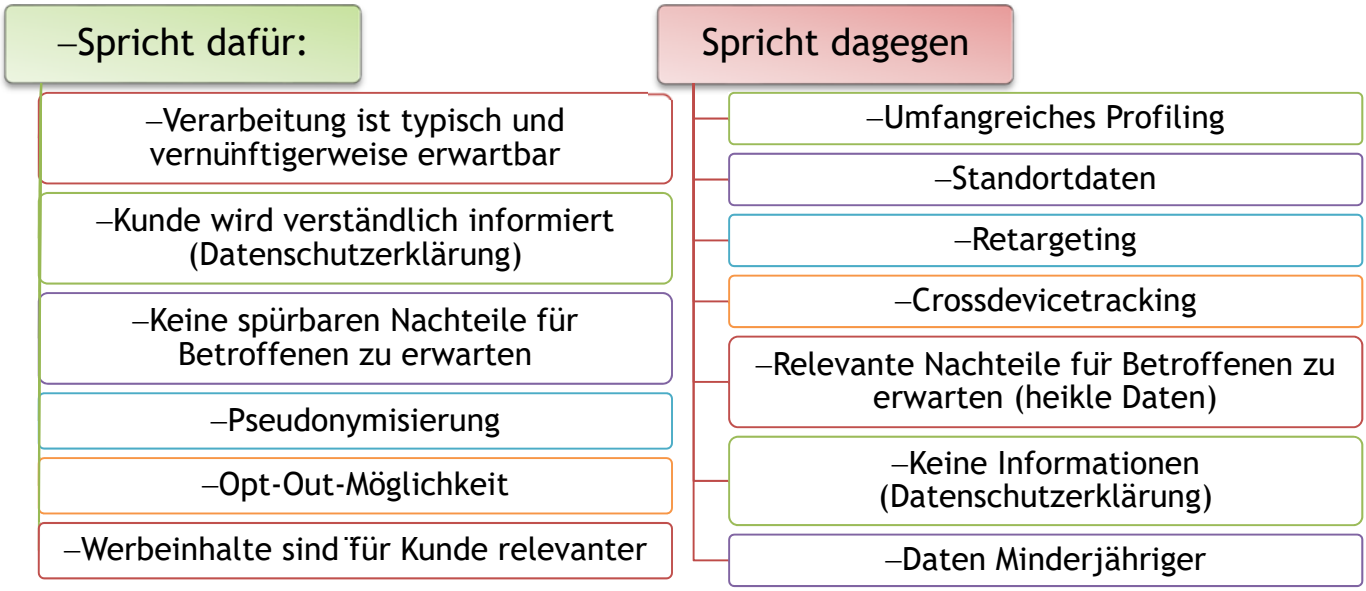
Die Prüfung, ob eine Datenverarbeitung auf diesen Erlaubnistatbestand gestützt werden kann, kann man sich wie eine Waage vorstellen, auf deren Gewicht man selbst Einfluss hat (Interessensabwägung). Auf der einen Seite steht das rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse des Seilbahnunternehmens, auf der anderen Seite dürfen die Rechte und Freiheiten des Betroffenen nicht ernsthaft beeinträchtigt werden.

Beispiel:
Das Seilbahnunternehmen kann z.B. ein berechtigtes Interesse haben, wenn die Verarbeitung in einem Kundenverhältnis stattfindet, wenn es personenbezogene Daten für Zwecke der Direktwerbung verarbeitet, um Betrug zu verhindern oder die Netzwerk- und Informationssicherheit Ihres IT-Systems sicherzustellen.

Das Schutzinteresse des Betroffenen sinkt beispielsweise mit technischen und organisatorischen Schutzmaßnahmen wie die Pseudonymisierung von Daten, der Informationen in einer verständlichen Datenschutzerklärung und vor allem, wenn Nutzer mit einer solchen Verarbeitung typischerweise rechnen müssen.

Beispiel: Direktwerbung
Die Datenverarbeitung zum Zweck der Direktwerbung kann ein berechtigtes Interesse darstellen:
Ein Unternehmen gelangt im Zusammenhang mit dem Verkauf eines Erzeugnisses in den Besitz der Kontaktdaten seiner Kunden und benutzt diese Kontaktdaten, um auf dem regulären Postweg für eigene, ähnliche Produkte zu werben. Das Geschäft verkauft seine Erzeugnisse auch über das Internet und verschickt Werbe-E-Mails, sobald eine neue Produktlinie verfügbar wird. Die Kunden werden unmissverständlich aufgeklärt, dass sie der Erfassung ihrer Kontaktdaten kostenfrei und ganz einfach widersprechen können, und wenn ein Kunde nicht von Anfang an Widerspruch eingelegt hat, wird er bei jeder weiteren Nachricht auf diese Möglichkeit hingewiesen.
Die Transparenz der Verarbeitung, die Tatsache, dass der Kunde berechtigterweise erwarten kann, als Kunde des Geschäfts Angebote für ähnliche Produkte zu erhalten, und der Umstand, dass er ein Widerspruchsrecht genießt, tragen zur Stärkung der Rechtmäßigkeit der Verarbeitung und zum Schutz der Rechte des Einzelnen bei. Andererseits sind wohl auch keine unangemessenen Folgen für das Recht des Einzelnen auf Privatsphäre zu verzeichnen. (bei diesem Beispiel haben wir vorausgesetzt, dass das Unternehmen keine komplexen Profile seiner Kunden erstellt, etwa indem eine detaillierte Analyse der Clickstream-Daten vorgenommen wird).

Argumente für die Abwägung berechtigt oder nicht?



3.2.7 Weiterverarbeitung von Daten

Eine Verarbeitung erhobener personenbezogener Daten zu einem anderen Zweck als dem ihrer Erhebung ist zulässig, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Ob die **Weiterverarbeitung mit den Zwecken**, für die die personenbezogenen Daten ursprünglich erhoben worden sind, **vereinbar** ist, ist Folgendes zu berücksichtigen:

- jede Verbindung zwischen den ursprünglichen und neu beabsichtigten Zwecken
- der Zusammenhang, in dem die Daten erhoben wurden
- die vernünftigen Erwartungen des Betroffenen auf Basis der Beziehung zum Verantwortlichen
- die Art der Daten (insbesondere ob sensible oder strafrechtlich relevante Daten vorliegen)
- mögliche Folgen der Weiterverarbeitung für betroffene Personen
- das Vorhandensein geeigneter Garantien (z.B. Pseudonymisierung)

Liegt eine solche Vereinbarkeit mit den ursprünglichen Zwecken vor, ist kein separater Erlaubnistatbestand als derjenige für die Erhebung notwendig.

Beispiele:
Kundendaten, die für eine Vertragsabwicklung erhoben wurden, werden für eine postalische Werbung für ein ähnliches Produkt verwendet.
Nach einem Autokauf wird vom Verkäufer eine Erinnerung bezüglich der Erneuerung der § 57a KFG-Plakette an den Käufer übermittelt.

Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbarer und rechtmäßiger Verarbeitungsvorgang.

Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, so muss er der betroffenen Person vor dieser Weiterverarbeitung **Informationen über diesen anderen Zweck** und alle anderen maßgeblichen Informationen zur Verfügung stellen.

Wenn der Zweck der Erhebung mit der Weiterverarbeitung **unvereinbar** ist, ist diese nur zulässig, wenn eine **Einwilligung** dafür vorliegt, oder eine **rechtliche Vorschrift** die Weiterverarbeitung vorsieht.

3.2.8 Verarbeitung besonderer Kategorien personenbezogener Daten („Sensible Daten")

Die Verarbeitung von „sensiblen Daten" ist nur in folgenden Fällen zulässig:

- mit ausdrücklicher Einwilligung des Betroffenen (z.B. Behandlung von leichten Verletzungen nach einem Schiunfall durch die Pistenrettung)
- Notwendigkeit der Datenverarbeitung für die Ausübung von Rechten und die Erfüllung von Pflichten aus dem **Arbeits- und Sozialrecht** (z.B. Erfassung der Krankenstandstage)
- Ermächtigung durch eine **Betriebsvereinbarung** oder einen Kollektivvertrag
- **Schutz lebenswichtiger Interessen** des Betroffenen oder einer anderen natürlichen Person, ohne dass der Betroffene seine Einwilligung erteilen kann (z.B. bei Bewusstlosigkeit in Folge eines Schiunfalls mit schwersten Verletzungen)
- Datenverarbeitung durch gewisse **Tendenzbetriebe**
- die sensiblen Daten wurden vom Betroffenen offensichtlich selbst veröffentlicht (z.B. in dem der Urlaubsgast ein Foto von seinem Gipsbein auf Facebook stellt)
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (z.B. im Fall der Notwendigkeit der Datenverarbeitung zur Abwicklung von Schadensfällen am Berg)
- aufgrund eines erheblichen öffentlichen Interesses auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats
- Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für bestimmte statistische Zwecke.

Sensible Daten können also nicht auf Basis der ansonsten praxisrelevanten Erlaubnistatbestände Vertragserfüllung oder überwiegende berechtigte Interessen verarbeitet werden!

3.2.9 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten

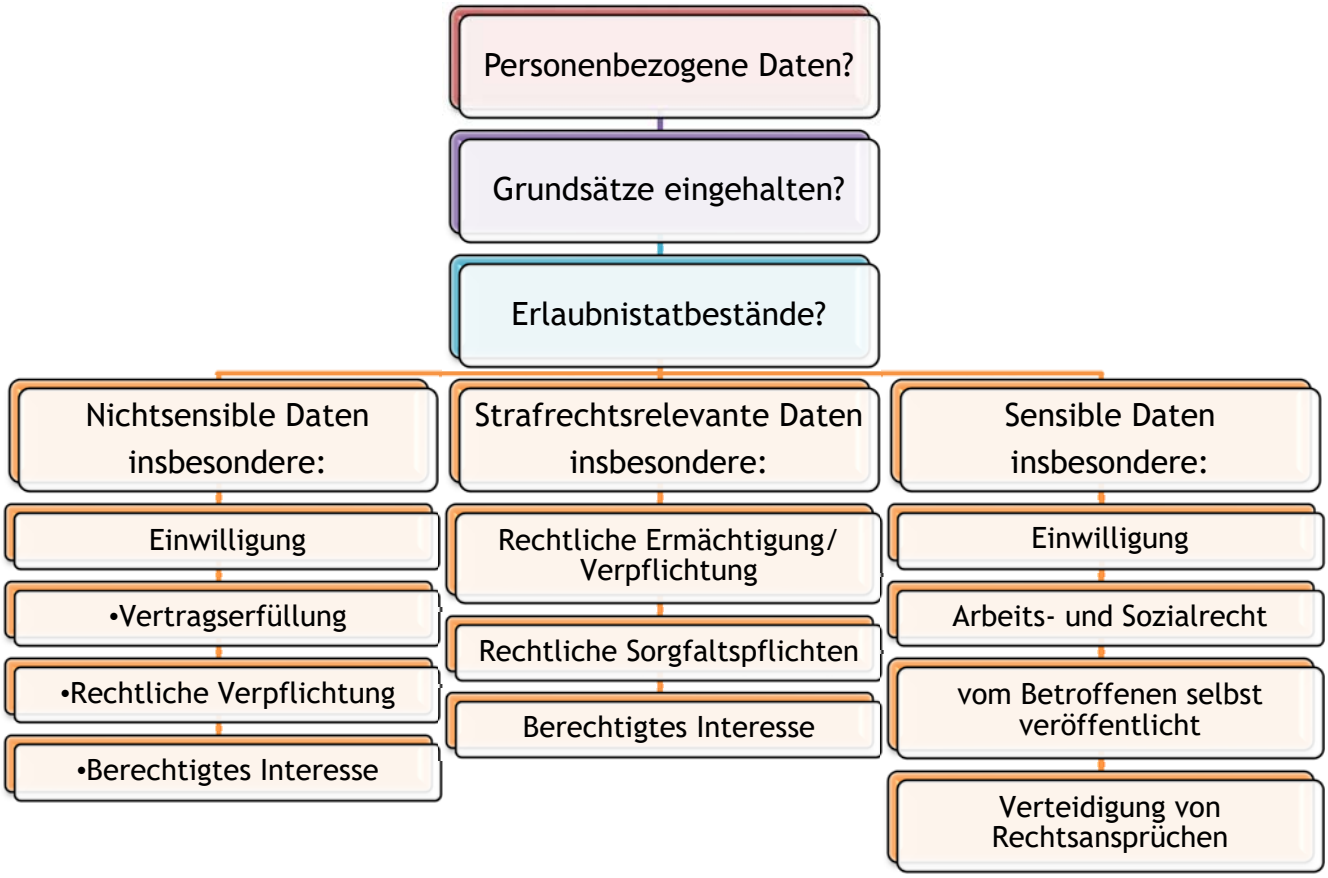
Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
- sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person gewährleistet.

Die Anzeige möglicher Straftaten oder Bedrohungen der öffentlichen Sicherheit in Einzelfällen oder in mehreren Fällen an die zuständige Behörde gelten als berechtigtes Interesse sofern keine Verschwiegenheitspflicht (z.B. Rechtsanwalt) besteht.

3.3 Zusammenfassung

Jede Verarbeitung personenbezogener Daten bedarf eines Rechtfertigungsgrundes. Zusammen mit den Grundsätzen der Datenverarbeitung spielen die Regelungen zur Rechtmäßigkeit der Datenverarbeitung eine zentrale Rolle. Um sicherzugehen, dass die die betriebenen Verarbeitungstätigkeiten rechtmäßig sind, muss das Seilbahnunternehmen jeder Verarbeitung einen Erlaubnistatbestand zuordnen können.



4 Aufgaben und Pflichten

4.1 Grundsätze der Datenverarbeitung

Artikel 5 DSGVO beschreibt die Grundsätze, die bei jeder Datenverarbeitung erfüllt sein müssen. Da diese Prinzipien an anderen Stellen der DSGVO wiederholt und präzisiert werden, können sie als eine „Präambel“ für sämtliche Datenverarbeitung im Seilbahnunternehmen angesehen werden. Im Einzelnen handelt es sich um folgende Grundsätze:

4.1.1 Rechtmäßigkeit

Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

„*Rechtmäßig*“ bedeutet, dass Daten nur aufgrund einer tauglichen Rechtsgrundlage verarbeitet werden dürfen (vgl. dazu oben Punkt 3.) und dabei die Bestimmungen der DSGVO eingehalten werden.

„*Nach Treu und Glauben*“ bedeutet, dass die Betroffenen über die Datenverarbeitung aufgeklärt werden müssen und hinsichtlich der näheren Umstände der Datenverarbeitung nicht in die Irre geführt werden dürfen.

„*In nachvollziehbare Weise*“ bedeutet, dass die Datenverarbeitung transparent erfolgen muss und den betroffenen Personen insbesondere mitzuteilen ist, welche Rechte ihnen nach der DSGVO zustehen (z.B. Recht auf Auskunft oder auf Löschung).

4.1.2 Zweckbindung

Personenbezogene Daten dürfen nur für im Vorhinein festgelegte, eindeutige und legitime Zwecke erhoben werden, an die der Verantwortliche gebunden ist.

Sollen die Daten zu anderen Zwecken weiterverarbeitet werden, muss für diese Weiterverarbeitung neuerlich geprüft werden, ob eine taugliche Rechtsgrundlage dafür vorliegt.

Beispiel:
Von Gästen wird anlässlich einer Vorsilvesterfeier im Bergrestaurant die Einwilligung eingeholt, ob ein Foto gemacht und an der Erinnerungsfotowand des Restaurants aufgehängt werden kann. Die Gäste stimmen diesem Verwendungszweck zu. Ein halbes Jahr später wird eine Hochglanzbroschüre für das Seilbahnunternehmen erstellt, der Geschäftsführer sucht nach gelungenen Gästefotos und will auch das besagte Fotos von der Vorsilvesterfeier für die Broschüre verwenden. Dies kommt einem Zweckwechsel gleich, für den das Unternehmen eine gesonderte Einwilligung der betroffenen Gäste einholen muss.

4.1.3 Datenminimierung

Personenbezogene Daten müssen dem Zweck nach angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.

Von der DSGVO wird damit auf eine Einschränkung der „Big Data Mentalität“ abgezielt, nach der in der Vergangenheit möglichst viele Daten erfasst und verarbeitet wurden (nach dem Motto: „*wer weiß, wofür wir die Daten eines Tages noch brauchen können…*“).

4.1.4 Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Unternehmen haben nach der DSGVO alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Dem Verantwortlichen wird damit aufgetragen, die Richtigkeit der von ihm verarbeiteten Daten aktiv zu überprüfen.

Beispiel:
Im Rahmen eines Beschwerdefalls kommt es zu einer Verwechslung. Aufgrund einer Namensgleichheit zweier Gäste wird die Beschwerde einer falschen Person zugeordnet und diese in der Dokumentation geführt und gespeichert. Sobald die Verwechslung erkennbar wird, sind die Daten im Beschwerdemanagementsystem richtig zu stellen.

4.1.5 Speicherbegrenzung

Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

MERKE: Gesetzliche Aufbewahrungsfristen wie z.B. nach § 132 der Bundesabgabenordnung (7-jährige Aufbewahrungspflicht für alle steuerrelevanten Belege und Unterlagen) oder nach den §§ 190 und 212 des Unternehmensgesetzbuches (7-jährige Aufbewahrungspflicht für sämtliche Bücher, Geschäftsbriefe und Belege) bleiben davon unberührt.

Beispiel:
Ein Kunde des Seilbahnunternehmens hat für 2017/2018 eine Saisonkarte erworben. Nachdem er im Frühjahr 2019 im Internet liest, dass seine personenbezogenen Daten nur zur Abwicklung des Vertrages verwendet werden dürfen, schreibt er das Seilbahnunternehmen per E-Mail an und beantragt die Löschung sämtlicher von ihm gespeicherten Daten. Im Umfang der 7-jährigen Aufbewahrungspflicht aller steuerrelevanten Belege und Unterlagen ist eine solche pauschale Löschung nicht möglich und muss unter Verweis auf die gesetzliche Aufbewahrungspflicht nicht durchgeführt werden.

4.1.6 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Davon umfasst ist auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (siehe 4.3).

MERKE: Der Verantwortliche ist für die Einhaltung der beschriebenen Grundsätze für die Datenverarbeitung verantwortlich und muss ihre Einhaltung nachweisen können (**„Rechenschaftspflicht“**).

4.2 Erstellung eines Verarbeitungsverzeichnisses

Nach Artikel 30 DSGVO hat jedes Seilbahnunternehmen ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen, die seiner Zuständigkeit unterliegen (*Records of processing activities*).

4.2.1 Sinn und Zweck des Verzeichnisses

Das Verzeichnis soll der Datenschutzbehörde in strukturierter Form einen ersten Eindruck darüber verschaffen, welche Datenverarbeitungen im Bergbahnunternehmen durchgeführt und ob die Pflichten nach der DSGVO erfüllt werden.

Im Ergebnis ist das Verzeichnis auch ein **Mosaik**, in dem die verschiedensten Datenverarbeitungen im Bergbahnbetrieb übersichtlich dargestellt werden. Die Erkenntnisse, die daraus gewonnen werden, können Grundlage für wichtige künftige Entscheidungen im Unternehmen sein (z.B. Ausschöpfung von Synergiepotentialen durch Beseitigung von Doppelgleisigkeiten und Mehrfachverarbeitungen). Dem Verarbeitungsverzeichnis sollte daher seitens der Unternehmensführung **größte Aufmerksamkeit** geschenkt werden.

4.2.2 Notwendige Angaben

a) Namen und Kontaktdaten des Verantwortlichen, des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
b) Die Zwecke der Verarbeitung
c) Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
d) Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern (z.B. US-amerikanischer Cloud-Dienstleister, der die Daten seiner europäischen Kunden auf Servern in den USA speichert) einschließlich der Auflistung der betreffenden Empfänger.
e) Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland (z.B. Übermittlung von Daten russischer Kunden an einen Reiseveranstalter in Russland) einschließlich der Auflistung der betreffenden Drittländer.
f) Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien.
g) Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

4.2.3 Relevante Datenverarbeitungen

Relevante Datenverarbeitungen in der Seilbahnwirtschaft, die im Verarbeitungsverzeichnis zu dokumentieren sind, können insbesondere sein:

- Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
- Pistenrettung
- Trainingsgruppen
- Flotten- und Pistenmanagement
- Tagesberichte
- Betriebstagebuch
- Krisenhandbuch
- Abwicklung von Schadensfällen
- Lost and Found
- Beschwerdemanagement

- Adressverwaltungen (sofern nicht in den zentralen Datenbanken integriert)
- Personalverwaltung samt Bewerbungsmanagement
- Sach- und Inventarverwaltung
- Zugriffsverwaltung für EDV-Systeme
- Zutrittskontrollsysteme
- Kundenbetreuung und Marketing für eigene Zwecke
- Bonussysteme (sofern nicht in der Kunden-/Lieferanten- /Personalverwaltung integriert)
- Bildverarbeitung (Videoüberwachung, Fotos)

Darüber hinaus alle sonstigen Verarbeitungstätigkeiten, die vom Seilbahnunternehmen in der Praxis geführt werden, unabhängig davon, ob diese in einer angekauften oder selbst programmierte Software, in einer „selbstgebastelten" Excel-Lösung oder in strukturierten Papierordnern erfolgen (siehe 1.3.2).

4.2.4 Umsetzung in der Praxis

Die DSGVO sieht keine Regelungen zu Struktur und Form des Verzeichnisses vor.

Wir empfehlen, die Hilfsmaterialien der Wirtschaftskammern in Anspruch zu nehmen, die ihren Mitgliedern ein benutzerfreundliches Formblatt mit zahlreichen Ausfüllhilfen und Mustern zur Verfügung stellt (zu den Links auf die betreffenden Seiten der Wirtschaftskammern siehe unten Punkt 5.3).

Eine Sammlung ausformulierter Bearbeitungszwecke bei typischen Datenverarbeitungen finden Sie bei 5.2.3.

4.2.5 Bildung von Clustern

In der Praxis hat sich die Bildung von Clustern bewährt. Damit können die einzelnen Verarbeitungstätigkeiten thematisch zugeteilt und übersichtlich geordnet werden. Typische Cluster können z.B. sein:

- Kunden
- Pisten und Bahnen
- Verwaltung
- Personal
- Marketing
- Bildverarbeitung

4.3 Auswahl und Implementierung geeigneter TOMs

Nach Artikel 24 DSGVO hat das Seilbahnunternehmen geeignete technische und organisatorische Maßnahmen (TOMs) zu setzen, um zu verhindern, dass Datenverarbeitungen zu (physischen, materiellen oder immateriellen) Schäden bei den betroffenen Personen führen.

Bei der Auswahl von TOMs sind folgende Kriterien zu berücksichtigen:

- Art, Umfang, Umstände und Zwecke der Datenverarbeitung
- Eintrittswahrscheinlichkeit eines Vorfalls
- Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen (Kunden und Mitarbeiter des Seilbahnunternehmens)

EMPFEHLUNG: Bei der Verarbeitung von sensiblen Gesundheitsdaten (insbesondere im Rahmen der Pistenrettung) sollte grundsätzlich immer ein **hohes Risiko** für die Betroffenen unterstellt werden. Bei der Auswahl und Umsetzung von TOMs ist darauf Rücksicht zu nehmen (bei hohem Risiko sind Maßnahmen in verstärktem Ausmaß umzusetzen oder durch zusätzliche Maßnahmen zu ergänzen).

MERKE: TOMs sind regelmäßig zu evaluieren und gegebenenfalls anzupassen (Planung eines Audits). Sie sind auch im Rahmen interner Datenschutz-Strategien nachzuweisen (siehe 4.11).

4.3.1 Beispiele für technische Maßnahmen:

- Datenschutz durch **Technikgestaltung** (*Data protection by design*), z.B. durch
  - Minimierung der Datenverarbeitung (vgl. auch Artikel 5 Abs. 1 lit. c DSGVO)
  - Schnellstmögliche Pseudonymisierung Herstellung von Transparenz in Bezug auf die Datenverarbeitung zur Ermöglichung der Wahrung der Rechte der Betroffenen

- Datenschutz durch **datenschutzfreundliche Voreinstellungen** (*Data protection by default*). Durch Voreinstellung ist sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, die zur Erfüllung des jeweiligen Verarbeitungszwecks erforderlich sind, und zwar in Bezug auf
  - die Menge der erhobenen personenbezogenen Daten,
  - den Umfang der Verarbeitung diese Daten,
  - die Speicherfrist dieser Daten und
  - die Zugänglichkeit dieser Daten

Ebenso ist sicherzustellen, dass personenbezogene Daten durch Voreinstellungen nicht öffentlich gemacht werden (z.B. keine automatische Voreinstellung von Einwilligungen).

Beispiel:
Vom Seilbahnunternehmen wird ein Bewerbertool eingesetzt, über das Bewerbungen elektronisch eingebracht werden können. Der Bewerber kann dabei in einer Checkbox anklicken, ob er für die Dauer von 1 Jahr evident gehalten wird. Datenschutzfreundliche Voreinstellung bedeutet, dass die Checkbox nicht standardmäßig angeklickt sein darf (das käme einem „opt-out“ gleich), sondern vom Bewerber aktiv auszuwählen ist („opt-in“).

4.3.2 Beispiele für organisatorische Maßnahmen:

- Ausarbeitung eines Löschungskonzeptes (Regelungen zur Speicherdauer von personenbezogenen Daten)

- Umstellung auf Pseudonymisierung, Verschlüsselung oder Anonymisierung (Festlegung von Kriterien zur schnellstmöglichen Umstellung)
- Schulung und Sensibilisierung von Mitarbeitern im Bereich Datenschutz
- Festlegung verbindlicher Vorgehensweisen bei Sicherheitsverletzungen Incident response policy
- Einführung von Prüf- und Kontrollverfahren zur Gewährleistung, dass Maßnahmen nicht nur am Papier stehen, sondern in der Praxis angewandt werden und funktionieren (Compliance System)

4.4 Datensicherheitsmaßnahmen

Nach Artikel 32 DSGVO haben das Seilbahnunternehme geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten.

Bei der Auswahl der Datensicherheitsmaßnahmen sind folgende Kriterien zu berücksichtigen:

- **Stand der Technik** (gemeint sind damit bereits verfügbare Maßnahmen, die sich in Praxis und Betrieb entsprechend bewährt haben und nach herrschender Auffassung führender Fachleute die erforderlichen Ziele erreichen - „best available techniques“)
- **Implementierungskosten (**erforderlich ist ein Aufwand, der angemessen ist)
- **Art, Umfang, Umstände und Zwecke** der Verarbeitung (werden z.B. sensible Gesundheitsdaten verarbeitet oder Kunden durch Videokameras systematisch überwacht?)
- Unterschiedliche Eintrittswahrscheinlichkeiten
- Schwere des Risikos für die betroffenen Personen

Neben der beispielhaften Erwähnung von **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten werden im Artikel 32 DSGVO auch Maßnahmen zur Absicherung der Fähigkeit, der Vertraulichkeit, der Integrität sowie der Verfügbarkeit und Belastung der Systeme angeführt.

4.4.1 Beispiele für Datensicherheitsmaßnahmen:

- **Zutrittskontrolle** (Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen)
  - z.B. durch Sicherheitsschlösser oder Chipkartensysteme
- **Zugangskontrolle** (Verwehrung des Zugangs zu Datenverarbeitungsanlagen für Unbefugte)
  - z.B. durch die eindeutige Authentifizierung jeden Mitarbeiters mittels Benutzer-kennung und Passwort
- **Zugriffskontrolle** (Gewährleistung, dass zugangsberechtigte Mitarbeiter ausschließlich zu den von ihrer Berechtigung umfassten personenbezogenen Daten Zugang haben)

- z.B. durch eine Rechteverwaltung, mit der festgelegt wird, welcher Mitarbeiter Zugriff auf welche Daten haben muss, um seine Aufgaben erledigen zu können)

- **Weitergabekontrolle** (Gewährleistung, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist)
  - z.B. durch Nutzung von virtuellen privaten Netzwerken (VPN), E-Mail Verschlüsselung oder Passwortschutz einzelner Dokumente (PFD-Verschlüsselung)

- **Eingabekontrolle** (Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind)
  - z.B. durch Protokollierung sämtlicher Zugriffaktivitäten (welcher Mitarbeiter hat wann auf welche Daten zugegriffen?)

- **Verfügbarkeitskontrolle** (Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt und wiederherstellbar sind)
  - z.B. durch Backup- und Recovery-Systeme, Überspannungsschutz, Brandschutzmaßnahmen, Klimaanlage

- **Trennbarkeit** (Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können)
  - z.B. durch getrennte Datenbanken, Ordner- und Laufwerkstrukturen

4.4.2 Broschüren der Wirtschaftskammern zur Datensicherheit

Für die nähere Auswahl konkreter Datensicherheitsmaßnamen empfehlen wir auch die Borschüren der Wirtschaftskammern zur Datensicherheit für KMU[5] und für Mitarbeiter[6] (jeweils in der 8. Auflage). Siehe dazu auch unten Punkt 5.3).

4.5 Durchführung von Folgenabschätzungen

Nach Artikel 35 DSGVO hat das Seilbahnunternehmen eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein

[5] http://wko.at/ic//IT_Handbuch_KMU_2017.pdf.

[6] http://wko.at/ic//IT_Handbuch_MA_2017.pdf.

hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (*Privacy impact assessment*).

Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen durchzuführen:

a) Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (z.B. von Gesundheitsdaten im Rahmen der **Pistenrettung**) oder von strafrelevanten Daten.
b) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. Einsatz flächendeckender **Videoüberwachung**).

EMPFEHLUNG: Ob die Verarbeitung sensibler Gesundheitsdaten im Rahmen der Pistenrettung „umfangreich" im Sinn der DSGVO ist und die Videoüberwachung von Lift- und Bahnanlagen als „systematisch, umfangreich" zu qualifizieren ist, wird erst durch die Entscheidungspraxis der Datenschutzbehörde und die Judikatur der unabhängigen Gerichte geklärt werden. Da die Unterlassung einer Folgenabschätzung sanktioniert werden kann, empfehlen wir jedoch aus Absicherungsgründen, in **beiden angeführten Fällen** eine Folgenabschätzung durchzuführen, die zumindest folgende Inhalte aufweist:

- Eine systematische Beschreibung der Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der vom Seilbahnunternehmen verfolgten berechtigten Interessen.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungs-vorgänge in Bezug auf den Zweck.
    - Dieses Kriterium dürfte bei der Pistenrettung eine geringere Rolle spielen, als bei der Videoüberwachung.
- Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen.
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.
    - Hier käme z.B. als gelinderes Mittel der Einsatz von Live-Kameras in Betracht, die keine Bilder aufzeichnen.

4.5.1 Vorherige Konsultation

Wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, muss da Seilbahnunternehmen künftig vor der Verarbeitung die Datenschutzbehörde konsultieren, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen wurden.

Im Rahmen dieser Konsultation sind der Datenschutzbehörde folgende Informationen zur Verfügung zu stellen:

a) Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unter-nehmen

b) Die Zwecke und die Mittel der beabsichtigten Verarbeitung

c) Die zum Schutz der Rechte und Freiheiten der betroffenen Personen vorgesehenen Maßnahmen und Garantien

d) Gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten

Als Ergebnis dieser Konsultation kann die Datenschutzbehörde **schriftliche Empfehlungen** aussprechen und weitere Befugnisse ausüben.

4.6 Benennung eines Datenschutzbeauftragten

Nach Artikel 37 DSGVO hat der Verantwortliche u.a. dann verpflichtend einen Datenschutzbeauftragten zu benennen, wenn

a) seine **Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen, oder
b) seine **Kerntätigkeit** in der **umfangreichen Verarbeitung besonderer Kategorien oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten** besteht

Ob eine dieser Voraussetzungen bei Seilbahnunternehmen erfüllt sind, ist fraglich und wird erst durch die Entscheidungspraxis der Datenschutzbehörde und die Judikatur der unabhängigen Gerichte geklärt werden. Wenn im Unternehmen aber z.B. eine **flächendeckende Videoüberwachung** zum Einsatz kommt (z.B. auch in Gondeln und in Gastronomiebetrieben) empfiehlt es sich im Zweifel einen Datenschutzbeauftragten zu benennen.

Unabhängig davon, kann das Unternehmen einen Datenschutzbeauftragten freiwillig benennen, was von Geschäftspartnern und Partnern und Kunden als zusätzliches Qualitätsmerkmal anerkannt werden dürfte.

Der Datenschutzbeauftragte hat folgende Aufgaben:

- Die **Unterrichtung und Beratung** des Seilbahnunternehmens und seiner Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO, dem DSG und allen sonstigen Datenschutzvorschriften
- Die **Überwachung der Einhaltung datenschutzrechtlicher Vorschriften**, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter, und der diesbezüglichen Überprüfungen
- Die Beratung in Bezug auf eine **Folgenabschätzung**
- Die **Zusammenarbeit mit der Aufsichtsbehörde** und damit verbunden die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in allen Vollzugsfragen

Zusätzliche Aufgaben (z.B. die Erstellung des Verzeichnisses aller Verarbeitungstätigkeiten) können dem Datenschutzbeauftragten übertragen werden.

Die Funktion des Datenschutzbeauftragten kann **ausgelagert** werden (Beauftragung nach § 1002 ABGB).

Hinweis: Auch wenn kein Datenschutzbeauftragter benannt wird, darf nicht übersehen werden, dass das Seilbahnunternehmen in jedem Fall einen Mitarbeiter mit dem nötigen Know How oder einen externen Experten benötigt, der die Pflichten und Aufgaben nach der DSGVO vollständig umsetzt.

4.7 Meldung von Datenschutz-Vorfällen

Nach Artikel 33 DSGVO sind ab 25.5.2018 sind alle Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der Datenschutzbehörde zu melden (*Data breach notification*).

Beispiel:
Im Verwaltungsbereich eines Seilbahnunternehmens wird eingebrochen und ein Firmenlaptop gestohlen. Auf dem Laptop waren Daten von Kunden und Mitarbeiten gespeichert. Ein solcher Vorfall wäre künftig der Behörde zu melden.

Eine **Ausnahme** von der Meldepflicht besteht dann, wenn der Vorfall voraussichtlich zu keinem Risiko für die Betroffenen führt (z.B., weil ihre Daten pseudonymisiert oder verschlüsselt waren).

Hinweis: Der Tatbestand der Meldepflicht wird noch nicht verwirklicht, wenn bloß eine Verletzung der jederzeitigen Verfügbarkeit von Daten (z.B. Serverausfall) vorliegt.

EMPFEHLUNG: Die Wirtschaftskammern haben ein Muster für eine Meldung an die Datenschutzbehörde erstellt, das im konkreten Anlassfall angepasst werden kann.[7]

Nach Artikel 34 DSGVO sind über meldepflichtige Vorfälle auch die betroffenen Personen (insbesondere Kunden) unverzüglich zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Dies Benachrichtigung ist dann nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

[7] Die Muster-Vereinbarung wird auf den Webseiten der Wirtschaftskammern zum Download zur Verfügung gestellt: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html .

a) Der Verantwortliche hat **geeignete technische und organisatorische Sicherheitsvorkehrungen** getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt (z.B. Verschlüsselung von Laptop-Festplatten).
b) Der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht
c) Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

4.8 Informierung der Betroffenen

4.8.1 Datenerhebung bei der betroffenen Person

Werden künftig Daten bei der betroffenen Person erhoben (insbesondere, weil sie von dieser Person selbst zur Verfügung gestellt werden), so sind ihr vom Seilbahnunternehmen nach Artikel 13 DSGVO zum Zeitpunkt der Erhebung dieser Daten folgende Informationen mitzuteilen, wenn und soweit die betroffene Person darüber nicht schon verfügt:

- Namen und Kontaktdaten des Unternehmens und gegebenenfalls des/der Datenschutzbeauftragten
- Die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung
- Wenn Rechtsgrundlage eine Interessenabwägung ist, die entsprechenden berechtigten Interessen
- Gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln

Zusätzliche Informationen sind mitzuteilen, wenn diese im Interesse einer fairen und transparenten Verarbeitung notwendig sind, insbesondere kann dies folgende Informationen betreffen:

- Dauer der Datenspeicherung bzw. wenn unmöglich die Kriterien für die Festlegung der Dauer,
- Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch,
- die Möglichkeit des Widerrufs der Einwilligung,
- das Bestehen eines Beschwerderechts bei der Datenschutzbehörde,
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.

EMPFEHLUNG: Diese Informationen können im Rahmen standardisierter Textbausteine erfolgen.

Beispiel:
Im Rahmen der Anmeldung einer neuen Trainingsgruppe wird als Beilage zum Anmeldeformular eine Namensliste der Teilnehmer übermittelt. Eine standardisierte Rückmeldung des Seilbahnunternehmens könnte lauten:
„Sehr geehrte Damen und Herren,
wir verarbeiten die von ihnen übermittelten Daten ausschließlich im Rahmen der Erfüllung unsere vertraglichen Verpflichtungen zur Abwicklung ihrer Buchung. Die von Ihnen übermittelten Daten werden nicht an Dritte weitergegeben und gelöscht, sobald sie nicht mehr für die Vertragserfüllung benötigt werden und gesetzliche Aufbewahrungsfristen abgelaufen sind.
Es stehen Ihnen die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch sowie das Recht zur Erhebung einer Beschwerde an die Datenschutzbehörde zu.
Mit freundlichen Grüßen“

4.8.2 Datenerhebung bei einer anderen als der betroffenen Person

Werden künftig Daten nicht bei der betroffenen Person erhoben (insbesondere, weil sie von einem Geschäftspartner zur Verfügung gestellt werden), so sind ihr vom Seilbahnunternehmen nach Artikel 14 DSGVO zum Zeitpunkt der Erhebung dieser Daten folgende Informationen mitzuteilen, wenn und soweit die betroffene Person darüber nicht schon verfügt:

- Namen und Kontaktdaten des Unternehmens und gegebenenfalls des Datenschutzbeauftragten
- Die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung
- Gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln

Zusätzliche Informationen sind wiederum mitzuteilen, wenn diese im Interesse einer fairen und transparenten Verarbeitung notwendig sind (vgl. im Detail Artikel 14 DSGVO).

4.9 Datenschutzerklärung

Das Seilbahnunternehmen hat geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen und alle Mitteilungen zu übermitteln, und zwar

- in einer **präzisen, transparenten, verständlichen und leicht zugänglichen Form** (z.B. in Form eines Links „Datenschutzerklärung“ auf den Webseiten des Seilbahnunternehmens) und
- in einer **klaren und einfachen Sprache**, insb. wenn Kinder (bis 14 Jahre) von der Datenverarbeitung betroffen sind

HINWEIS: Die Informationen sind auf den Webseiten dann „leicht zugänglich“, wenn sie über den link „Datenschutzerklärung“ am Ende jeder Seite abrufbar sind.

Relevante Mitteilungen sind insbesondere:

- **Recht auf Auskunft**
- **Recht auf Berichtigung**
- **Recht auf Löschung**
- **Recht auf Einschränkung der Verarbeitung**
- Mitteilungspflicht im Zusammenhang mit der **Berichtigung oder Löschung** personenbezogener Daten oder der **Einschränkung** der Verarbeitung
- Recht auf **Datenübertragbarkeit**
- Recht auf **Widerspruch**
- Mitteilung **automatisierter Entscheidungen** im Einzelfall einschließlich **Profiling**

Sinn und Zweck der Datenschutzerklärung:
Artikel 12 DSGVO beschreibt den Grundsatz der Transparenz, der zum Ziel hat, dass die betroffenen Personen einen effektiven Rechtsschutz haben und darüber informiert werden, welche Rechte sie geltend machen können und wie der Verantwortliche mit ihren Anfragen und Anbringen umzugehen hat.

Hintergrund ist, dass es bislang keine externe Hilfestellung für die Geltendmachung von Rechten im Datenschutz gab, weshalb nur wenige betroffene Personen ihren Rechtsschutz wahrgenommen haben und es eine hohe Zahl an unaufgeklärten Grundrechtsverletzungen gab. Durch den neuen Transparenzgrundsatz kommt es somit zu einer Stärkung der Betroffenenrechte (europaweite Stärkung der Verbraucherrechte).

EMPFEHLUNG: Die Datenschutzerklärung sollte nicht in das Impressum eingebettet werden, sondern **neben dem Impressum** dargestellt werden.

EMPFEHLUNG: Die Wirtschaftskammern haben ein Muster mit Textbausteinen für eine Datenschutzerklärung erstellt, die folgende Punkte berücksichtigt:

- DSGVO und Telekommunikationsgesetz 2003
- Webshop (Datenspeicherung)
- Cookies
- Web-Analyse Tools (z.B. Google Analytics, eTracker, Webtrekk)
- Newsletter (mit double Opt-in)

Seilbahnbetriebe können aus diesem Muster jene Inhalte übernehmen, die für sie in Frage kommen.[8]

[8] Die Muster-Datenschutzerklärung wird auf den Webseiten der Wirtschaftskammern zum Download zur Verfügung gestellt: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/muster-informationspflichten-website-datenschutzerklaerung.html.

4.10 Datenübermittlung ins Ausland

Der Datenverkehr innerhalb der EU/EWR unterliegt keinen besonderen Beschränkungen.

Beispiel:
Ein Bergbahnunternehmen will Newsletter versenden und zieht dafür ein Marketingunternehmen aus Hamburg hinzu. Für die damit einhergehende Datenüberlassung nach Deutschland ist keine Genehmigung der Datenschutzbehörde erforderlich.

Der Datenverkehr von Österreich in Drittländer (Länder außerhalb EU/EWR) ist allerdings nur nach Maßgabe der Artikel 44 ff. DSGVO zulässig, insbesondere aufgrund

- eines **Angemessenheitsbeschlusses** der Europäischen Kommission, z.B. USA (für Unternehmen, die sich der Privacy-Shield Vereinbarung unterworfen haben), Argentinien, Israel, Kanada, Neuseeland, Schweiz
- von **Standarddatenschutzklauseln**, die von der Europäischen Kommission erlassen wurden
- der **ausdrücklichen Einwilligung** des Betroffenen (nach Unterrichtung über die Risiken einer Übermittlung ohne Vorliegen eines Angemessenheitsbeschlusses oder geeigneter Garantien)

Beispiel:
Ein Seilbahnunternehmen will seine gesamte Personalverwaltung in die Cloud verlagern und schließt zu diesem Zweck eine Vereinbarung mit einem US-amerikanischen Cloud-Dienstleister ab. Nach den AGB des Cloud-Dienstleisters werden die Personaldaten auf amerikanischen Servern gespeichert. Wenn sich der Dienstleister nicht dem US Privacy Shield oder den Standarddatenschutzklauseln der Europäischen Kommission unterworfen hat, und auch sonst keine geeigneten Garantien im Sinne der Artikel 44 ff. DSGVO vorliegen, muss das Seilbahnunternehmen vor der Datenübermittlung in die Cloud die ausdrückliche Einwilligung seiner Mitarbeiter einholen.

4.11 Ausarbeitung interner Datenschutzstrategien

Als Verantwortliche unterliegen Seilbahnunternehmen der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO und müssen nachweisen, dass sie die allgemeinen Grundsätze für die Datenverarbeitung einhalten (siehe 4.1).

Weiters hat der Verantwortliche nach Artikel 24 Absatz 2 DSGVO im Wege von internen Datenschutzstrategien die Umsetzung geeigneten TOMs nachzuweisen (siehe 4.3).

EMPFEHLUNG: Aus Zweckmäßigkeitsgründen sollten nicht nur die Einhaltung der allgemeinen Grundsäte für die Datenverarbeitung und die Umsetzung geeigneter TOMs, sondern auch weitere getroffene Maßnahmen im Zuge der Umsetzung der DSGVO schriftlich dokumentiert werden.

Alle diese Inhalte können in „Internen Datenschutzstrategien“ oder in einem nach Kapiteln geordneten „**Datenschutzhandbuch**“ zusammengefasst werden. Eine solche Dokumentation könnte demnach z.B. folgenden Aufbau haben:

1. Verzeichnis der Verarbeitungstätigkeiten (Artikel 30 DSGVO)
2. Einhaltung der Grundsätze nach Artikel 5 DSGVO
3. TOMs nach Artikel 24 DSGVO
4. Datensicherheitsmaßnahmen nach Artikel 32 DSGVO
5. Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO
5. Datenübermittlung ins Ausland nach Artikel 44 ff. DSGVO
6. Wahrung der Betroffenenrechte

4.12 Zusammenfassung

- Neben der Einhaltung allgemeiner Grundsätze für die Datenverarbeitung, die als Präambel für den Datenschutz verstanden werden kann, haben Seilbahnunternehmen **ganz konkrete Aufgaben und Pflichten** umzusetzen.
- Das **Verzeichnis aller Verarbeitungstätigkeiten**, die **TOMs** und die **Datensicherheitsmaßnahmen** sowie die **Datenschutz-Folgenabschätzung** haben bei der Umsetzung der DSGVO große praktische Relevanz.
- Bei der Datenübermittlung in Drittstaaten (außerhalb EU/EWR) kann die ausdrückliche Einwilligung der betroffenen Personen erforderlich sein. Eine genaue **Einzelfallanalyse** ist unerlässlich.
- Es empfiehlt sich die getroffenen Maßnahmen zur Umsetzung der DSGVO im Rahmen von **„Internen Datenschutzstrategien“** oder in Form eines **„Datenschutzhandbuches“** des Seilbahnunternehmens schriftlich zusammenzufassen.

5 Hilfreiches

5.1 Checkliste

Folgende Punkte sollten im Rahmen der Umsetzung der neuen Rechtslage im Datenschutz auf deren Erledigung hin überprüft werden:

- ✓ Verzeichnisses aller Verarbeitungstätigkeiten erstellt?
- ✓ Alle Datenverarbeitungen im Bergbahnbetrieb auf das Vorliegen einer tauglichen Rechtsgrundlage hin geprüft?
- ✓ Risikobewertung durchgeführt und auf Grundlage dieser Risikobewertung geeignete „TOMs“ ausgewählt?

- ✓ Datensicherheitsmaßnahmen geprüft und gegebenenfalls adaptiert?
- ✓ Datenschutz-Folgenabschätzung (insbesondere in Bezug auf die Pistenrettung und Videoüberwachungen durchgeführt?
- ✓ Zielführendes Audit beschrieben?
- ✓ Grundsätze für die Datenverarbeitung werden eingehalten?
- ✓ Erfüllung von Informations- und Meldepflichten gewährleistet?
- ✓ Wahrung der Betroffenenrechte durch standardisierte Verfahren (Work-Flows) gewährleistet?
- ✓ Datenschutzerklärung auf den Webseiten und auf Social Media Plattformen eingerichtet?
- ✓ Datenübermittlungen ins Ausland geprüft?
- ✓ Datengeheimnis in Dienstverträgen vereinbart?
- ✓ Betriebsvereinbarungen zu Kontroll- und Überwachungsmaßnahmen abgeschlossen?
- ✓ Einwilligungen von Kunden und Mitarbeitern zur Verarbeitung von Fotos eingeholt?
- ✓ Bei Outsourcing (Beauftragung zur Verarbeitung von Daten) einen Auftragsverarbeiter-Vertrag abgeschlossen?

5.2 Muster

5.2.1 Datenschutzerklärung für Mitarbeiter

Liebe Mitarbeiterin, lieber Mitarbeiter,

mit Mai 2018 wird die Datenschutz-Grundverordnung wirksam. Diese sieht erweiterte Informationsverpflichtungen vor. Daher informieren wir Sie – in Erfüllung der neuen rechtlichen Vorschriften - über die von uns durchgeführten Datenverarbeitungen. Wir weisen darauf hin, dass es sich um Datenverarbeitungen handelt, die wir bereits in der Vergangenheit durchgeführt haben und sich daher im Arbeitsverhältnis keine Änderungen ergeben.

Im Rahmen Ihres Arbeitsverhältnisses werden die von Ihnen zur Verfügung gestellten Daten (z.B. Lebenslauf, Notfallkontakte) sowie jene, die aufgrund des Dienstverhältnisses anfallen (z.B. Gehaltsdaten, Krankenstände, Pflegeurlaub, Karenzzeiten), verarbeitet.

Allgemeine Datenverarbeitung im Rahmen des Arbeitsverhältnisses

Die Verarbeitung und Übermittlung der Daten erfolgt für die Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen

oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten. Ohne diese Daten können wir den Vertrag mit Ihnen nicht abschließen bzw. durchführen. Dies gilt auch für alle freiwilligen Sozialleistungen des Arbeitgebers sowie für externe Bildungs- und Weiterbildungsangebote.

Eine Übermittlung der im jeweiligen Einzelfall relevanten Daten erfolgt auf Grundlage der gesetzlichen Bestimmungen bzw. vertraglicher Vereinbarung an folgende Stellen:

{Nichtzutreffendes streichen}

- Lohnverrechnung (extern)
- Sozialversicherungsträger (einschließlich Betriebskrankenkassen);
- Bauarbeiter- Urlaubs- und -Abfertigungskasse;
- Bundesamt für Soziales und Behindertenwesen (Sozialministeriumsservice) z.B. gemäß § 16 BEinstG;
- Finanzamt;
- Betriebliche Vorsorgekassen (BV-Kassen) gemäß § 11 Abs 2 Z 5 und § 13 BMSVG;
- Lehrlingsstelle gemäß §§ 12 und 19 BAG und Berufsschulen;
- Arbeitsmarktservice;
- Arbeitsinspektorat, Verkehrs-Arbeitsinspektion und Land- und Forstwirtschaftsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz;
- Gemeindebehörden und Bezirksverwaltungsbehörden in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG usw.);
- gesetzliche Interessenvertretungen;
- Betriebsärzte;
- Kunden und Interessenten des Auftraggebers;
- Bildungs- und Weiterbildungsanbieter;
- Wahlvorstand für Betriebsratswahlen;
- Organe der betrieblichen Interessenvertretung (insbesondere Betriebsrat gemäß § 89 ArbVG, Sicherheitsvertrauensperson nach § 10 ASchG, Jugendvertrauensperson gemäß § 125 ff ArbVG und Behindertenvertrauensperson gemäß § 22a BEinstG);
- Betriebsratsfonds gemäß § 73 Abs 3 ArbVG;
- Rechtsvertreter;
- Gerichte;
- Gläubiger der betroffenen Person sowie sonstige an der allenfalls damit verbundenen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen;
- mit der Auszahlung an die betroffene Person oder an Dritte befasste Banken;

- vom Arbeitnehmer angegebene Gewerkschaft, mit Einwilligung der betroffenen Person;
- Mitversicherte;
- Pensionskassen;
- Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelversicherung;
- Betreiber der Betriebskantine;
- …….. [allenfalls ergänzen, insb im Hinblick auf externe Stellen, die mit der Abwicklung freiwilliger Sozialleistungen betraut sind].

Datenverarbeitung für Zwecke der Verwaltung und Sicherheit des Systems

Aufgrund der geltenden gesetzlichen Datensicherheitsbestimmungen werden eine Reihe Ihrer Daten für die Verwaltung und Sicherheit des Systems verarbeitet, wie etwa zur Verwaltung von Benutzerkennzeichen, die Zuteilung von Hard- und Software an die Systembenutzer sowie für die Sicherheit des Systems. Dies schließt automationsunterstützt erstellte und archivierte Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten mit ein. Ohne diese Datenverarbeitung ist ein sicherer Betrieb des Systems und damit eine Beschäftigung in unserem Unternehmen nicht möglich.

{Falls berufliche Mitarbeiterkontaktdaten im Intranet veröffentlicht werden}

Veröffentlichung beruflicher Kontaktdaten im Intranet

Zur Kontaktaufnahme durch Kollegen werden berufliche Kontaktdaten im Intranet veröffentlicht. Dies erfolgt aus unserem berechtigten Interesse an einem reibungslosen Geschäftsablauf. Wenn Sie das aus berücksichtigungswürdigen Gründen nicht wollen, können Sie gegen die Veröffentlichung Widerspruch einlegen.

{Falls berufliche Mitarbeiterkontaktdaten auf der Firmen-Website veröffentlicht werden}

Veröffentlichung beruflicher Kontaktdaten auf der Firmen-Website

Zur Kontaktaufnahme durch Kunden und Lieferanten werden berufliche Kontaktdaten von Mitarbeitern mit Außenkontakt im Internet veröffentlicht. Dies erfolgt aus unserem berechtigten Interesse an einem reibungslosen Geschäftsablauf. Wenn Sie das aus berücksichtigungswürdigen Gründen nicht wollen, können Sie gegen die Veröffentlichung Widerspruch einlegen.

Datenverarbeitung im Falle von Arbeitsrechtsstreitigkeiten

Kommt es während aufrechten Arbeitsverhältnisses oder nach Beendigung zu einer gerichtlichen Auseinandersetzung, werden die für die zweckentsprechende Rechtsverfolgung notwendigen Daten an Rechtsvertreter und Gerichte übermittelt.

Verarbeitung freiwilliger Angaben - Einwilligung

Die Angabe Ihres Religionsbekenntnisses erfolgt freiwillig und auf Grundlage Ihrer Einwilligung, wenn Sie entsprechende Rechte in Anspruch nehmen möchten oder den Kirchenbeitrag über den Arbeitgeber abführen lassen.

Die Angabe Ihrer Gewerkschaftszugehörigkeit erfolgt freiwillig und auf Grundlage Ihrer Einwilligung, wenn Sie den Gewerkschaftsbeitrag über den Arbeitgeber abführen lassen.

Die Angabe der Notfallkontakte erfolgt freiwillig und auf Grundlage Ihrer Einwilligung.

Die Veröffentlichung Ihres Fotos im Intranet/auf der Firmen-Website erfolgt freiwillig und auf Grundlage Ihrer Einwilligung.

Alle Einwilligungen können unabhängig voneinander jederzeit widerrufen werden. Ein Widerruf hat zur Folge, dass wir Ihre Daten ab diesem Zeitpunkt zu oben genannten Zwecken nicht mehr verarbeiten, und somit die entsprechenden Rechte, Vorteile etc nicht mehr in Anspruch genommen werden können. Für einen Widerruf wenden Sie sich bitte an*: …….. [bitte hier die entsprechenden Kontaktdaten ergänzen].*

{*Bei Unterstützung durch einen externen EDV*-Dienstleister} Eine Reihe von Daten werden zur Erbringung von [*z.B. Help-Desk-Diensten, Cloud-Diensten, Recruiting-Plattform*] an einen Auftragsverarbeiter weitergegeben.

{Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR}

Datenverarbeitung außerhalb der EU/des EWR

Ihre Daten werden zumindest zum Teil auch außerhalb der EU bzw des EWR verarbeitet, und zwar in …… *[Staaten aufzählen*]. Das angemessene Schutzniveau ergibt sich aus {nichtzutreffendes streichen}

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- Ausnahme für bestimmten Fall nach Art 49 Abs 1 DSGVO.
- Ausnahme für Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

Speicherdauer

Wir speichern Ihre Daten im Rahmen der gesetzlichen Aufbewahrungspflichten.

Ihre Rechte

Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu. Dafür wenden Sie sich an uns.

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren.

Sie erreichen uns unter folgenden Kontaktdaten:

……..

[bitte hier Ihr Unternehmen bzw die Personalabteilung und die Kontaktdaten ergänzen]

{falls ein Datenschutzbeauftragter vorhanden ist**}**

Unseren Datenschutzbeauftragten erreichen Sie unter …… *[Bitte hier die Kontaktdaten des Datenschutzbeauftragten ergänzen, z.B. Telefonnummer, datenschutzbeauftragter@unternehmen.at]*

5.2.2 Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen

Erläuterung: Dieses Muster kann entweder selbständig oder im Rahmen eines Dienstvertrages verwendet werden.

Diese Verpflichtungserklärung betrifft:

- Familienname:
- Vorname:

In Ausübung Ihrer beruflichen Tätigkeit erhalten Sie voraussichtlich Kenntnis über personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Datenschutzrechts sowie des Wettbewerbsrechts.

Mit Ihrer Unterschrift verpflichten Sie sich,

- das Datenschutzrecht zu wahren, insbesondere § 6 DSG, einschließlich entsprechender betrieblicher Anordnungen;
- Geschäfts- und Betriebsgeheimnisse zu wahren (§ 11 UWG);
- bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden durch Vereinbarung einer Konventionalstrafe pauschaliert, und zwar im Ausmaß von *[Anzahl eintragen]* Bruttomonatsentgelten.

Die zitierten Bestimmungen sind im Anhang zu dieser Erklärung abgedruckt.

Ihnen ist bekannt, dass

- die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist;
- personenbezogene Daten, die Ihnen auf Grund Ihrer beruflichen Beschäftigung anvertraut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen;
- es untersagt ist, Daten an unbefugte Empfänger innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen;
- es untersagt ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten;
- es untersagt ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verarbeiten;
- anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sorgfältig verwahrt und geheim zu halten sind;
- allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind;
- diese Verpflichtung auch nach Beendigung Ihrer Tätigkeit fortbesteht;
- Verstöße gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und schadenersatzpflichtig machen.

Hiermit erkläre ich, am [*Datum der Belehrung*] von meinem Arbeitgeber über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

Ort, Datum | Unterschrift des Verpflichteten

Datengeheimnis nach § 6 DSG

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich

zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Sicherheit der Verarbeitung nach Art. 32 Abs 4 DSGVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch anvertrauter Vorlagen nach § 11 UWG

(1) Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)

(2) Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.

(3) Die Verfolgung findet nur auf Verlangen des Verletzten statt.

5.2.3 Beispiele für Datenverarbeitungen

Nachfolgend aufgelistet sind Beispiele **typischer Datenverarbeitungen** samt Beschreibung der damit **verfolgten Zwecke**. Entnommen wurde diese Liste dem Entwurf einer Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung („White-List"). Bei diesen Datenverarbeitungen ist – soweit keine über die angeführten Zwecke hinausgehenden verfolgt werden - von keinem hohen Risiko für die Rechte und Freiheiten natürlicher Personen auszugehen.

Kundenverwaltung, Rechnungswesen, Logistik, Buchführung

Verarbeitung personenbezogener Daten im Rahmen jeglicher Geschäftsbeziehung mit Kunden und Lieferanten im Rahmen einer Gewerbeausübung samt systematischer Aufzeichnung aller die Einnahmen und Ausgaben betreffenden Geschäftsvorgänge.

Personalverwaltung für privatrechtliche Dienstverhältnisse

Verarbeitung und Evidenthaltung personenbezogener Daten für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist;

Verarbeitung und Evidenthaltung personenbezogener Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne der Art. 9 und 10 DSGVO im Rahmen dieser Ausnahme ist ausschließlich aufgrund einer gesetzlichen Ermächtigung oder aufgrund rechtlicher Verpflichtungen zulässig.

Kundenbetreuung und Marketing für eigene Zwecke

Verarbeitung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot sowie zur Durchführung von Werbemaßnahmen und Newsletter-Versand.

Sach- und Inventarverwaltung

Inventarverwaltung (Führung von Inventaraufzeichnungen), Unterstützung des Sachgüteraustausches und der Betriebsabrechnung, mit der Inventarverwaltung in Zusammenhang stehende Neben- und Hilfsaufzeichnungen über Lieferanten, Anschaffungskosten sowie Verwaltung der Zuteilung von Hard- und Software an EDV-Systembenutzer.

Zugriffsverwaltung für EDV-Systeme

Verwaltung von Benutzernamen und Passwörtern sowie Systemzugriffsprotokollierung.

Zutrittskontrollsysteme

Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt verarbeiten.

Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)

1. Allgemeine Voraussetzungen:

a) Räumlicher Erfassungsbereich

Örtlichkeiten, über welche der Verantwortliche verfügungsbefugt ist. Die Videoüberwachung darf räumlich nicht über die Liegenschaft hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter gemessen von der Grundstücksgrenze des überwachten Objekts. Die Videoüberwachung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.

b) Speicherdauer

Aufgenommene personenbezogene Daten sind vom Verantwortlichen spätestens nach 72 Stunden zu löschen, es sei denn eine längere Speicherdauer wurde in einem Gesetz, durch einen behördlichen Rechtsakt oder in einer Betriebsvereinbarung ausdrücklich festgelegt.

c) Kennzeichnung

Geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.

2. Allgemein zugängliche Örtlichkeiten, die dem Hausrecht des Verantwortlichen unterliegen

Bild- und Akustikverarbeitungen, welche für den vorbeugenden Schutz von Personen oder Sachen an allgemein zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich sind und kein gelinderes geeignetes Mittel zur Verfügung steht. In Fällen, in denen Arbeitnehmervertretungen gesetzlich verpflichtend einzurichten sind, ist das Vorliegen einer gültigen Betriebsvereinbarung, welche die Durchführung der Videoüberwachung regelt, Voraussetzung.

Bild- und Akustikdatenverarbeitung in Echtzeit

a) Räumlicher Erfassungsbereich

Örtlichkeiten, über welche der Verantwortliche verfügungsbefugt ist. Die Bilddatenverarbeitung darf räumlich nicht darüber hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter. Die Bild- und Akustikdatenverarbeitung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.

b) Kennzeichnung

Voraussetzung für die Ausnahme ist die geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.

Es erfolgt keine Aufzeichnung.

Bild- und Akustikverarbeitungen zu Dokumentationszwecken

Bild- und Akustikverarbeitungen, welche ausschließlich ein Dokumentationsinteresse verfolgen, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist. Strafrechtliche, verwaltungsstrafrechtliche oder zivilrechtliche Zwecke dürfen im Rahmen dieser Ausnahme nicht verfolgt werden.

Organisation von Veranstaltungen

Datenverarbeitung zur Abhaltung von Veranstaltungen, wie Einladung und Registrierung der Teilnehmer, Organisation von Reisen und Aufenthalten, Versorgung der Teilnehmer und Kommunikation vor und nach der Veranstaltung, Abrechnung von Geldleistungen (Honorare, Ersatz für Reisekosten), Abwicklung von Kulturprogrammen oder Übermittlung von Unterlagen.

5.3 Nützliche Links

- Aufsichtsbehörde, Rechtsdurchsetzung und Strafen:
  - Datenschutzbehörde https://www.dsb.gv.at/
  - Rechtsdurchsetzung https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Rechtsdurchsetzung-und-St.html
  - Strafen https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-behoerde-strafen-umsetzung-faq.html,
- Online-Ratgeber
  - dsgvo.wkoratgeber.at (Tipps zur Umsetzung der DSGVO)
  - dsgvo-informationsverpflichtungen.wkoratgeber.at (=Datenschutzerklärung)
  - it-safe.wkoratgeber.at (betrifft Datensicherheitsmaßnahmen)
- FAQ‘s
  - FAQ Onlinebereich: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-online-bereich-faq.html
  - FAQ Datensicherheit: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-datensicherheit-faq.html
  - FAQ Auskunftspflicht: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-auskunftspflichten-faq.html
  - FAQ Rechtmäßigkeit der Datenverarbeitung: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-einwilligung-rechtmaessigkeit-datenverarbeitung-fa.html
  - FAQ soziale Netzwerke: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-soziale-netzwerke-faq.html
  - FAQ Mitarbeiterdaten: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-mitarbeiterdaten-faq.html
  - FAQ Verarbeitungsverzeichnis: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-verarbeitungsverzeichnis-faq.html
  - FAQ sensible Daten: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-sensible-daten-faq.html
- Broschüren
  - Broschüre Datenschutz-Grundverordnung (Webshop)
  - IT-Sicherheitshandbuch für KMU (download)
  - IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter (download)
- Informationsblätter, Musterverzeichnisse usw. zu Datenschutz und Datensicherheit
  - www.wko.at/datenschutz
  - Musterdokumente für das Verarbeitungsverzeichnis sowie ein Mustervertrag für die Auftragsverarbeitung https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Musterdokumente-zur-EU-Datenschutzgrundverordnung.html
  - www.it-safe.at (hier sind insb die IT-Sicherheitshandbücher sind sehr lesenswert)