# Datenschutz – ein heißes Thema auch für Skischulen

**Es bleiben weniger als 200 Tage zur Umsetzung der EU-Datenschutzgrundverordnung (DSGVO). Die DSGVO tritt am 25. Mai 2018 in Kraft und legt allen Unternehmen, unabhängig von deren Größe, umfangreiche Pflichten zum Schutz personenbezogener Daten auf. Werden diese Pflichten nicht oder nur mangelhaft erfüllt, drohen hohe Strafen. Das gilt auch für Skischulen.**

## 1. Grundsätze

Die DSGVO hat sich zum Ziel gesetzt, den Schutz personenbezogener Daten innerhalb der EU in noch größerem Ausmaß zu vereinheitlichen und die Rechte betroffener Personen – also jener Personen, deren Daten gespeichert werden – zu stärken.
Um diese Ziele zu verwirklichen, legt die DSGVO den Datenschutz in die Eigenverantwortung der Unternehmen. Sie müssen ab 25. Mai 2018 in ihrem Umfeld dafür sorgen, dass personenbezogene Daten angemessen geschützt sind. Das bedeutet im Wesentlichen Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Die personenbezogenen Daten sollen also davor geschützt sein, dass sie von Dritten eingesehen oder gar entwendet werden. Es muss auch sichergestellt sein, dass die Daten nicht unzulässig verändert oder manipuliert und dass sie bei Verlust (z.B. aufgrund eines Hackerangriffs oder infolge eines Computerviruses) jederzeit wiederhergestellt werden können.
Dabei sind auch noch die allgemeinen Grundsätze des Datenschutzes einzuhalten. Dies sind etwa Rechtmäßigkeit der Verarbeitung, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit und Speicherdauerbegrenzung.

## 2. Rechtmäßigkeit und Zweckbindung

Nach der DSGVO sind Datenverarbeitungen verboten, es sei denn, sie erfolgen „rechtmäßig“. Rechtmäßig bedeutet, dass eine von sechs Voraussetzungen vorliegen muss, die in der DSGVO genannt werden. Eine Datenverarbeitung ist etwa dann rechtmäßig, wenn die Daten zur Vertragserfüllung benötigt werden, wenn eine wirksame Einwilligung vorliegt, wenn eine rechtliche Pflicht zur Verarbeitung besteht oder wenn überwiegende Interessen des Verarbeiters jene des Betroffenen überwiegen.
Bei jeder einzelnen Datenverarbeitung ist zu prüfen, auf welcher dieser Grundlagen sie erfolgt. Speichert eine Skischule etwa Mitarbeiterdaten, wird das in der Regel zulässig sein, weil sich schon aus den Steuer- und Sozialversicherungsgesetzen eine Pflicht zur Speicherung ergibt. Speichert die Skischule Gästedaten, wird dies zunächst auch rechtmäßig sein, allerdings nur in solchem Maß, als die Speicherung dieser Daten zur Erfüllung des Skikursvertrages notwendig ist. Werden die Gästedaten für andere Zwecke verarbeitet, z.B. erhalten die Gäste einen Newsletter, kann diese Verarbeitung nicht mehr auf den Rechtmäßigkeitsgrund der Vertragserfüllung gestützt werden, da ein Newsletter nicht unbedingt zur Vertragserfüllung erforderlich ist. Es muss hier geprüft werden, ob allenfalls ein anderer Grund, etwa

überwiegende berechtigte Interessen der Skischule oder eine gültige Einwilligung des jeweiligen Empfängers, vorliegt. Daten dürfen also immer nur für einen bestimmten Zweck verwendet werden.

### 3. Betroffenenrechte

Die Rechte betroffener Personen wurden mit der DSGVO erweitert. Neben den ohnehin schon bestehenden Auskunfts-, Berichtigungs- und Löschungsrechten wurde auch ein Recht auf Datenportabilität vorgesehen. Jeder Betroffene kann verlangen, dass seine Daten in einem gängigen Format an einen Dritten weitergegeben werden. Wenn also ein Gast die Skischule wechselt, könnte er verlangen, dass seine Daten an die neue Skischule übertragen werden.
Wichtig sind auch die Informationsrechte. Bei Datenerfassung ist jeder Betroffene proaktiv über bestimmte Umstände aufzuklären. Er muss etwa Informationen über seine Rechte, die Daten des Verarbeiters und Ähnliches erhalten. Hier gilt es zu überlegen, wie man diesen Informationspflichten organisatorisch am besten nachkommt. Werden Daten über die Website erfasst, wird dies regelmäßig in einer Datenschutzerklärung geschehen, wobei zu beachten ist, dass diese Informationspflichten auch schon bei der Erfassung von IP-Adressen zur Anwendung kommen.

### 4. Dokumentations- und Nachweispflichten, Verarbeitungsverzeichnis, Auftragsverarbeiter

Besonders bedeutsam und wohl auch aufwändig sind die zahlreichen Dokumentations- und Nachweispflichten, die die DSGVO von Unternehmen fordert. Grundsätzlich gilt, dass der Datenschutz im Unternehmen zu dokumentieren ist und im Bedarfsfall auch der Behörde nachzuweisen ist.
Dies fängt beim sogenannten Verarbeitungsverzeichnis an, geht über eine lückenlose Dokumentation der Sicherheitsmaßnahmen, über den Nachweis der Einwilligungen bis hin zur Dokumentation von Verträgen mit sogenannten Auftragsverarbeitern. Auftragsverarbeiter sind externe Dritte, die in irgendeiner Weise Daten für das Unternehmen verarbeiten. Das kann eine ausgelagerte Lohnbuchhaltung, die Werbeagentur (Erstellung der Homepage und Auswertung von Daten), eine Druckerei, die Adressdaten erhält, oder auch der IT-Dienstleister sein. Mit ihnen allen sind Verträge abzuschließen, die einen ganz bestimmten Inhalt haben müssen: Sie regeln insbesondere die exakten Pflichten des Auftragsverarbeiters, der die Daten nur auf dokumentierte Weise verarbeiten darf.
Mehr Schwierigkeiten als diese Verträge dürfte die Erstellung eines Verarbeitungsverzeichnisses mit sich bringen. Dort sind alle Datenverarbeitungen im Unternehmen zu erfassen, zu beschreiben und auch die Maßnahmen anzuführen, die das Unternehmen zur Erreichung der Ziele der DSGVO setzt.
Die Behörde kann ab 25. Mai 2018 jederzeit die Vorlage dieses Verzeichnisses verlangen. Das Verzeichnis ersetzt die bisherige Anmeldung im Datenverarbeitungsregister (Stichwort: DVR-Nummer). Diese entfällt dann gänzlich. Umso wichtiger ist es, ein exaktes Verarbeitungsverzeichnis zu führen.

### 5. Technische und Organisatorische Maßnahmen (TOMs)

Wie bereits oben erwähnt, hat jedes Unternehmen ein angemessenes Schutzniveau im Hinblick auf personenbezogene Daten herzustellen. Dabei geht es um die Implementierung geeigneter technischer, aber auch organisatorischer Maßnahmen. Grundsätzlich soll die gesamte IT eines Unternehmens so gestaltet sein, dass größtmöglicher Datenschutz gewährleistet ist („privacy by design“). Dazu gehört etwa, dass die IT auf dem Stand der Technik ist, geeignete Sicherheitsmaßnahmen getroffen werden (Firewall, Virenschutz, etc.) oder etwa auch unternehmensinterne Zugriffsberechti-

gungen genau verteilt werden („as needed“ – nicht jeder darf etwa die Mitarbeiterdaten einsehen).
Gleichermaßen sind organisatorische Vorkehrungen zu treffen: Dazu zählen etwa die Erlassung interner Datenschutzrichtlinien und die Schulung von Mitarbeitern in Bezug auf den Datenschutz.
All dem sollte eine Risikoanalyse vorausgehen, bei der zuerst der Ist-Stand im Unternehmen erhoben wird und sodann evaluiert wird, welche Maßnahmen ergriffen werden müssen, um ein angemessenes Schutzniveau zu erreichen.

## 6. Bilder und Videos

Bilder und Videos gelten als personenbezogene Daten, wenn darauf einzelne Personen erkennbar sind. Das bedeutet, dass auch für Fotos oder Videos, die von Skischulen angefertigt werden, die neuen datenschutzrechtlichen Bestimmungen gelten. Sie dürfen also z.B. nur dann auf der Website eines Unternehmens für Marketingzwecke verwendet werden, wenn diese Verwendung „rechtmäßig“ im Sinne der DSGVO erfolgt und die Informationspflichten gegenüber dem Betroffenen eingehalten wurden.
Daneben ist aber ohnehin schon jetzt das Recht auf das eigene Bild zu beachten. Grundsätzlich ist demnach die Zustimmung einer erkennbar abgebildeten Person erforderlich, wenn Fotos oder Videos dieser Person verwendet werden. Die DSGVO sieht jedoch noch zusätzliche Pflichten vor und insbesondere fallen Verletzungen ab 25. Mai 2018 unter den massiven Strafrahmen der DSGVO (siehe unten Punkt 8.).
In diesem Bereich müssen Skischulen in Zukunft daher noch vorsichtiger agieren.

## 7. Sonstige Pflichten

Die DSGVO kennt noch weitere Pflichten, die aber nicht jedes Unternehmen treffen. Zu diesen Pflichten zählen etwa die Ernennung eines Datenschutzbeauftragten oder die Durchführung einer Datenschutz-Folgenabschätzung. Letztere ist eine vertiefte Risikoanalyse bei kritischen Datenverarbeitungen (z.B. bei systematischer Überwachung von Personen). Skischulen werden von diesen weiteren Pflichten eher nicht betroffen sein, wobei dies allerdings in jedem einzelnen Fall zu klären ist.

## 8. Strafen und Schadenersatz

Auch bisher gab es schon zahlreiche Pflichten im Bereich des Datenschutzes, die aber oft schlicht missachtet wurden. Ein Grund dafür war wohl, dass es kaum oder nur geringe Strafen bei Verstößen gab.
Das ändert sich mit der DSGVO schlagartig: Die Strafdrohung geht jetzt bis zu EUR 20 Millionen oder 4% des jährlichen Konzernumsatzes, je nachdem, welcher Betrag höher ist. Es kann also richtig teuer, ja sogar existenzbedrohend werden, wenn man sich nicht an das Datenschutzrecht hält.
Daneben sieht die DSGVO vor, dass jede betroffene Person, deren Recht auf Datenschutz verletzt wird, Schadenersatzansprüche geltend machen kann. Das mag zwar bei einer Einzelperson nicht viel ausmachen, wenn aber etwa Datensätze von 10.000 Betroffenen von Hackern gestohlen werden und jeder Betroffene macht EUR 500,- an Schadenersatz gegen das Unternehmen geltend, mit der Begründung, es habe keine ausreichenden Sicherheitsvorkehrungen getroffen, summiert sich die Forderung auf EUR 5 Millionen.

## 9. Zusammenfassung und Tipps

Ab 25. Mai 2018 wird die Eigenverantwortung für den Datenschutz in die Hände der Unternehmen gelegt. Unternehmen müssen ab diesem Zeitpunkt dafür sorgen, dass personenbezogene Daten angemessen geschützt sind und Datenverarbeitungen rechtmäßig und nur für einen bestimmten, definierten Zweck erfolgen. Auch umfangreiche Informations-, Dokumentations- und Nachweispflichten sowie die Pflicht zur Führung eines Verarbeitungsverzeichnisses werden eingeführt.
Der 25. Mai 2018 scheint noch weit weg zu sein, tatsächlich aber ist es höchste Zeit, mit der Umsetzung zu beginnen. Angesichts der umfangreichen Pflichten und des hohen organisatorischen sowie technischen Aufwandes ist die Zeit knapp. Auch den Skischulen ist im Hinblick auf die durch die DSGVO eingeführten hohen Strafen anzuraten, die neuen rechtlichen Rahmenbedingungen genau zu beachten.

Hier ein paar Tipps, wie man vorgehen sollte:

a) Die Umsetzung wird Geld kosten. Daher: Ausreichend budgetäre Mittel einplanen.
b) Jemand im Unternehmen sollte mit den Agenden des Datenschutzes und der Umsetzung der DSGVO betraut werden – es sollte also einen Projektverantwortlichen geben. Ihm sollte auch ein Team zur Seite gestellt werden.
c) Als nächster Schritt empfiehlt es sich, den IST-Stand aller Datenverarbeitungen zu erheben. Hier wird es auch nötig sein, mit dem externen EDV-Betreuer zu kooperieren.
d) Dann sollte wohl das Verarbeitungsverzeichnis angegangen werden und erstellt werden. Das schafft mehr Klarheit, wo es „Lücken" im betrieblichen Datenschutz gibt.
e) Danach kann man sich die TOMs überlegen und umsetzen.
f) Zu prüfen ist auch, ob allfällige Einwilligungen den neuen Regelungen entsprechen.
g) Zusätzlich werden die Verträge mit den Auftragsverarbeitern anzupassen sein.
h) Schlussendlich bedarf es auch einer laufenden Evaluierung und Kontrolle.

Der Tiroler Skilehrerverband hat sich auch dieses wichtigen Themas angenommen und wird in Kürze weitere Hilfestellungen, z.B. in Form von Checklisten anbieten. Weitere Infos gibt es auch auf der Website der Datenschutzbehörde www.dsb.gv.at und bei der Wirtschaftskammer Österreich www.wko.at/datenschutz .

**Dr. Georg Huber, LL.M.**

*Rechtsanwalt*

**Mag. Melanie Gassler-Tischlinger, LL.M.**

*Rechtsanwältin*

*Greiter Pegger Kofler & Partner*

*6020 Innsbruck, Maria-Theresien-Straße 24*

*T +43 512 57 18 11 Fax: +43 512 58 49 25*

*office@lawfirm.at / www.lawfirm.at*

*Foto: Julia Türtscher, Blickfang*