Rechtliche Rahmenbedingungen elektronischer Zutrittskontrollsysteme

Clemens M. Waß[1]

SkiData AG
Untersbergstraße 40, 5083 Salzburg
clemens.wass@skidata.com

Schlagworte: Zutrittskontrollsysteme, Skigebiet, Parkraum, Personenkontrolle, Chipkarte, KeyCard, RFID, NFC, Dynamic Packaging, Internet

Abstract: Elektronische Zutrittskontrollsysteme spielen in der heutigen Informations- und Unterhaltungsgesellschaft, in der die Zugangsberechtigung zu verschiedensten Dienstleistungen immer mehr an Bedeutung gewinnt, eine zentrale Rolle. Gleichgültig, ob es sich um den Zugang zu Skigebieten, Parkräumen, Sportveranstaltungen oder Konzerten handelt, eine korrekte Erteilung von Zutrittsberechtigungen für Nutzer, eine exakte Kontrolle des Zugangs selbst und eine detaillierte Abrechung der Leistungen sind unerlässlich.

1. Einleitung

Zutrittskontrollsysteme sind aus dem Alltag nicht mehr wegzudenken. Gleichgültig, ob es sich um den Zugang zu Skigebieten, zu nicht öffentlichen Parkflächen, sportlichen Großveranstaltungen, Messen oder anderen Einrichtungen handelt: Eine einfache und effiziente Kontrolle der Berechtigung ermöglicht den Kunden einen schnellen und komfortablen Zugang und stellt andererseits für den Betreiber sicher, dass nur Kunden mit gültiger Zutrittsberechtigung auch wirklich Zutritt erlangen. Weiters erhält der Betreiber mitunter wesentliche Daten, die für die Erbringung der vertraglich zugesicherten Leistungen nötig sind.

1 Der Beitrag ist die persönliche Ansicht des Autors und kein Beitrag der SkiData AG.

2. Technische Grundlagen

Unter „elektronischen Zutrittskontrollsystemen" werden technische Systeme verstanden, die basierend auf elektronisch gespeicherten Zutrittsberechtigungen, die mittels Lesegeräten kontrolliert werden, Personen oder Fahrzeugen Zutritt zu bestimmten Einrichtungen gewähren oder den Zutritt verhindern.[2] Die Kontrollsysteme können beispielsweise Leser mit Schranken oder Drehkreuzen beinhalten, um eine physikalische Sperre zu erreichen, oder aber aus einfachen Lesegeräten bestehen, die von natürlichen Personen bedient werden, um die Zutrittsberechtigungen händisch auszulesen. Anwendungsfälle sind etwa Zutrittssysteme zu Skigebieten, Parkplätzen, Veranstaltungen, Thermen oder sonstigen Einrichtungen, die eine Zutrittskontrolle aus verschiedensten Gründen benötigen.

Als Zutrittsberechtigung können verschiedenste Geräte dienen. Wurden in der Vergangenheit oftmals „Strichcode-Tickets" verwendet, geht die Tendenz seit einigen Jahren vermehrt in die Richtung komfortabler Berührungslostechnologie. Zu diesem Zweck werden zB RFID-Chips[3] verwendet, oder aber auch Mobiltelefone, die über Bluethooth[4] oder die Darstellung von elektronischen 2-D-Strichcodes[5] am Display mit dem Leser kommunizieren. Eine weitere zukünftige Technologie, die zum Einsatz kommen wird, ist NFC[6], ein Übertragungsstandard für kurze Strecken von etwa 10 cm. Durch die geringe Reichweite wird NFC kein unmittelbarer Konkurrent zu Bluetooth oder Wireless LAN sein, zur Übermittlung von (personenbezogenen) Daten, die gerade nicht über einen großen Bereich empfangbar sein sollen, ist NFC jedoch hervorragend geeignet. Dadurch ist NFC als Zutrittsschlüssel geradezu prädestiniert.

Zur Vereinzelung von Personen oder Fahrzeugen kommen regelmäßig bekannte Geräte wie Drehkreuze mit einem oder mehreren Armen, Schranken, Türen oder sonstige Personenschleusen zum Einsatz. Die Vereinzelung ist nötig, um jede einzelne Zutrittsberechtigung gesondert automatisiert kontrollieren zu können. Dadurch wird sichergestellt, dass nur Personen oder Fahrzeuge mit einer Berechtigung Zutritt erhalten, eine aufwendige Kontrolle durch natürliche Personen kann entfallen.

---

2 Vgl Wikipedia, http://de.wikipedia.org/wiki/Zutrittskontrollsystem (15. 4. 2007).

3 Abk f Radio Frequency Identification, vgl Wikipedia, http://de.wikipedia.org/wiki/RFID (15. 4. 2007).

4 Vgl Wikipedia, http://de.wikipedia.org/wiki/Bluetooth (15. 4. 2007).

5 Vgl Wikipedia, http://de.wikipedia.org/wiki/Strichcode#2-D-Strichcode (15. 4. 2007).

6 Abk f Near Field Communication, vgl Wikipedia, http://de.wikipedia.org/wiki/Near_Field_Communication (15. 4. 2007).

3. Ausgewählte rechtliche Problemfelder

Der rechtliche Rahmen, in dem sich Hersteller, Betreiber und Nutzer von elektronischen Zutrittskontrollsystemen bewegen, ist vielfältig und kann hier nur auszugsweise dargestellt werden.

3.1 E-Commerce

Die Buchung von Zutrittsberechtigungen erfolgt immer häufiger auch online, weshalb die Normen aus dem Bereich des E-Commerce regelmäßig Anwendung finden. Der Zutrittsleser erhält über eine Onlineverbindung die Information über die erfolgreiche Erteilung der Berechtigung und gewährt dem Nutzer den Zutritt, sobald er vor Ort ist. Im Fall der Onlinebuchung sind insb die Informationspflichten des ECG zu beachten, aber auch die bekannten AGB-rechtlichen Fragestellungen tauchen in alter Tradition in neuem Gewand auf.

Eine der neuesten Erscheinungen im Bereich der Urlaubsbuchung ist die individuelle Zusammenstellung einzelner Komponenten zu einem Paket, das sog „Dynamic Packaging". Entgegen der bisherigen Praxis bucht der Kunde kein starres, vorgefertigtes Pauschalangebot, sondern wählt einzelne Element aktiv aus.[7] So kann der Kunde zB einen Flug, ein Mietauto, ein Hotel, einen Skipass und eine Zutrittsberechtigung für eine Therme in einem buchen. Eine Berührung mit elektronischen Zutrittssystemen hat er mitunter bereits hier, wenn er die ID einer bestehenden KeyCard oder eines Mobiltelefons eingibt, um diese mit der entsprechenden Berechtigung zu versehen.[8]

Interessant wird sein, wie der Internetanbieter die einzelnen AGB zum Vertragsbestandteil machen will. Die Anforderungen des ECG und der allgemeinen AGB-Kontrolle sind in jedem einzelnen Fall für jedes Paket zu beachten. Hier kann es insgesamt zu einer langen Liste von Vertragsbedingungen kommen; es stellt sich die Frage, ob es dem Verbraucher zumutbar ist, diese alle zur Kenntnis zu nehmen und ob diese gültiger Vertragsbestandteil werden. Entscheidend ist wie immer die Präsentation und der Inhalt der AGB im Einzelfall.

---

7 Vgl TravelWeekly, http://www.travelweekly.co.uk/Articles/2007/03/07/22871/dynamic-packaging-knowledge-base.html (15. 4. 2007).

8 Ein Bsp für das Aufladen von KeyCards findet sich auf der Website des Skigebiets Ski amadé, http://urlaubsplaner.skiamade.com/skitickets/ (15. 4. 2007).

Eine weitere wesentliche Frage für den Verbraucher ist, ob und inwieweit die nationalen Umsetzungsgesetze zur Pauschalreise-RL[9] zur Anwendung gelangen. In der Club-Tour-Entscheidung[10] hat der EuGH festgehalten, dass der Begriff Pauschalreise dahin auszulegen ist, dass er Reisen einschließt, die von einem Reisebüro auf Wunsch und nach den Vorgaben eines Verbrauchers oder einer beschränkten Verbrauchergruppe organisiert werden. Um nichts anderes handelt es sich bei Internetplattformen, die einzelne Bausteine aus verschiedenen Datenbanken für den Verbraucher zusammenstellen. Dadurch gerät der Internetanbieter jedoch mitunter in die Situation, dass er die Pauschalreise zusammenstellt und folglich nicht nur Vermittler ist, sondern Veranstalter mit den entsprechend weiteren Folgen.[11]

Von der Buchung und Erteilung der Zutrittsberechtigung als eigenständigem Dienst ist die spätere Gewährung des Zutritts als solchem zu unterscheiden. Obwohl hier elektronische Geräte, nämlich die Leser und die Zutrittsberechtigung, zum Einsatz kommen, handelt es sich diesbezüglich um keinen „elektronisch" erbrachten Dienst, da dieser in „materieller" Form erbracht wird. Das ECG verweist nämlich bei der Information von Diensten der Informationsgesellschaft auf § 1 Abs 1 Z 2 Notifikationsgesetz 1999, das wiederum in Anlage 1 den Zugang zu gebührenpflichtigen Straßennetzen, Parkplätzen, usw ausdrücklich ausnimmt, auch wenn elektronische Geräte bei der Ein- und Ausfahrt den Zugang kontrollieren und/oder die korrekte Gebührenentrichtung. Zutrittskontrollsysteme per se sind somit keine Dienste der Informationsgesellschaft.

Zu Grenzfällen kann es freilich kommen, je weiter sich die angebotenen Dienstleistungen von klassischen „materiellen" Anwendungen entfernen und „elektronischer" werden, um in der Terminologie des ECG zu bleiben. Beispielsweise wäre denkbar, dass Parkautomaten neben dem Verkauf der Parkplatzberechtigung auch gleichzeitig die Möglichkeit bieten, andere Dienstleistungen zu buchen. Durch den individuellen Abruf des Nutzers und mangels physischer Anwesenheit des Vertragspartners kann es gegebenenfalls zur Anwendung des ECG kommen.

9 RL 90/314/EG, ABl L 158.

10 EuGH, 30. 4. 2002, Rs. 400/00 – Club Tour, EuZW 2002, 402 m Anm *Tonner*.

11 Weiters dazu *Führich*, http://www.reiserecht-fuehrich.de/ (15. 4. 2007).

3.2 Datenschutz

Eine bedeutsame Rolle für den Bereich elektronischer Zutrittskontrollsysteme nimmt der Datenschutz ein und muss dies auch tun. Insb Technologien, die berührungslos Daten auslesen können, bergen ein gewisses Missbrauchspotential in sich. In diesem Zusammenhang sind ua die genannten RFID-Chips als Kennzeichnung von Waren ins Kreuzfeuer der Kritik geraten. Die Befürchtungen gehen dahin, dass das Kaufverhalten von Kunden über die Grundsätze – insb über den Zweckbindungsgrundsatz – des DSG 2000 hinaus verwertet wird.[12]

Hat ein Verbraucher eine Zutrittsberechtigung gekauft, sei es ein Parkticket, einen Skipass, eine Zutrittsberechtigung zu einem Hotelzimmer anstelle eines Schlüssels etc, müssen je nach Umfang der in Anspruch genommenen Dienstleistung unterschiedliche Daten gespeichert werden. Je mehr Komfort gewünscht wird und je mehr Leistungen über ein und dasselbe System in Anspruch genommen werden, desto komplizierter wird freilich das datenschutzrechtliche Geflecht. Dies nicht zuletzt deswegen, weil regelmäßig verschiedene Dienstleistungserbringer – und somit unterschiedliche natürliche oder juristische Personen – Zugriff auf denselben „Schlüssel", nämlich die Zutrittsberechtigung haben.

So ist es denkbar, dass der Verbraucher zuhause über das Internet verschiedene Zutrittsberechtigungen auf seine KeyCard bucht, indem er die Nummer der KeyCard eingibt, anschließend im Zielgebiet durch die Karte Zutritt zum vorreservierten Parkplatz erhält, im Hotel direkt auf sein Zimmer geht, ohne sich an der Rezeption anmelden zu müssen, sich am nächsten Tag ohne lästiges Warten an der Kasse direkt zum Skilift begibt, nachmittags mit derselben Karte eine Therme besucht und abends möglicherweise die KeyCard noch als Zahlungsmittel für die Hotelbar und das Pay-TV-Programm benutzt. Eine weitere Anwendungsmöglichkeit der Zutrittskontrollsysteme kann zB auch Diebstahlschutz sein, wenn nämlich ein Chip in Skier eingebaut wird und nach Meldung des Diebstahls der Zutritt für den Fahrer mit den gestohlenen Skiern gesperrt wird. Die Dienstleistungserbringer auf der anderen Seite ersparen sich durch die Verwendung elektronischer Zutrittskontrollsysteme nicht nur aufwendige händische Kontrollen, sie erhalten auch Daten, die bei der Nutzung der Zutrittssysteme entstehen, müssen jedoch bei deren Verwendung das Datenschutzgesetz beachten.

12 Siehe dazu *Knyrim/Haidinger*, RFID-Chips und Datenschutz, RdW 2005/1b, 2.

§ 1 Abs 1 DSG 2000 gewährt jedem das verfassungsrechtlich gewährleistete Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gegenüber jedermann, soweit ein schutzwürdiges Interesse daran besteht. Soweit kein Personenbezug gegeben ist, spielt das Datenschutzgesetz keine Rolle. Dies ist etwa der Fall bei einfachen Parktickets oder Tagesskikarten, die ohne Kenntnis der Person verkauft werden. Zu beachten ist jedoch, dass über eine allfällige Identifikationsnummer der Zutrittsberechtigung ein Personenbezug hergestellt werden kann. In Verbindung mit einer Bezahlung über Kreditkarte kann dies sogar schnell dazu führen, dass ein Personenbezug gegeben ist. Schließlich kann bei Parking-Anwendungen mitunter ein Personenbezug über eine Nummerntafelerkennung des Kraftfahrzeugs hergestellt werden.[13] Personenbezogene Daten sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Indirekt personenbezogen sind Daten für den datenschutzrechtlichen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Eine weitere Voraussetzung für den Schutz nach dem DSG ist das Vorliegen eines schutzwürdigen Interesses. Ein solches liegt dann nicht vor, wenn die Daten öffentlich zugänglich sind, sich also zB aus dem Telefonbuch ergeben. Daten, die durch Zutrittskontrollsysteme erfasst werden, werden jedoch so gut wie nie veröffentlicht worden sein.

Die Grundsätze für jegliche Datenverarbeitung finden sich in den §§ 6 bis 9 DSG 2000. Die durch die Zutrittskontrollsysteme erlangten Daten dürfen demnach nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden und die Verarbeitung muss sich an den Zweckbindungs- und Wesentlichkeitsgrundsatz halten.[14] Nach § 7 DSG 2000 dürfen Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen. Weiters setzt die Zulässigkeit einer Datenverwendung voraus, dass die dadurch verursachten Eingriffe nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen. Bei der Verarbeitung von nichtsensiblen Daten

13 In Spanien wird überlegt, ein Aufdrucken der Nummerntafeln auf Parktickets verpflichtend zu machen. Siehe weiters zur Nummerntafelerkennung Wikipedia, http://de.wikipedia.org/wiki/Automatische_Nummernschilderkennung (15. 4. 2007).

14 Knyrim/ Haidinger, aaO.

sind schutzwürdige Geheimhaltungsinteressen nach § 8 Abs 1 Z 4 DSG 2000 insbesondere dann nicht verletzt, wenn die Verwendung der Daten zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist. Eine Verarbeitung von nichtsensiblen Daten bei Zutrittskontrollsystemen ist somit ohne Zustimmung möglich, soweit dies zur Erfüllung vertraglicher Pflichten nötig ist. Den Betroffenen kommt gegenüber dem datenverarbeitenden Auftragnehmer allerdings eine Reihe von Rechten (insb §§ 25 ff DSG 2000) zu.

Denkbar ist schließlich, dass die Zutrittssysteme eine Verbindung zu sensiblen Daten aufweisen können. Sensible Daten sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben. Dies ist etwa dann der Fall, wenn Zutritt zu einem Kino gewährt wird, in dem ein Film mit einer besonderen Ausrichtung gezeigt wird oder Ähnliches. Nachdem andere Ausnahmen des § 9 DSG 2000 kaum die Datenverarbeitung decken werden, ist hier die ausdrückliche Zustimmung des Betroffenen notwendig.

3.3 Persönlichkeitsrechte

Elektronische Zutrittskontrollsysteme überprüfen gelegentlich nicht nur die Gültigkeit der Zugangsberechtigung, sondern machen je nach technischer Ausgestaltung auch Foto- oder Videoaufnahmen der betreffenden Personen, um deren Identität zu überprüfen, wodurch es zu einem Eingriff in die Privatsphäre dieser Personen kommen kann. Eine Foto- oder Videoaufzeichnung ist dann identifizierend, wenn sie auf Grund eines oder mehrerer Merkmale letztlich einer bestimmten Person zugeordnet werden kann.

Der OGH hat in diesem Zusammenhang festgestellt, dass, sofern ein Eingriff in die Privatsphäre feststeht, den Eingreifenden die Behauptungs- und Beweislast dafür trifft, dass er in Verfolgung eines berechtigten Interesses handelte und dass die gesetzte Maßnahme ihrer Art nach zur Zweckerreichung geeignet war. Entspricht er dieser Behauptungs- und Beweislast, kann der Beeinträchtigte behaupten, dass die Maßnahme nicht das schonendste Mittel zur Zweckerreichung darstellt. Stellt sich dabei heraus, dass die Maßnahme nicht das schonendste Mittel war, erübrigt sich die Vornahme einer Interessenabwägung.[15]

15 OGH 19. 12. 2005, 8 Ob 108/05y; vgl dazu ausführlich Anm *Thiele*, http://www.eurolawyer.at/pdf/OGH_8_Ob_108–05y.pdf.

Das berechtigte Interesse des Betreibers von Zutrittskontrollsystemen liegt regelmäßig eben in der Kontrolle des Zugangs und der Einhaltung der Vertragsbedingungen. Aufnahmen werden angefertigt, um zu überprüfen, ob tatsächlich der Berechtigte zutritt, oder ob die Zutrittsberechtigung unerlaubterweise an einen Dritten weitergegeben wurde. Häufig sehen die AGB von Betreibern vor, dass Zutrittsberechtigungen nicht übertragbar sind, so zB Skitickets und hier insb Mehrtages- oder Saisonkarten. Die Eignung besteht insofern, als dass der Zutritt entsprechend den Vertragsbedingungen nicht gewährt wird, wenn die Berechtigung an eine dritte Person weitergegeben wird. Um das schonendste Mittel handelt es sich insofern, als dass eine Identifikation nur über das Foto einer Person durchgeführt werden kann. Dem Betreiber kann nicht zugemutet werden, sich jeden einzelnen Inhaber einer Zutrittsberechtigung ohne technische Unterstützung zu merken oder jede Person einzeln zu überprüfen. Dies gilt insb in Bereichen, wo eine große Anzahl von Personen überprüft werden muss, zB bei Skigebieten oder bei Großveranstaltungen, wobei bei Letzteren erschwerend ein zeitliches Element hinzutritt, wenn tausende Besucher innerhalb von wenigen Minuten in ein Stadion strömen, dass beispielsweise 80 000 Zuseher fasst.