

Forum Zukunftstechnologie: „RFID – Ready for Business“

RFID – Recht und Privacy



Referent:
Rechtsanwalt Stefan Pflieger

Einführung

- RFID ist seit Jahrzehnten im Einsatz, die technischen Grenzen sind jedoch bei weitem noch nicht ausgeschöpft.
- Die Anwendungsmöglichkeiten von RFID Technologien sind vielfältig.
Anfangen beim industriellen Einsatzmöglichkeiten (Supply Chain Management) oder der Verhinderung von Markenpiraterie bis hin zum intelligenten Kühlschrank oder dem Einkaufswagen mit Rezeptvorschlägen ist vieles denkbar.
- Gerade die zunehmenden technischen Möglichkeiten führen dazu, dass aus den gesammelten Daten umfassende Nutzerprofile zusammengeführt werden können (Beispiel aus dem Internet: Amazon).

Chancen und Risiken

- Es besteht daher die Gefahr, dass durch diese Vielzahl an Möglichkeiten auch im Alltagsbereich (Handel) verdeckte Risiken im Umgang mit Daten geschaffen werden.
- Es wird vermehrt nach der datenschutzrechtlichen Relevanz gefragt und angezweifelt, ob der derzeitige Rechtsstand ein noch ausreichendes Schutzniveau bietet.
- Datenschutzrecht allerdings technologieneutral und kann sich auch auf (vermeintlich) neue technische Vorgänge einstellen.
- Wer danach personenbezogene Daten erheben will, braucht nach wie vor die Einwilligung des Betroffenen. Datenschutzrechtliche Grundkonstruktion bleibt erhalten.

Datenschutz - Anknüpfungspunkt

- Kernthematik juristischer Bewertungen der RFID-Technologie ist der Datenschutz.
- Anknüpfungspunkt ist hierbei der Begriff der

„personenbezogenen Daten“ iSd Datenschutzrechts (§ 3 BDSG):
Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

- Grundrecht auf informationelle Selbstbestimmung

BVerfG (Volkszählungsurteil) hat das **Grundrecht auf informationelle Selbstbestimmung** geprägt und unter Hinblick auf moderne Technologien ausgeführt, dass jede Person die Möglichkeit haben muss, auch unter veränderten technologischen Bedingungen grundsätzlich über Erhebung, Verarbeitung und Nutzung seiner Daten zu bestimmen.

Exkurs: Arbeitsgerichtliche Vorgaben

- 2004 hat das Bundesarbeitsgericht (BAG) entschieden, dass eine Videoüberwachung am Arbeitsplatz nicht lückenlos erfolgen darf.
- Ausnahme: Verdacht einer strafbaren Handlung
- Der Mitarbeiter würde einem ständigen Überwachungsdruck ausgesetzt; jedenfalls sei die Überwachung nicht zulässig, wenn der Mitarbeiter nicht wisse, wann die Kamera eingeschaltet ist und wann nicht.
- Das BAG knüpft in seiner Entscheidung also auch an die Dauer und die Erkennbarkeit an.

RFID-Technologien haben es aber gerade an sich, ständig Informationen zu senden, ohne dass der Betroffene hiervon Kenntnis hat. Mithin könnte man diese Rechtsprechung auf RFID übertragen.

Datenschutz – personenbezogene Daten auf RFID-Tag

Entscheidende Frage

- Ist eine Verbindung zwischen den auf dem RFID-Tag gespeicherten Daten und einer Person möglich?

3 Fallgruppen

- Auf dem RFID-Tag wird lediglich der eigene Code (EPC) gespeichert. Dies ist für sich genommen noch kein personenbezogenes Datum. (Bsp. Ware liegt nicht mehr im Regal...)
- Es treten Umstände hinzu, die einen Bezug zu einer Person herstellen (bspw. Bezahlungssystem).
- Auf RFID-Tag werden personenbezogene Daten iSd BDSG gespeichert (ec-Karten, Krankenversicherungskarten, SIM-Karten).

Datenschutz - Einwilligung

Grundsatz § 4 BDSG:

Die Erhebung von Daten ist grundsätzlich nur dann zulässig, wenn der Betroffene einwilligt („Verbot mit Erlaubnisvorbehalt“) oder das BDSG oder eine sonstige Rechtsnorm dies erlaubt.

wirksame Einwilligung gem. § 4, 4a BDSG

- vorherige Information (§§ 4 Abs. 3, 6c BDSG)
- schriftlich im Vorfeld
- nachträgliche Genehmigung reicht nicht aus
- in AGB möglich (bes. Hinweis erforderlich; § 4a Abs.1 BDSG a.E.)

Ausnahmefall gem. § 28 BDSG

Wenn Ausnahmefall greift, ist Einwilligung entbehrlich

Datenschutz – Ausnahme § 28 BDSG

Zweckbestimmung (§ 28 Abs.1 Nr. 1 BDSG)

- Speicherung der Daten zulässig, wenn dies zur Vertragserfüllung notwendig ist

Berechtigtes Interesse (§ 28 Abs. 1 Nr. 2 BDSG)

- der verarbeitenden Stelle und kein entgegenstehen schutzwürdiger Interessen des Betroffenen
- Wertentscheidung § 4 BDSG: im Zweifel überwiegen Rechte des Betroffenen
- Aber: für Unternehmen wird berechtigtes Interesse an Werbe- bzw. Marktforschungszwecken bejaht (Bsp. Kundenkartenmodelle)
- Aber: kein berechtigtes Interesse hinsichtlich Bewegungsprofile (Kaufverhalten, Verweildauer)

Datenschutz – Grundsätze II

- Auskunftsrecht (§§ 19, 34 BDSG)
- Benachrichtigungspflicht (§§ 19a, 33 BDSG)
eine solche besteht wenn die Daten ohne Kenntnis des Betroffenen erhoben wurden.
- Zweckbindung (§ 14 BDSG)
Personenbezogene Daten dürfen nur für (vorher) festgelegte Zwecke erhoben werden.
- Erforderlichkeit (§ 28 BDSG)
Datenerhebung darf nur erfolgen, wenn dies für entspr. Sachaufgabe erforderlich ist.
- Datensparsamkeit (§ 3a BDSG)
- Verantwortliche Stelle (§ 3 Abs. 7 BDSG)
(...) „...jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“

„unsichtbare“ Datenerhebung

- Grundsatz
Unter Datenerhebung fällt gem. § 3 Abs. 3 BDSG das (gezielte) Beschaffen von Daten des Betroffenen.
- Durch technischen Gegebenheiten von RFID ist die Möglichkeit gegeben, dass alle Transponder im räumlichen Umfeld eines Lesegeräts ausgelesen werden.
- Verantwortliche Stelle ist datenschutzrechtlichen Grundsätzen ausgesetzt.
- Nach §§ 20, 35 BDSG müssen diese Daten unverzüglich **gelöscht** werden, weil deren Speicherung unzulässig war:
u.a. keine Einwilligung, keine Zweckbestimmung...

Absicherung von RFID-Systemen

- Hinsichtlich personenbezogener Daten schreibt § 9 BDSG geeignete Schutzmechanismen vor um die Einhaltung der Vorschriften des BDSG zu gewährleisten.

„...haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes (...) zu gewährleisten...“

- Es muss hierbei jedoch eine Abwägung zwischen Aufwand und Schutzzweck erfolgen;

Hinweise zum Aufbau eines solchen Sicherheitskonzepts auf dem aktuellen Stand der Technik: www.bsi.de; „IT-Grundschutz“

Verstöße gegen Datenschutzrecht

- Bußgeld bis zu 250.000,- EUR; im Falle von Fahrlässigkeit die Hälfte
- iFv Bereicherungs- oder Schädigungsabsicht ist ein Verstoß gegen das BDSG sogar strafbar (§ 43 BDSG)
- Auskunftspflicht gegenüber Aufsichtsbehörde (für nicht-öffentlichen Bereich in Bayern : Regierung von Mittelfranken)
- ggf. Kontrollen vor Ort (§ 38 Abs. 4 BDSG)

Strafrechtlicher Schutz von RFID-Systemen

- **263a StGB**
Wer (...) das Vermögen eines anderen dadurch schädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger und unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- **269 StGB**
- *Wer (...) beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart speichert oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.*
- **274 Abs. 1 Nr. 2 StGB**
Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer (...) beweiserhebliche Daten (§202a StGB), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht einen anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert (...).
- **303a StGB**
Wer rechtswidrig Daten (202a StGB) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft.
- **303b StGB**
Wer eine Datenverarbeitungsanlage die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist (...) stört (...) wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Vielen Dank für Ihre Aufmerksamkeit!



Rechtsanwälte SPR
www.spr-anwaelte.de