LIEBENSTEIN LAW
Kanzlei für Wirtschafts- und Gesundheitsrecht

Prof. Dr.
Hans-Hermann Dirksen
Rechtsanwalt | Hochschullehrer

LIEBENSTEIN LAW
Kanzlei für Wirtschaftsrecht
Eschersheimer Landstr. 351
60320 Frankfurt/Main
mail@liebenstein-law.de
www.liebenstein-law.de
+49 69 2729 5921

Identifizieren Sie sich!

Was Sie jetzt über Auto-ID und Datenschutz wissen müssen

LIEBENSTEIN LAW – Kanzlei für Wirtschaftsrecht

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Prof. Dr. Hans-Hermann Dirksen
Rechtsanwalt | Hochschullehrer

LIEBENSTEIN LAW
Kanzlei für Wirtschafts- und Gesundheitsrecht
Eschersheimer Landstr. 351
60320 Frankfurt/Main
mail@liebenstein-law.de
www.liebenstein-law.de
+49 1573-1979-280

FOM Hochschule für Oekonomie & Management
University of Applied Sciences

Auto-ID-Systeme & DSGVO

Die **automatische Identifikation und Datenerfassung** (Auto-ID) beschreibt den Vorgang der Datenerhebung, Datenerfassung sowie Datenübertragung von Identifikationsdaten von Personen und Gegenständen sowie Informationen durch technische Mittel.

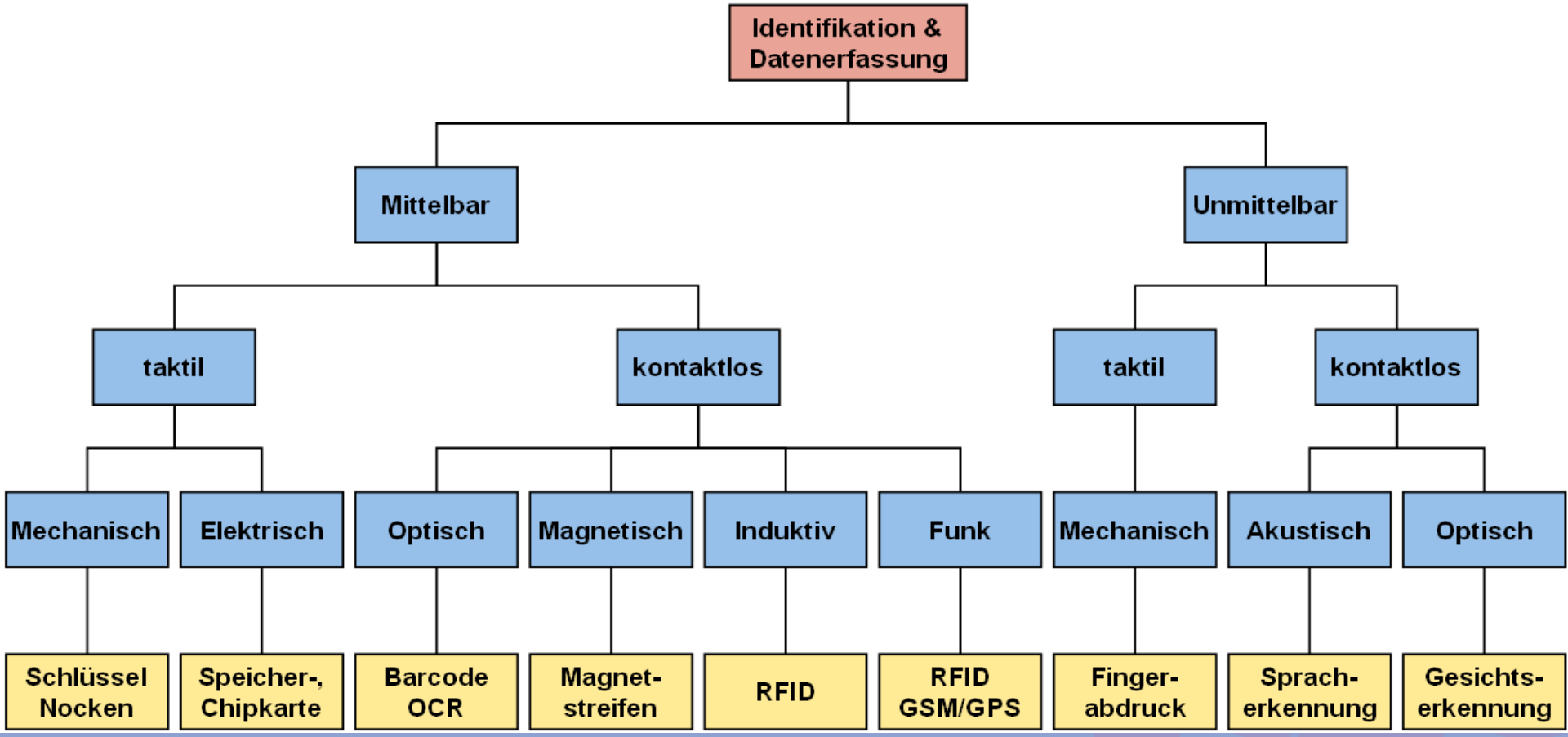
Maßgeblich ist, dass die eingesetzten technischen Mittel eine bestimmte Information auf einem entsprechenden Informationsträger selbstständig erkennen und verarbeiten können.

Beispiele für Auto-ID-Verfahren sind

- Scannerkassen-Systeme und die zugehörigen Barcodes
- Scanner für biometrische Merkmale,
- Lesegeräte für RFID-Chips,
- Scanner für die Texterfassung und
- Kartenlesegeräte mit Chipkarten.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT



Von Dr. Martin Wölker - http://www.identifikation.info/idpages/pmw/sites/identifikation.info/Basics/Uebersicht, CC-by-sa 2.0/de, https://de.wikipedia.org/w/index.php?curid=2273560

Die automatische Identifikation bietet bei der **Vernetzung** von Produktionsstätten entscheidende Vorteile. Prozesse können synchronisiert werden, da jederzeit ein reales Abbild von voneinander abhängigen Prozessen verfügbar ist und deren Relationen immer sichtbar sind.

Das bedeutet, dass unterschiedliche Wertschöpfungsprozesse **parallel** oder aber optimiert gestaffelt gestartet werden können und den Zusammenführungspunkt zeitlich richtig erreichen.

Dadurch können **Produktionszeiten** und die damit verbundenen Lieferzeiten reduziert werden. Auch das Bestandsmanagement kann über die automatische Identifikation besser bewertet und die Nachschubsteuerung effizienter organisiert werden.

Aufgrund der automatischen Identifikation wird der gesamte interne Materialfluss transparenter und so können aufgrund vorauseilender **Informationen** Rüstprozesse organisiert und der Bearbeitungsprozess kann mit dem Eintreffen der Objekte gestartet werden.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Datenschutzgrundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO, GDPR), ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden.

Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Art. 2 DSGVO Sachlicher Anwendungsbereich

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Art. 4 DSGVO Personenbezogene Daten

Der Begriff der „personenbezogenen Daten“ wird im Artikel 4 DSGVO weit gefasst:

„personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;

als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; …

Inhalte sowohl auf einer Auto-ID als auch im Hintergrundinformationssystem sind personenbezogene Daten, **wenn sie einer Person zugeordnet werden können.**

Selbst wenn die betreffenden Daten lediglich aus **Ziffernfolgen** oder **binärcodierten Werten** bestehen, kommt ihnen gleichwohl die Eignung als personenbezogenes Datum zu.

Deshalb kann die **Referenznummer** eines Auto-ID-Systems ebenso eine solche Einzelangabe sein, sofern sie sich auf eine Person beziehen lassen, wie **Parameter über die Umstände der Nutzung** des Auto-ID-Systems oder eines aufgestellten Scanner-Geräts.

Parameter von Umständen können Daten über Ort und Zeitpunkt, Häufigkeit und Dauer der Registrierung einer oder Daten über gleichzeitige Registrierung anderer Scanner beinhalten.

Auf Grundlage der beim Einsatz von Auto-ID-Systemen anfallenden Daten können Bewertungen generiert oder vorgenommen werden, die zu **Prognose- oder Planungsdaten bezüglich einer Person** führen – sei es nur, um die Kaufkraft anhand registrierter Produkte eines Kunden, Ausleihbedarf anhand der Leseinteressen eines Bibliothekbenutzers oder um den im kommenden Quartal möglichen Bedarf an Beförderungsleistungen eines Fahrgastes abzuschätzen.

Sollten die wahrscheinlichen Standorte, die eine Person etwa in einem Ladengeschäft oder Marktplatz ansteuern wird, bestimmte Produktgruppen repräsentieren, dann geben diese Prognosedaten beispielsweise **Auskünfte über seine Kaufinteressen** und **indirekt auch über seine Lebensumstände**.

Durch **Datenspuren** und das dadurch erschließbare **Kontextwissen** sind neue, bislang nicht durchführbare Auswertungen von anonymem oder pseudonymem Verhalten möglich.

Außerdem besteht die Möglichkeit, dass durch das Verhalten des Betroffenen selbst – absichtlich oder unabsichtlich – die Rückbeziehbarkeit von anonymen oder pseudonymen Daten erleichtert wird.

Eine solche Personalisierung von zunächst nicht personenbezogenen Daten ergibt sich entweder aus der **erstmaligen Zuordnung von Datenspuren oder Kontextdaten zu einer bestimmbaren Person** oder **durch Rückbezug von pseudonymisierten, anonymisierten und verschlüsselten Daten auf die ursprünglich dahinter stehende Person**.

Maschinendaten/Prozessdaten/Produktdaten

Maschinendaten sind im Wesentlichen alle Informationen, die auf einer Industriemaschine abgerufen werden.

Prozessdaten umfassen die Informationen, die zum Betrieb der Maschine erforderlich sind und direkt von der Operation generiert werden. In erster Linie sind dies die Steuerdaten, aber beispielsweise auch Informationen zum Stromverbrauch usw.

Produktdaten werden an den Verarbeitungseinheiten gemessen und liefern wertvolle Informationen über den Produktionsprozess im Zusammenhang mit dem Betrieb einer Anlage. In Bezug auf die Qualität einer Produktion sind die Daten wie Stückzahl, Gewicht, Dicke oder Temperatur wesentlich.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Verbot mit Erlaubnisvorbehalt

Grundsätzlich ist die Verarbeitung personenbezogener Daten **verboten**, es sein denn es sind bestimmte Voraussetzungen und mindestens eine der folgenden Bedingungen des Art. 6 DSGVO erfüllt:

- Es liegt die **Einwilligung** der betroffenen Person vor

- Es liegt ein **berechtigtes Interesse** an der Datenverarbeitung vor und schutzwürdige Interessen des Betroffenen stehen dem nicht entgegen

- Die Datenverarbeitung ist **erforderlich**:
  1. zur Erfüllung eines Vertrags
  2. für vorvertragliche Maßnahmen auf eine Anfrage hin;
  3. zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen;
  4. zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person;
  5. im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt.

Einwilligung

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn die betroffene Person ihre Einwilligung erteilt hat (Art. 6 Abs. 1 lit. a) DSVO).

Die DSGVO normiert bestimmte Anforderungen, die an die Einwilligung in die Datenerhebung und -verarbeitung gestellt werden. Eine wirksame Einwilligung muss zunächst hinreichend bestimmt und eindeutig sein, sich also auf konkrete **Fälle** und alle **Zwecke** der Verarbeitung beziehen.

Des Weiteren muss der Betroffene ausreichend informiert worden sein und die Einwilligung ohne Zwang abgegeben haben.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

21. Neue Rechte der Betroffenen Art. 13 ff DSGVO

- Informationspflicht
- Auskunft
- Berichtigung
- Sperrung
- Löschung
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht auf Einschränkung der Verarbeitung

Art. 13 und 14 DSGVO regeln **Informationspflichten** gegenüber dem Betroffenen, wenn personenbezogene Daten von ihm erhoben werden.

Dazu gehören Informationen zu der Identität der verantwortlichen Stelle, die Verarbeitungszwecke und zur Speicherfrist.

Zudem verlangt Art. 12 Abs. 3 DS-GVO grundsätzlich eine unverzügliche Unterrichtung.

Die Frist und geforderte Benachrichtigung bereiten bei Auto-ID-Systemen Schwierigkeiten, deren **Verarbeitungsvorgänge unmerklich im Hintergrund oder in Situationen stattfinden**, die dem Betroffenen keine Zeit, keine Aufmerksamkeit oder keine adäquate Möglichkeit einer Kenntnisnahme einräumen.

Information gemäß Artikel 13 EU-DSGVO

Im Folgenden möchten wir der Informationspflicht gemäß Artikel 13 DSGVO nachkommen.

Welche Daten / Datenarten sind konkret betroffen?

Es werden die personenbezogenen Daten wie Name, Firma, Anschrift, Kontaktdaten und Kursbuchungen erfasst und verarbeitet. Bei ärztlichen Fortbildungen erfolgt die Erfassung/Identifizierung zum Teil per Barcode / Identifikationsnummer oder falls nicht zur Hand über das Geburtsdatum.

Verarbeitungszwecke

Die Daten werden zur Verwaltung der Kursbuchungen, Übermittlung von organisatorischen Hinweisen zur Veranstaltung, Erstellung von Teilnahmeunterlagen, Vergabe von Fortbildungspunkten und der Abrechnung der Kursgebühren verwendet.

Die Art. 17 und 18 DSGVO beinhalten **Regelungen zur Löschung und zur Sperrung** von personenbezogenen Daten.

Für Auto-ID-Systeme, die an vielen Orten aufgestellt sind und in ihrem Ansprechbereich markierte Gegenstände registrieren, ist das Recht auf Löschung und Sperrung gemäß Art. 17 und 18 DSGVO ein wichtiger Baustein im Schutzprogramm, zumal die Lesegeräte vernetzt und mit Hintergrundinformationssystemen verbunden sind, in denen Registrierumstände und weitere Informationen hinterlegt werden können.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Auftragsverarbeitung

Um eine Auftragsdatenverarbeitung handelt es sich, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag verarbeitet (Art. 4 Abs. 8 DSGVO). Es sind dabei umfangreiche Regeln und Qualitätsstandards einzuhalten.

Die Verarbeitung muss so organisiert sein und mit solchen technischen Mitteln erfolgen, dass die Datenschutzanforderungen der DSGVO insgesamt eingehalten werden und der Schutz der Rechte der betroffenen Person gewährleistet wird (Art. 28 Abs. 1).

Auch wenn der Verantwortliche zugestimmt hat, bleibt der ursprüngliche Verarbeiter vollständig haftbar (Art. 28 Abs. 4 S. 2 DSGVO).

Der Auftragsverarbeitung muss ein in Textform (Art. 28 Abs. 9 DSGVO) gefasster **Vertrag** oder ein anderer Rechtsakt zugrunde liegen, der den Datenverarbeiter an den Verantwortlichen bindet und Punkte wie den Zweck der Datenverarbeitung, ihre Dauer, die Art der verarbeiteten Daten und die Rechte und Pflichten des Verantwortlichen regelt.

Zudem soll das Vertragswerk sicherstellen, dass die Daten in Übereinstimmung mit vom Verantwortlichen festgelegten Regeln übermittelt werden und dass die mit der Verarbeitung betrauten Personen Verschwiegenheitspflichten befolgen.

Der Auftragsverarbeiter soll außerdem dem Verantwortlichen und der Kontrollstelle alle Informationen bereitstellen, die für die Kontrolle der Einhaltung seiner Pflichten notwendig sind (Art. 28 Abs. 3).

Auftragsverarbeitung - Beispiele:

Lohnbuchhaltung in der Cloud;
Nutzen einer CRM-Anwendung in der Cloud;
Versendung von Newslettern und Mailings über einen Cloud-Anbieter;
Nutzen eines externen Call-Centers für den Kundenservice;
Nutzen eines Anrufdienstes für eingehende Anrufe;
Durchführung von Gewinnspielen über eine externe Agentur;
Managed Hosting von Webseiten/Onlineshops.

Auto-ID-Systeme & DSGVO

Art. 22 DSGVO - Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Die betroffene Person hat das **Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Scoring

Das bedeutet, dass die Auswertung z. B. der Arbeitsleistung, der finanziellen Lage, des Gesundheitszustandes oder des Verhaltens einer Person zum Zweck einer selbsttätig getroffenen Entscheidung ohne menschliche Einflussnahme **grundsätzlich nicht zulässig** ist.

Ausnahmen hiervon ergeben sich abgesehen von einer erteilten Einwilligung für den Fall, dass das Profiling im Rahmen des Abschlusses eines Vertrages oder dessen Erfüllung erfolgt oder wenn es durch Rechtsvorschrift zugelassen ist (Art. 22 Abs. 2).

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

T-O-M DATENSCHUTZ – ART. 24 DSGVO

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um:

sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

T-O-M DATENSICHERHEIT – ART. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

d) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

e) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Um RFID-Anwendungen datenschutzgerecht zu realisieren, ist es erforderlich, risikoadäquat **organisatorische und vor allem technische Schutzmaßnahmen** zu treffen.

Insbesondere ist die effektive Gewährleistung datenschutzrechtlicher Anforderungen im Kontext allgegenwärtiger Datenverarbeitung, in dem sich realer und virtueller Sozialraum verbindet, ohne datenschutzgerechte bzw. datenschutzfreundliche **Technik** (Privacy Enhancing Technologies, PET) nicht denkbar.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Art. 35 DSGVO - Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko **für die Rechte und Freiheiten natürlicher Personen zur Folge**, so führt der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Wann ist eine Folgenabschätzung erforderlich?

1. die systematische and umfassende Bewertung der Persönlichkeit auf der Basis automatisierter Datenverarbeitung einschließlich Profiling, die die Grundlage von Entscheidungen mit Rechtswirkungen für den Einzelnen bildet oder sich auf ähnliche Weise auf den Einzelnen auswirkt (Art. 35 Abs. 3 lit. a DSGVO);

2. die Verarbeitung sensitiver Daten gemäß Art. 9 Abs. 1 oder Art. 10 DSGVO (Art. 35 Abs. 3 lit. b DSGVO).

3. die großflächigen Videoüberwachung im öffentlichen Raum (Art. 35 Abs. 3 lit. c DSGVO).

Für Auto-ID-Anwendungen verspricht eine im Vorfeld durchzuführende Datenschutz-Folgenabschätzung und eine gegebenenfalls erforderliche Beratung durch die Aufsichtsbehörde eine sinnvolle Ergänzung des datenschutzrechtlichen Schutzprogramms.

Ein Risiko, das eine Datenschutz-Folgenabschätzung erfordert, ist insbesondere anzunehmen, wenn eine solche Anwendung Verarbeitungsvorgänge durchführt, die in der systematischen und umfassenden **Auswertung** von Profildaten einer natürlichen Person bestehen, um etwa Aufenthaltsorte, Präferenzen oder Verhalten zu analysieren oder solche Aspekte für Maßnahmen mit rechtlicher Wirkung oder erheblicher Auswirkung **vorherzusagen**.

Wenn ganze Auto-ID-Infrastrukturen Verwendung finden, haben Verarbeitungsvorgänge das Potential, Profile von Betroffenen zu bilden und auszuwerten und damit letztlich Bewegung, Handlungen und Verhalten von Personen zu überwachen.

Auto-ID-Systeme & DSGVO

DATENSCHUTZPRINZIPIEN

- Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 lit. a, 1. Fall DSGVO)
- Grundsatz der Fairness (Art. 5 Abs. 1 lit. a, 2. Fall DSGVO)
- Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a, 3. Fall DSGVO)

- Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO)

- Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO)

- Grundsatz der sachlichen Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)
- Grundsatz der begrenzten Speicherung (Art. 5 Abs. 1 lit. e DSGVO)
- Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO)
- Grundsatz der Verantwortlichkeit (Art. 5 Abs. 2 DSGVO)

- **Privacy by Design (Art. 25 Abs. 1 DSGVO)**
- **Privacy by Default (Art. 25 Abs. 2 DSGVO)**

Privacy by Design

Die Grundsätze des Datenschutzes müssen bereits vor Beginn der technischen Planung in die Konzeptionieren von Verarbeitungsvorgängen integriert werden. Daher ergeben sich drei Handlungsfelder für „Datenschutz durch Technikgestaltung“:

- Technik von Verarbeitungsvorgängen, *z. B. durch das Softwaredesign*
- Geschäftsabläufe, z. B. durch „Funktionstrennung“
- Gestaltung datenschutzfreundlicher Architektur, sowohl physisch als auch elektronisch.

Privacy by Default

Ziel ist, dass Verantwortliche Systeme bereitstellen, deren Werkseinstellungen bereits möglichst datenschutzfreundlich sind.

Benutzer eines Systems sollen hierbei jedoch explizit nicht davor geschützt werden, freiwillig und informiert datenschutzunfreundlichere Einstellungen vorzunehmen, vielmehr sollen betroffene Personen befähigt werden, die Verarbeitung personenbezogener Daten zu überwachen.

Auto-ID-Systeme & DSGVO

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Rollen

Die Datenschutzgrundverordnung sieht mehrere Rollen vor:

1. Zum einen die **betroffenen** Personen, also die in der EU ansässigen Personen,

2. Zum anderen die natürliche oder juristische Person, die für die Datenverarbeitung **verantwortlich** ist („Verantwortlicher“ – „Controller“),

3. Dann die natürliche oder juristische Person, die im Auftrag des Verantwortlichen die Daten **verarbeitet** („Auftragsverarbeiter“ – „Processor“),

4. und die nationalen Aufsichtsbehörden.

5. Schließlich die Datenschutzbeauftragten.

Für die Datenverarbeitung Verantwortlicher

„die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;“

Beispiele für Verantwortliche sind Arbeitgeber, Krankenhäuser und Firmen, die über ihre Webseiten Produkte und Dienstleistungen anbieten.

Anforderungen an Verantwortliche

Die Verantwortlichen müssen den betroffenen Personen ihre Rechte einräumen und z.B. informieren, welche Daten zu welchem Zweck wie lange gespeichert werden:

Organisatorische und technische Maßnahmen
Sie müssen angemessenen Schutz der Daten (nach Stand der Technik) gewährleisten. Pseudonymisierung kann ein Ansatz sein.

Information bei Zwischenfällen
Bei einem Zwischenfall sind die Betroffenen (ohne ungerechtfertigte Verzögerung) und Behörden (innerhalb 72 Stunden) zu informieren.

Vertrag mit Auftragsverarbeitern
Falls sie Daten im Auftrag bei einer weiteren natürlichen oder juristischen Person verarbeiten lassen, müssen sie mit diesen einen Vertrag abschließen.

Datenschutzbeauftragter
bei Firmen ab 10 (bald 20) Mitarbeitern ist ein Datenschutzbeauftragter verpflichtend.

Medizinproduktehersteller

Im Gegensatz zu den Krankenhäusern und Arztpraxen betreffen die Datenschutzgesetze die Medizinproduktehersteller nur **indirekt**.

Diese müssen aber Systeme entwickeln, mit denen die Betreiber Datenschutz-konform arbeiten können.

Medizinproduktehersteller betreffen die folgenden regulatorischen Anforderungen:

- Die MDR fordert die Einhaltung des Datenschutzes u.a. bei den klinischen Prüfungen.
- Die ISO 13485:2016 fordert, dass die Hersteller die Vertraulichkeit von Gesundheitsinformationen gewährleisten und dazu notwendige Methoden implementieren müssen.
- Die ISO 13485:2016 fordert zudem, dass die Hersteller alle regulatorischen Anforderungen (nicht nur) an den Datenschutz erfüllen.

Konsequenzen für Hersteller

Für die Hersteller ergeben sich dadurch grundsätzliche Konsequenzen bei der Gestaltung der Produkte und Prozesse.

Diese müssen u.a. folgende Systemanforderungen erfüllen

- Gezieltes Löschen der Datensätze einzelner Personen/Patienten
- Export von Datensätzen in verarbeitbarem Format z.B. XML
- IT-Sicherheit der Produkte gewährleisten. Das schließt die Fähigkeit ein, kurzfristig Patches und Updates einzuspielen bzw. zu entfernen
- Mitarbeiter (z.B. Entwickler) schulen
- Verfahrensanweisungen für Entwicklung, Support, Außerbetriebnahme, Post-Market Surveillance, Risikomanagement

Ein Hersteller sollte vor allem dafür Sorge tragen, dass sein Produkt die Anforderungen an „security by design“ und „security by default“ erfüllt.

Mithin muss der Hersteller bereits im Designvorgang darauf achten, dass zum einen im Produkt selbst und zum anderen auch bei den damit in Zusammenhang stehenden Verarbeitungsprozessen, standardmäßig der Datenschutz und die Sicherheit implementiert sind.

Da Art. 5 Abs. 2 DSGVO eine Rechenschaftspflicht verlangt, muss alles entsprechend dokumentiert werden.

Alles, was nicht dokumentiert ist, ist nicht passiert!

Herausforderungen für Hersteller intelligenter Medizinprodukte oder Medizinprodukte-Apps bei der Verarbeitung personenbezogenen Daten

Bei einigen Medizinprodukten/Apps werden allerdings die Medizinproduktehersteller selbst zu Betreibern.

Wichtig ist daher im Einzelfall zu beurteilen, ob der Hersteller Verantwortlicher im Sinne des Datenschutzrechts ist.

Zur Beurteilung der Verantwortlichkeit muss der konkrete technische und organisatorische Ablauf des Produkt-/App-Einsatzes betrachtet werden.

Sofern der Hersteller Verantwortlicher ist, muss geprüft werden, für wessen und welche Daten er verantwortlich ist und welche Pflichten er dadurch hat.

Ein verantwortlicher Hersteller muss die Prinzipien, die in der DSGVO festgelegt sind, erfüllen.

Konsequenzen für Betreiber

Die Betreiber wie die Krankenhäuser finden sich ebenfalls in der Rolle der „Verantwortlichen“ wieder und müssen die entsprechenden gesetzlichen Anforderungen erfüllen:

- Gespeicherte Daten identifizieren, Zweckbestimmungen klären
- Prozesse und Systeme für die Datenverarbeitung identifizieren
- Sicherheit der Informationstechnik prüfen und herstellen
- Konformität der Datenverarbeitung überprüfen und herstellen (das betrifft auch Webseiten)
- Verträge mit Auftragsverarbeitern überprüfen bzw. erstellen
- Datenschutzerklärungen verbessern bzw. erstellen
- Datenschutzbeauftragten benennen
- Verfahrensanweisungen überarbeiten oder erstellen (z.B. Umgang mit Notfällen)
- Beschwerdemanagement einrichten (Webseite, Personen, Prozesse, Systeme)
- Mitarbeiter schulen

Auto-ID-Systeme & DSGVO

Durch die Anforderungen der DSGVO muss einem **Hersteller** bewusst sein, was seine Kunden (die **Betreiber**) benötigt, um sich rechtskonform zu verhalten.

Aus diesem Grund sollte ein **Hersteller** dem **Betreiber** Informationen darüber zur Verfügung stellen, wie das Produkt funktioniert, welche Datenverarbeitungen stattfinden und wie der **Betreiber** die gesetzlichen Anforderungen im Produkt abbilden kann.

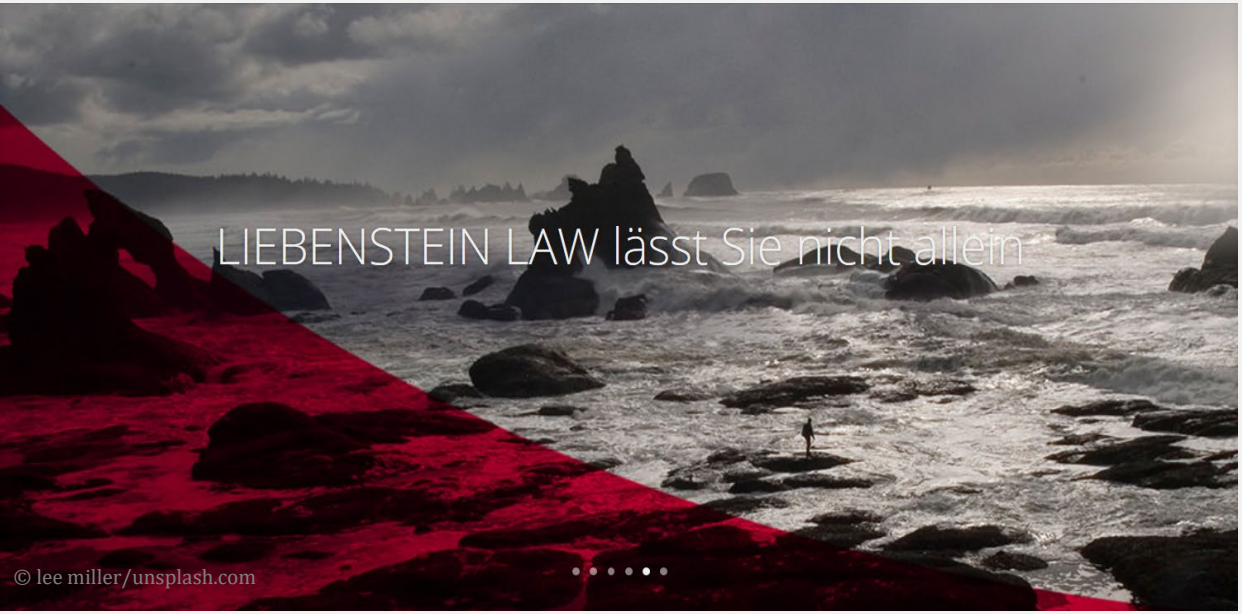
Ohne diese Informationen vom **Hersteller** ist ein **Betreiber** nicht in der Lage, eine Einschätzung des mit der Datenverarbeitung verbundenen Risikos vorzunehmen. In Konsequenz ist er dann auch nicht in der Lage, die im konkreten Sachverhalt erforderlichen technischen und organisatorischen Schutzmaßnahmen usw. zu treffen.

Dadurch dürfte es ihm auch nicht möglich sein, der ihm obliegenden Rechenschaftspflicht nachzukommen, um sich rechtskonform zu verhalten.

Hochschule für Oekonomie & Management
University of Applied Sciences

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Ich bedanke mich sehr herzlich für Ihre Aufmerksamkeit!



Prof. Dr. Hans-Hermann Dirksen
Rechtsanwalt | Hochschullehrer

LIEBENSTEIN LAW
Kanzlei für Wirtschaftsrecht
Eschersheimer Landstr. 351
60320 Frankfurt/M.
mail@liebenstein-law.de
www.liebenstein-law.de
+49 1573-1979-280