

## Anhang:

### Datenschutzerklärung für die Nutzung von Facebook-Plugins (Like Button)

Auf unseren Seiten sind Plugins des sozialen Netzwerks Facebook, 1601 South California Avenue, Palo Alto, CA 94304, USA integriert. Die Facebook-Plugins erkennen Sie an dem Facebook-Logo oder dem "Like-Button" ("Gefällt mir") auf unserer Seite. Eine Übersicht über die Facebook-Plugins finden Sie

hier: <http://developers.facebook.com/docs/plugins/> Wenn Sie unsere Seiten besuchen, wird über das Plugin eine direkte Verbindung zwischen Ihrem Browser und dem Facebook-Server hergestellt. Facebook erhält dadurch die Information, dass Sie mit Ihrer IP-Adresse unsere Seite besucht haben. Wenn Sie den Facebook „Like-Button“ anklicken während Sie in Ihrem Facebook-Account eingeloggt sind, können Sie die Inhalte unserer Seiten auf Ihrem Facebook-Profil verlinken. Dadurch kann Facebook den Besuch unserer Seiten Ihrem Benutzerkonto zuordnen. Wir weisen darauf hin, dass wir als Anbieter der Seiten keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch Facebook erhalten. Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von facebook unter <https://de-de.facebook.com/policy.php>

Wenn Sie nicht wünschen, dass Facebook den Besuch unserer Seiten Ihrem Facebook-Nutzerkonto zuordnen kann, loggen Sie sich bitte aus Ihrem Facebook-Benutzerkonto aus.



**Verstöße gegen geltendes Datenschutzrecht können zugleich aber auch Straftaten nach dem Strafgesetzbuch (StGB) sein:**

- Verletzung des Briefgeheimnisses §202
- Ausspähen von Daten §202a
- Computerbetrug §263a
- Fälschung technischer Aufzeichnungen §268
- Fälschung beweisrelevanter Daten §269
- Täuschung im Rechtsverkehr bei DV §270
- Datenveränderung §303a
- Computersabotage §303b



## **Strafbarkeit von Datenschutzverstößen**

### **Schadensersatz (Art. 82, Abs. 2 EU DS-GVO)**

**„Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.“**

### **Bußgelder und Sanktionen (Art. 83, 84 EU DS-GVO)**

Früher gab es eine Höchstsumme für Bußgelder, die bei Datenschutzverstößen gefordert wurden. Inzwischen können die Bußgelder in der Höhe von bis zu vier Prozent der Jahresumsätze des Unternehmens gefordert werden und das kann je nach Unternehmensgröße teuer werden.

weitergeben.

Andererseits gilt auch hier: Er darf, wenn er ein berechtigtes Interesse hat, es zu tun.

Doch der Artikel 88 der EU DS-GVO über den Beschäftigtendatenschutz hat bisher immer noch nicht seine endgültige Fassung.

Bis zum 25. Mai 2018 darf jeder Mitgliedstaat der Kommission noch die Rechtsvorschriften mitteilen, die er hier gerne aufgenommen hätte.

## **Werbung, Newsletter, Briefpost, Telefonmarketing**

Eine Einwilligung des Kunden scheint hier nicht mehr nötig zu sein.

Nach Art. 6 EU DS-GVO geht es hier genau wie bei der Videoüberwachung um die Berechtigten Interessen des Verantwortlichen oder Dritten, solange die Interessen der Grundrechte und –freiheiten der betroffenen Personen nicht überwiegen.

Der Erwägungsgrund 47 nennt sogar ausdrücklich die Direktwerbung ein berechtigtes Interesse von Unternehmen.

Profiling dagegen ist nicht erlaubt (Art. 4 Nr. 4 EU DS-GVO)

Unter Profiling versteht man das automatische Erstellen von Profilen. Hier werden Daten erfasst, mit denen Kundenangebote nach Alter, Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel optimiert werden sollen.

## **Einwilligung in Datenverarbeitung erst ab 16**

Erst ab 16 Jahren soll es künftig möglich sein, der Datenverarbeitung persönlicher Daten zuzustimmen. Die Kommission, die die Europäische Datenschutz-Grundverordnung ausgearbeitet hat, war der Überzeugung dass Kinder das Internet ohnehin viel zu häufig nutzen. Bisher war konnte man bereits ab dem Alter von 13 Jahren in die Verarbeitung einwilligen. Damit soll die Anmeldung bei Facebook und Co künftig schwieriger werden. Doch es bleibt fraglich, ob Kinder unter 16 dann tatsächlich die Einwilligung der Eltern einholen.

Außerdem wird es besondere Anforderungen an die Sprache geben, in der Datenschutz-Erklärungen geschrieben werden, wenn sie sich an Kinder richten. Die Sprache soll möglichst einfach und leicht gewählt werden. (Art. 12 EU DS-GVO)



## **Beschäftigtendatenschutz (Art. 88)**

Natürlich waren Mitarbeiterdaten immer schon besonders schützenswert. Schließlich handelt es sich hier meistens auch um sensible Daten wie finanzielle Situation, Religionszugehörigkeit, manchmal Gesundheitsdaten und vieles mehr, was nicht in fremde Hände geraten sollte.

Wie mit diesen Daten umzugehen ist, hatte das BDSG (Bundesdatenschutzgesetz) mit seinem § 32 geregelt. Doch im Grunde stand dort mit vielen Worten nichts anderes, als dass es erlaubt ist, die Daten von Beschäftigten zu verarbeiten, wenn das für das Arbeitsverhältnis nötig ist oder eine Straftat damit aufgedeckt wird.

Der Artikel 88 der EU DS-GVO ist da sehr viel eindeutiger und soll die Vorschriften europaweit einheitlich machen.

Danach ist die Verarbeitung von Beschäftigungsdaten zulässig,

- zur Einstellung und Erfüllung des Arbeitsvertrages
- für Management, Planung und Organisation der Arbeit
- um Vielfalt und Gleichheit am Arbeitsplatz zu erfassen
- wenn sie der Gesundheit und Sicherheit am Arbeitsplatz dient
- zum Schutz des Eigentums der Arbeitgeber und Kunden
- und zum beenden des Beschäftigungsverhältnis

### **Betriebsvereinbarungen behalten weiterhin Gültigkeit**

Die Vorschriften müssen aber immer „angemessen“ sein und besondere Maßnahmen zur Wahrung der menschlichen Würde enthalten. Zu den besonderen Maßnahmen gehört vor allem auch, ob und wem diese Beschäftigtendaten weitergegeben werden. Erlaubt ist die Weitergabe beispielsweise innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben.

Unter diese Beschäftigtendaten fallen auch die Daten, die aus Überwachungssystemen am Arbeitsplatz gewonnen werden.

Damit ist zwar die Überwachung nicht verboten, aber immerhin die Weitergabe.

### **Videoüberwachung von Arbeitnehmern**

So lange das Bundesdatenschutzgesetz noch gilt, und die Firmenkasse beispielsweise per Videoüberwachung gegen Diebstahl geschützt wird, darf der Arbeitgeber den Mitarbeiter nicht entlassen, weil auf den Aufnahmen klar erkennbar ist, dass er während seiner Arbeitszeit nichts anderes macht, als Liebesbriefe zu schreiben oder im Internet auf Datingseiten unterwegs ist. Diese Dinge darf der Arbeitgeber nicht wissen, also gelten die Videoaufnahmen nicht als Beweis für die Arbeitsunlust des Mitarbeiters.

Das ändert sich mit Einführung der EU DS-GVO. Ab 2018 darf der Arbeitgeber sehr wohl wissen, was er sieht. Er darf diese Informationen nur nicht an Fremde



## Videoüberwachung...

Videoaufzeichnung des Arbeitnehmersverhaltens waren bisher nur in engen Grenzen erlaubt. Auswertungen der Beobachtungsergebnisse zum Zweck einer mitarbeiterbezogenen Leistungs- und Verhaltenskontrolle waren unzulässig.

Wurde beispielsweise ein Mitarbeiter beim Diebstahl beobachtet, durfte das nur dann ausgewertet werden, wenn die Kamera zum Schutz vor Diebstahl eingesetzt wird.

## Die EU DS-GVO macht Videoüberwachung einfacher

Hier gibt es künftig keine konkreten Regelungen mehr. Es gelten die gleichen Vorschriften wie für alle anderen Arten der Datenverarbeitung aus: Es muss lediglich vorab geprüft werden, ob Rechte und Freiheiten von Personen mit der Videoüberwachung verletzt werden. (Art. 35) und ob es eine rechtliche Grundlage gibt.

Jede Art der Datenverarbeitung und damit auch die Videoüberwachung ist rechtmäßig, wenn

- die Betroffenen eingewilligt haben
- damit Verträge erfüllt werden (Kaufverträge, Dienstleistungsverträge)
- Verpflichtungen erfüllt werden müssen (Finanzamt – Steuererklärungen)
- sie zum Schutz lebenswichtiger Interessen nötig sind
- Wahrung einer Aufgabe im öffentlichen Interesse bzw. Ausübung öffentlicher Gewalt (Polizeiakten)

Falls keiner dieser genannten Rechtsgrundlagen zutreffen, dürfen personenbezogene Daten also trotzdem verarbeitet werden, wenn damit die berechtigten Interessen des Verantwortlichen gewahrt werden und keine Interessen, Grundrechte oder Grundfreiheiten des Betroffenen überwiegen. Hier müssen die allgemeinen Interessen abgewägt werden. Ob man darf oder nicht, ist damit Auslegungssache

Die EU-DSGVO unterscheidet nicht mehr zwischen verdeckter und offener Beobachtung. Derzeit sieht es so aus, als müsse niemand mehr auf eine Videoüberwachung hinweisen.

Regelungen über die Videoüberwachung von Arbeitnehmern gibt es gar nicht mehr.



## Cloud-Computing

- Vertrag mit Diensteanbieter zwingend erforderlich
- Technisch-organisatorische Maßnahmen des Dienstleisters überprüfen
- Erstmals VOR der Beauftragung und dann regelmäßig
- Datenübermittlung ins Ausland muss getrennt geprüft werden.

Hier gilt auch: Egal, wohin die Daten künftig übermittelt und gespeichert werden sollen – es gilt die EU DS-GVO, nach der jeder, der Dienstleistungen im Gebiet der Europäischen Union anbietet, dies nach dieser Verordnung tun müssen. Anbieter aus Drittländern müssen dann einen EU-Vertreter schriftlich bestellen. **Cloud-**

### Computing in der Praxis

Daten werden vom Cloud-Service-Provider (CSP) regelmäßig an einen externen Dienstleister zur Verarbeitung überlassen

Cloud-Service-Provider (CSP) hat seine Subunternehmer hinsichtlich der dort eingesetzten technisch-organisatorischen Maßnahmen nach zu überprüfen.

Speicherort für Daten in der Cloud wechselt in Sekundenbruchteile – damit ist es nicht nachvollziehbar, wo die Daten sich befinden

→ **Eine Überprüfung ist daher kaum möglich**

→ **Cloud-Computing bleibt damit im Bereich der Weitergabe personenbezogener Daten deshalb höchst kritisch.**



## Elektronische Daten sicher löschen und vernichten

- Daten löschen
- Anschließend physikalisch zerstören
- USB-Sticks, Speicherkarten, SSD können durch sechsmaliges Überschreiben gelöscht werden, wobei jeweils die Bitmuster des vorherigen Durchgangs umgekehrt werden. Im letzten Löschlaf wird der Datenträger mit der Bit-Folge 01010101 überschrieben...
- ... oder man verwendet eine entsprechende Software... 😊

### „Herr Müller ist leider heute nicht erreichbar. Er hat seinen Scheidungstermin...“

- Private Telefongespräche
- Mitgehörte Telefongespräche
- Auskunft am Telefon

Egal, ob privat oder dienstlich: Der Scheff darf Telefongespräche grundsätzlich nicht mithören.

Aber er darf, wenn er ein berechtigtes Interesse hat und der Arbeitnehmer sein Ok gegeben hat.

Das Interesse des Scheffs ist nach dem Datenschutzgesetz nie berechtigt, wenn der Mitarbeiter mit Interessenvertretung wie Betriebsrat, Personalrat, Jugend- und Auszubildendenvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragten telefoniert.

Wenn der Scheff ein berechtigtes Interesse hat, zuzuhören, was am Telefon besprochen wird, braucht er sich nicht ausdrücklich die Genehmigung einzuholen. Es reicht, wenn der Mitarbeiter weiter telefoniert, wenn er mitbekommen hat, dass der Scheff mithört.

Ein heimliches Mithören ist immer verboten.

### Auskunft am Telefon

Grundsätzlich gilt:

Keine Auskunft zu personenbezogenen Daten am Telefon.

Anonymisiert, also ohne Nennung des Namens ist es aber ok.

Also:

Ok ist: „der Kollege, der das bearbeitet ist krank (oder im Urlaub oder sonst wo)...“

Nicht ok ist: „Herr Maier ist krank (oder im Urlaub oder sonst wo)...“





- Computer auch bei kurzzeitigem Verlassen des Arbeitsplatzes sperren
- Keine gefundenen und erhaltenen Speichermedien ohne Prüfung auf Schadsoftware verwenden
- Auf fremde Personen (Besucher, Handwerker usw) achten und ansprechen
- Computer abends immer ganz herunter fahren – nicht in den Standby/Ruhezustand
- Keine mobilen Endgeräte am Arbeitsplatz oder im Auto liegen lassen
- Mobile Endgeräte (z.B. Notebooks, Smartphones, die verwendet werden – egal, ob von Kunden oder eigene) sicher aufbewahren.

**Leider ist alles was sicher ist auch gleichzeitig unbequem.**

### **Sichere Passwörter**

- sind mindestens acht Zeichen lang
- bestehen aus einem Mix von Groß- und Kleinbuchstaben
- enthalten mindestens eine Ziffer
- enthalten mindestens ein Sonderzeichen
- enthalten keine wahrnehmbare Systematik
- enthalten kein Wort aus einer bekannten Sprache
- werden nie für mehrere unterschiedliche Einloggvorgänge verwendet

### **Papierdokumente sicher vernichten**

#### **je nach Sicherheitsklasse:**

- vertrauliches Schriftgut
- geheimzuhaltendes Schriftgut
- maximale Sicherheitsanforderung

**je höher die Sicherheitsklasse,  
desto kleiner müssen die Schnipsel sein.**



Bundesdatenschutzbeauftragten genehmigen lassen, es sei denn, sie haben einen betrieblichen Datenschutzbeauftragten bestellt.

**Für all diese Verpflichtungen stellen wir unseren Kunden gerne auf Wunsch den externen Datenschutzbeauftragten!**

Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

## **Datensicherheit (Art. 32)**

Ging es bisher im BDSG nur darum, die Daten mit „geeigneten Mitteln“ ganz allgemein gegen Verlust, Zerstörung und Diebstahl zu schützen, wird die EU DSGVO hier sehr viel konkreter.

Ab 2018 ist der aktuelle Stand der Technik zu berücksichtigen, die Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten der Betroffenen, die tatsächlichen Risiken von Vernichtung, Verlust oder Veränderung. Hier geht es unter anderem auch um den Schutz vor Hackern, Viren und Trojanern.

Seien wir ehrlich: 100prozentige Sicherheit im Internet gibt es nicht. Das weiß natürlich auch der Gesetzgeber. Doch im Ernstfall müssen wir nachweisen, dass wir alle Maßnahmen für einen geeigneten Schutz unternommen haben.

Dazu gehören unter anderem verschlüsselte Datenübermittlungen, sichere Passwörter und ein gutes Backup-Management. In welchem Fall welche Maßnahmen sinnvoll und erforderlich sind, darüber beraten wir Sie gerne.

## **Psst... Nichts weitersagen.**

### **Wie wir zum Datenschutz beitragen können:**

- sicheres Passwort wählen
- sensible Daten auf mobilen Datenträgern verschlüsseln
- Unterlagen und Daten mit einer sicheren Methode vernichten
- Personenbezogene Daten nur für den bestimmten Zweck erheben und verwenden
- Grundsatz der Datensparsamkeit beachten
- Datengeheimnis beachten (auch untereinander)
- Interne Regelungen zum Datenschutz beachten (keine privaten eMails, kein privates Surfen)
- Virens Scanner auf dem aktuellen Stand halten
- automatische Updates für Computer, Geräten und Software einrichten
- sicheren einmaligen Benutzernamen wählen (der Benutzername „admin“ ist es nicht!)
- Backups aktuell halten



- Wenn das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt
- Wenn Archivzwecke oder wissenschaftliche und historische Forschungszwecke dem entgegenstehen

## **Namen, Fotos und Kontaktdaten ehemaliger Mitarbeiter von der Webseite entfernen**

Gelöscht werden müssen aber unverzüglich alle Namen, Fotos und Kontaktdaten ehemaliger Mitarbeiter, sobald sie nicht mehr im Unternehmen beschäftigt sind.

Wenn alle Versuche, etwas zu löschen, vergeblich sind, gibt es eine ergänzende Verpflichtung für Unternehmen nach Artikel 19:

Eine Mitteilungspflicht gegenüber allen Empfängern besteht nicht, wenn sie unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Das rechtfertigt letztendlich auch die Speicherung der Mitarbeiterdaten aus 1996 im Internetarchiv, die längst nicht mehr bei uns beschäftigt sind.

Übersetzt heißt das: Wir tun was wir können, aber nicht mehr.

## **Ein Datenschutzbeauftragter ...**

### **... ist künftig auch europaweit gesetzlich vorgeschrieben für**

- **Unternehmen mit mindestens 10 Mitarbeitern**, von denen mehr als neun regelmäßig mit personenbezogenen Daten arbeiten
- **unabhängig von der Unternehmensgröße** in:
  - o Gesundheitswesen (incl. Ärzte und Zahnärzte)
  - o Gewerkschaften
  - o Markt- und Meinungsforschungsinstitute

## **Zum Datenschutzbeauftragten**

kann bestellt werden, wer die notwendige Fachkunde besitzt. Geschäftsführer/Vorstände sowie Führungskräfte sind jedoch aufgrund des Interessenkonflikts ausgeschlossen.

Der Betriebliche Datenschutzbeauftragte kann entweder ein Mitarbeiter des Unternehmens sein (interner Datenschutzbeauftragter) oder ein externer Dienstleister sein (externer Datenschutzbeauftragter).

Unternehmen müssen die Inbetriebnahme eines neuen Verfahrens (Hard- und Software) zur Verarbeitung von personenbezogenen Daten vom Landes- bzw.



# Das Recht auf Vergessen

Darüber brauchte sich früher kaum jemand Gedanken zu machen. Damals waren die gängigen Medien, mit denen Informationen veröffentlicht wurden, Zeitungen, Radio und Fernsehen. Radio und Fernseher waren ziemlich flüchtige Medien. Wer nicht genau in dem Moment das Gerät eingeschaltet hatte, wenn eine Information gesendet wurde, den hat sie nicht erreicht. Und da es täglich neue Informationen gab, war auch das, was man hier mitbekommen hatte, schnell vergessen.

Die Zeitung war da schon etwas nachhaltiger. Schließlich kann man das, was schwarz auf weiß geschrieben steht, getrost nach Hause tragen, jedem zeigen, der es wissen möchte, aufbewahren und bei Bedarf immer noch einmal lesen, um sich die Information in Erinnerung zu rufen.

Aber selbst dann noch wird mit jeder Zeitung irgendwann nur noch Fisch eingewickelt oder der Ofen angeheizt. Denn nichts ist so alt wie die Zeitung von gestern.

In Zeiten des Internets sieht es da schon etwas anders aus. Das Internet vergisst nichts. Hier sind die Informationen immer und jederzeit abrufbar. Für immer. Oder zumindest so lange, bis derjenige, der die Macht und den Zugangscode hat, die Informationen dort entfernt.

Und selbst dann noch sind sie irgendwo vorhanden.

Das Recht auf Vergessen bleibt trotz aller Gesetze und Verordnungen nur ein frommer Wunsch. Das Internet ist bisher noch weit davon entfernt, irgendetwas zu vergessen.

Es gibt Internet-Archive, in dem alle Seiten, die jemals im Internet gestanden haben, archiviert sind.

## Das Internet vergisst nichts

Das bekannteste dieser Archive ist vielleicht das:

<https://web.archive.org/>

Die erste hier gespeicherte Seite der ms computer gmbh ist aus 1996.

Der Art. 17 EU DS-GVO regelt das Recht auf Vergessenwerden.

Danach müssen Daten gelöscht werden

- sobald sie nicht mehr benötigt werden
  - wenn die Einwilligung zur Datenverarbeitung widerrufen wird und es sonst keine Rechtsgrundlage gibt
  - wenn die Daten von vornherein unrechtmäßig verarbeitet wurden
- wenn eine Rechtspflicht zum Löschen nach einem anderen Gesetz besteht.

## Freie Meinungsäußerung und öffentliche Gesundheit

Ein Recht auf Vergessen besteht allerdings nicht, wenn

- das Recht auf freie Meinungsäußerung bzw. die Informationsfreiheit überwiegt
- Wenn die Datenspeicherung aufgrund einer rechtlichen Verpflichtung vorgeschrieben ist



Rechnungsbetrag um einen „Risikozuschlag“ wie sie es nennt. Das Schreiben an des Kunden erfolge automatisch.

Herr Maier möchte die Information schriftlich. Mit Name und Adresse der Auskunftfei, die die Liste erstellt hat.

Die Dame am Telefon zögert ein bisschen.

„Ich weiß nicht, ob ich die Adresse herausgeben darf.“

Und außerdem habe sie sich an die letzte Datenschutzschulung erinnert, dass Auskünfte grundsätzlich nicht m Telefon erteilt werden dürften.

Am Telefon könnte ja jeder sein.

„Nu mach mal halblang Mädels“, kontert Maier. „Sie haben mich unter der bei Ihnen seit Jahren hinterlegten Telefonnummer erreicht. Wer soll denn hier sonst ans Telefon gehen!“ Das Telefonfräulein ist immer noch unschlüssig.

„Wenn Sie mir schreiben, dann möchte ich bitte alle Informationen, die in Ihrer Firma über mich gespeichert sind, an wen die Daten weitergegeben werden und wie.“

Herr Maier kennt sich mit Datenschutz aus.

Und das Lieferantenfräulein willigt ein.

Als sie den Hörer aufgelegt hat, wendet sie sich an den Datenschutzbeauftragten ihres Unternehmens, damit der die Informationen zusammenstellt und Herrn Maier zusendet.

An die Auskunftfei wendet er sich schriftlich.

Dann hat er auch etwas in der Hand.

Er will Auskunft über alles, was dort über ihn gespeichert ist.

Und fordert die sofortige Richtigstellung der falschen Daten.

Die Information über das eingeleitete Konkursverfahren ist durch nichts belegt und muss deshalb geändert werden.

Doch ein „Geschmäcke“ bleibt.

Bis seine Bonität bei allen wieder ins rechte Licht gerückt ist, wird eine Zeit dauern.

Welcher Schaden ihm dadurch entstanden ist, lässt sich für eine Schadensersatzklage nur schwer ermitteln.

Was er aber auf jeden Fall als Schadensersatz geltend machen kann, sind die Mehrkosten aufgrund der negativen Auskunft für die Futtermittellieferung

## **Die Anfrage eines Betroffenen:**

- muss unverzüglich an den Datenschutzbeauftragten weitergeleitet werden
- der ist verantwortlich für die Wahrung der Betroffenenrechte
- und wird die Anfrage auf Rechtmäßigkeit prüfen, ggf. Maßnahmen einleiten und die weitere Kommunikation mit dem Betroffenen übernehmen.



## Grundsatz der Transparenz

Vereinfacht ausgedrückt heißt das:

Man darf alles, muss aber die Betroffenen informieren.

Und jeder Betroffene darf jederzeit Einspruch erheben.

**Alles ist verboten, nur das nicht, was erlaubt ist**

Auch wenn es heißt, in der EU DS-GVO gelte wie beim BDSG auch der Grundsatz, dass zunächst mal jede Datenverarbeitung verboten ist, es sei denn, es gebe eine gültige Rechtsgrundlage, die die Verarbeitung ausdrücklich erlaubt, wrscheint mir dieser Grundsatz der Transparenz trotz allem eher nach dem System zu arbeiten:

**Alles ist erlaubt, nur das nicht, was verboten ist.**

## Rechte der Betroffenen

**Diese Rechte können nicht per Vertrag ausgeschlossen werden:**

- Recht auf Auskunft (Art 15 EU DS-GVO)
- Recht auf Berichtigung falscher Daten (Art 16, 19 EU DS-GVO)
- Recht auf Löschung bzw. Sperrung (Art 17 EU DS-GVO)
- Schadensersatz.

## Ein Geschmäcke bleibt...

Fritz Maier wundert sich.

Er hat den Halbjahresbedarf der Futtermittel für seinen Bauernhof immer auf Rechnung erhalten.

Plötzlich kriegt er ein Schreiben des Lieferanten, dass er „... nun künftig nur noch auf Vorkasse beliefert“ würde. Und die Futtermittelfirma würde auch etwas mehr als sonst berechnen.

Herr Maier ist sauer. Er hat bisher immer alle Zahlungsziele eingehalten. Und irgendwie will er auch jetzt erst die Ware, dann das Geld. So viel Vertrauen war doch bisher auch da.

Er will wissen, was da los ist und ruft an.

„Es tut mir leid, ich hab nur die Anweisung bekommen, dass ich bei Ihnen künftig nur auf Vorkasse liefern darf. Warum hat mir niemand gesagt“, erklärt die Dame am Telefon mit weinerlicher Stimme.

Schon falsch.

Herr Maier hat ein Recht auf die Auskunft und das sagt er auch.

„Ich erkundige mich mal und rufe Sie dann zurück“, verspricht die Frau daraufhin.

Und das tut sie dann auch.

„Uns liegt eine Liste der Firma vor, die für uns die Bonität unserer Kunden überprüft. Auf dieser Liste sind die Unternehmen aufgeführt, für die im vergangenen Monat ein Konkursantrag gestellt wurde. So eine Liste kriegen wir jeden Monat. Auf dieser sind sie auch aufgeführt.“

Diese Firmen stelle sie dann in der Buchhaltung um auf Vorkasse und erhöhe den



Dienstleistungen hier anbietet, der eine Niederlassung im Gebiet der Europäischen Union hat oder jemanden hat, der für ihn Daten im Auftrag bei uns verarbeitet. Aber auch, wenn die Daten nicht innerhalb der EU verarbeitet werden – sobald es eine Niederlassung hier gibt, oder sonst wie Geschäfte im Gebiet der EU abgewickelt werden, gilt die EU DS-GVO.

Das Gleiche gilt auch für alle, die das Verhalten von Betroffenen innerhalb der Union beobachten. Mit der sogenannte „Facebook-Klausel“ muss jeder, der eine Internetseite besucht, die Möglichkeit haben, zu entscheiden, ob er will, dass seine Informationen beispielsweise auch in Facebook gespeichert werden oder nicht.

## **Die Facebook-Klausel**

Wer auf seine Internet-Seite Facebook-Plugins einbindet, hat damit eine direkte Verbindung zu Facebook hergestellt. Jeder Besuch der Seite wird dem Account des Nutzers zugeordnet.

Wer also solche Internetseiten besucht, hinterlässt Spuren. Und findet entsprechende Werbevorschläge auf seiner Facebook-Seite wieder, sobald er das nächste Mal hier online ist.

Jeder, der den Like-Button anklickt, der in eine Webseite integriert ist, dessen Daten werden auch bei dem Unternehmen Facebook gespeichert. Natürlich ist das nicht nur bei Facebook so, sondern bei allen anderen sozialen Medien auch.

Man kann sich davor schützen, indem man sich vor dem Besuch der Seite bei den entsprechenden sozialen Medien auslogged.

Doch das muss man wissen. Deshalb ist jeder Webseitenbetreiber, der ein solches Plugin verwendet verpflichtet, in seiner Datenschutzerklärung darauf hinzuweisen. (Muster im Anhang)

## **Der EU-Vertreter (Art. 27 Abs. 1)**

Alle, die nach diesem „Marktortprinzip“ aus Art. 3 verpflichtet sind, sich an die EU DS-GVO zu halten, müssen einen EU-Vertreter schriftlich bestellen. Seine Aufgaben sind in etwa die gleichen, die hier bei uns der Datenschutzbeauftragte übernimmt.

Einen EU-Vertreter zu bestellen ist nicht nötig, wenn die Datenverarbeitung nur gelegentlich stattfindet, keine sensiblen Daten in größerem Umfang verarbeitet werden und Risiken für die Rechte und Pflichten einzelner Bürger unwahrscheinlich erscheinen.

Auch Unternehmen wie Amazon und Facebook müssen deshalb ebenfalls ab dem 25. Mai 2018 einen solchen EU-Vertreter haben.



Es dürfen nur die Daten gespeichert werden, die für das, was man machen möchte, geeignet sind. Die Daten müssen dafür erforderlich sein und das, was wir tun, muss für die Aufgabe angemessen sein.

Diese Grundsätze sind für uns längst selbstverständlich. Mit der EU DS-GVO gelten sie ab dem 25. Mai 2018 auch über die Grenzen unseres Bundesgebietes hinaus. In der neuen Datenschutzverordnung sind die Grundsätze mit diesen Begriffen aufgeführt:

- Rechtmäßigkeit
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Auf dem Papier scheinen es ein paar mehr zu sein. Doch die tatsächliche Bedeutung ist die gleiche.

## **Die Anwendungsbereiche**

### **Sachlicher Anwendungsbereich (Art. 2)**

Es geht immer noch um den Schutz personenbezogener Daten.

Die EU-DSGVO ist hier aber noch ein bisschen genauer: Schützenswert sind die Daten natürlicher Personen. Und nicht nur die Daten, die automatisiert verarbeitet werden, sondern alle, die irgendwo irgendwie ganz oder teilweise automatisiert verarbeitet werden und auch die, die sonst irgendwo abgelegt sind.

Worum es nicht geht: Firmendaten. Wenn hier irgendwelche Informationen durchsickern, ist es nicht Sache der Datenschutz-Grundverordnung, sondern eine zivilrechtliche Angelegenheit.

### **Räumlicher Anwendungsbereich (Art. 3)**

Der räumliche Anwendungsbereich ist einer der wesentlichen Änderungen. Hier gilt das sogenannte „Marktortprinzip“. Damit ist nicht nur derjenige dazu verpflichtet, sich an unsere Europäische Datenschutz-Grundverordnung zu halten, der seinen Firmensitz innerhalb der Union hat, sondern auch jeder, der Waren und





## Grundsätze des Datenschutzes

- Informationelle Selbstbestimmung
- Datensparsamkeit
- Verantwortlichkeit
- Rechtmäßigkeit
- Datensicherheit
- Verhältnismäßigkeit

### Was heißt das?

- **Informationelle Selbstbestimmung**

Jeder darf selbst entscheiden, wer welche Informationen über ihn bekommt und hat auch das Recht jederzeit überall nachzufragen, ob und welche Daten über ihn gespeichert sind.

- **Datensparsamkeit**

Nur so viele Daten speichern, wie wirklich für die Aufgabe benötigt werden. Es ist zum Beispiel nicht nötig, Eure Staatsangehörigkeit irgendwo zu speichern, wenn ihr eine Waschmaschine kaufen wollt.

- **Verantwortlichkeit**

Derjenige, dem die Daten anvertraut wurden, trägt die Verantwortung dafür, was damit passiert.

- **Rechtmäßigkeit**

Natürlich dürfen wir nicht einfach irgendwelche Daten speichern wie es uns einfällt. Es muss erlaubt sein.

Was erlaubt ist, steht im Bundesdatenschutzgesetz.

- **Datensicherheit**

hier geht's um Backups und alles, was hilft, die Daten vor Verlust und Zerstörung zu schützen

- **Verhältnismäßigkeit**



# Grundregeln der EU DS-GVO

**Alles ist verboten!**

... Nur nicht das, was erlaubt ist.

## Datenschutz

Die Erhebung von personenbezogenen Daten ist nur erlaubt, wenn sie nicht verboten ist – wenn also die EU DS-GVO oder ein anderes Gesetz es nicht ausdrücklich verbietet (Arzt, Anwalt, Geistlicher: Schweigepflicht) oder es nach einem anderen Gesetz angeordnet ist (Finanzamt: Steuererklärung)

## Die EU DS-GVO

Ab dem 25. Mai 2018 wird der Datenschutz über die neue EU Datenschutz-Grundverordnung geregelt.

Sie soll die Vorschriften in Europa einheitlicher machen. Dabei wird es Vereinfachungen geben, neue Regeln und manches wird einfach nur ein bisschen anders sein.

## Ziele der EU-DSGVO

Die Europäische Datenschutz-Grundverordnung wird das derzeit gültige Bundesdatenschutzgesetz natürlich nicht völlig über den Haufen werfen.

Doch ein paar Änderungen in der Praxis wird es geben.

Wer jetzt bereits damit beginnt, die Änderungen anzupassen, hat es im kommenden Jahr leichter. In einem Jahr können wir schon eine ganze Menge umsetzen.

Das Ziel der neuen DS-GVO ist der Schutz unserer Grundrechte und Grundfreiheiten und hier vor allem der Schutz unserer Daten.



Und der ruft im Labor an, wo die Tests ausgewertet wurden.

„Guten Tag. Ich bin der Anwalt der Familie. Mein Name ist Schulz. Ich hätte gerne das Ergebnis des Vaterschaftstests von Herrn Maier und den Zwillingen Jan und Eva Müller gewusst...“

„... ach ja – ist der Vater?... zu 98% sagt der Test?... Vielen Dank. Sie haben mir sehr geholfen.“

Dieses Vorgehen ist mehr als zweifelhaft.

Es mag ja sein, dass der Anwalt die schriftliche Vollmacht des mutmaßlichen Vaters, der sich hier testen lassen hat und auch die der Kinder hat. Bleibt die Frage: Woher weiß die Laborangestellte das?

Woher weiß sie, dass Herr Schulz auch Herr Schulz ist?

Eine solche Auskunft am Telefon zu geben, geht gar nicht.

Da könnte ja jeder kommen.

Ergebnisse von Vaterschaftstests gehören zu den Schutzwürdigen Daten.

Es wäre interessant, mal bei der Bank anzurufen und dort telefonisch nach dem Kontostand zu fragen. Ob es hier wohl eine Auskunft gäbe?



Sie weiß, dass solche Daten begehrt sind. Manchmal kriegt sie auch Post und Emails von Adresshandelsfirmen. Hier allerdings ist sie diejenige, die solche Adressen mit entsprechenden personenbezogenen Daten kaufen soll.

Manchmal ist das legal. Es gibt seriöse Adresshandelsunternehmen. Das sind solche, die sich nach dem Datenschutzgesetz richten und ihrer Meldepflicht nachkommen, die hier für solche Unternehmen – egal in welcher Größe – vorgeschrieben ist (§ 4d BDSG) Diese Unternehmen haben dann Ihre Daten bei den Betroffenen direkt erhoben und sie um Erlaubnis gefragt, ob sie für Werbezwecke verwendet werden dürfen. Denn alles ist erlaubt, wenn der Betroffene eingewilligt hat.

Aber Fienchens Mann am Telefon hatte ihre Einwilligung garantiert nicht. Denn Fienchen gibt niemals Einwilligungen, ihre Adresse für irgendwelche Werbungen verwenden zu dürfen. Sie hat sogar einen Aufkleber am Briefkasten „Bitte keine Werbung einwerfen“

## **Schutzwürdige Daten**

### **Personenbezogene Daten**

- Persönliche Grunddaten
- Familiäre Daten
- Daten über Wohnverhältnisse
- Daten über Einkommen, Vermögen oder Besteuerung
- Daten natürlicher Personen in Verträgen
- Werturteile
- IP-Adressen
- ...

### **Besondere personenbezogene Daten**

- Rassistische und ethnische Herkunft
- Politische Meinung
- Religiöse oder philosophische Gesinnung
- Gewerkschaftszugehörigkeit
- Gesundheit und Sexualleben
- ...

## **Neulich im Fernsehen.**

Sat1 – „Familien-Fälle“

Eigentlich eine traurige Geschichte.

Eine Mutter stirbt und hinterlässt ihre Kinder der Freundin. Die soll gut für sie sorgen und sie von den Großeltern fern halten. Wer der Vater ist, weiß keiner.

Die Kinder würden es aber gerne wissen und die Freundin sucht. Schließlich gibt es ein paar Vaterschaftstest und einen Streit vorm Familiengericht.

Die Pflegemutter der Kinder hat einen Anwalt.



## Gute Gründe für den Datenschutz

- Mitarbeiter, Kunden und Lieferanten sollen es als selbstverständlich voraussetzen können, dass der Datenschutz in unserem Unternehmen sichergestellt ist.
- wir setzen die Einhaltung des Datenschutzes in anderen Unternehmen und Einrichtungen, mit denen wir zu tun haben, ebenfalls als selbstverständlich voraus.
- Datenschutz und der Schutz der Persönlichkeit ist ein Grundrecht aller Menschen
- Ein gut umgesetzter Datenschutz kann das Vertrauen der Kunden steigern und das Ansehen des Unternehmens fördern.
- Datenschutz ist europaweit gesetzlich vorgeschrieben.

## „Ich möchte mit Ihnen über Gott sprechen...“

Das Telefon klingelt.

Fienchen freut sich.

Bestimmt ruft grad die Uni Tübingen an, wo sie eine Bewerbung laufen hat.

Vielleicht eine Einladung zum Vorstellungsgespräch?

„Hallo, hier ist Fienchen – guten Tag?“

sagt sie freundlich erwartungsfroh in den Hörer.

„Hier ist Ferjwklöasgr von der Firma Jölkj era.“ Fienchen hat kein Wort verstanden.

Sie guckt auf das Display. Da steht „privat“ – Nummer unterdrückt.

Sie ahnt es – es ist wohl nicht die Uni.

Währenddessen plappert der freundliche Mann am anderen Ende munter weiter.

Ob sie immer noch mit Mann und 2 Kindern in der 4-Zimmer-Wohnung mit Garten am Stadtrand lebt? Den alten BMW fahre sie auch immer noch? Er hätte da ein Angebot. Es gäbe da eine neue Sorte Frühstücksflocken, ganz ähnlich wie die Smacks, die ihre Kinder sicherlich gerne essen (so oft, wie sie die einkauft). Ob er ihr da mal eine Kiste zur Probe schicken darf. Die Adresse habe er ja.

Fienchen sagt: „Oh, gut dass Sie anrufen. Ich würde gern mit Ihnen mal über Gott sprechen und ich hätte ja sonst vielleicht keine Gelegenheit dazu gehabt. Bitte sagen Sie mir doch noch mal deutlich und zum Mitschreiben Ihren Namen und die Firma, für die Sie arbeiten und dann können wir uns ein bisschen privat unterhalten.“

Das, was Fienchen dann noch verstanden hat, kurz bevor der Mann den Hörer auflegte, war etwas wie „@\$%&/E“. Es kann aber auch „blöde Kuh“ geheißen haben.

Fienchen freut sich.

Dem hat sie's gegeben.

Bleibt die Frage: Woher hat der Mann all ihre persönlichen Daten? Die Telefonnummer – die kann noch nach dem Zufallsprinzip gewählt worden sein. Der Automat wählt irgendwie wahllos eine Nummer und Fienchen ist dran.

Aber woher hat er dann die Adresse, die dazu gehört?

Woher weiß er, welches Auto sie fährt, kennt Familienstand und das Lieblingsessen der Kinder?



In diesem Urteil des Verfassungsgerichts wurde der Begriff des informationellen Selbstbestimmungsrechtes geprägt.  
In dieses Grundrecht darf nur eingegriffen werden, wenn ein Gesetz das ausdrücklich erlaubt.  
In den Datenschutzgesetzen des Bundes und der Länder ist der Begriff wiederzufinden.

Die Grundlage für all diese Maßnahmen, mit der wir hier die persönlichen Daten, die uns von unseren Auftraggebern anvertraut wurden, ist seit dem das Bundesdatenschutzgesetz.



# Volkszählung 1983

## Viele haben verweigert

**Mit dem Urteil des Bundes-Verfassungsgerichtes vom 15.12.83 wurde das Datenschutzrecht aus dem Artikel 2 des Grundgesetzes entwickelt.**

„Es begab sich aber zu der Zeit, dass ein Gebot von dem Kaiser Augustus ausging, daß alle Welt geschätzt würde. Und diese Schätzung war die allererste und geschah zu der Zeit, da Cyrenius Landpfleger von Syrien war. Und jedermann ging, daß er sich schätzen ließe, ein jeglicher in seine Stadt.“ (Lukasevangelium, Kapitel 2, Vers 1)

So fängt die Weihnachtsgeschichte an. Damals sollte sich das Volk zum ersten Mal zählen lassen, heißt es in der Bibel.

1983 sollte es wieder gezählt werden. Doch es wollte nicht.

Alle dachten an den gläsernen Menschen aus George Orwells Buch „1984“ mit seinem „Big Brother“, der jeden einzelnen seines Volkes auf Schritt und Tritt beobachtete, alles wusste und daraufhin Entscheidungen traf, die vielleicht gut für die Regierung waren, eher zweifelhaft für die Allgemeinheit und ganz bestimmt nicht immer gut für den Einzelnen.

In den 70er Jahren hielten RAF und Terroristenfahndung die Bundesrepublik in Atem und man hielt die Rasterfahndung für eine gute Idee, den Terrorismus zu bekämpfen.

Die Rasterfahndung funktioniert nach dem Ausschlussverfahren:

Um die Terroristen zu ermitteln, wurden wurden alle Menschen ausgeschlossen, die nicht ins „Raster“ passten.

Dazu gehörten damals beispielsweise die, die in der gesetzlichen Krankenversicherung versichert sind.

Jeder, der einen festen Wohnsitz beim Einwohnermeldeamt angemeldet hatte, wurde ebenfalls ausgeschlossen.

Und einige Kriterien mehr.

Je mehr Infos man hatte, desto mehr konnte der Kreis der Verdächtigen eingeschränkt werden, indem man immer weiter ausschloss, wer diese Kriterien nicht erfüllte.

Trotzdem blieben hier am auch jede Menge Personen hängen, die mit Terrorismus nichts zu tun hatten. Sie waren zunächst mal verdächtig und hatten dadurch jede Menge Unannehmlichkeiten. Es konnte passieren, dass ein vollkommen unschuldiger sich plötzlich zunächst mal im Polizeigewahrsam wieder fand, bevor sich herausstellte, dass er mit Terrorismus nichts zu tun hat. Und wer dann einmal im Gefängnis saß – etwas bleibt immer hängen.

Aktuelle Daten aus einer Volkszählung, die die richtigen Fragen stellt, hätten den Fahndern gefallen. Man hätte noch mehr Menschen in den Kreis der Verdächtigen einbeziehen können.

Mehrere Verfassungsbeschwerden zum Schutz des allgemeinen Persönlichkeitsrechts und der Menschenwürde wurden eingereicht.

Das Bundesverfassungsgericht gab dem Recht und der Artikel 2 des Grundgesetzes wurde um die „informelle Selbstbestimmung“ erweitert.



dass der Mann weltweit nie mehr einen Job bekommt.

Die Daten könnten bei elite-partner.com auftauchen oder im Facebook veröffentlicht werden.

Prism könnte drauf zugreifen und den Autoverkäufer als mutmaßlichen Terrorist beobachten.

Vermieter weltweit könnten es erfahren und – wenn sie ihre Wohnung überhaupt an ihn vermieten – einen höheren Preis beispielsweise als Gefahrenzuschlag verlangen.

In einer Stuttgarter Tatortfolge wurden die Akten der Staatsanwalt digitalisiert. Ein Mann, dessen Frau bei einem Verkehrsunfall ums Leben gekommen war, hat dort nach den Verursachern recherchiert, die damals frei gesprochen wurden und einen nach dem anderen in Selbstjustiz entsorgt.

Wenn jetzt in Anlehnung an diese Geschichte einer der Geschädigten aus den Eigentumsdelikten unseres Autoverkäufer an dessen Adresse, die Adresse seiner Familie, sein Kfz-Kennzeichen und sonstige personenbezogenen Daten käme – es wäre ein Leichtes, Rached Gedanken in die Tat umzusetzen. Das Auto zerkratzen, anonyme Drohbriefe zu schreiben, ihm aufzulauern und ihn zu verprügeln – der Fantasie sind da keine Grenzen gesetzt.

Und deshalb müssen personenbezogene Daten geschützt werden.





## Was bedeutet Datenschutz?

- Schutz der Menschen vor dem Umgang mit ihren Daten
- Schutz vor unberechtigter Speicherung
- Schutz vor fremder (unberechtigter) Kenntnisnahme und Verwendung
- Schutz vor „unsauberem“ Umgang
- Schutz vor dem Verlust der Daten

## Eine zweite Chance?

Ein Automobilverkäufer wird wegen Unterschlagung und Veruntreuung von Firmengeldern verurteilt.

Wir wissen nicht, warum das nächste Autohaus ihn trotzdem einstellt.

Vielleicht hatte der Arbeitgeber einfach nicht nach Vorstrafen gefragt und der Bewerber hat von sich aus nichts erzählt. Hätte ich wohl auch nicht.

Vielleicht wollten sie ihm aber auch eine zweite Chance geben.

Die hat er genutzt, um seine Fähigkeiten, sich um anderer Leute Eigentum zu kümmern, weiterzuentwickeln.

Und dann war er plötzlich und von einem Tag auf den anderen nicht mehr an seinem Arbeitsplatz.

Gerüchten zufolge wurde er entlassen, weil es wieder Unregelmäßigkeiten gegeben hat.

„Hast du schon gehört...?“

„Ich hab mich schon gewundert, wo er ist...“

Der vorbestrafte Autoverkäufer hatte bei seiner neuen Jobsuche wieder Glück.

Das allerdings war von kurzer Dauer, denn die Gerüchte erreichten auch den neuen Arbeitgeber.

Der neue Mitarbeiter verschwand auch hier plötzlich und unerwartet.

Gegen diese Entwicklung ist im Grunde rein rechtlich nichts einzuwenden.

Gerüchte entstehen.

Man glaubt es oder glaubt es nicht.

Gegen Verleumdung könnte man sich zur Wehr setzen.

Wenn diese Gerüchte der Wahrheit entsprechen, ist das schon schwieriger.

Doch der Schaden, den der Automobilverkäufer hier durch die Gerüchte hat, ist begrenzt.

Ein Computer kann hier viel mehr Schaden anrichten.

Datenschutzrechtlich spielt dieser Fall so wie es da abgelaufen ist, keine Rolle.

Das BDSG (Bundesdatenschutzgesetz) bezieht sich auf personenbezogene Daten die „automatisch“, also per Computer verwaltet und bearbeitet werden. (§ 1 Abs. 2, Satz 3 BDSG)

Wer unberechtigten Zugriff auf die Personaldaten des Autohauses hat oder womöglich sogar auf die Daten des Amtsgerichts könnte mehr anrichten.

Die Daten könnten in einem Pool landen, auf den alle Unternehmer zugreifen können, so



<b>Inhalt</b>	<b>Seite</b>
<b>Allgemeines</b>	
Staatliche Überwachung – Sicherheit total	2
Was bedeutet Datenschutz?	6
Volkszählung 1983	8
Gute Gründe für den Datenschutz	10
Schutzwürdige Daten	11
Grundregeln der EU DS-GVO	13
Grundsätze des Datenschutzes	14
Anwendungsbereiche	15
Facebook-Klausel	16
EU-Vertreter	16
Grundsatz der Transparenz	17
Rechte der Betroffenen	17
Recht auf Vergessen	19
Der Datenschutzbeauftragte	20
Datensicherheit	21
Pssst... Nichts weitersagen.	21
Papierdokumente vernichten	22
Elektronische Daten vernichten	23
Telefongespräche	23
Cloud-Computing	24
Videoüberwachung	25
Beschäftigtendatenschutz	26
Werbung	27
<b>Strafbarkeit und Rechtsfolgen</b>	<b>28</b>



Und diese regelmäßigen Zahlungstransfers nach Südfrankreich? Wofür? Warum sind Sie letzte Nacht eigentlich so lange um den Block gelaufen? Sie hatten Ihr Handy nicht ausgeschaltet – da weiß man, wo Sie sind.

Nach der Arbeit steigen Sie ins Auto, um etwas Persönliches zu erledigen. Verzichten Sie auf die Verwendung Ihres Navigationssystems. Andernfalls lässt sich leicht herausfinden, wohin Sie fahren. Machen Sie einen Umweg, meiden Sie die Autobahn mit den ganzen Mautstationen! Sie fragen sich bestimmt schon, warum Ihnen so hartnäckig aufgelauert wird? Warum gerade Ihnen? Es gibt doch keinen Grund, aus dem sich irgendjemand für Sie interessieren könnte.

Sind Sie sicher? Sind Sie absolut sicher?

Haben Sie nicht neulich gegen den G-8-Gipfel demonstriert? Dann verfügt die Polizei sogar über Ihre Geruchsprobe. Haben Sie nicht bis vor Kurzem in jenem Studentenwohnheim gelebt, in dem auch ein gewisser Abu Mehsud untergekommen war? Das waren gar nicht Sie, das muss ein anderer Müller gewesen sein? Na, wenn man so heißt, liegt eine Verwechslung nahe, selber schuld. Und wie steht es mit Ihrer Lebensgefährtin, die kauft jede Menge Haarfärber, Fleckenlöser und Batterien. Das bedeutet: Wasserstoffperoxid, Azeton, Schwefelsäure! Halten Sie uns für blöd? Daraus kann jeder Idiot eine Bombe bauen. Natürlich behaupten Sie, Ihre Lebensgefährtin habe nicht vor, eine Bombe zu bauen. Das würde jeder antworten. Sollten Sie allerdings die Wahrheit sagen – wo liegt dann das Problem? Wir helfen Ihnen doch nur, diesen Verdacht aus der Welt zu schaffen, indem wir genau hinschauen. Das muss auch für Sie eine Erleichterung sein.

Kein Grund zur Beunruhigung also. Alles geschieht zu Ihrem Besten. Der Staat ist Ihr Vater und Ihr Beschützer. Er muss wissen, was seine Kinder treiben. Wenn Sie nichts Schlimmes verbergen, haben Sie auch nichts zu befürchten. Die Entscheidung aber, was schlimm ist, überlassen Sie bitte den Spezialisten. Wenn Sie mitspielen, müssen Sie keine Angst haben. Wir sind nicht die Stasi oder das FBI. Sie leben in einer gesunden Demokratie. Da kann man schon ein bisschen Vertrauen von Ihnen erwarten. Was? Der Staat soll Ihnen vertrauen? Wo kämen wir da hin! Schon das Grundgesetz sagt, dass alle Gewalt vom Volke ausgeht. Und Gewalt gilt es einzudämmen. Da sind Sie ja wohl einer Meinung mit dem Innenministerium.



## Staatliche Überwachung Sicherheit total

Unter dem Vorwand, uns vor terroristischen Gefahren schützen zu wollen, späht der Staat seine Bürger aus. Von dieser Politik der Angst dürfen wir uns nicht verrückt machen lassen

Wenn wir Angst haben, raschelt es überall. (Sophokles)

Früh raus. Der Wecker klingelt. Es ist noch dunkel. Nicht gleich Licht machen, eine Minute auf dem Bettrand sitzen bleiben. Die Morgenluft einatmen. Das Fenster ist gekippt, die Tür zum Flur offen. In der Küche wartet die Espressomaschine. Wo sind die Hausschuhe? Sich strecken, aufstehen, das Licht anknipsen.

Sie ziehen den Vorhang am Küchenfenster zu, damit der Nachbar von gegenüber nicht hereinschauen kann. Sie kochen sich einen doppelten Espresso und nehmen einen Schluck. Jetzt kann der Tag beginnen. Sie setzen die Tasse auf dem Tisch ab. Am Rand haben Sie zwei wunderschöne Fingerabdrücke hinterlassen. So scharf konturiert und vollständig wie die in Ihrem Reisepass. Oder die in den Datenbanken der U. S. Customs and Border Protection seit Ihrem letzten Sommerurlaub in Florida. Beruflich sind Sie viel unterwegs? Dann kennt man das Muster auf der Kaffeetasse, die Sie gerade ins Arbeitszimmer tragen, auch in Schweden, Georgien und im Jemen.

Wie jeden Morgen rufen Sie Ihre privaten E-Mails ab. Die sind schon überprüft worden – nicht nur von Ihrem Virenscanner. Sie rufen noch die eine oder andere Webseite auf – die Kripo weiß, welche, wenn sie möchte, und kann das auch in sechs Monaten noch überprüfen. Sie nehmen schnell noch eine Überweisung vor – die Behörden wissen, an wen. Zum Glück heißen Sie Müller, das schützt ein wenig. Bei Ihrem Kollegen Tarik al-Sultan, der neulich zum Bergsteigen in Kaschmir war, verschickt der Computer gerade den gesamten Inhalt der Festplatte an den Verfassungsschutz. Greifen Sie etwa gerade nach dem Telefon, um mit Tarik etwas Vertrauliches zu besprechen, das nicht ins Büro gehört? Lassen Sie es lieber sein. Besuchen Sie ihn zu Hause, wenn Sie ungestört reden wollen. Es sei denn, Tarik wurde als Gefährder eingestuft, weil er regelmäßig Geld an seinen arbeitslosen Cousin in Pakistan schickt. Dann ist seine Wohnung ohnehin verwantzt.

Sie eilen zur Haustür hinaus. Die Überwachungskamera Ihres Wohnkomplexes beobachtet jeden Ihrer Schritte. Auch beim Betreten der U-Bahn-Station werden Sie gefilmt, ebenso auf dem Bahnsteig und in der Einkaufspassage, wo Sie eine Zeitung kaufen. Haben Sie schon mal versucht, vor einer Überwachungskamera unschuldig zu wirken? Das ist noch schwieriger, als auf einem gestellten Foto natürlich zu lächeln. Warum wandert Ihr Blick ständig nach oben? Zweimal haben Sie direkt in die Kamera geschaut. Und jetzt greifen Sie sich schon wieder ins Haar. Wenn das noch einmal passiert, wird die biometrische Verhaltensanalyse den Alarm auslösen. Warum sind Sie so nervös? Laut Ihrer Patientenkarte bekommen Sie seit Neuestem Beruhigungsmittel verschrieben. Und die Payback-Karte verzeichnet einen erhöhten Alkoholkonsum. Sie haben am Bankautomaten wieder 1000 Euro abgehoben. Wozu brauchen Sie so viel Bargeld? Außerdem ist Ihr Stromverbrauch im letzten Monat um 12,4 Prozent gestiegen. Verstecken Sie jemanden? In der Stadtbibliothek leihen Sie sich in letzter Zeit merkwürdige Bücher aus, über zivilen Ungehorsam und die Pariser Kommune. Reichen Ihnen die historischen Schmöker nicht?



# Grundlagen zu Datenschutz und Datensicherheit im Unternehmen



**MS Computer GmbH – Reutlingen**