BOLLENBERGER & BOLLENBERGER
Beratungsgruppe

Datenschutzgrundverordnung (DSGVO)

B&B – Ihre Berater mit MEHRWERT!

Sehr geehrte Klientin, sehr geehrter Klient!

Mit dieser B&B-Mappe kommen wir unserer Unternehmensphilosophie „Mit uns die Zukunft in Griff " nach. Wir wollen jedem unserer Klienten nicht nur die klassischen Leistungen der Steuerberatung bieten, sondern auch jeden umfassend beraten, über Neuerungen der Rechtswelt am Laufenden halten, für neue Entwicklungen sensibilisieren und auch dabei helfen, das Unternehmen auch in Zukunft erfolgreich zu führen.

Neben den klassischen Aufgaben eines Steuerberatungsunternehmens (Lohnverrechnung, Buchhaltung, Jahresabschluss) wollen wir Ihr Wegbegleiter bei höchstpersönlichen Anliegen, Ihr Berater in allen wirtschaftlichen Fragen und Ihr Coach bei der Weiterentwicklung Ihres Unternehmens sein. Neue Entwicklungen, wie z.B. die fortschreitende Digitalisierung oder neue rechtliche Anforderungen, wie z.B. die Datenschutzgrundverordnung, sehen wir als große Herausforderung für unsere Klienten. Wir möchten gerne einen Teil zur Problemlösung beitragen.

Mit der vorliegenden Mappe versuchen wir einen kompakten Überblick über die neue Rechtsmaterie der Datenschutzgrundverordnung zu geben. Diese Mappe soll die ersten notwendigen Schritte erleichtern und vereinfachen. Wir beziehen unser Wissen aus Seminaren, Fachartikeln, Fachbüchern und von diversen Plattformen (z.B. WKO). Die Verwendung dieser Mappe und jede Information zu derartigen Sachverhalten durch Personen aus der B&B-Gruppe ist ein besonderes Service und schließt jede Form der Haftung aus.

Wir bieten ein gemeinsames Hineinwachsen in diese neue Rechtsmaterie an!

Ihr B&B Team

To do - das Wichtigste zuerst

☐ Erstellen des Datenverarbeitungsverzeichnisses

- wenn nötig: Bestellung eines Datenschutzbeauftragten

☐ Datenschutz-Folgeabschätzung

☐ Jeder Mitarbeiter muss Folgendes unterschreiben: „Datenschutzerklärung für Mitarbeiter

☐ Verpflichtungserklärung von Mitarbeitern zum Datengeheimnis und zur Wahrung von Geschäfts- & Betriebsgeheimnissen –

☐ Nachweis Schulung der Mitarbeiter

☐ Ergänzung der Email-Signatur

☐ Informationspflicht für Webseiten

☐ Einholen der schriftlichen Einwilligung bei der Verarbeitung von sensiblen Daten

☐ Zulässigkeit der Videoüberwachung bzw. Bildverarbeitung

☐ Abschluss Auftragsverarbeitungsvertrag

☐ Recht des Betroffenen auf Auskunft

☐ Hat Betroffener ein Widerspruchsrecht?

☐ Recht auf Löschung, Berichtigung, Einschränkung der Verarbeitung

☐ Datenverlust – Meldung an die Aufsichtsbehörde

☐ Erfolgt eine Datenübermittlung ins EU-Ausland?

☐ Laufende Prüfung der Zulässigkeit einer Datenanwendung Prüfschema

Nachkontrolle: Anforderungen DSVGO erfüllt?

Das B&B Team unterstützt Sie gerne.

Grundsätzliches

Das Datenschutzgesetz 2000 (DSG 2000) ist das geltende österreichische Datenschutzgesetz und damit die wichtigste Rechtsvorschrift zum Datenschutz in Österreich.
Das Datenschutz-Anpassungsgesetz 2018 trat mit 25. Mai 2018 parallel zum In-Geltung-Treten der EU-Datenschutz-Grundverordnung – DSGVO in Kraft.
Der österreichische Nationalrat hatte dann am 20. April 2018 das Datenschutz-Deregulierungsgesetz 2018 mit wesentlichen Entschärfungen beschlossen.

DSG

DSAG
DSGVO

DS-Deregulierungs-gesetz

Die ab 25.5.2018 in Kraft getretene Datenschutz Grundverordnung ist auf den ersten Blick langwierig und komplex. Wir wollen unseren Klienten einen kompakten und verständlichen Überblick für eine erste praktische Umsetzung geben! In diesem Sinne versuchen wir hier mit möglichst einfachen Worten eine Erklärung zu geben. Die dazu in der Verordnung verwendeten Fachbegriffe führen wir jeweils rechts an.

Grundsatz der europäischen Grundrechtecharta:

Grundrecht

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten! Datenschutz ist ein Grundrecht!
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. “

Für jeden von uns ist es sicherlich ein ureigenes Bedürfnis, dass seine Daten geschützt werden. Datenverlust ist eine besonders unangenehme Form von Nacktheit und kann daher zu persönlich höchst schwerwiegenden Folgen führen. Auch wenn diese neuen Vorschriften für uns als Unternehmen aufwendig und lästig sind,

jeder will Schutz für seine Daten

sollten wir nicht vergessen, dass für uns selbst der Datenschutz von größtem persönlichem Interesse ist!

Ausnahmen vom Datenverarbeitungsverbot

Verbot der Datenverarbeitung

Grundsätzlich besteht daher ein generelles Verbot der Verarbeitung von personenbezogenen Daten. Diese Daten darf ein Unternehmen nur dann verarbeiten, wenn es einen der folgenden Punkte erfüllt:

- bei Einwilligung durch die betroffene Person
- zur Erfüllung eines Vertrages
- bei der Erfüllung einer rechtlichen Verpflichtung
- wenn es lebenswichtige Interessen zu schützen gilt
- bei öffentlichem Interesse
- bei Wahrung der berechtigten Interessen des Verantwortlichen

Personenbezogene Daten

Geschützt sind alle personenbezogenen Daten! Personenbezogene Daten sind Informationen, welche eine natürliche Person identifizierbar machen.

z.B. Name, Adresse, Geburtsdatum, Kfz-Nummerntafel, Familienstand, Anzahl der Kinder, Bankdaten, Kreditkartendaten, Standortdaten

Normale und sensible Daten

Bei den personenbezogenen Daten unterscheidet man zwei Kategorien:
Einerseits gibt es sogenannte normale Daten.

Normale Daten

Name, Adresse, Bankdaten, …

Sensible Daten

Andererseits gibt es sensible Daten. Sie führen zu einem erhöhten Bestandsschutz und eine schriftliche Einwilligung für die Verarbeitung ist ein Muss!

Fingerabdruck, Iris-Scan, genetische Daten, biometrische Daten, Krankengeschichte, sexuelle Orientierung, Daten zum Sexualleben, ethnische und rassische Herkunft, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit

Faustregel bei der Unterscheidung ist die Wichtigkeit der Information für die jeweilige Person. Je wichtiger, desto eher handelt es sich um sensible Daten.

Unternehmen sind jetzt generell dazu angehalten, möglichst wenige Daten zu erfassen. Ein Ziel der neuen Regeln ist auch die Datenminimierung.

In einem sogenannten „Verarbeitungsverzeichnis " muss erfasst werden, **warum welche Daten gespeichert werden, was mit ihnen geschieht und wann sie wieder gelöscht werden.**

Freibeweis

Ein Unternehmen muss beweisen, dass es alles Mögliche getan hat, um die Daten zu schützen. Wenn das Unternehmen belangt wird, herrscht grundsätzlich Beweislastumkehr - d.h., das Unternehmen muss seine Unschuld beweisen! Strafen gibt es auch bei Fahrlässigkeit!

Betroffene Person

Wann ist jemand eine betroffene Person? Das ist jede natürliche Person über welche Identifizierbares verarbeitet wird.

formlose Beschwerde durch Jeden

Jede betroffene Person kann formlos und ohne Kosten bei der Datenschutzbehörde Beschwerde einbringen, wenn diese Person der Ansicht ist, dass die Verarbeitung ihrer personenbezogenen Daten gegen die neue EU Verordnung oder das österreichische Datenschutzgesetz verstößt.

Die Aufsichtsbehörden können aber bei offenkundig unbegründeten oder exzessiven Beschwerden eine angemessene Gebühr festsetzen oder das Tätigwerden verweigern.

Beschwerden können binnen eines Jahres ab Kenntniserlangung vom beschwerenden Ereignis erhoben werden. Allerdings spätestens binnen drei Jahren ist die Beschwerde einzubringen nachdem das behauptete Ereignis stattgefunden hat. Zusätzlich können Schadenersatzansprüche gerichtlich geltend gemacht werden.

binnen drei Jahren

Datenweitergabe durch Unternehmer

Dann gibt es noch den Auftragsverarbeiter. Er verarbeitet ohne Eigeninteresse im Auftrag des Verantwortlichen personenbezogene Daten.

Auftragsverarbeiter

Cloud-Betreiber, Paketzusteller, Druckerei wenn sie durch Adressaufdruck Sendungen personalisiert, Know-Your-Customer-Checks, Callcenter für Kundenbefragungen, Inkasso

Was müssen Unternehmen sofort tun?

Jedes Unternehmen muss zuerst feststellen, welche Daten es über Personen besitzt. Dabei ist es egal, in welcher Form diese Daten vorliegen.

Daten kann ich z.B. auf Karteikarten per Hand geschrieben haben, in einem geschriebenen oder ausgedruckten Adressbuch führen. Personalakte oder Patientenkarteien sind sehr oft in Papierform vorhanden. Daten können auf meinem Computer, in meinem Kopierer, einem USB-Stick, in meinem Handy oder in meiner Cloud gespeichert sein.

Die Verordnung beschränkt sich also nicht nur auf digital gespeicherte Daten, sondern auf alle Informationen von Personen im eigenen Unternehmen, also auf jede strukturierte Sammlung von personenbezogenen Daten.

Ich muss daher alle Geschäftsprozesse auf ihren Umgang mit personenbezogenen Daten durchleuchten. Wer darf auf welche Daten zugreifen? Potenzielle Risikobereiche sind zu identifizieren.

z.B. jede Form von Direktmarketing (E-Mail Informationen, Versand von SMS, das Anrufen von potenziellen Kunden)

Zustimmung des Kunden für diese Marketingmaßnahme ist notwendig!

Verantwortlicher

Ein zentraler Begriff der Datenschutzgrundverordnung ist der sogenannte Verantwortliche. Damit ist immer das Unternehmen gemeint (das Einzelunternehmen, die Personengesellschaft, die Kapitalgesellschaft). Es ist zweckmäßig eine Ansprechperson für Datenschutz zu nominieren!

Der Verantwortliche hat die Kontrolle über die Verarbeitung von personenbezogenen Daten und hat die Entscheidungshoheit zu

welchem Zweck und mit welchen Mitteln die Datenverarbeitung erfolgen soll.

Unternehmen sind verpflichtet das sogenannte Verarbeitungsverzeichnis zu führen. Der gesamt Prozess der Datenverarbeitung muss dokumentiert werden. In diesem Verzeichnis sind sämtliche Datenkategorien anzuführen, die verarbeitet werden, ebenso die Zwecke der Verarbeitung, Empfänger der Daten, Speicherfristen und Datensicherungsmaßnahmen. Neben diesen Pflichtangaben sollte auch die jeweilige Rechtsgrundlage der Verarbeitungstätigkeiten, etwa ein Vertrag mit einem Kunden, eine Einwilligung oder eine gesetzliche Verpflichtung, im Verarbeitungsverzeichnis dokumentiert werden.

Datenverarbeitungs-verzeichnis

Diese Verfahrensverzeichnisse sind stets aktuell zu halten. Eine Pflicht zur persönlichen Führung besteht nicht, insofern könnte diese Tätigkeit fremdvergeben werden.

Zusätzlich verkompliziert wird die Sache, weil kein Unternehmen bei Null anfängt und daher alle bisher verwendeten Systeme zur Datenerfassung und Datenbearbeitung auf den Prüfstand müssen.

Neu ist die Pflicht einer Datenschutz-Folgeabschätzung. Dies ist vor der Verarbeitung notwendig, wenn möglicherweise eine Beeinträchtigung der datenschutzrechtlichen Sphäre einer betroffenen Person zu befürchten ist.

Datenschutz Folgeabschätzung

Es ist zur prüfen, ob ein Datenschutzbeauftragter notwendig ist (für die meisten Unternehmen nicht notwendig).

Die einerseits neuen erweiterten Informationsverpflichtungen und andererseits die generell neuen Vorschriften über die Verarbeitung von personenbezogenen Daten führen zu einem Handlungsbedarf bei Mitarbeitern.

Mitarbeiter

Jede Form der Erhebung von personenbezogenen Daten bei natürlichen Kunden bzw. Geschäftspartnern führt zu einer Reihe von Notwendigkeiten.

Man muss zuerst die Zustimmung zur Verarbeitung einholen und dann den Kunden über diese Verarbeitung informieren. Auf Anfrage muss der Betrieb Auskunft über beispielsweise die Art der Daten geben und auf Wunsch die Datenlöschung gewährleisten.

Wenn jemand in meinem Auftrag personenbezogene Daten verarbeitet, dann muss ich mit ihm darüber einen Vertrag abschließen.

Profiling

Achtung bei Profiling! Dabei handelt es sich um eine stark verfeinerte Auswertung von Kundendaten. Durch automatisierte Verarbeitung von personenbezogenen Daten wird Verhalten vorhergesagt. Hier sind dann besondere Anforderungen zu erfüllen!

Informationspflicht bei Datenerhebung

Durch jede Form der Datenerhebung von natürlichen Personen, muss diese Person über den Grund, die Art und Weise der Verarbeitung, die Speicherdauer und Weitergabe der Daten und die Rechtsgrundlage informiert werden.

Diese Informationspflicht besteht auch bezüglich Datenweitergabe an andere Unternehmen, um Aufträge abwickeln zu können, oder an öffentliche Stellen, selbst wenn ich dazu gesetzlich verpflichtet bin.

Wo erhebe ich Daten? – bei Bestellungen, bei Anfragen, bei Gewinnspielen, bei Marketing-Aktivitäten (Messestand), …

Wo gebe ich Daten weiter? – Buchhaltung, Lieferungen durch andere Unternehmen, Beiziehung von Sublieferanten, …

Dem Kunden muss jederzeit die Möglichkeit gegeben werden, gegen weitere Werbezusendungen einen Widerspruch einlegen zu können.

Werbesendungen

Was ist das Auskunftsrecht von Betroffenen?

Betroffenen steht das Recht zu, dass Unternehmen sie darüber aufklären, wie und welche Daten von ihnen verarbeitet werden. Ansprechpartner ist der Verantwortliche! Eine Überprüfung der auskunftssuchenden Person ist notwendig!

Ausweis verlangen und kopieren!

Mit der Auskunft müssen Betroffene soweit Einblick in die verarbeiteten Daten erhalten, dass sie Berichtigungsanträge stellen können.

Das bedeutet, dass man nicht nur pauschal angibt, dass man etwa Kontodaten verarbeitet, sondern ich muss konkret angeben, welche Daten von welchen Konten des Anfragenden verarbeitet werden.

Diese Auskunft ist dem Inhaber der Daten binnen einer Frist von einem Monat zu erteilen.

Monatsfrist

Privatpersonen haben das Recht, dass ihre Daten unverzüglich gelöscht werden. Löschungsbegehren dürfen aber beim Unternehmen nicht dazu führen, dass es vertragliche oder gesetzliche Verpflichtungen nicht einhalten kann.

Recht auf Löschung

Gewisse Daten sind zur Erfüllung eines Auftrages einfach unerlässlich. Die Bundesabgabenordnung schreibt aus Gründen des Rechnungswesens (Buchhaltung) vor, dass bestimmte Informationen sieben Jahre lang aufbewahrt werden müssen.

Ich muss auch keine Daten löschen, die ich zur Abwehr fremder Rechtsansprüche oder zur Begründung eigener Rechtsansprüche benötige.

Ein Baustoffunternehmer, der auch noch nach Jahrzehnten wegen versteckter Baumängel in Anspruch genommen werden könnte, darf Daten sogar über die lange Verjährungsfrist des Zivilrechts von 30 Jahren hinaus speichern.

Ich muss ein Konzept entwickeln, welche Daten genau wie lange erforderlich sind und welche nicht. Das ist von Betrieb zu Betrieb individuell.

Das Auskunftsrecht von Betroffenen ist kostenlos – nicht jedoch, wenn das Auskunftsrecht über Gebühr in Anspruch genommen wird oder zu weit geht. Hier darf ein angemessener Kostenersatz verlangt werden oder auch eine Auskunft verweigert werden. Verweigern darf ich insbesondere dann, wenn indirekt schützenswerte Daten anderer Personen weitergegeben werden müssten.

Wichtig: Die neuen Regeln betreffen auch alte Daten, soweit diese weiterhin gespeichert und damit verarbeitet werden!

Sollte die Auskunft vom Betroffenen als nicht ausreichend empfunden werden, kann er sich an die Datenschutzbehörde wenden – die daraufhin folgenden Verfahren werden nähere Erkenntnisse bringen, welche Abgrenzungen beim Umfang der Daten-Auskünfte getroffen werden können.

Das Datenschutz-Deregulierungsgesetz hat den Schutz für Geschäfts- und Betriebsgeheimnisse festgehalten. Betroffenen Personen kann das Auskunftsrecht über ihre personenbezogenen Daten dann verweigert werden, wenn durch die Auskunftserteilung ein Geschäfts- bzw. Betriebsgeheimnis des Verantwortlichen oder eines Dritten gefährdet würde.

Was müssen Firmen bei Datenverlust tun?

Bei Datenpannen, unzulässigen Zugriffen (Cyberattacken wie Hacking oder Datendiebstahl) und Datenlecks herrscht Handlungsbedarf!

Data Breach Notification

Der Verantwortliche hat nach Erkennen einer solchen Tat unverzüglich (binnen 72 Stunden) die zuständige Datenschutzbehörde zu verständigen. Zusätzlich ist der Verantwortliche zu einer umfassenden Dokumentation derartiger Datenverletzungen verpflichtet.

Für den Fall, dass die Datenverletzung auch die Rechtssphäre einer betroffenen Person hochriskant berührt, muss auch die betroffene Person benachrichtigt werden.

Was darf die Datenschutzbehörde?

Klärung durch Rechtsprechung

Da die Verordnung erst mit 25. Mai 2018 in Kraft tritt, kann es einige Zeit dauern, bis viele Detailfragen in der Rechtsanwendung durch die Rechtsprechung geklärt werden. Die Datenschutzbehörde hat sehr weitreichende Befugnisse. Gerade am Beginn der Anwendung des neuen Datenschutzrechtes wird die Behörde bei Vergehen Verwarnungen aussprechen, wenn offensichtlich ist, dass das Unternehmen versucht hat, die neuen Regeln sehr genau umzusetzen.
Jene Unternehmen, die zeigen, dass sie das Thema Datenschutz ernst nehmen, haben weniger zu befürchten als jene, die wenig bis gar keine Aktivitäten gesetzt haben.

Was sind die Strafen?

Die Höhe der Strafe hängt von der Art des Verstoßes ab.
Geldbußen betragen bis zu Euro 10 Mio. oder bis zu 2 % vom Jahresumsatz.

z.B. fehlendes oder mangelhaftes Verzeichnis von Verarbeitungstätigkeiten, mangelhafte Datensicherungsmaßnahmen

Geldbußen

Geldbußen betragen bis zu Euro 20 Mio. oder bis zu 4 % vom Jahresumsatz.

z.B. Verletzung des Auskunfts- oder Löschungsrechts der betroffenen Person, Vornahme von Datenverarbeitungen ohne Vorliegen eines Erlaubnistatbestandes

Geldbußen können direkt gegen juristische Personen verhängt werden.

Das Datenschutz-Deregulierungsgesetz 2018 bringt hier Entschärfungen für die Unternehmen. Es wird ausdrücklich das

Verhältnismäßigkeitsprinzip integriert, welches bei der Verhängung von Strafen für Angemessenheit im Einzelfall sorgen soll.

Es wird das Prinzip „Beraten statt Strafen " explizit verankert. Die Geldstrafen des Kataloges gemäß Art. 83 DSGVO sollen erst bei Wiederholungstätern zum Einsatz kommen. Bei erstmaligen Verstößen soll die Datenschutzbehörde aus den ihr zur Verfügung stehenden Mitteln im Einklang mit Art. 58 DSGVO zunächst eine Verwarnung aussprechen.

Doppelbestrafungsverbot I: Hat bereits eine andere Verwaltungsbehörde eine Verwaltungsstrafe in der Sache verhängt, darf die Datenschutzbehörde dies nicht noch einmal in derselben Angelegenheit tun.

Doppelbestrafungsverbot II: Die Datenschutzbehörde darf neben der juristischen Person eines Unternehmens nicht zusätzlich noch dessen rechtlichen Vertreter bzw. verantwortlichen Beauftragten für denselben Verstoß strafen.

Es entfällt die Möglichkeit für Datenschutzorganisationen ohne Gewinnerzielungsabsicht, nach Beauftragung durch die betroffene Person in deren Namen Schadensersatzansprüche einzufordern; damit werden Gemeinschaftsklagen gegen Unternehmen verhindert.

Die günstigere Rechtsmaterie soll zur Anwendung gelangen. Hat ein Verursacher Normen des bisher geltenden DSG 2000 verletzt, die zum Zeitpunkt des Inkrafttretens des neuen Datenschutzgesetzes noch nicht anhängig gemacht wurden, ist diese Verletzung nach demjenigen Recht (alte vs. neue Rechtslage ab 25.5.2018) zu beurteilen, die für den Verursacher günstiger ist.

Verarbeite ich Daten im Auftrag für Andere?

Auftragsverarbeiter

Zieht ein Verantwortlicher (eine andere Firma) mich zur Datenverarbeitung heran, dann bin ich ein sogenannter Auftragsverarbeiter. Ich bin weisungsgebunden und dem Verantwortlichen (der anderen Firma) zuzurechnen. Ich bin der „verlängerte Arm “.

Marketingaktionen, Newsletter Versand, Inkasso, Marktumfragen,.....

Sub-Auftraggeber

Der Auftragsverarbeiter darf ohne Zustimmung des Verantwortlichen keine Sub-Auftragsverarbeiter beauftragen.
Der Auftragsverarbeiter muss ein Verzeichnis seiner Verarbeitungstätigkeiten führen.
Er haftet den betroffenen Personen neben dem Verantwortlichen.

Jedes Unternehmen muss, wenn es Daten weitergibt, um etwas mit diesen Daten machen zu lassen, dieses Auftragsverhältnis durch einen Auftragsverarbeitungsvertrag regeln!

Praxistipps

Durch die Verordnung treffen Unternehmen eine Reihe an Datenschutz-Verpflichtungen – sollte es zu einer Hacker-Attacke kommen sind die Folgen oft desaströs: Betroffene Dateninhaber sind zu verständigen, sie haben weiters einen Anspruch auf materiellen sowie immateriellen Schadenersatz, wenn ihre Daten durch ein intern oder extern verursachtes Leck publik werden und direkt in Geld messbare Schäden eingetreten sind oder die Daten-Inhaber durch das Bekanntwerden bloßgestellt wurden.

Die Versicherungswirtschaft bietet spezielle Cyber Versicherungen an.

Cyber Versicherung

Eine Email mit einer Schadsoftware verlässt mein Unternehmen und es kommt in einem anderen Unternehmen dadurch zu einem Schaden. Die Versicherung deckt daher nicht nur meinen Schaden, sondern auch berechtigte Schadenersatzforderungen des anderen Unternehmens bzw. die Kosten, diese Ansprüche abzuwehren.

Die Kosten einer Betriebsunterbrechung können durch eine Versicherung gedeckt werden.

Viele haben auf ihrem Handy Kundendaten gespeichert und vergessen dabei Vorsorge zu treffen.
Es gibt Funktionen, mit denen kann jeder bei seinem verlorenen Handy, seine Daten löschen oder sperren. Voraussetzung ist es vorher am Handy die nötigen Einstellungen zu machen.

Der Zugang zu Handy, Laptop, Tablet und ähnlichem unbedingt mittels Zugangsbeschränkung (Code) sichern! Keine Sicherung bedeutet mindestens Fahrlässigkeit mit endsprechenden Folgen!

Allgemeine Grundsätze der Datenverarbeitung

Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Jede Datenverarbeitung von personenbezogenen Daten ist ohne Zustimmung der betroffenen Person, und wenn nicht eine sonstige gesetzliche Bestimmung die Verwendung zulässt, verboten.

Verbotsprinzip

Datenverarbeitung ist nur unter folgenden Bedingungen rechtmäßig:

- Einwilligung

  Möglich ist diese schriftlich, mündlich oder elektronisch (z.B. Anklicken eines Kästchens beim Besuch der Internetseite)

  Es ist notwendig, einen Nachweis der Erteilung der Einwilligung zu haben (Mündlich ist damit praktisch bedeutungslos.).

  Die Einwilligung hat sich auf einen oder mehrere bestimmte Zwecke zu beziehen! Pauschale Einwilligungen sind unwirksam.

  Jede betroffene Person ist vor Abgabe der Einwilligung von der Möglichkeit des jederzeitigen Widerrufs zu informieren!

Erlaubnistat-bestände

Nachweispflicht

Bestimmter Zweck

Wiederrufs-möglichkeit

- Erfüllung eines Vertrages

  Die betroffene Person muss Vertragspartei des Vertrages sein.

  Das Erhalten eines Pakets durch Paketzusteller

- Erfüllung einer rechtlichen Verpflichtung

  z.B. Aufgrund von Verpflichtungen aus Steuer-, Arbeits- und Sozialrecht oder Geldwäschegesetz

- Wahrung berechtigter Interessen
  Das ist eine Art Auffangtatbestand, wenn für ein Unternehmen die Datenverarbeitung zur Wahrung berechtigter Interessen erforderlich ist.

> So muss jeder als Patient in einer Arztpraxis damit rechnen, dass der Arzt seine Patienteninformationsdaten automationsunterstützt verarbeitet. Der Zweck dieser Datenverarbeitung liegt im täglichen Geschäft des behandelnden Arztes. Keineswegs vom Zweck umfasst ist aber, diese Daten einem Medizinproduktlieferanten zu übermitteln.

Grundsatz der Zweckbindung

Zweck

Ich muss die betroffene Person von Beginn an über den Zweck der Datenverarbeitung informieren.

> Das Religionsbekenntnis ist für die Lohnverrechnung notwendig, für die Buchhaltung jedoch nicht.

Der festgelegte Zweck dient auch zur Bestimmung der Dauer der Datenspeicherung.

Grundsatz der Datenminimierung und Speicherbegrenzung

Personenbezogene Daten müssen auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Die Dauer der Speicherung ist auf das unbedingt erforderliche Mindestmaß zu beschränken.

Löschfristen

Der Verantwortliche muss Fristen für ihre Löschung oder regelmäßige Überprüfungen vorsehen.

> Bei Back-ups, die zur Sicherung aller Daten dienen, ist das sofortige Löschen praktisch unmöglich, ein „Herauswachsen " von Daten aus dem Datenpool ist laut herrschender Meinung zulässig.

Grundsatz der Richtigkeit

„Zeig mir die Daten, und ich sage dir, um welche Person es sich handelt " – Daraus folgt die Verpflichtung dafür zu sorgen, das sich die Daten stets in einem korrekten Zustand befinden.

Wenn Bonitätsdaten falsch sind, bekomme ich keinen Bankkredit oder keinen Telekomvertrag.

Grundsatz der Integrität und Vertraulichkeit

Unbefugte dürfen keinen Zugang zu den Daten haben.

Grundsatz der Rechenschaftspflicht

Der Verantwortliche hat die Verantwortung für die Einhaltung sämtlicher Grundsätze.

Grundsatz der Technikgestaltung

Privacy by Design

Der Verantwortliche muss datenschutzfreundliche Techniken einsetzen. Es geht dabei um technische Mittel zur Erhöhung Datenminimierung und Datenbegrenzung und um technische Mittel zur Pseudonymisierung (ohne Zusatzfunktion können Daten nicht mehr einer Person zugeordnet werden)

Schaffung von Zugriffsschranken und Zugriffskontrollen, Erstellung eines Datenbankmanagementsystems (wer darf was tun bzw. sehen), Abwehr interner Datenangriffe (keine Möglichkeit für USB-Sticks, Abwehr externer Datenangriffe (Cybercrime).

Grundsatz der datenschutzfreundlichen Voreinstellung

Privacy by Default

Durch Voreinstellungen sollen nur jene personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Mit uns die Zukunft in Griff. Ihr Erfolg ist unser Ziel.

www.bollenberger.com

Ihr Ansprechpartner betreffend Datenschutz:

Margit Bollenberger

datenschutz@bollenberger.com