Datenschutz im Unternehmen – Die Anforderungen steigen! Ein Überblick und ein Ausblick

**** Autoren AUBIZ GmbH, Jens Großkreuz und RA Dirk Trettin***

Der langjährige Chief Executive Officer von Google, Eric Smith, wird sinngemäß dahingehend zitiert, dass seiner Auffassung nach der Schutz der Privatsphäre überholt sei:

"Wir wissen wo du bist, wir wissen wo du warst und wir wissen mehr oder weniger auch, was du gerade denkst."

Aus psychologischer Sicht beschreibt der Begriff Privatsphäre, inwieweit ein Mensch anderen Menschen Zutritt zu seiner eigenen Welt gewährt. Jeder Mensch muss versuchen, für sich eine ausgewogene Balance zwischen Zurückgezogenheit und Selbstöffnung zu finden. Diese informationelle Selbstbestimmung bedarf eines gesetzlichen Schutzes, weil die technischen Möglichkeiten der Datenverarbeitung enorme Eingriffe in die Privatsphäre ermöglichen.

Überblick über das geltende Datenschutzrecht

Jedes Unternehmen unterhält Daten, die gewissen Regelungen und Anforderungen unterliegen. Aufgrund der immer stärker werdenden digitalen Vernetzung jedoch müssen die Grundlagen für die Einhaltung des Datenschutzes gelegt werden. Die komplexen Regeln des Datenschutzes sind unbedingt einzuhalten und dem Datenschutz entsprechende Aufmerksamkeit zu widmen. Die drohenden Geldbußen und Strafen sind erheblich und können im Ernstfall die Existenz des Unternehmens gefährden.

Verstöße gegen die Datenschutzgesetze können unterschiedliche Rechtsfolgen und Sanktionen begründen. Denkbar sind zum einen direkte Sanktionen aus den Datenschutzgesetzen, wie z.B. Bußgelder, Geldstrafen oder Freiheitsstrafen und Gewinnabschöpfung. Darüber hinaus werden unter Umständen Haftungstatbestände erfüllt, die zu Schadensersatzansprüchen und Unterlassungsansprüchen führen können. Im Falle von Verstößen können aber auch wettbewerbsrechtliche Probleme auftreten, die zu Abmahnungen führen.

Ein weit verbreiteter Irrglaube über die Bedeutung von Datenschutz leitet sich aus dem Wortstamm ab: „Daten schützen". Dabei sollen nicht die Daten per se geschützt werden, sondern vielmehr ist es die Person, die hinter den Datensätzen steckt.

Datenschutz basiert somit auf dem allgemeinen Persönlichkeitsrecht und der informationellen Selbstbestimmung, welche unantastbar im Grundgesetz verankert sind. Der Schutz personenbezogener Daten geht demnach jeden Einzelnen an – sowohl in der Rolle des zu Schützenden als auch des Schützers.

Die Notwendigkeit zum Datenschutz ergibt sich zum einen aus den gesetzlichen Erfordernissen auf Landes- und Bundesebene. Jeder Unternehmer und Selbständige, der personenbezogene Daten verarbeitet – und das betrifft jeden – ist zum Datenschutz verpflichtet. Daten von Kunden, Mandanten, Patienten, Geschäftspartnern, Lieferanten, Dienstleistern oder auch Mitarbeitern, sogar E-Mail-Adressen, sind Ziel von Cyberangriffen. Auch unternehmenseigene Unterlagen, beispielsweise Bankdaten oder personenbezogene Angaben, eignen sich für Identitätsdiebstähle und damit verbundene Betrugszwecke. Dies gilt für schriftliche oder digitale Daten.

Vor allem unter Mitbewerbern sind Abmahnungen wegen Fehlern im Impressum, Datenschutzerklärung oder Verlinkungen auf Homepages besonders beliebt. Spezialisierte Anwaltskanzleien mahnen deshalb oft zu Recht ab.

Neben dem Bundesdatenschutzgesetz (BDSG) beinhalten auch weitere gesetzliche Normen datenschutzrechtliche Vorgaben. Bei Nichteinhaltung der spezifischen Einzelheiten drohen zum Teil empfindliche Strafen. Ein Verstoß gegen die Bestimmungen des BDSG etwa kann mit einer Geldstrafe von bis zu 300.000 Euro oder einer Freiheitsstrafe von bis zu zwei Jahren geahndet werden.

Im Sinne des BDSG sind personenbezogene Daten alle Einzelanga-

Bildquelle: ©K.C.-Fotolia.com

ben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierzu zählen unter anderem Vorname und Name, Geschlecht, Geburtsdatum, Haar- und Augenfarbe, Religionszugehörigkeit, Berufsausbildung, Familienstand sowie Anzahl der Kinder. Sprich alle Daten, die eine Person beschreiben beziehungsweise identifizieren.

Darüber hinaus kennt das BDSG mit Rasse oder Ethnie, politischer Meinung, religiöser oder weltanschaulicher Überzeugung, Gewerkschaftszugehörigkeit sowie Angaben zu Gesundheit und Sexualleben die sogenannten sensiblen Daten einer natürlichen Person.

Bereits Unternehmen mit mehr als neun Mitarbeitern, die computergestützt mit personenbezogenen Daten arbeiten, benötigen einen internen oder externen Datenschutzbeauftragten. Wird trotz der bestehenden Pflicht kein Datenschutzbeauftragter bestellt oder erfolgt die Bestellung nicht rechtzeitig, drohen Bußgelder von bis zu 50.000 Euro.

Der Datenschutzbeauftragte unterstützt die Geschäftsleitung bei der Umsetzung des betrieblichen Datenschutzes. Das Unternehmen schützt sich auf diese Weise vor Sanktionierung durch die Aufsichtsbehörde sowie vor Datenschutzskandalen mit häufig einhergehender negativer Presse. Dies ist nicht nur für Unternehmen, die den privaten Endverbraucher beliefern, von hoher Relevanz. Die „Baustelle“ Datenschutz betrifft jeden.

Durch die Weiterentwicklung der technischen Möglichkeiten und die Verbreitung von elektronischen Endgeräten in nahezu jeden Haushalt wird der Datenschutz immer wichtiger werden. Der Datenmissbrauch wird zunehmen und die öffentliche Wahrnehmung zu diesem Thema wird steigen.

Für Unternehmen bedeutet dies, dass ein datenschutzkonformes Auftreten im Markt an Bedeutung gewinnen wird. Die datenschutzrechtlichen Regelungen werden stetig komplexer und folgen der technischen Entwicklung. Unternehmen müssen sich also den steigenden Erwartungen der Kunden anpassen und die steigenden Datenschutzregelungen umsetzen.

Die Beschwerden bei den Datenschutzbehörden steigen seit Jahren an. Zugleich werden die Überwachungen der Datenschutzbehörden zunehmen und das Risiko von Bußgeldern wird steigen, ebenso das Risiko von Abmahnungen durch Mitbewerber und Verbraucherschutzorganisationen.

Dies gilt im Übrigen nicht nur für große Unternehmen, sondern auch für kleine Betriebe in jedem Bereich – gewerblich oder freiberuflich.

Insgesamt wird das Datenschutzrecht strenger und die Sanktionen werden verschärft. Anders als Richtlinien ist eine Verordnung unmittelbar anwendbares Recht. Die Neuregelungen sollen zudem den heutigen technischen Standards Rechnung tragen.

Die DSGVO betrifft alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, und zwar unabhängig davon, ob das betreffende Unternehmen in der EU ansässig ist oder nicht. Die Definition des Begriffs „personenbezogene Daten“ ist dabei keineswegs auf Name, Anschrift oder Ausweisnummer beschränkt, sondern weitergefasst als bisher.

Bildquelle: ©marius-Fotolia.com

Folglich wird die konsequente Umsetzung von Datenschutz künftig nicht mehr nur eine lästige Verpflichtung sein, sondern wird eine wesentliche Kernaufgabe eines jeden Unternehmens. Bereits jetzt schon werden Unternehmen von der Auftragsvergabe ausgeschlossen, die keinen ordnungsgemäßen Umgang im Datenschutz nachweisen können.

Ausblick auf das neue europäische Datenschutzrecht

Am 25. Mai 2018 tritt in der EU eine neue Datenschutzverordnung (DSGVO) in Kraft, um das europäische Datenschutzrecht zu vereinheitlichen.

Vielmehr besagt die Verordnung, dass selbst Unternehmen, die lediglich eine Social-Media-Adresse speichern, die sich auf einen EU-Bürger bezieht, unter die neue Regelung fallen können.

Werden die Vorgaben der Verordnung nicht erfüllt, sind heftige Bußgelder die Folge. So können bei Verstößen, die sich auf die Bereiche Kontrolle und Beherrschung beziehen, Bußgelder von bis zu 10 Millionen Euro oder 2 Prozent des Jahresumsatzes verhängt werden. Bei Verstößen im Bereich Rechte und Pflichten sieht es noch düsterer aus. Hier können bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes eingefordert werden.

Dabei greift übrigens stets der jeweils höhere Betrag. Wie die bestehende Regelung unterscheidet auch die neue Verordnung zwischen Datenverantwortlichen und Datenverarbeitern.

Die Datenverarbeiter werden in die Pflicht genommen, und das ist neu. Bislang lag die gesamte Verantwortung beim Datenverantwortlichen. So müssen Datenverarbeiter ab Mai 2018 Verstöße gegen das Datenrecht melden und den Datenverantwortlichen benachrichtigen, wenn sie der Ansicht sind, dass eine Anweisung für die Datenverarbeitung nicht regelkonform ist.

Die mit Abstand weitreichendste Änderung dürfte die Umkehr der Beweislast sein. Verstöße gegen den Datenschutz müssen nicht länger von der zuständigen Behörde nachgewiesen werden. Unternehmen müssen vielmehr belegen, dass sie die Regeln einhalten.

Wurde gegen datenschutzrechtliche Regeln verstoßen, drohen Bußgelder von bis zu vier Prozent des weltweiten Jahresumsatzes. Unternehmen müssen mehr denn je dokumentieren, warum personenbezogene Daten verarbeitet werden dürfen, wie die Verarbeitung stattfindet und welche Sicherheitsmaßnahmen eingesetzt werden, um die Daten zu schützen.

Die Herausforderung liegt hierbei im Aufbau eines Dokumentationssystems. Datenschutzaufsichtsbehörden können die Dokumentation einsehen.

Zukünftig müssen Unternehmen ihre Kunden und Nutzer wesentlich umfangreicher und häufiger als heute darüber informieren, dass ihre Daten verarbeitet werden. Dies gilt auch, wenn Daten von Dritten geliefert werden – durch Adresshandel oder bei einer Bonitätsprüfung. Auch wenn Bestandsdaten für neue Zwecke verarbeitet werden, lebt die Informationspflicht wieder auf. Wer seine Kundenadressen für ein Mailing nutzen will, muss regelmäßig die betroffenen Kunden spätestens vor der Datenselektion und dem Mailingversand informieren. Der Kunde würde deshalb zwei Briefe nacheinander erhalten: die Information und das eigentliche Mailing. Um Verbraucher nicht unnötig zu verwirren, müssen Unternehmen die Umsetzung der Informationspflicht sorgfältig planen.

Die Übergangsfrist bis zur Anwendung der DSGVO sollte genutzt werden, um etwa Geschäftsmodelle, Prozesse und Verträge an das neue Recht anzupassen.

Andernfalls laufen Geschäftsführer und Vorstände Gefahr, persönlich zu haften.

Die höhere Transparenz nach außen erleichtert es Verbraucherschützern und Wettbewerbern, gegen unzulässige Aktionen vorzugehen. Wie hoch der Umstellungsaufwand sein wird, hängt vom Unternehmen ab. Sicher jedoch ist, dass überall Anpassungsbedarf besteht.

Pro Verstoß gilt:

1. Verantwortungsloser Umgang mit Personendaten (formaler Verstoß):
   Bis zu 50.000,00 EUR

   Beispiel: Ein Datenschutzbeauftragter wurde nicht oder nicht ordnungsgemäß bestellt.

2. Fahrlässige oder vorsätzliche Datenschutzverletzung (materieller Verstoß):
   Bis zu 300.000,00 EUR

   Beispiel: Ein Mitarbeiter gibt personenbezogene Kundendaten ohne deren Einwilligung an ein bekanntes Unternehmen weiter.

3. Vorsätzliche Datenschutzverletzung mit Bereicherungs- oder Schädigungsabsicht:
   Bis zu 2 Jahre Haft

   Beispiel: Ein Mitarbeiter verkauft personenbezogene Kundendaten ohne deren Einwilligung an einen Wettbewerber

Bildquelle: ©nikoendres-Fotolia.com