TOENNES & FELSNER
RECHTSANWÄLTE
FACHANWÄLTE

Ist Ihr Unternehmen fit für die neuen DATENSCHUTZ-Regeln?

DATENSCHUTZ ist zur Zeit das Thema. **Ab dem 25.05.2018** muss jedes Unternehmen die Vorgaben der neuen EU-Datenschutz-Grundverordnung (DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG neu) praktisch umgesetzt haben. Diese Vorschriften machen einige Änderungen im Unternehmensalltag erforderlich, welche schnell umgesetzt werden sollten, da andernfalls nicht nur Schadensersatzansprüche und stark erhöhte Bußgelder (bis 20 Mio. Euro oder bis 4% des gesamten weltweit erzielten Jahresumsatzes) drohen, sondern insbesondere DER GUTE RUF DES UNTERNEHMENS – gerade im Umgang mit Kundendaten! – Schaden nehmen könnte.
Dementsprechend bieten wir an, Sie bei der Vorbereitung und Umsetzung der wesentlichen Neuerungen in Ihrem Unternehmen vertrauensvoll zu begleiten. Wir helfen Ihnen dabei, alle datenschutzrelevanten Bereiche in Ihrem Unternehmen zu erkennen und diejenigen herauszufiltern, für welche tatsächlich HANDLUNGSBEDARF besteht. Für diese können wir Ihnen dann konkret die vorzunehmenden, praktischen Maßnahmen – individuell zugeschnitten auf Ihr Unternehmen – erläutern.
Die folgenden Punkte geben Ihnen eine gute Übersicht über die

zentralen Anforderungen der DSGVO & des neuen BDSG für Unternehmen,

mit welcher es Ihnen SOFORT und PROBLEMLOS möglich sein wird, mit den Vorbereitungen auf das neue Datenschutzrecht zu starten, um sich alsbald wieder auf Ihr eigentliches Geschäft konzentrieren zu können:

1. Datenschutzbeauftragte/r

Sie benötigen einen Datenschutzbeauftragten, wenn Sie in der Regel mindestens 10 Personen ständig mit der automatisierten (= unter Einsatz von EDV/ nicht nur handschriftliche Karteikarten) Verarbeitung (= alle Tätigkeiten von Speicherung/ Erhebung bis Löschung) personenbezogener Daten beschäftigen.
Dies ist die „Grundregel“, von welcher es selbstverständlich Ausnahmen gibt. So ist ein Datenschutzbeauftragter – auch bei weniger als 10 Personen – etwa erforderlich, wenn Sie geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten, wenn die Verarbeitung besonders sensibler Daten (z.B. religiöse Überzeugung, Gesundheit, etc.) zur Kerntätigkeit Ihres Unternehmens zählt oder wenn Ihre Kerntätigkeit eine Datenverarbeitung betrifft und aufgrund ihres Zwecks oder Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung/ Überwachung von betroffenen Personen erforderlich ist.
Ein Datenschutzbeauftragter kann grundsätzlich auch aus dem eigenen Unternehmen gestellt werden. Er muss jedoch bestimmte gesetzliche Vorgaben erfüllen.

2. Verzeichnis von Datenverarbeitungstätigkeiten

Sobald Sie nicht nur gelegentlich personenbezogene Daten verarbeiten, müssen Sie ein Verzeichnis über alle Datenverarbeitungstätigkeiten/ -prozesse in Ihrem Unternehmen, aus sämtlichen Abteilungen, (fort-) führen. Dies wird bei fast allen Unternehmen gegeben sein, da es hier weder auf eine bestimmte Anzahl von Beschäftigten, noch auf eine automatisierte Verarbeitung ankommt.
Die Erstellung und Fortführung des Verarbeitungsverzeichnisses ist die **wohl wichtigste Maßnahme**, da Sie es auf Anfrage – schriftlich oder elektronisch – mit den gesetzlich vorgesehenen Inhalten sofort bereitstellen müssen. Da diese Abfrage den Aufsichtsbehörden allenfalls wenig Umstände bereiten wird, gehen wir davon aus, dass das Verarbeitungsverzeichnis in der Praxis häufig abgefragt werden wird.
Neue Verarbeitungsprozesse sollten stets in das Verarbeitungsverzeichnis nachgetragen werden. Sämtliche Datenschutzmaßnahmen, auch die im Folgenden aufgeführten, sollten durch Eintragung in das Verarbeitungsverzeichnis vernünftig dokumentiert werden.

3. Informationspflichten & Auskunftsrechte; Anpassung von Verträgen/ Rechtstexten

Grundsätzlich ist zunächst einmal jede Verarbeitung von Daten (ob bloße Speicherung oder Löschung) verboten, es sei denn, dass sie ausdrücklich durch Gesetz erlaubt ist oder die betroffene Person wirksam ihre **Einwilligung** erteilt.
Damit eine Einwilligung wirksam ist, müssen wiederum mehrere Voraussetzungen erfüllt sein. So ist eine Einwilligung z.B. für jeden Einzelfall einer Datenverarbeitung, und nicht pauschal, abzugeben. Der Einwilligende muss zuvor wirksam über sämtliche Zwecke der beabsichtigten Datenverarbeitung informiert werden. Der Einwilligende muss zudem eine echte Wahlfreiheit zur Abgabe haben. Die Einwilligung darf nicht an die Erfüllung eines Vertrages geknüpft werden, zu dessen Erfüllung die Daten nicht benötigt werden. Der Einwilligende muss ordnungsgemäß über sein Widerrufsrecht informiert werden.
Über die verarbeiteten Daten und über die Rechte der hiervon betroffenen Personen müssen diesen nun dementsprechend vorab zusätzliche, erheblich umfassendere und transparenter zu formulierende **Informationen** erteilt und nachträglich, auf Anfrage, zudem unverzüglich und unentgeltlich **Auskünfte** erteilt werden. Es muss etwa umfassend und in verständlicher Sprache über Verarbeitungszwecke, Rechtsgrundlagen, Dauer der Speicherung, das Widerrufsrecht bezüglich Einwilligungen, Rechte auf Berichtigung, Löschung und Einschränkung der Datenverarbeitung, Beschwerderecht bei der Aufsichtsbehörde, Kategorien der Empfänger der Daten, Kontaktdaten der Verantwortlichen uvm. informiert/ Auskunft erteilt werden.
So müssen insbesondere gültige, rechtskonforme Verträge mit Ihren Kunden/innen und sonstigen Geschäftspartnern/innen, Arbeitsverträge mit Ihren Mitarbeitern/innen, ggf. Betriebsvereinbarungen, Verträge zur Auftragsdatenverarbeitung, Rechtstexte auf Ihrer Internetseite – insbesondere die Datenschutzerklärung (!) – und Einwilligungserklärungen neu erstellt/ ergänzt werden.

Eine besondere Bedeutung kommt hierbei den **Verträgen mit Auftragsdatenverarbeitern** zu. Auftragsverarbeiter sind dabei i.d.R. externe Dienstleister, die in Ihrem Auftrag personenbezogene Daten in irgendeiner Weise verarbeiten. Konkret handelt es sich dabei um Verträge mit Firmen wie z.B. IT-Servicefirmen, Softwareherstellern, Web-/ Server-/ Apphoster, Cloud-Dienstleister, Rechenzentren, von denen Sie etwa Software/ Programme für die Datenerfassung, Datenkonvertierung oder zum Einscannen von Dokumenten bzw. zur Herstellung/ Verwaltung/ Archivierung von Kundenkarteien, Terminverwaltung, Buchführung, Lohn- und Gehaltsabrechnung, Textverarbeitung, Spracherkennung, Backups/ Sicherheitsspeicherungen oder allgemeine Datenspeicherung beziehen, oder welche für Sie etwa Internetseiten und die Verwaltung der darauf befindlichen Kontaktformulare, Nutzeranfragen oder Email-Dienste, Onlineshops, Domains und Server/ externen Speicherplatz, Werbeadressenverarbeitung zur Verfügung stellen oder betreuen, Akten/ Daten/ Datenträger entsorgen, sonstigen externen Support in Form von Prüfungen/ Wartungen (Fernwartung) Ihres Computersystems und entsprechender automatisierter Verfahren durchführen oder aber die bloße Nutzung von Google Analytics. Mit diesen Firmen müssen bis zum 25.05.2018 – elektronisch oder schriftlich – Verträge abgeschlossen/ angepasst werden, damit neue oder bestehende Auftragsverarbeitungen (weiter) genutzt werden können.
Sollten die **Rechtstexte auf Ihrer Internetseite** (AGB, Datenschutzerklärung, Impressum, Widerrufsbelehrung) schon längere Zeit nicht mehr aktualisiert worden sein, so ist jetzt ein sehr günstiger Zeitpunkt, dies nachzuholen. Eine Anpassung der **Datenschutzerklärung** an das neue Datenschutzrecht ist unbedingt erforderlich!

4. Technische & Organisatorische Maßnahmen (TOMs)

Für jeden Datenverarbeitungsprozess müssen geeignete TOMs vorhanden sein, um den Schutz dieser Daten – z.B. vor dem Zugriff unberechtigter Personen – zu gewährleisten. Diesbezüglich lässt sich den neuen Datenschutzvorschriften lediglich entnehmen, dass die TOMs „angemessen“ und „verhältnismäßig“ sein und dem „Stand der Technik“ (= TOMs, die zur Verfügung stehen und die sich bereits in der Praxis bewährt haben). entsprechen sollen. Durch TOMs sollen etwa Stabilität, Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit der verwendeten Computersysteme und Dienste, Wiederherstellbarkeit von Daten, und gewisse Kontrollen und Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser TOMs sichergestellt werden. Folglich sind die jeweils erforderlichen TOMs für jeden Einzelfall – etwa nach Eintrittswahrscheinlichkeit, Schwere der Risiken, Größe des Unternehmens, etc. – individuell zu bestimmen. Konkrete, den meisten Unternehmen zumutbare Maßnahmen könnten etwa Passwörter, Verschlüsselungen, Pseudonymisierungen und fachgerechte Datensicherungen sein.

5. Datenschutzfolgenabschätzung

Ist absehbar, dass ein bestimmter Datenverarbeitungsvorgang voraussichtlich ein hohes Risiko für persönliche Rechte und Freiheiten betroffener Personen birgt, so müssen Sie zunächst – dokumentiert – die Folgen für den Schutz der personenbezogenen Daten ab-

schätzen. Dies ist etwa der Fall bei der Einführung neuer Technologien, bei denen Umfang und Eingriff in die Persönlichkeitsrechte noch nicht sicher feststehen, bei dem Profiling, bei der Verarbeitung besonders sensibler Daten (Gesundheit, Rasse, Religion, etc.) oder bei einer umfangreichen öffentlichen Videoüberwachung. Ist ein solches Risiko festzustellen, so ist als nächstes zu prüfen, ob ausreichende Abhilfe-/ Sicherheitsvorkehrungen vorhanden sind. Bleibt trotzdem noch ein Risiko bestehen, so muss die zuständige Aufsichtsbehörde diesbezüglich konsultiert werden.

6. Internes Maßnahmen-/ Verfahrenspaket

Wir raten dazu, dass Sie selbst, unternehmensintern, ein dokumentiertes „Verfahrenspaket" mit „internen Datenschutzrichtlinien" – einerseits zur vorsorglichen Vermeidung von Datenschutzverletzungen und andererseits zur Bestimmung eines klaren Ablaufplans für den Fall des Eintritts von Datenschutzverletzungen und wenn die Erteilung von Auskünften oder die Löschung/ Herausgabe von Daten verlangt wird – festlegen. Schließlich sind Sie nach den neuen Vorschriften im Falle des Eintritts einer Datenschutzverletzung (= Vorfall, der zu einer unbeabsichtigten/ unrechtmäßigen Vernichtung, Verlust, Veränderung oder unbefugten Offenlegung personenbezogener Daten geführt hat) als Verantwortlicher verpflichtet, diese Verletzung unverzüglich und möglichst **binnen 72 Stunden** nach Kenntniserlangung der zuständigen Aufsichtsbehörde und den betroffenen Personen zu melden.

Wenn dies gewünscht ist, berät Herr Rechtsanwalt Kolbeck – Tätigkeitsschwerpunkt Informationstechnologierecht und Datenschutz – Sie und die in Ihrem Unternehmen mit Datenverarbeitungsvorgängen betrauten Mitarbeiter/innen individuell zu allen relevanten Themen.

Rechtsanwälte Toennes, Felsner & Kolbeck

Schloßstrasse 27
D- 49074 Osnabrück

Telefon: +49 541 200982-0
Telefax: +49 541 200982-10

Homepage: www.toennes-felsner.de
E-Mail: info@toennes-felsner.de