GUTcert Interview

Das vorliegende Interview wurde im August 2018 von Andreas Lemke (Prokurist der GUTcert) geführt mit Rechtsanwalt Bartels LL.M., Partner der HK2 Rechtsanwälte, Berlin

Daten sind Macht: EU Datenschutz – Schreckgespenst oder Chance für mehr Transparenz?

In der Öffentlichkeit wird immer wieder die europäische Harmonisierung des EU-Datenschutzes diskutiert, die augenscheinlich zunehmend an Wichtigkeit gewinnt. Momentan scheint kein Projekt der EU so viel Aufmerksamkeit zu bekommen, wie die Datenschutz-Grundverordnung (DSGVO). Alle Unternehmen müssen sich spätestens jetzt mit dem Datenschutz und den daraus resultierenden Risiken auseinandersetzen. Und betroffen sind viele: Prozess-verantwortliche, Auftragsverarbeiter oder die Aufsichtsbehörde selbst.

Zum Thema sprach Andreas Lemke, GUTcert Prokurist und im Unternehmen Verantwortlicher für die Informationstechnik mit Rechtsanwalt Karsten U. Bartels.

Rechtsanwalt Karsten U. Bartels LL.M. ist spezialisiert auf das IT-, Datenschutz- und IT-Sicherheitsrecht. Er ist Partner bei HK2 Rechtsanwälte, Berlin, Vorstandsmitglied des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT), stellvertretender Vorsitzender der Arbeitsgemeinschaft IT-Recht des Deutschen Anwaltsvereins e.V., Geschäftsführer der Datenschutz-beratungsgesellschaft Comtection GmbH und Referent und Autor zahlreicher Beiträge zum Datenschutz- und IT-Sicherheitsrecht. Er vermittelt Unternehmen, wie sie den konkreten Einsatz von Maßnahmen nach dem Stand der Technik abwägen und ein begrenztes Unterschreiten des Standes der Technik gesetzeskonform realisieren können.

Lemke: Ein guter Zeitpunkt, um das Thema Datenschutz intensiver zu betrachten und auch Seiten zu beleuchten, die für viele Betroffene noch im Verborgenen sind.

Der Datenschutz wurde im Mai 2016 mit einer Übergangsfrist bis zum 25. Mai 2018 in der EU-Datenschutz-Grundverordnung (DSGVO) europäisch harmonisiert. Neben Neuerungen zur Umsetzung des Datenschutzes wird auch die Unternehmenshaftung ausgeweitet. Je nach Art des Verstoßes drohen zukünftig Bußgelder – bis zu 4% des Jahresumsatzes.

Wer ist von diesen Regelungen betroffen? Und wieso wird jetzt erst mit der DSGVO das Thema so präsent – es gab doch schon lange nationale Gesetze, z.B. in Deutschland das BDSG?

Bartels: Die DSGVO gilt für Unternehmen, öffentliche Stellen und Behörden in der EU, die personenbezogene Daten verarbeiten, unabhängig davon, wo die Daten verarbeitet werden. Ausnahmeregelungen für Klein- oder Kleinstunternehmen gibt es nicht. Für die Anwendbarkeit der DSGVO kommt es nicht darauf an, ob die Verarbeitung personenbezogener Daten zum Kern der der Tätigkeit des Verantwortlichen gehört oder nicht.

Der Fokus auf die DSGVO ist in den letzten Monaten in der Tat massiv gestiegen. Das begründet sich vor allem mit den signifikant gestiegenen Bußgeldern, die bei Verstößen drohen. Das alte BDSG, das bis zum 24.05.2018 galt, kannte zwar auch Bußgelder. Deren niedriger Rahmen hat viele Unternehmen bislang allerdings eher einschätzen lassen, die Non-Compliance sei günstiger als die Implementierung gesetzlicher Maßnahmen zu mehr Datenschutz.

Ihr GUTcert Ansprechpartner:
Andreas Lemke, Prokurist
Mail: andreas.lemke@gut-cert.de
Fon: +49 30 2332021-41

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin

Diese Einschätzung war auch in der Regel richtig. Mit der DSGVO werden die Bußgelder nun bilanzrelevant. Übrigens gehören IT-Sicherheit und Datenschutz zum Risikomanagement, für das Geschäftsleiter auch persönlich haften können. Diese Ansprüche sind gesellschaftsrechtlicher Natur und nicht neu, werden aber nun vermehrt ernst genommen.

Lemke: Was für Unternehmen sind denn im besonderen Maße betroffen? Und gibt es Branchen/Dienstleister, die momentan noch im Unklaren sind? Gibt es gewisse Erfahrungswerte aus Ihrer datenschutzrechtlichen Arbeitspraxis?

Bartels: Aktuelle Erhebungen machen deutlich, dass tatsächlich noch die breite Mehrheit der Unternehmen im Unklaren ist. Auch **große Konzerne und Unternehmen**, die der sogenannten dualen Aufsicht unterliegen, wie zum Beispiel Betreiber Kritischer Infrastrukturen, haben – trotz des zum Teil sehr guten IT-Sicherheitsniveaus – noch keinen DSGVO-konformen Datenschutz. Unsere Arbeit besteht in solchen Fällen oft darin, eine **koordinierende Hand** zu sein, die alle zu treffenden Maßnahmen wertet, im Blick behält und die betreffenden Parteien entsprechend anweist. Die daraus entstehenden Aufgaben sind für die Verantwortlichen im Unternehmen dann klarer und leichter abzuarbeiten.

Unserer Erfahrung nach sehen sich auch insbesondere die **kleinen und mittelständischen Unternehmen** (KMU) überfordert bei der Umsetzung der DSGVO. Diesen Eindruck kann ich verstehen, jedoch kann ich gleichermaßen beruhigen: Wir haben bei unseren Kunden und Mandanten die Erfahrung gemacht, dass praktische und wirtschaftlich effiziente Lösungen in jedem Fall zu finden sind. Eine gute (Basis-)Möglichkeit sind **kosteneffiziente DSGVO-Pakete**, die alle wichtigen Dokumente und eine entsprechende Anleitung enthalten. In den letzten Monaten haben wir speziell für die Ingenieurs- und Personaldienstleisterbranche entsprechende Pakete entwickelt. Die positive Resonanz war enorm. Aufgrund der großen Nachfrage befinden wir uns deshalb derzeit in der Erstellung eines analogen, branchenübergreifenden Pakets für KMU.

Auch gilt es, folgendes **im Blick** zu behalten: Nur weil die DSGVO auch auf kleine Unternehmen anwendbar ist, bedeutet dies nicht, dass Unternehmen ohne Ansehung ihrer Größe, Tätigkeit und wirtschaftlichen Stärke dieselben Maßnahmen zu ergreifen hätten. Unternehmen dürfen und sollen **angemessene** technische, organisatorische und rechtliche Maßnahmen ergreifen.

Besondere Umstellungsanforderungen treffen Unternehmen, die datengetriebene Geschäftsmodelle betreiben, sensible Daten (z.B. Gesundheitsdaten) verarbeiten und die Datenverarbeitung auslagern. Die bisherige Auftragsdatenverarbeitung (ADV) beispielsweise wurde als Auftragsverarbeitung (AV) in der DSGVO signifikant anders geregelt. Hier sind sämtliche ADV-Vereinbarungen an das neue Recht anzupassen, unabhängig davon, ob man diese als Auftraggeber oder Auftragnehmer geschlossen hat.

Des Weiteren möchte ich den Blick dafür schärfen, dass die DSGVO-Umsetzung kein „Projekt" ist, mit dem man nach dessen Ende nicht mehr befasst ist. Die DSGVO wird uns viele Jahre erhalten bleiben und **dauerhaft beschäftigen**. Das lässt sich aber ressourcenverträglich managen.

Die DSGVO bietet derzeit an vielen Stellen auch noch zahlreiche **Auslegungsmöglichkeiten**. Das wird von Unternehmen häufig als Unsicherheitsfaktor bewertet. Allerdings unterschätzen die Verantwortlichen noch deutlich die dadurch entstehenden, vielseitigen Möglichkeiten.

Lemke: Was bedeutet hier „Stand der Technik": Welche konkreten Maßnahmen sind im Normalfall notwendig?

Ihr GUTcert Ansprechpartner:
Andreas Lemke, Prokurist
Mail: andreas.lemke@gut-cert.de
Fon: +49 30 2332021-41

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin

GUTcert Interview

Bartels: Die Umsetzung der DSGVO bedeutet, dass diverse Dokumente (Verfahrensverzeichnisse etc.) erstellt, Prozesse (Datenschutz-Folgenabschätzung etc.) eingerichtet und technische und organisatorischen Maßnahmen (z.B. zur Abwehr von Hackerangriffen) getroffen werden müssen. Es kann an vielen Stellen mit Mustern und Standardlösungen gearbeitet werden. Die Maßnahmen haben nun allerdings den Stand der Technik (Art. 32 DSGVO) zu berücksichtigen. Deshalb muss es eine Auseinandersetzung mit möglichen Lösungen geben. Das ist eine technisch-juristische Aufgabe, die von der IT und den Juristen erledigt werden sollte.

Lemke: Unter welchen konkreten Voraussetzungen brauche ich einen Datenschutzbeauftragten? Und reicht es aus, wenn ich der Behörde einen „vermeintlichen" Beauftragten melde?

Bartels: Ob der datenschutzrechtlich Verantwortliche einen Datenschutzbeauftragten zu benennen hat, richtet sich unter anderem danach, ob er in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 BDSG-neu). Das ist schnell der Fall, da hier die Headcounts zählen und nicht die Vollzeitangestellten und es auch nicht darauf ankommt, ob der Mitarbeiter mit etwa der Verarbeitung von Kundendaten betraut ist. Wer z.B. einer Datenschutz-Folgenabschätzung unterliegt, muss einen Datenschutzbeauftragten benennen, unabhängig von der Mitarbeiterzahl.

Lemke: Wodurch entstehen i.d.R. Verletzungen des Datenschutzes und was ist der „Worst Case" für Unternehmen?

Bartels: Verletzungen des Datenschutzrechts bestehen häufig darin, dass es keine hinreichende Rechtsgrundlage für die Zulässigkeit der Verarbeitung der personenbezogenen Daten gibt – die Daten also nicht verarbeitet werden dürften. Zudem gibt es nur verhältnismäßig wenig Unternehmen, die der Dokumentations-/ Rechenschaftspflicht nachkommen. So genügt es nicht, IT-Sicherheitsmaßnahmen zu implementieren. Sie müssen auch detailliert dokumentiert werden.

Natürlich wirkt es sich auch aus, ob die Mitarbeiterinnen und Mitarbeiter hinreichend geschult werden. Der Datenschutz beginnt mit der Information über Rechte und Pflichten der Betroffenen.

Die zu befürchtenden Schäden sind nicht nur unmittelbar materieller Art. Gerade ein Reputationsverlust kann massive Folgen haben. Noch nicht hinlänglich bekannt ist, dass die DSGVO auch einen Schadenersatz wegen immaterieller Schäden kennt.

Lemke: Welche Chancen birgt der Datenschutz für Unternehmen?

Bartels: Datenschutz im Unternehmen schafft Vertrauen. Innerhalb der EU können deutsche Unternehmen mit einem mustergültigen Datenschutzniveau auch Wettbewerbsvorteile für sich verbuchen. Weltweit betrachtet ist das anders zu bewerten.

In diesem Zusammenhang ist das Thema Zertifizierung von Relevanz. Gestatten Sie mir daher eine Gegenfrage: Wie steht es eigentlich um das Thema Zertifizierung? Wann können sich Unternehmen im Sinne der DSGVO zertifizieren lassen und wem nutzt aus Ihrer Sicht eine Zertifizierung?

Ihr GUTcert Ansprechpartner:
Andreas Lemke, Prokurist
Mail: andreas.lemke@gut-cert.de
Fon: +49 30 2332021-41

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin

GUTcert Interview

Lemke: Eine Zertifizierung nach der EU-DSGVO durch akkreditierte Zertifizierungsstellen setzt gemäß Art. 42 Abs. 5 EU-DSGVO voraus, dass die zuständigen Bundes- oder Landesdatenschutzbehörden oder der Europäische Datenschutzausschuss gemäß Art. 63 EU-DSGVO die Kriterien für die Zertifizierung genehmigt haben. Daraus muss dann ein Zertifizierungsprogramm im Sinne der ISO/IEC 17065 i.V.m. ISO/IEC 17067 entwickelt werden.

Nachdem die DAkkS dieses Zertifizierungsprogramm geprüft und die Akkreditierungsfähigkeit erfolgreich festgestellt hat, läuft das Genehmigungsverfahren durch die zuständige Landesdatenschutzbehörde. Erst dann können Zertifizierungsstellen ihrerseits die Akkreditierung beantragen und Zertifizierungen nach DSGVO durchführen.

Wenn alle Beteiligten den bisher angedachten Zeitplan einhalten, könnte es durchaus noch in diesem Jahr zu den ersten Zertifizierungen kommen. Die GUTcert führt allerdings bereits jetzt mit ihren Experten Datenschutz-Audits gemäß EU-DSGVO durch. Im Rahmen eines sog. Gap-Audits wird untersucht, inwieweit die eingeführten Prozesse und Abläufe zur Verarbeitung personenbezogener Daten die Anforderungen der europäischen EU-DSGVO erfüllen. Dabei können Inhalte und Methoden bereits bestehender Managementsysteme wie Informationssicherheit nach ISO 27001 oder Qualität nach ISO 9001 ggf. angepasst oder sogar übernommen werden.

Geprüfte Unternehmen erhalten im Ergebnis einen aussagekräftigen Bericht mit einer Übersicht zum Erfüllungsstand der Anforderungen der EU-DSGVO, in dem auch das neue Bundesdatenschutzgesetz (BDSG-neu) berücksichtigt wird. Dieser Bericht kann die Basis werden für das weitere Ausgestalten und Optimieren des Datenschutzsystems.

Herr Bartels, ist es Ihrer Meinung nach sinnvoll, die Anforderungen aus der DSGVO in ein ISMS einzubinden?

Bartels: Ein ISMS ist für mittelständische und große Unternehmen nahezu unerlässlich und gilt an sich schon als eine technische und organisatorische Maßnahme im Sinne von Art. 32 DSGVO. Ein solches System trägt zur Professionalisierung des Datenschutzes, der Transparenz und der Nachhaltigkeit bei.

Bei inhaltlichen Rückfragen zum Thema wenden Sie sich gerne an die Gesprächspartner.

HK2 Rechtsanwälte

Karsten U. Bartels LL.M. (HK2 Rechtsanwälte)
Email: Bartels@hk2.eu
Tel: +49 030 27 89 00 - 0

Weitere Informationen und Veranstaltungen zum Thema Datenschutz und ISMS:

Prüfung nach Art. 42 DSGVO
gut-cert.de/produkte/managementsysteme-azav/informationssicherheit/datenschutz.html

GUTcert - Neujahrstagung am 18. Januar 2019 in Berlin
gut-cert.de/exzellenz/gutcert-neujahrstagung.html

TeleTrusT - IT-Sicherheitsrechtstag am 25.10.2018 in Berlin
teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dsgvo/it-sicherheitsrechtstag-2018

Ihr GUTcert Ansprechpartner:
Andreas Lemke, Prokurist
Mail: andreas.lemke@gut-cert.de
Fon: +49 30 2332021-41

GUTcert AFNOR Group
GUT Certifizierungsgesellschaft für Managementsysteme mbH
Umweltgutachter
Eichenstraße 3 b, 12435 Berlin