



Inhalt:

[DSGVO – Missverständnisse und rechtliche Unsicherheiten](#)

[Die E-Vergabe kommt. Für alle Bereiche!](#)

[amendos Seminare 2018](#)

DSGVO – Missverständnisse und rechtliche Unsicherheiten

Der Stichtag für das endgültige Inkrafttreten der Datenschutz-Grundverordnung (DSGVO), der 25. Mai 2018, rückt immer näher. Trotzdem hat sich laut dem Branchenverband Bitkom etwa jedes dritte Unternehmen noch nicht mit diesem Thema beschäftigt. Obwohl bei Nichterfüllung der DSGVO hohe Strafen drohen und das Risiko, das der Umgang mit vertraulichen Kundeninformationen mit sich bringt, nicht unerheblich ist, wird das Thema immer wieder verdrängt oder gar ignoriert. Doch was sind die Ursachen dieses zögerlichen und unter Umständen gefährlichen Vorgehens der Unternehmen? Welche Missverständnisse liegen vor? Einige Antworten darauf gibt der folgende Artikel.



Nach dem Inkrafttreten der EU-Datenschutz-Grundverordnung (EU-DSGVO) am 25.05.2016 endet nun im kommenden Mai die zweijährige Übergangsphase. Eigentlich Zeit genug für Unternehmen, sich nicht nur mit den Änderungen (im Vergleich zum alten Bundesdatenschutzgesetz) vertraut zu machen, son-

dern ebenfalls entsprechende Maßnahmen zu planen und umzusetzen, um die Verarbeitung von personenbezogenen Daten gemäß der neuen Verordnung auszurichten. Dennoch sind laut vielen aktuellen Studien erst wenige Unternehmen dementsprechend vorbereitet. Einige sind der Meinung, die DSGVO betreffe sie nicht. Andere wiederum schrecken vor dem vermeintlich großen Anpassungsaufwand zurück.

Ein weiterer, überaus wichtiger Faktor sind teilweise große rechtliche Unsicherheiten, die ein Zögern der Firmen verursachen. Die DSGVO ist recht umfangreich geraten und besteht aus 99 Artikeln und 173 sogenannten Erwägungsgründen. Wie bei solchen Verordnungen häufig, besteht bei einigen Artikeln ein großer Interpretationsspielraum. Viele Anwaltskanzleien rechnen daher mit einer großen Anzahl an Gerichtsverfahren, um bei strittigen Punkten Klarheit zu schaffen.

	Bundesdatenschutzgesetz <u>BDSG</u>	EU Datenschutz-Grundverordnung <u>DSGVO</u>
In Kraft getreten	1977	2016 Ende Übergangsphase: 25.05.2018
Umfang	ca. 26 Seiten	ca. 72 Seiten
Geltungsbereich	Deutschland	EU und weltweit (ohne Polizei und Justiz)
Überarbeitungen	1990, 2001, 2003, 2006, 2009, 2017	n/a
Gerichtsentscheidungen	über 700	1
Bußgelder	"kann" bis zu 300 Tsd €, bzw. 2 Jahre Freiheitsstrafe	"muss" bis zu 20 Mio €, bzw. 4% vom Konzern- Jahresumsatz
Schadensersatz	nur für materielle Schäden	für Schäden aller Art
Aufgaben des Datenschutzbeauftragten	auf Datenschutz hinwirken	unterrichten, beraten, überwachen , etc.
Ziel	"nicht erwischen lassen"	Compliance erreichen und nachweisen

Abbildung 1: Vergleich BDSG und DSGVO

Ebenfalls durch den großen Umfang der DSGVO sind einige Missverständnisse entstanden. Dies beginnt schon beim Unterschied zwischen dem eingangs erwähnten Datum des Inkrafttretens und dem Ende der Übergangsphase. Gerade viele kleine und mittlere Unternehmen glauben, dass sie jetzt einen Datenschutzbeauftragten haben müssen. Allerdings ist diese Pflicht, wie auch im alten BDSG, so nicht vorhanden. Ob man einen Datenschutzbeauftragten braucht regelt Artikel 37 DSGVO. Dort heißt es:

„Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn:

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.“

Die Meldepflichten von Datenpannen (Verlust etc.) nach DSGVO sind ebenfalls nicht etwa komplett neu. Vielmehr gibt es Änderungen gegenüber den Informationspflichten nach dem Bundesdatenschutzgesetz. Generell kann man aber von einer Verschärfung sprechen, insbesondere, wenn man die 72-Stunden-Frist zur Meldung an die zuständige Aufsichtsbehörde betrachtet. Dennoch: Es gibt schon jetzt eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten. Unternehmen müssen also keinen komplett neuen Melde-Prozess aufsetzen, wenn sie schon gemäß BDSG auf solche Fälle vorbereitet waren.

Einführung in die IT-Prozessoptimierung

Themen:

- Prozessreifegrad (u.a. CMMI, COBIT 5)
- IT-Prozessoptimierung
- Prozess-Implementierung
- Kontinuierliches Prozessmanagement

Termin: 16.04.-17.04.2018 in Hamburg

Ein weiteres Missverständnis im Zusammenhang mit der DSGVO ist das vermeintliche Verbot der Datenübermittlung ins Ausland. Die DSGVO verbietet nicht etwa die Datenübermittlung in Drittstaaten wie die USA, sondern sie stellt mehrere Anforderungen an eine solche Übermittlung. Dabei geht es um die Garantie, dass das Datenschutzniveau beim Empfänger dem der DSGVO entspricht. Für den Nachweis gibt es verschiedene Wege, da-

runter den „Privacy Shield“, bei dem die Aufsichtsbehörden allerdings weiterhin Bedarf für Nachbesserungen sehen. Denkbar ist es aber auch, dass ein Empfänger aus einem Drittstaat ein Datenschutz-Zertifikat nach DSGVO erlangt und so den Nachweis erbringt. Allerdings sind solche Zertifikate aktuell noch nicht möglich, da laut Artikel 42 DSGVO die Zertifizierungsverfahren, die zu einem DSGVO-Zertifikat führen sollen, zuerst genehmigt werden müssen. Eine solche Genehmigung ist bisher aber noch nicht erfolgt.



Lese-Tipp: Compliance-Risiken beim IT-Outsourcing minimieren

Auch im technischen Bereich gibt es Unklarheiten und Missverständnisse. So entsteht oft der Eindruck, dass durch die DSGVO nur noch mittels verschlüsselter E-Mails kommuniziert werden darf. Allerdings sieht die DSGVO in dieser Hinsicht keinen Zwang vor. Vielmehr besagt Artikel 32: Ob eine Verschlüsselung zum Einsatz kommen soll oder nicht, hängt von dem zu ermittelnden Schutzbedarf der Daten, dem Risiko für die Betroffenen sowie weiteren Faktoren ab: beispielsweise Stand der Technik, Implementierungskosten und Art, Umfang, Umstände und Zwecke der Verarbeitung. Eine Verschlüsselung ist also nicht obligatorisch, sondern eine wichtige Maßnahme bei entsprechendem Bedarf an Schutz für die Vertraulichkeit der Daten.

Fazit

Wie man sieht gibt es kurz vor dem Wirksamwerden der DSGVO am 25.05.2018 noch viel Unsicherheit bezüglich der neuen Verordnung. Dabei hat sich, verglichen zu anderen Ländern der EU, in Deutschland nicht grundsätzlich alles verändert, da es schon das starke Bundesdatenschutzgesetz gab. Nichtsdestotrotz ist es unumgänglich, dass Unternehmen die eigene Datenschutzpraxis überprüfen und das Daten-schutzmanagement bis zum Stichtag gegebenenfalls anpassen und weiterentwickeln. Die Zeit wird knapp und die drohenden Strafen durch Abmahnungen bei Nichtbeachtung sind nicht unerheblich.

Michael Pfitzmann

Die E-Vergabe kommt – für alle Bereiche!

Mit der Vergaberechtsreform vom April 2016 haben sich die vergaberechtlichen Vorschriften für öffentliche Einrichtungen nicht nur bezüglich der Inhalte geändert, sondern auch bezüglich der Kommunikationswege: Bereits seit dem 18. April 2017 müssen die zentralen Beschaffungsstellen des Bundes, der Länder und der Kommunen ihre Vergabeverfahren komplett elektronisch abwickeln. Dies betrifft sowohl die Auftragsbekanntmachung, die barrierefreie Bereitstellung der Vergabeunterlagen – und hier insbesondere die Leistungsbeschreibung – als auch die Angebotsabgabe. Nun kommt die elektronische Vergabe schrittweise sowohl für den Oberschwellen- als auch für den Unterschwellenbereich. Was bedeutet dies für Auftraggeber und Auftragnehmer?

Für die verbindliche und vorgeschriebene Einführung der E-Vergabe gelten die folgenden Stichtage:

- Im **Oberschwellenbereich** müssen ab dem **18. Oktober 2018** alle Vergaben ausschließlich elektronisch durchgeführt werden (vgl. § 97 Abs. 5 GWB), ausgenommen sind hiervon lediglich Vergaben im Bereich Verteidigung und Sicherheit.

Lese-Tipp:

[amendos Spezial "Outsourcing – Teil 1"](#)

- Im **Unterschwellenbereich** müssen bereits jetzt die Bekanntmachungen auch elektronisch erfolgen und die Vergabeunterlagen uneingeschränkt im Internet bereitgestellt werden (vgl. § 28 und § 29 UVgO). Ab dem **1. Januar 2020** müssen dann auch Teilnahmeanträge und Angebote zwingend elektronisch eingereicht werden (ausgenommen sind geschätzte Auftragswerte unter 25.000 € oder Vergabeverfahren ohne veröffentlichte Auftragsbekanntmachung; siehe § 38 Abs. 1-4 UVgO).

Öffentliche Auftraggeber benutzen eine große Anzahl von unterschiedlichen Vergabepattformen. Dadurch sind Bieter gezwungen verschiedene Bieterclients zu installieren und zu verwenden. Im Rahmen des Projekts XVergabe, initiiert durch Bundesministerium des Innern (BMI) und das Beschaffungsamt des

BMI, wird eine Schnittstelle zwischen Bieter-Software und unterschiedlichen Vergabeplattformen geschaffen, sodass nur ein Bieterclient notwendig ist.

Ohne XVergabe

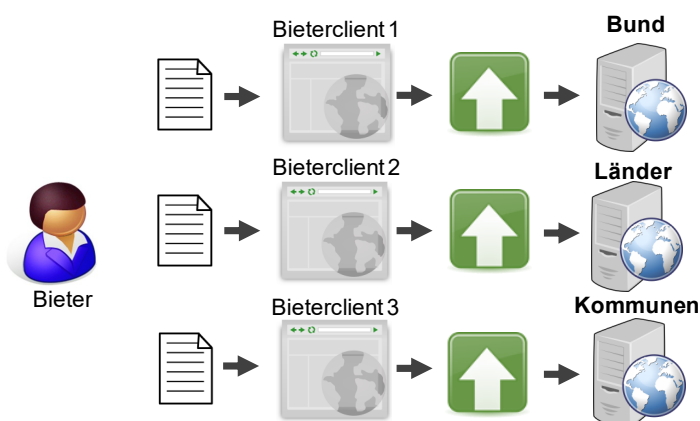
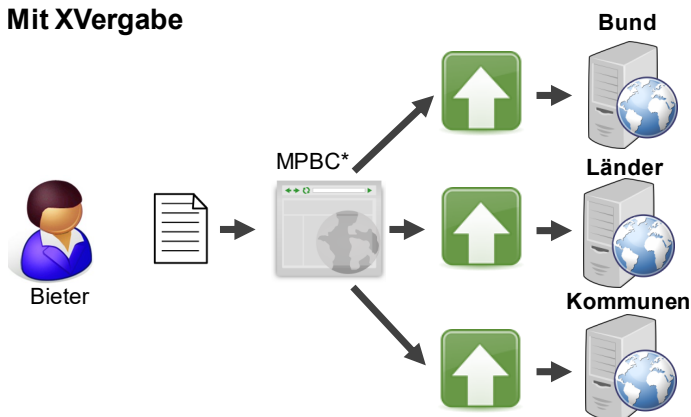


Abbildung 1: Ein Bieter, viele proprietäre Bieterclients

Bisher hat nur die E-Vergabe Plattform des Bundes ([e-Vergabe](#)) die XVergabe-Schnittstelle umgesetzt. Sie ist jetzt mit der Bieter-Software von drei verschiedenen Anbietern kompatibel – AI – Angebotsassistent, bi – Bieterclient, subreport CAMPUS – die allerdings allesamt kostenpflichtig sind.

Mit XVergabe



Quelle: XVergabe.org

*MPBC: Multi-Plattform-Bieter-Client

Abbildung 2: Ein Bieterclient, viele Vergabeplattformen

Wann weitere Anbieter folgen und weitere öffentliche Vergabeplattformen die XVergabe implementieren, bleibt abzuwarten. Bis dahin ist es durchaus sinnvoll, den e-Vergabe-eigenen webbasierten Angebots-Assistenten ([AnA](#)) AnA-Web zu nutzen.

Unabhängig von der gewählten Bieter-Software und der Vergabeplattform sollten Auftraggeber und Auftragnehmer gleichermaßen sicherstellen, dass alle eingesetzten Systeme vorweg ausgiebig getestet wurden, um später unangenehme Überraschungen zu vermeiden. Dies bezieht sich vor allen Dingen auf zu spät „eingegangene“ Angebote und die dar-

Seminare 2018

PM	IT-Projekte erfolgreich aus der Krise führen Hamburg, 27.09.-28.09.2018
	Project Management Offices im IT-Umfeld Hamburg, 04.06.-05.06.2018
	Kommunikationskompetenz in Projektkrisen Hamburg, 04.06.-05.06.2018
	Soft Skills für Projektleiter/innen Hamburg, 06.06.-07.06.2018
ITSM	Einführung in die Prozessoptimierung Hamburg, 16.04.-17.04.2018
	Prozessdokumentation gestalten Hamburg, 18.04.2018
	IT Service Management und Agilität Hamburg, 18.06.2018
	Erstellung von IT-Servicekatalogen Hamburg, 19.06.2018
Outsourcing	Grundlagen IT-Providermanagement Hamburg, 07.06.-08.06.2018
	IT-Providerwechsel Hamburg, 19.09.2018
	IT-Providermanagement – live im Betrieb Hamburg, 20.09.-21.09.2018
	Öffentliche IT-Ausschreibungen Hamburg, 19.04.-20.04.2018
	IT-Outsourcing Hamburg, 23.04.-24.04.2018

www.amendos.de/seminare

aus resultierenden Haftungsfragen im Falle eines Ausschlusses.

Vor Abgabe eines elektronischen Angebotes sollte sich der potenzielle Auftragnehmer mit den Funktionen und möglichen Beschränkungen des Bieter-Tools vertraut machen. Testläufe einer Angebotsabgabe sind hierzu ein geeignetes Mittel. So lässt sich feststellen, ob es beispielsweise Beschränkungen bezüglich der zulässigen Dateigröße gibt, die nicht angegeben wurden. Andere Schwachstellen, die möglicherweise zutage treten, können veraltete Softwareversionen oder Proxy-Server sein. Ein weiterer zu berücksichtigender Aspekt im Rahmen einer Angebotsabgabe ist die Bandbreite des Internetanschlusses. Gerade Unternehmen in ländlichen Gebieten mit einer teilweise noch schlecht ausgebauten Netzinfra-

struktur sollten diesem Umstand bei der Angebotsabgabe unbedingt in Form eines großzügigen zeitlichen Puffers Rechnung tragen. Ansonsten kann die Übertragung „auf dem letzten Drücker“ schnell zum Angebotsausschluss führen. Im Sinne des fairen Wettbewerbes bleibt zu hoffen, dass die Bundesregierung den Breitbandausbau zügig vorantreibt.

Öffentliche Ausschreibung von IT-Leistungen

Themen:

- **Rechtsgrundlagen**
- **Ablauf eines IT-Vergabeverfahrens**
- **effizienten Gestaltung der Vergabe und Vermeidung von Fehlern**

Termin: 19.04.-20.04.2018 in Hamburg

Aber nicht nur der Auftragnehmer muss sicherstellen, dass seine Angebotsabgabe reibungsfrei funktioniert. Auch der Auftraggeber hat seinerseits verschiedene Anforderungen zu erfüllen. Zuallererst muss er dafür Sorge tragen, dass das Vergabeportal für die Angebotsabgabe stets zu erreichen ist, stellt dieses doch gleichsam seinen virtuellen Briefkasten dar. Weiterhin fällt in die Zuständigkeit des Auftraggebers, die generelle Funktionalität des zur Vergabepattform gehörenden Bieterclients zu gewährleisten. Ebenso sollte er sicherstellen, dass die Kompatibilität mit der Schnittstelle XVergabe zu anderen Bieterclients tatsächlich vorhanden ist. Dies lässt sich durch wechselseitige Kompatibilitätstests feststellen. Selbstverständlich ist es nicht immer möglich alle Störungen vorherzusehen und zu vermeiden. Deshalb wäre es wünschenswert, wenn die Vergabestellen für ihre jeweiligen Vergabeportale einen Support betreiben, der auch jenseits der üblichen Bürozeiten zu erreichen ist.

Um die Umstellung auf die E-Vergabe zu erleichtern hat die Bundesregierung bewusst darauf verzichtet, die Benutzung elektronischer Signaturen vorzuschreiben. Nach § 53 Abs. 1 VgV können Angebote, Interessenbekundungen, Teilnahmeanträge etc. grundsätzlich in Textform nach § 126b BGB eingereicht werden. Eine fortgeschrittene oder qualifizierte elektronische Signatur kann nur in Ausnahmefällen verlangt werden, so im Falle erhöhter

Sicherheitsanforderungen (vgl. § 53 Abs. 3 und 4 VgV). Ob und welche Signatur benötigt wird, ist in der jeweiligen Bekanntmachung ausgewiesen. Sollte der Bieter bisher noch kein Zertifikat für eine entsprechende Signatur haben, ist dies bei der Terminplanung für die Abgabe eines Angebotes zu berücksichtigen, da die Beschaffung eines solchen Zertifikates durchaus mehrere Wochen in Anspruch neh-

IT-Outsourcing – Konzeption, Angebotseinholung und Vergabe, Transition

Seminar

Themen:

- Initiierung eines Outsourcing-Projekts
- Erstellung eines Konzepts
- Vergabe- und Transitionsphase

Termin: 23.-24.04.2018 in Hamburg

men kann.

Im Umkehrschluss bedeutet der Verzicht auf eine elektronische Signatur jedoch nicht, dass ein Angebot einfach per E-Mail in Textform abgegeben werden kann. Denn um die Unversehrtheit der Angebote sicherzustellen, dem Geheimhaltungsgrundsatz zu genügen und Manipulationen auszuschließen müssen alle Bieterunterlagen verschlüsselt übermittelt, entgegengenommen und bis zur „Öffnung“ aufbewahrt werden.

Fazit:

Die komplette elektronische Durchführung von Vergabeverfahren, ober- und unterhalb des Schwellenwertes ist beschlossene Sache. Für den Oberschwellenbereich ist der 18. Oktober 2018 das verbindliche Einführungsdatum. Es ist also höchste Zeit, sowohl auf Auftraggeber- als auch auf Auftragnehmerseite einerseits die technischen, andererseits aber auch die personellen Voraussetzungen zu schaffen.

Petra Bleshey

Impressum:

amendos gmbh | Frankenstraße 3 | 20097 Hamburg | Tel (040) 248 276 00
Fax (040) 248 276 01 | www.amendos.de | info@amendos.de

Geschäftsführer: Dipl. Oec. Jörg Bujotzek

Handelsregister: AG Hamburg HRB 105648 | Umsatzsteueridentifikationsnummer: DE 814989917

Erscheinungsweise: 4 / jährlich | Bezug: kostenfrei als PDF

Copyright: amendos gmbh | Herausgeber und inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV: Dipl. Oec. Jörg Bujotzek | Nachdruck, auch auszugsweise, nur mit Genehmigung der amendos gmbh.