zvei
electrifying ideas

Leitfaden

Öffentliche Auftragsvergabe und Datenschutz

Spannungsfeld für Medizintechnikhersteller

Verband der Elektro- und Digitalindustrie

Inhalt

1 Einleitung und Problemstellung

Die im ZVEI organisierten Medizintechnikhersteller haben Schwerpunkte beispielsweise in den Bereichen der Bildgebenden Diagnostik, der Patientenüberwachung und der Elektrochirurgie. Damit stellen diese Unternehmen wichtige technische Grundlagen für eine moderne Versorgung in Arztpraxen (ambulant) und Krankenhäusern (stationär) zur Verfügung. Der Vertrieb im stationären Sektor ist dabei stark durch die Regelungen zum öffentlichen Vergabewesen geprägt.
Hersteller treten hier über Produkte und Dienstleistungen in Preis- und Qualitätswettbewerb und unterliegen dabei auch vielfältigen Anforderungen an den Datenschutz. Verlässliche Rahmenbedingungen sind in diesem komplexen Spannungsfeld eine wichtige Voraussetzung für ein faires Agieren zwischen Anbietern und Auftraggebern.
In Deutschland herrscht nicht zuletzt durch die Einführung der Europäischen Datenschutzgrundverordnung (DSGVO) ein hohes Datenschutzniveau. Dabei müssen sowohl Privatunternehmen als auch die öffentliche Hand die datenschutzrechtlichen Vorgaben einhalten. Das Datenschutzrecht ist immer dann maßgeblich, wenn personenbezogene oder personenbeziehbare Daten verarbeitet werden. Ihm kommt damit nahezu in allen Lebenslagen eine bedeutende Rolle zu, auch in Vergabeverfahren.
Bevor auf die Besonderheiten des Datenschutzes in der Auftragsvergabe eingegangen wird, sollen nachfolgend zunächst die wichtigsten datenschutzrechtlichen Grundprinzipien dargestellt werden.

2 Datenschutz im Grundsatz

2.1 Rechtsgrundlagen

Datenschutzrechtliche Vorgaben und Obliegenheiten ergeben sich nicht allein aus der DSGVO. Auch weitere Rechtsakte wie das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze, Regelungen zum kirchlichen Datenschutz und eine Vielzahl an bereichspezifischen Gesetzen beinhalten Regelungen zu diesem Rechtsgebiet.
Der Datenschutz besitzt auf nationaler wie europäischer Ebene Verfassungsrang und schützt das Recht des Einzelnen auf informationelle Selbstbestimmung.

2.2 Systematik

Nach der DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, außer sie wird durch einen Erlaubnistatbestand einer Rechtsvorschrift ausdrücklich erlaubt. Ein solcher Erlaubnistatbestand ist beispielsweise die Einwilligung der betroffenen Person in die Datenverarbeitung oder das berechtigte Interesse des Verantwortlichen. Bei letzterem muss im Einzelfall eine Abwägung erfolgen und die Verarbeitung ist dann zulässig, wenn die Interessen des Verarbeiters diejenigen der betroffenen Person überwiegen.
An bestimmte („besondere“) Kategorien personenbezogener Daten stellt die DSGVO noch einmal höhere Anforderungen für eine Verarbeitung. Hierzu zählen auch Gesundheitsdaten, wie sie beispielsweise bei Anwendungen von Medizintechnik entstehen. Eine Verarbeitung ist hier nur unter strengen Voraussetzungen möglich.
Daten können auch im Auftrag eines Verantwortlichen durch einen Auftragsverarbeiter verarbeitet werden. Dabei handelt der Auftragsverarbeiter auf Weisung des Verantwortlichen. Beispiele für Auftragsverarbeiter sind im Bereich der Medizintechnik externe Wartungsdienstleister, E-Mail-Provider, Cloud-Anbieter oder Callcenter zur Kundenbetreuung. Um die datenschutzrechtlichen Regelungen in solchen Konstellationen einzuhalten, wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein Auftragsverarbeitungsvertrag (AVV) geschlossen.
Neben der Auftragsverarbeitung kennt die DSGVO auch die sogenannte gemeinsame Verantwortlichkeit. Im Unterschied zur Auftragsverarbeitung handelt ein gemeinsamer Verantwortlicher nicht (ausschließlich) auf Weisung des anderen Verantwortlichen. Vielmehr legen sie gemeinsam die Zwecke und die Mittel zur Verarbeitung fest.

2.3 Datensicherheitsaspekte

Eine weitere wichtige Obliegenheit nach der DSGVO ist die Gewährleistung von Datensicherheit. So ist der Verantwortliche wie auch der Auftragsverarbeiter angehalten, unter Berücksichtigung des Stands der Technik und je nach Schwere des zu erwartenden Risikos geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Hierzu zählen die Verschlüsselung und Pseudonymisierung von Daten, aber z. B. auch die datenschutzrechtliche Schulung von Mitarbeitern.
In diesem Zusammenhang obliegt dem Verantwortlichen bzw. Hersteller auch die Einhaltung der zwei Grundsätze

„Privacy by Design“ (Datenschutz durch Technikgestaltung), also das frühzeitige Ergreifen von TOMs im Entwicklungsstadium

sowie

„Privacy by Default“ (Datenschutz durch datenschutzfreundliche Voreinstellungen), also die datenschutzfreundliche Ausgestaltung der Werkseinstellungen.

Aus Herstellersicht sind dies zentrale datenschutzrechtliche Anforderungen, die bereits bei der Entwicklung jeglicher Produkte angemessen berücksichtigt werden müssen.

3 Öffentliche Auftragsvergabe

Das Vergaberecht hat zum Ziel, Beschaffungen der öffentlichen Hand nach wirtschaftlichen Gesichtspunkten im Rahmen des geltenden Rechts zu gewährleisten. Die öffentliche Hand zahlt mit dem Geld des Bürgers. Ein besonderes Vergabeverfahrensrecht soll einen ordnungsgemäßen Ablauf der Beschaffungen gewährleisten.

3.1 Wirksamkeit

Ein öffentlicher Auftrag ist von Beginn an unwirksam, wenn der öffentliche Auftraggeber generell gegen ein Gesetz verstoßen hat[1]. Das trifft allerdings nur zu, wenn dieser Verstoß in einem Nachprüfungsverfahren nach dem Gesetz gegen Wettbewerbsbeschränkungen (**GWB**) ab den EU-Schwellenwerten festgestellt worden ist. Insoweit wird die Wirkung von § 134 BGB im Vergaberecht eingeschränkt. Verstreichen die einschlägigen Fristen, ohne dass ein Verstoß vor der zuständigen Vergabekammer geltend gemacht wurde, oder folgt die Vergabekammer oder das Beschwerdegericht einem rechtzeitig gestellten Feststellungsantrag nicht, ist der Vertrag[2] von Anfang an wirksam. Unterhalb der erwähnten Schwellenwerte bleibt in der Regel nur der Sekundärrechtsschutz, gerichtet auf Schadensersatz (s. u. „Rechtsschutz“).

3.2 Datenschutz in Vergabeverfahren

Zum zu beachtenden Rechtsrahmen gehört auch die DSGVO. Sowohl der Auftraggeber, aber auch der Auftragnehmer bzw. Bieter sind hier in der Pflicht. Dass Gesetze einzuhalten sind, ist in einem Rechtsstaat selbstverständlich, sodass neben den Postulaten aus dem Gesetz selbst keine zusätzlichen Datenschutzforderungen aufgestellt werden sollten. Sie verkomplizieren und überfrachten lediglich das Rechtsleben.
Wie erwähnt, können Verstöße gegen Vorschriften der DSGVO das Ende eines Vergabeverfahrens bedeuten. Die Einhaltung datenschutzrechtlicher Regeln hat also für die erfolgreiche Durchführung einer Vergabe erhebliche Bedeutung.
Datenschutzrechtliche Regelungen und sich daraus ergebende Folgerungen können Konsequenzen für das gesamte Vergabeverfahren sowohl auf Auftraggeber- als auch auf Auftragnehmerseite haben.
Der im Vergabeverfahren dafür relevante Teil ist zunächst die Eignungsprüfung. Der Auftraggeber erstellt dazu ein Anforderungsprofil, für dessen Einhaltung der Bieter Nachweise, Zeugnisse und Referenzen übermitteln muss, die i. d. R. eine Vielzahl an personenbezogenen Daten der beim Bieter Beschäftigten enthalten. Dazu gehören Namen, geschäftliche Kontaktdaten, häufig zudem

[1] Vgl. § 134 Bürgerliches Gesetzbuch (BGB)
[2] Vgl. Formulierung des § 135 GWB

berufliche Qualifikationen. Daneben können auch Daten und Informationen zur Gesundheit oder strafrechtliche Verurteilungen erforderlich sein. Es stellt sich für beide Seiten die Frage, ob und auf welcher Rechtsgrundlage die Verarbeitung solcher Daten zulässig ist.
Von der Eignungsprüfung abgesehen, ist das Datenschutzrecht von besonderer Relevanz, wenn der Auftragsgegenstand eine Auftragsverarbeitung beinhaltet, also der Bieter personenbezogenen Daten im Auftrag und nach Weisung des Auftraggebers verarbeiten soll. Dafür stellt die DSGVO Anforderungen. Bereits bei der Gestaltung des Anforderungsprofils sollte beachtet werden, wie diese Voraussetzungen dem Recht entsprechend eingebunden werden können. Insbesondere ist (vom Auftraggeber) abzuwägen, ob die gesamte datenschutzrechtliche Beurteilung des Auftragnehmers bereits im Rahmen der Eignungsprüfung erfolgen sollte oder ob eine Aufgliederung der Bewertung sinnvoll ist.
Eindeutige Vorgaben für eine datenschutzkonforme Durchführung von Vergabeverfahren existieren nicht. Verallgemeinerungen sind kaum möglich. In der Regel ist die Prüfung im Einzelfall erforderlich. Daher besteht große Unsicherheit, wie die zum Teil umfangreichen datenschutzrechtlichen Vorgaben umgesetzt werden sollen. Insgesamt sollte darauf geachtet werden, die geforderten Daten mit Personenbezug auf das – bei vernünftiger Würdigung – erforderliche Maß zu beschränken.

3.3 Datenschutz und Eignungsprüfung

Ein relevanter Anwendungsbereich der Datenverarbeitung und damit des Datenschutzes ist die Eignungsprüfung. Der Auftragnehmer übermittelt entsprechend dem Anforderungsprofil personenbezogene Daten seiner Mitarbeiter an den Auftraggeber. Für die damit einhergehende Verarbeitung der Daten müssen Auftraggeber wie Auftragnehmer neben der Bestimmung einer Rechtsgrundlage die allgemeinen datenschutzrechtlichen Bestimmungen einhalten.
Die Verarbeitung einschließlich der Übermittlung personenbezogener Daten ist nur zulässig, wenn eine entsprechende Rechtsgrundlage dies ausdrücklich erlaubt. Die Rechtfertigung richtet sich nach Art. 6 DSGVO[3].
Hilfsweise kann die Interessensabwägung[4] einschlägig sein. Lediglich in besonderen Ausnahmefällen kann die Datenverarbeitung auf eine Einwilligung[5] gestützt werden. Primärer Anknüpfungspunkt bei der Bestimmung der Rechtsgrundlage[6] ist der Zweck der Datenverarbeitung. Zu beachten ist, dass sich für die unterschiedlichen Datenkategorien auch verschiedene Zwecke und daher auch unterschiedliche Rechtsgrundlagen ergeben können. Bei Gesundheitsdaten ist kumulativ das Eingreifen einer weitergehenden Rechtsgrundlage erforderlich.
Die Verpflichtungen in diesem Bereich treffen aber nicht nur den Auftraggeber. Auch der Bieter muss vor der Übermittlung von personenbezogenen Daten an den Auftraggeber prüfen, ob eine einschlägige Rechtsgrundlage gegeben ist. Dass die gewünschten Daten im Anforderungsprofil aufgeführt sind, reicht allein nicht aus. Außer den für den Auftraggeber beschriebenen Rechtsgrundlagen ergibt sich eine Rechtfertigung für den Auftragnehmer bzw. Bieter u. U. aus dem Beschäftigungsverhältnis mit dem Mitarbeiter. Für welche Daten diese Rechtsgrundlage zutreffen könnte, ist im Einzelfall zu prüfen.
Ein besonderes Problem stellen in diesem Zusammenhang Führungszeugnisse dar. Zwingende Gründe für den Ausschluss eines Bieters vom Vergabeverfahren definiert § 123 I GWB. Dabei handelt es sich um bestimmte strafrechtliche Verurteilungen von leitenden Angestellten. In der Praxis wird teilweise für den Nachweis, dass entsprechende Ausschlussgründe nicht vorliegen, die Vorlage von Führungszeugnissen verlangt. Die Zulässigkeit dessen ist datenschutzrechtlich zweifelhaft. Zwar könnte die Verarbeitung von Daten über Verurteilungen[7] zulässig sein. Aufgrund der hohen Sensibilität entsprechender Straftaten[8] gelten aber besondere Anforderungen für deren Verarbeitung.
Das kann dazu führen, dass Führungszeugnisse in Vergabeunterlagen nicht enthalten sein dürfen, sondern ein anderes Procedere genutzt werden könnte, etwa Eigenerklärungen des Bieters oder Einsichtnahmen in das Wettbewerbsregister.
Von den erwähnten Punkten abgesehen, gelten im Vergabeverfahren die allgemeinen datenschutzrechtlichen Pflichten für die Datenverarbeitung, vor allem der Grundsatz der Datensparsamkeit und Informationspflichten. Nach dem Grundsatz der Datensparsamkeit dürfen

[3] Für den Auftraggeber ist eine Rechtfertigung primär in Art. 6 l S. 1 lit. C DSGVO (Erfüllung einer rechtlichen Verpflichtung) oder Art. 6 l 1 lit. e DSGVO (Erfüllung einer Aufgabe im öffentlichen Interesse) zu suchen.
[44] Vgl. Art. 6 l 1 lit. f DSGVO.
[5] Vgl. Ar. 6 l 1 lit. a DSGVO.
[6] Vgl. Art. 9 II DSGVO.
[7] Vgl. Art. 6 l 1 lit c. DSGVO i. V. m. § 123 I, III GWB.
[8] Vgl. Art. 10 S. 1 DSGVO

nur solche Daten verarbeitet werden, die für die Erfüllung des jeweiligen Zwecks erforderlich sind. Dabei sind der Umfang der Datenerhebung zu prüfen sowie, ob nicht pseudonymisierte oder gar anonymisierte Daten ausreichen[9]. Zudem müssen die Parteien die betroffenen Personen vorher über die jeweilige Datenverarbeitung zum Zwecke des Vergabeverfahrens und über die Rechte der Betroffenen informieren. Dies ist bereits vor Durchführung des Vergabeverfahrens zu beachten, um eine rechtzeitige Information zu gewährleisten.
Um die Eignungsprüfung nicht mit zusätzlichen Bewertungen der Kriterien der Auftragsverarbeitung zu überfrachten, empfiehlt es sich, die konkrete Beurteilung der datenschutzrechtlichen Kriterien aufzuteilen und z. B. ein umfassendes Datenschutzkonzept erst von den im Teilnahmewettbewerb qualifizierten Bietern anzufordern.

3.4 Datenschutz und Leistungserbringung bzw. Auftragsinhalt

Neben der Eignungsprüfung sind Fragen des Datenschutzes im Bereich der Auftragsverarbeitung zu beachten. Nutzt die verantwortliche Stelle für die Verarbeitung personenbezogener Daten einen Auftragnehmer, ist eine Auftragsverarbeitung gegeben, wenn der Auftragnehmer ausschließlich auf Weisung des Auftraggebers handelt[10]. Im Gegensatz zu anderen Fällen der Datenübermittlung an Dritte erfordert die Zugänglichmachung personenbezogener Daten an einen Auftragsverarbeiter keine gesonderte Rechtsgrundlage[11]. Sie ist privilegiert unter der Voraussetzung, dass die Parteien einen AVV[12] schließen.

Für Vergabeverfahren spielt Auftragsverarbeitung eine Rolle, wenn der zu vergebende Auftrag eine Datenverarbeitung durch den Auftragnehmer beinhaltet. Die Einhaltung der entsprechenden Vorgaben, insbesondere nach Art. 28 DSGVO, muss entsprechend bereits als Bedingung in den Vergabeunterlagen enthalten sein. Dies ist bei klinisch relevanten Aufträgen häufig zu bejahen, da etwa bei Wartung und Support für Medizinprodukte eine Zugriffsmöglichkeit – diese ist insoweit datenschutzrechtlich hinreichend – des Auftragnehmers auf Vitaldaten, Messergebnisse u. ä. im Regelfall nicht auszuschließen ist. Zumindest aus Sicht des Auftraggebers werden sich diese Daten regelmäßig durchaus einer spezifischen natürlichen Person zuordnen lassen. Der Abschluss eines AVV[13] ist insoweit daher unerlässlich.
Für den Abschluss des AVV sind die formellen Voraussetzungen[14] zu beachten, insbesondere wenn die Vereinbarung durch Zuschlag geschlossen werden soll.
Eine Unterbeauftragung durch den Auftragnehmer ist vergaberechtlich regelmäßig zulässig und kann folglich vom Auftraggeber nicht untersagt werden. Allerdings sieht die DSGVO vor, dass der Auftraggeber dem Einsatz von Sub-Auftragsverarbeitern zustimmen muss. Die Zustimmung kann zwar auch generell erteilt werden, dann muss der Auftragnehmer den Auftraggeber jedoch über eine etwaige Änderung der unterbeauftragten Sub-Auftragsverarbeiter in Kenntnis setzen und dem Auftraggeber ein Einspruchsrecht einräumen[15].

3.5 Folgen eines Rechtsverstoßes gegen die DSGVO

Ein Verstoß gegen die Regeln der DSGVO kann mit einem Bußgeld von bis zu 20 Mio. Euro bzw. 4 Prozent des weltweiten Umsatzes der jeweiligen Verantwortlichen geahndet werden. Behörden und öffentliche Stellen sind von Bußgeldern zwar (weitgehend) ausgenommen, doch drohen sowohl dem Auftraggeber wie dem Auftragnehmer Untersagungsverfügungen der Aufsichtsbehörden, was zum Abbruch des Vergabeverfahrens führen kann. Zudem können die betroffenen Personen bei Verstößen gegen die DSGVO Schadensersatz verlangen. Für den Bieter kann die Missachtung datenschutzrechtlicher Vorgaben ferner als „schwere Verfehlung“[16] gewertet werden, die einen fakultativen Ausschlussgrund begründet.

---

[9] Dies sind wichtige Mechanismen, um das Datenschutzniveau zu verbessern bzw. rechtliche Restriktionen ganz zu suspendieren, welche sowohl auf die Produktentwicklung als auch etwa nachgelagerte Serviceaktivitäten durchschlagen.
[10] Eigenständiges Handeln wird sich hier indes nie ganz vermeiden lassen; vgl. etwa die Erfüllung zwingender gesetzlicher Vigilanz-Verpflichtungen aus Art. 83 Abs. 3 lit. e, f MDR.
[11] Vgl. Art. 6 DSGVO.
[12] Vgl. Art. 28 III DSGVO.
[13] Vgl. Art. 28 III DSGVO.
[14] Vgl. Art. 28 IX DSGVO.
[15] Vgl. Wortlaut Art. 28 Abs. 2 S. 2 DSGVO.
[16] Vgl. § 124 I Nr. 3 GWB

3.6 Rechtsschutz

Sollte sich in einem Vergabeverfahren der öffentlichen Hand ein Bieter benachteiligt fühlen, stellt sich die Frage der Rechtsschutzmöglichkeiten. Man spricht in diesem Zusammenhang von Nachprüfungsverfahren, sich im Einzelfall an eine dritte, vom öffentlichen Auftraggeber unabhängige staatliche Institution wenden zu können, falls der Auftraggeber sich bei seinem Einkaufsverhalten nicht rechtmäßig verhalten hat. Von Relevanz ist dabei der geschätzte Auftragswert, wenn er die von der EU gesetzten Schwellenwerte erreicht oder überschreitet. Erreicht oder überschreitet er diese, stehen die EU-rechtlichen Überprüfungsverfahren vor den Vergabekammern und in zweiter Instanz vor den Oberlandesgerichten in Deutschland zur Verfügung. Ab den Schwellenwerten[17] haben die Bieter Anspruch darauf, dass der Auftraggeber bzw. die Vergabestelle die Bestimmungen über das Vergabeverfahren einhält. Der Anspruch erfasst alle Vergabebestimmungen. Nur dann, wenn eine Regel verletzt wird, die zumindest auch den Schutz des Antragstellers beinhaltet, besteht ein Rechtsschutzinteresse.
Unterhalb der Schwellenwerte existiert in Deutschland kein einklagbarer Anspruch auf Einhaltung des Vergaberechts. Einige Bundesländer haben es unternommen, dies zu ändern, mit unterschiedlichen Möglichkeiten. Ist mangels eigenen Rechts auf Vornahme oder Unterlassung einer bestimmten Handlung des Auftragsgebers im Vergabeverfahren oder nach Abschluss des Vergabeverfahrens primärer Rechtsschutz nicht möglich, sind die Bieter auf Sicherung oder Durchsetzung von zivil-rechtlichen Ansprüchen reduziert. Es gelten dann die zivilrechtlichen und zivilprozessualen Regeln.
Eröffnet ist dann der Weg zu den Zivilgerichten einschließlich für einen vorläufigen Rechtsschutz auf Schadensersatz (sekundärrechtlicher Anspruch) aus Vertrag oder vorvertraglicher Obliegenheiten und deren Verletzung sowie Schadensersatzansprüche aus deliktischem Verhalten, wobei die Einhaltung der Vergaberegeln als Obliegenheit der öffentlichen Auftraggeber bei Vertragsschluss angesehen wird.

4 Anforderungen an Medizintechnikhersteller

4.1 Relevanter Normenkatalog

Die Anforderungen bzw. Standards sind vielschichtig (vgl. etwa NIST, BSI, ISO) und können nicht sämtlich vorgehalten werden – gerade die ISO 27001 ist für Unternehmen, die nicht primär als IT-Service-Provider agieren, äußerst aufwändig und zunächst fachfremd. Hier sollte berücksichtigt werden, dass auch hieran angelehnte, angemessene IT-Sicherheitsvorkehrungen, Prozesse etc. den datenschutzrechtlichen Anforderungen grundsätzlich genügen.

4.2 Internationaler Datentransfer

Der Transfer von Daten in Drittstaaten gestaltet sich spätestens seit der Schrems II-Rechtsprechung des EuGH als äußerst problematisch. Dies gilt auch, wenn etwa die Muttergesellschaft eines Herstellers in einem Drittstaat sitzt. Auch für den Einsatz von Dienstleistern ist dies von großer Bedeutung. Insbesondere der Serverstandort sollte sich stets innerhalb der EU bzw. des Europäischen Wirtschaftsraums befinden, um der etwas nebulösen Interessenabwägung in einem äußerst sensiblen Umfeld zu entgehen. Es gibt allerdings Drittstaaten (z. B. Japan), für welche die EU einen gleichwertigen Datenschutzlevel grundsätzlich anerkennt. Beim Datenaustausch mit diesen „sicheren“ Drittstaaten erhöht sich bei geeignet formulierten AVVs die Chance, dass die Sorgfaltspflichten erfüllt werden.

4.3 Technologische Innovation

Der Einsatz neuartiger Technologien wie Cloud-Lösungen, Künstliche Intelligenz (KI) etc. birgt zahlreiche technische Herausforderungen und rechtliche Unsicherheiten (siehe Data Act oder KI-Verordnung). Hier sollten idealerweise klare, realistische und interessengerechte Regelungen erlassen werden.

[17] Vgl. § 97 VI GWB

4.4 Vernetzung und Standards

Grundlage hierfür ist die voranschreitende Vernetzung im Klinikumfeld, welche nur bei Anwendung einheitlicher Übertragungsstandards gelingen kann. Auch hier wäre daher ein harmonisierender Eingriff durch den Gesetzgeber grundsätzlich wünschenswert.

5 Abkürzungen und Glossar

Art.	Artikel (eines Paragrafen)
AVV	Auftragsverarbeitungsvertrag
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSGVO	Datenschutz-Grundverordnung
GWB	Gesetz gegen Wettbewerbsbeschränkungen
ISO 27001	Diese Norm der Internationalen Organisation für Standardisierung gilt als internationaler Benchmark, um den Sicherheitsstand in einem Unternehmen zu bewerten. Ein entsprechendes Zertifikat bestätigt IT-Compliance gegenüber Kunden und Partnern.
TOM	Technische und organisatorische Maßnahmen

Anonymisierung

Umkehrbare Techniken sind Formen des Pseudonymisierens (s. u.) und unumkehrbare Techniken sind Formen des Anonymisierens. Letzteres ist erreicht, wenn Daten so verändert werden, dass sie keine personenbezogenen oder personenbeziehbaren Informationen mehr enthalten.

Eignungsprüfung

Im April 2016 ist das Gesetz zur Modernisierung des Vergaberechts (VergRModG) in Kraft getreten. Die Reform dient der Umsetzung dreier EU-Vergaberichtlinien von 2014. Ein Ziel dieser Richtlinien und damit auch der Vergaberechtsreform in Deutschland war die Vereinfachung der Prüfung, ob ein Unternehmen grundsätzlich geeignet ist, einen öffentlichen Auftrag auszuführen. Dazu hat der europäische Gesetzgeber in Artikel 59 der Richtlinie 2014/24/EU die sog. Einheitliche Europäische Eigenerklärung (EEE) eingeführt, die die Eignungsprüfung durch eine in allen EU-Mitgliedstaaten einheitliche Form der Eigenerklärung vorstrukturieren und erleichtern soll. Die EEE stellt einen vor-läufigen Beleg der Eignung eines Unternehmens und des Nichtvorliegens von Ausschlussgründen dar. Die EEE enthält eine Eigenerklärung mit Versicherung des Unternehmens (z. B. zu den Aspekten „Ausschlussgründe“ und „Vorgaben des öffentlichen Auftraggebers“). Hinzu kommen Pflichten des Bieters zur Übermittlung von Nachweisen.

EU-Schwellenwert

Das Vergaberecht umfasst alle Regeln und Vorschriften, die die öffentliche Hand beim Einkauf von Gütern und Leistungen und bei der Vergabe von Konzessionen befolgen muss. Immer dann, wenn beispielsweise eine Bundes- oder Landesbehörde Papier oder Büromöbel beschaffen oder ein neues Bürogebäude errichten lassen will, muss es diese Regeln beachten. Dabei ist zu unterscheiden, ob die Vergabe ober- oder unterhalb der EU-Schwellenwerte erfolgen soll. Nur im so genannten Oberschwellenbereich kann ein unterlegener Bieter oder Bewerber die Verletzung von Verfahrensvorschriften im Rahmen eines Nachprüfungsverfahrens vor den Vergabekammern und gegebenenfalls vor den Oberlandesgerichten geltend machen. Aufträge im Oberschwellenbereich müssen standardisiert und europaweit bekannt gemacht werden.

Pseudonymisierung

DSGVO Art. 4 (5): „Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.”

Kontakt
Andreas Bätzel • Referent Innovation Medizintechnik und Gesundheitsmarkt • Fachverband Elektromedizinische Technik • Tel.: +49 69 6302 388 • Mobil: +49 162 2664 929 • E-Mail: andreas.baetzel@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Lyoner Straße 9 • 60528 Frankfurt am Main
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 27.07.2022