Hinweise zur Nutzung von E-Mail-Kommunikation im Vergabeverfahren

1. Anwendungsbereich

Nach § 8 Abs. 2 S. 2 Thüringer Vergabegesetz (ThürVgG) kann unterhalb der Schwellenwerte nach § 106 Gesetz gegen Wettbewerbsbeschränkungen bei der Durchführung einer Verhandlungsvergabe bei der Vergabe von Liefer- und Dienstleistungsaufträgen beziehungsweise einer Freihändigen Vergabe bei der Vergabe von Bauleistungen die Kommunikation einschließlich der Angebotsabgabe per E-Mail erfolgen. Dabei sind jedoch zwingend die Voraussetzungen der §§ 10 und 11 Vergabeverordnung (VgV) einzuhalten.

Achtung: Eine einfache, unverschlüsselte E-Mail erfüllt diese Voraussetzungen nicht!

Die Einhaltung der Vorgaben des § 8 Abs. 2 S. 2-4 ThürVgG kann auf verschiedenen Wegen sichergestellt werden. Die nachfolgenden Ausführungen sollen hierbei als Orientierung dienen.

2. Rechtsgrundlagen

§§ 10 und 11 VgV regeln detailliert die Anforderungen an die verwendeten elektronischen Mittel. Die Vertraulichkeit der übermittelten Daten und die Integrität der Angebote müssen jederzeit gewahrt werden. Nur die Berechtigten dürfen Zugriff auf die übermittelten Daten haben. Die Daten müssen durch eine sichere SSL-Verschlüsselung während der Übertragung geschützt werden, sodass Dritte keinen Zugriff auf die Informationen erlangen können.

Insbesondere muss nach § 10 VgV die genaue Bestimmung von Tag und Uhrzeit des Datenempfangs erfasst werden (§ 10 Abs. 1 Nr. 1 VgV), es darf kein vorfristiger Zugriff auf die empfangenen Daten erfolgen (§ 10 Abs. 1 Nr. 2 VgV), die Festlegung und Änderung des Termins für den erstmaligen Zugriff sowie der Zugriff auf die empfangenen Daten darf nur durch die Berechtigten möglich sein (§ 10 Abs. 1 Nr. 3 und 4 VgV) und es dürfen keine empfangenen Daten an Unberechtigte übermittelt werden (§ 10 Abs. 1 Nr. 5 VgV).

§ 11 Abs. 1 VgV sieht vor, dass die elektronischen Mittel allgemein verfügbar, diskriminierungsfrei sowie kompatibel mit allgemein verbreiteten Geräten und Programmen sein müssen und den Zugang von Unternehmen zum Vergabeverfahren nicht einschränken dürfen. Technische und organisatorische Maßnahmen müssen gewährleisten, dass Vergabeverfahren jederzeit durchgeführt werden können. Allen Interessenten müssen die gleichen Informationen zur Verfügung gestellt werden. Es dürfen nur gängige, weit verbreitete und normierte Datenformate (z.B. PDF, XML, ZIP) genutzt werden, spezielle Softwareanforderungen oder zusätzliche Tools dürfen nicht erforderlich sein, um die Inhalte zu öffnen oder zu bearbeiten.

Darüber hinaus muss der öffentliche Auftraggeber nach § 11 Abs. 2 VgV für die gesamte elektronische Kommunikation, wie das Senden, Empfangen oder Weiterleiten von Daten, sowie das Speichern von Daten in einem Vergabeverfahren die Unversehrtheit, die Vertraulichkeit und die Echtheit der Daten jederzeit gewährleisten. Die

Authentifizierung der Bieter muss sichergestellt sein, ebenso die Vertraulichkeit und Verschlüsselung der Angebote sowie die Integrität der übermittelten Angebote.

Diese Anforderungen gelten als erfüllt, wenn die unter Buchstabe a) oder b) dargestellten Verfahrensweisen eingehalten werden. Weicht die Vergabestelle von diesen Verfahrensweisen ab, ist die Einhaltung der §§ 10 und 11 VgV auf andere geeignete Art und Weise durch die Vergabestelle mittels entsprechender und zu dokumentierender technischer und organisatorischer Vorkehrungen sicherzustellen.

a) Nutzung einer Online-Vergabeplattform mit einer Angebotsmöglichkeit per E-Mail

Auf dem Markt erhältliche Online-Vergabeplattformen, welche die Durchführung von Vergabeverfahren per E-Mail ermöglichen, können eingesetzt werden, sofern sie die Voraussetzungen nach §§ 10 und 11 VgV erfüllen. Dies ist vom jeweiligen Anbieter nachzuweisen.

b) Voraussetzungen und Verfahrensschritte im Falle der E-Mail-Kommunikation bzw. Angebotsabgabe per E-Mail

Angebote und Teilnahmeanträge müssen nach § 10 Abs. 1 VgV verschlüsselt übermittelt, entgegengenommen und aufbewahrt werden. Die Angebote dürfen zudem erst zum Öffnungstermin zugänglich sein. Diese Anforderungen können z. B. wie folgt sichergestellt werden: Das Angebot wird in eine passwortgeschützte „zip-Datei“[1] umgewandelt bzw., falls das Angebot aus mehreren Dokumenten besteht, werden diese in einem Ordner zusammengetragen und dieser Ordner in einen passwortgeschützten „zip-Ordner“ umgewandelt. Den so erzeugten passwortgeschützten und verschlüsselten Ordner kann der Bieter als Anlage per E-Mail an die von der Vergabestelle benannte E-Mailadresse versenden.

Um sicherzustellen, dass das Angebot nicht vor dem Submissionstermin geöffnet werden kann, teilt der Bieter der Vergabestelle das Passwort zum Öffnen der „zip-Datei“ bzw. des „zip-Ordners“ zeitnah nach dem geplanten Submissionstermin mit. Hierfür stellt die Vergabestelle einen anderen, gesonderten Kommunikationskanal zur Verfügung, über den nur das Passwort gesendet wird. Als Kommunikationskanal kommt dabei z. B. in Frage: eine gesonderte, d. h. von der E-Mail-Adresse, an die das Angebot übermittelt wurde, abweichende E-Mailadresse, eine Telefonnummer zur Übermittlung einer SMS oder eine Fax-Nummer zur Übermittlung eines Telefaxes.

Darüber hinaus enthält § 10 Abs. 2 VgV Vorgaben zu Datenaustauschschnittstellen und Interoperabilität von Programmen bzw. Dateien. Im Falle einer Übermittlung per

[1] Sog. „zip-Dateien bzw. -Ordner“ sind an der Dateiendung „.zip“ erkennbar. Es handelt sich dabei um ein Dateiformat, das zu einer Komprimierung und in Kombination mit einem Passwort zur Verschlüsselung der enthaltenen Dateien genutzt werden kann.
Ein Programm für die Umwandlung von Dateien oder Ordnern in „zip-Dateien“ oder „zip-Ordner“ (z. B. die Programme „7-Zip“, „PeaZip“ oder „WinRAR“) sowie entsprechende Anleitungen zur Verschlüsselung und Passwortsicherung sind kostenfrei im Internet verfügbar.

E-Mail ist seitens der Vergabestelle sicherzustellen, dass sie allgemein verfügbare Datei- und E-Mail-Formate öffnen und einsehen kann.

§ 11 VgV stellt weitere inhaltliche Anforderungen an die vom Auftraggeber verwendete Kommunikationsform auf elektronischem Weg. Jeder Bieter muss grundsätzlich mittels eines gewöhnlichen PCs mit Internetzugang sowie gewöhnlicher (branchen-)üblicher Softwareausstattung am Vergabeverfahren teilnehmen können.

Während des gesamten Vergabeverfahrens muss der Auftraggeber nach § 11 VgV die Unversehrtheit, die Vertraulichkeit und die Echtheit aller verfahrensbezogenen Daten sicherstellen. Die Echtheit der Daten ist gewährleistet, wenn die Quelle der Daten bzw. der Sender zweifelsfrei nachweisbar und damit die Authentizität und die Unversehrtheit (Veränderungsschutz bzw. Integrität) der Daten gegeben ist. Da E-Mail-Adressen frei verfügbar sind und insbesondere bestimmte Bezeichnungen, wie z. B. Unternehmensnamen ohne große Hindernisse auch von „externen“ und „unberechtigten“ Personen für E-Mail-Adressen genutzt werden könnten oder aber abgesendete E-Mails virtuell „abgefangen“ und verändert werden könnten, sind spezielle zusätzliche Anforderungen an die Echtheit der Daten zu stellen, um den Vorgaben des § 11 Abs. 2 VgV Genüge zu tun.

Den Anforderungen an die Echtheit der Daten kann einerseits dadurch entsprochen werden, dass auf - kostenpflichtige - Anbieter zurückgegriffen wird, die eine Signatur einer E-Mail-Adresse nach dem sog. S/MIME- oder PGP-Standard herstellen. Die in der Regel kostenpflichtigen Angebote ermöglichen es, auch E-Mails von online-E-Mail-Anbietern (z. B. gmx.de, web.de, gmail.com) direkt signieren zu können, ohne dass ein E-Mail-Programm (z. B. Outlook, Thunderbird) auf dem PC installiert sein muss. Für S/MIME (Secure/Multipurpose Internet Mail Extensions) ist in der Regel die Verwendung eines E-Mail-Clients wie Microsoft Outlook, Mozilla Thunderbird oder Apple Mail erforderlich, um die volle Funktionalität der Verschlüsselung und digitalen Signatur zu nutzen. Diese E-Mail-Programme bieten integrierte Unterstützung für S/MIME oder ermöglichen die Installation von Erweiterungen, die S/MIME-Funktionen bereitstellen. Die direkte Nutzung von S/MIME in webbasierten E-Mail-Diensten ohne zusätzliche Software ist zwar grundsätzlich möglich, jedoch kaum verbreitet und meist auf kostenpflichtige Business-Lösungen beschränkt. PGP (Pretty Good Privacy) ist ein kostenloses Verschlüsselungsverfahren, das jedoch aus Sicherheitsgründen nicht uneingeschränkt empfohlen wird. Obwohl es möglich ist, PGP ohne Kosten zu nutzen, beispielsweise durch Open-Source-Dienste[2] oder Browser-Plugins, birgt diese Vorgehensweise potenzielle Sicherheitsrisiken. Die Verwendung von Online-Tools zur Schlüsselerzeugung oder Browser-Erweiterungen kann die Integrität des Verschlüsselungsprozesses gefährden.

Ein Nachteil der kostenpflichtigen Anbieter ist, dass sowohl die Vergabestelle als auch der Bieter denselben Anbieter nutzen und damit die entsprechenden Zugänge „kaufen“ müssen, um die Verschlüsselung und die Signatur anwenden und auslesen zu können. Insofern hätte die Vergabestelle im Rahmen der Ausschreibungsunterlagen bzw. der Aufforderung zur Abgabe eines Angebotes die Pflicht, den (potentiellen) Bieter darüber zu informieren, welcher bzw. welche Anbieter für E-Mail-Signaturen von der Vergabestelle akzeptiert wird bzw. werden (d. h. welche Anbieter die

[2] Der Open-Source-Dienst https://pgpkeygen.com/ ist kostenfrei und ohne Anmeldung verfügbar.

Vergabestelle für sich selbst beschafft hat). Der Bieter wäre dann gehalten, sich bei einem der von der Vergabestelle akzeptierten Anbietern eine eigene Signatur zu beschaffen. Aus Sicht der Bieter könnte diese Lösung dazu führen, von einer Angebotsabgabe Abstand zu nehmen. Denn: möchte sich der Bieter auf mehrere Angebotsaufforderungen verschiedener Vergabestellen bewerben, müsste er sich ggf. bei mehreren verschiedenen Anbietern jeweils kostenpflichtig die jeweils akzeptierte Variante erwerben. Eine landesweit einheitliche Anbieterlösung existiert nicht und ist auch nicht geplant.

Die vorgenannten Sicherheitsanforderungen können auch mittels des kostenlosen Verschlüsselungs- und Signatur Programms „Gpg4Win“ (speziell für Windows-Betriebssysteme; im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik entwickelt) oder „GNU Privacy Guard“ (Kurz: „GnuPG“; für die Betriebssysteme Linux und Windows, für andere Betriebssysteme z. T. mit Zusatzprogrammen nutzbar) hergestellt werden. Das Programm GnuPG kann auf der Internetseite https://www.gnupg.org/download/index.html, das Programm „Gpg4Win“ https://www.gpg4win.de heruntergeladen werden.

Diese Programme erfordern es jedoch, dass ein von den Programmen unterstütztes E-Mail-Programm auf dem PC des Bieters und der Vergabestelle installiert ist. „Gpg4win“ ist für die Verwendung mit dem E-Mail-Programm Outlook konzipiert, welches jedoch von Microsoft nur im Rahmen von Softwarepaketen kostenpflichtig für Windows-Betriebssysteme erworben werden kann. Alternativ stellt „Gpg4Win“ im Downloadpaket ein eigenes E-Mail-Programm zur Verfügung, „Claws Mail“, welches im Vergleich zu Outlook jedoch weniger Bedienkomfort verspricht.

„GnuPG“ ist mit allen anderen, kostenfrei[3] oder kostenpflichtig[4] herunterladbaren, E-Mail-Programmen verwendbar, bietet jedoch - je nach E-Mail-Programm - unterschiedlich guten Bedienkomfort. Sofern ein E-Mail-Programm keinerlei „GnuPG“-Einbindung aufweist, ist eine Verschlüsselung mit Hilfe des kostenfreien Programms „Kleopatra“[5] dennoch möglich.

Weitere Informationen und insbesondere Anleitungen zu den Programmen finden sich für „GnuPG“ auf der Homepage des Entwicklers[6] und für „Gpg4Win“ auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik[7] sowie auf der Internetseite https://www.gpg4win.de/documentation-de.html.

Um den Transparenzanforderungen des § 11 Abs. 3 VgV gerecht zu werden, müssen allen interessierten Unternehmen die Spezifikationen der technischen Ausstattung und der Verschlüsselungstechnologie, die zur elektronischen Übermittlung von Angeboten und Teilnahmeanträgen notwendig ist, zugängig gemacht werden. Der Auftraggeber hat also dafür zu sorgen, dass die Informationen über Geräte, Software, Formate und weitere Spezifikationen (z. B. Verschlüsselung) diskriminierungsfrei und transparent verfügbar sind und die Bieter wissen, was sie brauchen, um formgerechte Teilnahmeanträge, Angebote und Interessenbestätigungen abzugeben.

---

[3] Z. B. „Mozilla Thunderbird“ mit der Erweiterung „Enigmail 2.0“
[4] Z. B. KMail/Kontact (für die Betriebssysteme Linux, Windows und MacOS X
[5] Herunterladbar auf: https://apps.kde.org/de/kleopatra
[6] https://gnupg.com/index.de.html
[7] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/E-Mail-Verschluesselung/GPG4Win/gpg4win_node.html

Es ist möglich, dies durch einen Verweis auf allgemein zugängliche Quellen (z. B. Internetseiten) zu gewährleisten, sofern sichergestellt ist, dass die Informationen für alle Interessenten gleich sind.

Bei Verwendung der o. g. Programme sind die Informationen über die technischen Spezifikationen der Hard- bzw. Softwarekomponenten über die bereits erwähnten Internetseiten allgemein verfügbar. Es empfiehlt sich, die (potentiellen) Bieter explizit darauf hinzuweisen.