Berlin, 1. Februar 2018

Handreichung zur „technischen no-spy-Klausel“

1. Vorbemerkung:

Die nachfolgenden Ausführungen beziehen sich auf Ziffer 2.3 der EVB-IT Überlassung Typ A-AGB. Sie gelten entsprechend für Ziffer 1.4 EVB-IT Pflege S-AGB, Ziffer 2.4 EVB-IT Kauf-AGB, Ziffer 1.5 EVB-IT Instandhaltungs-AGB und EVB-IT Dienstleistungs-AGB, dort bezogen auf die jeweiligen Vertragsgegenstände, d.h. auf Programmstände von Software bzw. Hardware.

2. Ziffer 2.3 der EVB-IT Überlassung Typ A-AGB im Wortlaut:

Der Auftragnehmer überlässt die Standardsoftware* frei von Schaden stiftender Software*. Dies ist mit aktueller Scan-Software zu einem angemessenen Zeitpunkt vor der Lieferung zu prüfen. Der Auftragnehmer erklärt, dass die Prüfung keinen Hinweis auf Schaden stiftende Software* ergeben hat. Diese Regelung gilt für jede, auch die vorläufige und Vorabüberlassung, z.B. zu Testzwecken.

Der Auftragnehmer gewährleistet darüber hinaus, dass die von ihm zu liefernde Standardsoftware* frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Standardsoftware*, anderer Soft- und/oder Hardware oder von Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch

- ***Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,***
- ***Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder***
- ***Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.***

Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Funktionsweise angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert **(„opt-in“) wurde.**

3. Hinweise:

Der erste Absatz der Ziffer soll die Virenfreiheit der Software absichern. Der Auftragnehmer erklärt mit Lieferung automatisch die Virenfreiheit der Software; er kann sich dabei auch entsprechende Erklärungen des Herstellers zu Eigen machen. Einer gesonderten Erklärung des Auftragnehmers bedarf es nicht. Die Regelung in den AGB nimmt dem Auftraggeber aber nicht das Recht, sich die Virenfreiheit vom Auftragnehmer auch nach Vertragsschluss ausdrücklich bestätigen zu lassen. Ein denk-

barer Anwendungsfall dafür wäre, wenn ein bestimmter zu überlassender Programmstand zum Vertragsschluss dem Auftragnehmer selbst noch nicht vorlag (z.B. weil dieser ihm vom Hersteller erst später, z.B. im Zuge der Mängelbehebung überlassen wird) und seine mit Vertragsschluss abgegebene Erklärung noch nicht darauf bezogen sein konnte.

Im zweiten Absatz wird geregelt, dass der Auftragnehmer gewährleistet, dass die Software keine unerwünschten Funktionen aufweist, die die Integrität, Vertraulichkeit und Verfügbarkeit von Software, Hardware oder Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen. Hierbei handelt es sich um Funktionen in der Software, über die ohne Kenntnis des Auftraggebers z.B. Daten ausgelesen oder verändert oder die Funktion der Software beeinflusst werden können (z.B. Backdoors). Die AGB-Klausel legt fest, was als unerwünscht gilt. Eine Funktion gilt als unerwünscht, wenn sie so weder

- vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch
- vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Funktionsweise angeboten und vom Auftraggeber so bezuschlagt, noch
- im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in“) wurde.

Nachfolgend sind diese Fälle näher erläutert.

a) <u>In der Leistungsbeschreibung geforderte Funktionen</u>

In der Leistungsbeschreibung geforderte Funktionen sind naturgemäß nicht unerwünscht, jedenfalls soweit sie auch tatsächlich nur das tun, was sie gemäß Leistungsbeschreibung tun sollen oder für deren Umsetzung selbstverständliche Funktionen mit enthalten.

> *<u>Beispiel</u>: Die Software soll eine Schnittstelle zur Kommunikation mit der Buchhaltungssoftware aufweisen. In diesem Fall ist weder die Schnittstelle unerwünscht, noch die Kommunikation der Software mit der Buchhaltungssoftware über diese Schnittstelle. Nun wird der Auftraggeber aber nicht alle Funktionen der Software im Einzelnen aufführen wollen und können. Die Software wird demnach Funktionen haben, die nicht beschrieben wurden, z.B. hat sie eine Druckfunktion oder Funktionen wie „Speichern unter“ oder „Per E-Mail senden an“. Diese Funktionen sind aber nicht unerwünscht, wenn sie sich im Übrigen völlig harmlos verhalten und dadurch die Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers auch nicht gefährden.*
>
> *Eindeutig unerwünscht wäre jedoch, wenn die Software z.B. ohne Kenntnis des Auftraggebers personenbezogene Daten sammelt, das Nutzungsverhalten und die Nutzungsdauer einzelner Anwender erfasst und diese zusammen mit weiteren Inhaltsdaten über die Schnittstelle an Dritte, bspw. eine Stelle im Ausland, übermittelt.*
>
> *Das ergibt sich einerseits schon aus dem Kontext „Vergabe durch einen öffentlichen Auftraggeber“ sowie dem Zweck „Einsatz in einer Behörde“. Andererseits ist das Verbot solcher Funktionen bereits Teil der Leistungsbeschreibung - jedenfalls dann, wenn diese auf die Bedingungen der EVB-IT Überlassung Typ A-AGB bzw. deren Ziffer 2.3 Bezug nimmt: Absatz 1 der Ziffer statuiert die allgemeine Pflicht, die Standardsoftware frei von Schaden stiftender Software zu überlassen. Absatz 2 macht deutlich, dass es Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers gibt, die zu wahren sind.*

b) Vom Auftragnehmer im Angebot beschriebene Funktionen

Hat die Software aus den Beispielen unter a) auch eine solche möglicherweise unerwünschte sicherheitsrelevante Funktion, so kann der Auftragnehmer dies dem Auftraggeber in seinem Angebot unter konkreter Beschreibung der Aktivität und der Funktionsweise mitteilen.

Widerspricht die so mitgeteilte Funktion der Leistungsbeschreibung oder gefährdet diese die Integrität, Vertraulichkeit oder Verfügbarkeit der Standardsoftware, anderer Soft- und/oder Hardware oder von Daten und widerspricht sie den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers, so wird dieser das Angebot zu Recht ausschließen.

Achtung: Bestehen diese Bedenken nicht und erteilt der Auftraggeber auf ein solches Angebot den Zuschlag, ist die Funktion nicht mehr unerwünscht im Sinne dieser Regelung.

Wichtig: Damit der Auftragnehmer überhaupt die Gelegenheit erhält, in seinem Angebot auf sicherheitsrelevante Funktionen der angebotenen Software hinzuweisen, ist es sinnvoll, dass der Auftraggeber den Auftragnehmer über den Fragenkatalog oder sonst in geeigneter Form z.B. mittels eines Formulars auffordert, solche Funktionen enumerativ und unter konkreter Beschreibung der Funktionsweise mitzuteilen. Dies kann z.B. durch die Möglichkeit erfolgen, dem Auftragnehmer ein Feld für Freitext zu eröffnen. Es sollte ausdrücklich klargestellt werden, dass pauschale Verweise auf Handbücher, allgemeine Beschreibungen oder auch Datenblätter, die daneben noch andere Informationen enthalten und die das Entscheidende nicht klar erkennbar hervorheben, diesen Anforderungen nicht genügen. Denkbar sind hingegen konkrete Verweise auf ein bestimmtes Kapitel eines Datenblattes oder in ähnlichen Dokumenten, soweit sich dieses Kapitel auf sicherheitsrelevante Funktionen bezieht, die erforderlichen Informationen enthält und als Unterlage mitgeliefert wird.

Berücksichtigen sollten Vergabestellen, dass Auftragnehmer, die nicht selbst Hersteller der Hard- oder Software sind, praktisch nur dann in der Lage sein werden, die geforderten Angaben zu machen, wenn sie ihrerseits von den Herstellern (bzw. von Vorlieferanten oder Subunternehmern) die erforderlichen Informationen oder Bestätigungen erhalten. In der ersten Zeit nach Veröffentlichung der aktuellen EVB-IT AGB und später auch bei neuen Produkten kann für die Informationsbeschaffung beim Hersteller ein längerer Zeitraum erforderlich sein. Dies sollte z.B. bei der Bemessung der Angebotsfristen berücksichtigt werden.

Hersteller sollten sich auf derartige Anfragen von ihren Vertragspartnern in der Lieferkette einstellen und dementsprechend künftig die erforderlichen Informationen und Bestätigungen vorhalten bzw. bei neuen Produkten kurzfristig erstellen, damit ihre Produkte in Vergabeverfahren berücksichtigt werden können.

c) Im Einzelfall vom Auftraggeber ausdrücklich autorisierte Funktionen („opt-in“)

Während a) und b) die Frage betreffen, ob die fragliche Funktion anfänglich vereinbart wurde und damit nicht unerwünscht sein kann, regelt der dritte Punkt den Fall, dass eine solche Funktion nachträglich im Einzelfall vom Auftraggeber autorisiert wird. Ebenso bedürfen solche Funktionen einer ausdrücklichen Autorisierung durch den Auftraggeber, die im Rahmen von neuen Programmständen, z.B. Sicherheitspatches geliefert werden.

Das sogenannte „opt-in“ bedeutet dabei, dass eine ausdrückliche Zustimmung vor der Aktivierung erforderlich ist und dies weder stillschweigend noch nachträglich erfolgen kann.

Die Grundintention ist, dass der Auftraggeber über sicherheitsrelevante Funktionen eine informierte Entscheidung treffen können muss. Vice versa bedeutet dies aber auch, dass ein Auftraggeber, der bei hinreichender Transparenz und Informiertheit über Art, Umfang und Auswirkungen einer Funktion deren Autorisierung vorgenommen hat, diese Entscheidung gegen sich gelten lassen muss.