

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Betreff:

AW: V11377 FB Zuvex Penetrationstest [REDACTED]

Annahme Vertrag

hiermit nehmen wir das Vertragsangebot V11.377 "Zuvex Penetrationstest" [REDACTED] vom 08.06.2017 an.

Der Vertrag ist somit wirksam.

Mit freundlichen Grüßen

[REDACTED]

Freie und Hansestadt Hamburg
Finanzbehörde

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

**Finanzbehörde
Gänsemarkt 36
20354 Hamburg**

– im Folgenden „Auftraggeber“ genannt –

und

**Dataport
Anstalt des öffentlichen Rechts
Altenholzer Straße 10 - 14
24161 Altenholz**

– im Folgenden „Auftragnehmer“ genannt –

wird folgender Vertrag geschlossen:

1 Vertragsgegenstand und Vergütung

1.1 Projekt-/Vertragsbezeichnung

Zuvex Penetrationstest

1.2 Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung.

1.3 Die Leistungen des Auftragnehmers werden

nach Aufwand gemäß Nummer 5.1

zum Festpreis gemäß Nummer 5.2

zuzüglich Reise- und Nebenkosten – soweit in Nummer 5.3 vereinbart – vergütet.

2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieser Vertrag (Seiten 1 bis 6) mit Anlage(n) Nr. 1 und 2
- Allgemeine Vertragsbedingungen von Dataport (AGV) in der bei Vertragsschluss geltenden Fassung (s. Nr. 11.1)
- Dataport Datenschutz-Leitlinie über technische und organisatorische Maßnahmen bei der Datenverarbeitung im Auftrag (s. Nr. 11.1)
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistung) in der bei Vertragsschluss geltenden Fassung
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

2.2 Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

3 Art und Umfang der Dienstleistungen

3.1 Art der Dienstleistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- 3.1.1 Beratung
- 3.1.2 Projektleitungsunterstützung
- 3.1.3 Schulung
- 3.1.4 Einführungsunterstützung
- 3.1.5 Betreiberleistungen
- 3.1.6 Benutzerunterstützungsleistungen
- 3.1.7 Providerleistungen ohne Inhaltsverantwortlichkeit
- 3.1.8 sonstige Dienstleistungen: Zuvex Penetrationstest gem. Anlage(n) Nr. 2

3.2 Umfang der Dienstleistungen des Auftragnehmers

3.2.1 Der Umfang der vom Auftragnehmer zu erbringenden Dienstleistungen ergibt sich aus

- folgenden Teilen des Angebotes des Auftragnehmers vom _____
Anlage(n) Nr. _____
- der Leistungsbeschreibung des Auftragnehmers
Durchführung eines Penetrationstests
Anlage(n) Nr. 2
- folgenden weiteren Dokumenten:
Ansprechpartner
Anlagen Nr. 1

Es gelten die Dokumente in

- obiger Reihenfolge
- folgender Reihenfolge: 1, 2

3.2.2 Der Auftragnehmer wird den Auftraggeber auf relevante Veränderungen des Standes der Technik hinweisen, wenn diese für den Auftragnehmer erkennbar maßgeblichen Einfluss auf die Art der Erbringung der vertraglichen Leistungen haben.

3.2.3 Besondere Leistungsanforderungen (z. B. Service-Level-Agreements über Reaktionszeiten):

3.3 Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers

Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers sind

- a) die Mitwirkungsleistungen des Auftraggebers gemäß Nummer 8
- b) folgende weitere Faktoren:

4 Ort der Dienstleistungen/Leistungszeitraum

4.1 Ort der Dienstleistungen in den Räumlichkeiten des Auftraggebers und des Auftragnehmers

4.2 Zeiträume der Dienstleistungen

Leistungen (gemäß Nummer 3.1)	Geplanter Leistungszeitraum		Verbindlicher Leistungszeitraum	
	Beginn	Ende	Beginn	Ende
gem. Nr. 3.1.8		31.12.2017	01.05.2017	

4.3 Zeiten der Dienstleistungen

Die Leistungen des Auftragnehmers werden nach Absprache erbracht sowie

4.3.1 während der üblichen Geschäftszeiten des Auftragnehmers an Werktagen (außer an Samstagen und Feiertagen)

Montag bis Donnerstag von 08:00 bis 17:00 Uhr
 Freitag bis _____ von 08:00 bis 15:00 Uhr

4.3.2 während sonstiger Zeiten

_____ bis _____ von _____ bis _____ Uhr
 _____ bis _____ von _____ bis _____ Uhr
 an Sonn- und Feiertagen am Sitz des Auftragnehmers von _____ bis _____ Uhr

5 Vergütung gem. Leistungsnachweis Dienstleistung

5.1 **Vergütung nach Aufwand**

- ohne Obergrenze
- mit einer Obergrenze in Höhe von

Bezeichnung des Personals/der Leistung (Leistungskategorie)					Preis innerhalb der Zeiten gemäß Nr. 4.3
Pos.	SAP-Artikel-Nr.	Artikelbezeichnung	Menge	Mengen-einheit	Einzelpreis
1	21010600	Unterstützungsleistungen extern			Angebotspreis gem. Vergabe

Die Abrechnung erfolgt nach Aufwand.

Reisezeiten

- Reisezeiten werden nicht gesondert vergütet.
- Reisezeiten werden vergütet gemäß

Rechnungsstellung

Die Rechnungsstellung erfolgt kalendermonatlich nachträglich gem. Leistungsnachweis.

Der Leistungsnachweis für Personalleistungen wird kalendermonatlich nachträglich erstellt und zugesandt. Er gilt für jeden Monat als genehmigt, wenn und soweit der Auftraggeber nicht innerhalb von 14 Kalendertagen nach Erhalt Einwände geltend macht.

Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt vereinbart

- gemäß Ziffer 6.4 EVB-IT Dienstleistung
- anderweitige Regelung:

5.2 Festpreis

Für die vom Auftragnehmer zu erbringenden Dienstleistungen zahlt der Auftraggeber einen **jährlichen Festpreis** in Höhe von **insgesamt**

Der **jährliche Festpreis** setzt sich wie folgt zusammen:

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengeneinheit	Einzelpreis	Gesamtpreis

Die Rechnungsstellung des jährlichen Festpreises erfolgt

Der Auftragnehmer behält sich eine Preisänderung gemäß seinem jeweils gültigen Leistungsverzeichnis vor. Sofern die vorgenannten Preise nicht im Leistungsverzeichnis abgebildet sind, gilt Ziffer 6.4 EVB-IT Dienstleistung.

5.3 Reisekosten und Nebenkosten

- Reisekosten werden nicht gesondert vergütet.
- Reisekosten werden vergütet gemäß
- Nebenkosten werden nicht gesondert vergütet.
- Nebenkosten werden vergütet gemäß

6 Rechte an den verkörperten Dienstleistungsergebnissen

(ergänzend zu/abweichend von Ziffer 4 EVB-IT Dienstleistung)

- 6.1 Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen, die seinem Bereich zuzuordnen sind, einfache, nicht übertragbare Nutzungsrechte* an den Dienstleistungsergebnissen einzuräumen:
- 6.2 Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen außerhalb seines Bereiches einfache, nicht übertragbare Nutzungsrechte* an den Dienstleistungsergebnissen einzuräumen:
- 6.3 Abweichend von Ziffer 4 EVB-IT Dienstleistung räumt der Auftragnehmer dem Auftraggeber das ausschließliche, dauerhafte, unbeschränkte, unwiderrufliche und übertragbare Nutzungsrecht an den Dienstleistungsergebnissen, Zwischenergebnissen und vereinbarungsgemäß bei der Vertragserfüllung erstellten Schulungsunterlagen ein. Dies gilt auch für die Hilfsmittel, die der Auftragnehmer bei der Erbringung der Dienstleistung entwickelt hat. Der Auftragnehmer bleibt zur beliebigen Verwendung der Hilfsmittel und Werkzeuge, die er bei der Erbringung der Dienstleistung verwendet hat, berechtigt.
- 6.4 Sonstige Nutzungsrechtsvereinbarungen

7 Verantwortliche Ansprechpartner siehe Anlage 1

des Auftraggebers: _____

des Auftragnehmers: _____

8 Mitwirkungsleistungen des Auftraggebers

Folgende Mitwirkungsleistungen (z. B. Infrastruktur, Organisation, Personal, Technik, Dokumente) werden vereinbart:

8.1 Der Auftraggeber benennt mindestens zwei Mitarbeiterinnen/Mitarbeiter, die dem Auftragnehmer als Ansprechpartnerinnen/Ansprechpartner zur Verfügung stehen.

8.2 Änderungen der Anlage 1 Ansprechpartner sind unverzüglich schriftlich mitzuteilen. Hierfür wird eine neue Anlage 1 vom Auftraggeber ausgefüllt. Die Anlage wird auf Anforderung durch den Kundenbetreuer zur Verfügung gestellt. Die neue Anlage ist an _____ zu senden.

9 Schlichtungsverfahren

Die Anrufung folgender Schlichtungsstelle wird vereinbart:

10 Versicherung

Der Auftragnehmer weist nach, dass die Haftungshöchstsummen gemäß Ziffer 9.2.1 EVB-IT Dienstleistung durch eine Versicherung abgedeckt sind, die im Rahmen und Umfang einer marktüblichen deutschen Industriehaftpflichtversicherung oder vergleichbaren Versicherung aus einem Mitgliedsstaat der EU entspricht.

11 Sonstige Vereinbarungen

11.1 Die AGV und die Dataport Datenschutz-Leitlinie sind im Internet unter www.dataport.de veröffentlicht.

11.2 Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen in Ansehung ihrer Art, des Zwecks und der Person des Auftraggebers zum Zeitpunkt des Vertragsschlusses nicht der Umsatzsteuer. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.

11.3 Hamburgisches Transparenzgesetz

Die Vertragspartner vereinbaren über die Vertragsinhalte Verschwiegenheit, soweit gesetzliche Bestimmungen, wie insbesondere das Hamburgische Transparenzgesetz (HmbTG), dem nicht entgegenstehen. Unabhängig von einer möglichen Veröffentlichung kann der Vertrag Gegenstand von Auskunftsanträgen nach dem HmbTG sein.

Der Auftraggeber erklärt durch Ankreuzen, ob dieser Vertrag bei Vertragsschluss nach dem HmbTG veröffentlicht werden soll. Dieser Vertrag wird nur wirksam, wenn bei Nr. 11.3.1 oder Nr. 11.3.2 ein Kreuz gesetzt wird.

11.3.1 Erklärung der Nichtveröffentlichung

Der Auftraggeber erklärt mit Auswahl dieser Option, dass er diesen Vertrag zurzeit nicht im Informationsregister veröffentlichen wird.

Sollte der Auftraggeber zu einem späteren Zeitpunkt eine Veröffentlichung vorsehen, so wird er den Auftragnehmer hierüber unverzüglich informieren und alle notwendigen Schritte einleiten, damit vertrauliche Informationen (insbesondere personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse) nicht an Dritte herausgegeben bzw. veröffentlicht werden.

11.3.2 Erklärung der Veröffentlichung und Rücktrittsrecht nach HmbTG

Der Auftraggeber erklärt mit Auswahl dieser Option, dass er diesen Vertrag bei Vertragsschluss im Informationsregister veröffentlichen wird. Er wird alle notwendigen Schritte einleiten, damit vertrauliche Informationen (insbesondere personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse) nicht an Dritte herausgegeben bzw. veröffentlicht werden.

Der Auftraggeber kann von diesem Vertrag bis einen Monat nach Veröffentlichung im Informationsregister ohne Angabe von Gründen zurücktreten.

Der Auftraggeber verpflichtet sich, unverzüglich nach Vertragsschluss die Veröffentlichung im Informationsregister zu veranlassen und teilt dem Auftragnehmer das Datum der Veröffentlichung mit.

Macht der Auftraggeber vom Rücktrittsrecht Gebrauch, so gilt für den Fall, dass der Auftragnehmer schon vor Ablauf der Rücktrittsfrist mit der Durchführung des Vertrages beginnt, Folgendes:

- a) Die beiderseits erbrachten Leistungen sind zurückzugewähren.
- b) Ist eine Rückgewähr nicht möglich, so leistet der Auftraggeber Wertersatz.
 - Für die Berechnung des Wertersatzes gelten die in dem Vertrag genannten Leistungsentgelte.
 - Aufwände, für die kein Leistungsentgelt ausgewiesen ist, sind nach dem jeweils gültigen Stundensatz zu vergüten, wenn und soweit sie für die Erfüllung des Vertrages erforderlich waren. Dies gilt vor allem für vorbereitende Tätigkeiten.
 - Für gelieferte Hard- und Software wird das volle Leistungsentgelt erstattet. Verschlechterungen, auch wenn sie durch die bestimmungsgemäße Ingebrauchnahme entstehen, bleiben bei der Wertermittlung außer Betracht. Die Pflicht zum Wertersatz entfällt, soweit der Auftragnehmer die Verschlechterung oder den Untergang zu vertreten hat oder der Schaden gleichfalls bei ihm eingetreten wäre.
- c) Hat der Auftragnehmer zur Erfüllung des Vertrages verbindliche Bestellungen bei Lieferanten oder Unterauftragnehmern vorgenommen, die weder storniert noch von dem Auftragnehmer anderweitig verwendet werden können, so nimmt der Auftraggeber die entsprechenden Lieferungen oder Leistungen gegen Zahlung des mit dem Lieferanten oder Unterauftragnehmer vertraglich vereinbarten Preises ab. Dies gilt jedoch dann nicht, wenn sich die Lieferung aus von dem Auftragnehmer zu vertretenden Gründen verschlechtert hat oder untergegangen ist. Der Auftragnehmer setzt sich in jedem Fall nach Kräften für eine Minimierung des Schadens ein.
- d) Im Übrigen finden die Bestimmungen der §§ 346 ff BGB entsprechende Anwendung, soweit sich nicht aus den vorstehenden Regelungen etwas anderes ergibt.

11.3.3 Erteilung von Auskünften

Sollte der Auftraggeber zu irgendeinem Zeitpunkt die Erteilung einer Auskunft an eine antragstellende Person vorsehen, so wird er den Auftragnehmer hierüber unverzüglich informieren und alle notwendigen Schritte einleiten, damit vertrauliche Informationen (insbesondere personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse) nicht an Dritte herausgegeben bzw. veröffentlicht werden. Der Auftragnehmer wird hierzu dem Auftraggeber einen Schwärzungsvorschlag unterbreiten.

11.4 Mit diesem Vertrag wird eine etwaige Vorvereinbarung abgelöst. Rechte und Pflichten der Vertragsparteien bestimmen sich ab dem Zeitpunkt seines Wirksamwerdens ausschließlich nach diesem Vertrag.

11.5 Dieser Vertrag beginnt am 01.05.2017 und endet mit Abschluss des Projektes.

Hamburg _____, 08.06.2017 _____
Ort Datum

Hamburg _____, _____
Ort Datum

Ansprechpartner
zum Vertrag über die Beschaffung von IT-Dienstleistungen
Zuvex Penetrationstest

Vertragsnummer/Kennung Auftraggeber:

Auftraggeber:

Finanzbehörde
Gänsemarkt 36
20354 Hamburg

Rechnungsempfänger:

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

Vertragliche Ansprechpartner des
Auftraggebers gem. Nr. 7 EVB-IT:
Zentraler Ansprechpartner des
Auftragnehmers gem. Nr. 7 EVB-IT:



Fachliche Ansprechpartner des
Auftraggebers gem. Nr. 8.1 EVB-IT:

1. _____
Tel.
2. _____
Tel.

Technische Ansprechpartner des
Auftraggebers:

1. _____
Tel.
2. _____
Tel.

Ändern sich die Ansprechpartner in dieser Anlage, wird die Anlage gem. Nr. 8.2 EVB-IT ohne die Einleitung eines Änderungsvertrages ausgetauscht.

Ort

Datum

Leistungsbeschreibung

Durchführung eines Penetrationstests

verantwortlich:



Version: 1.3 vom: 30.03.2017

Status: Gültig

Schutzstufe: keine Schutzstufe

Zielgruppe: FB, Dataport

Inhaltsverzeichnis

1	Einleitung.....	1
2	Rahmenbedingungen.....	1
3	Vorgaben für den Penetrationstest.....	1
3.1	Black Box Test.....	1
3.2	White Box Test.....	1
3.3	Ergebnisbericht.....	2
4	Kriterien für Auswahl des Anbieters	2
5	Schlussbestimmungen.....	2

1 Einleitung

Die Freie und Hansestadt Hamburg betreibt die Sicherheitsinfrastruktur Zuvex bei Dataport. Zuvex bietet die Möglichkeit eines sicheren Zugriffs von extern auf interne Anwendungen des [REDACTED] Mitarbeiter der FHH und externe Personen, [REDACTED], können so über das Internet unabhängig von Ort, Zeit [REDACTED] auf eine freigegebene interne Anwendung zugreifen.

Die Sicherheitsinfrastruktur beinhaltet eine ganze Reihe von Sicherheitsmaßnahmen, sowohl organisatorischer als auch technischer Natur. Diese Maßnahmen und ihre Durchschlagskraft sollen über einen Penetrationstest überprüft werden. Der Penetrationstest soll extern durchgeführt werden. Der letzte Penetrationstest fand nach Aufbau der Infrastruktur im Jahr 2013 statt, eine Umstellung der zugrundeliegenden Technik in 2016 macht einen erneuten Test erforderlich.

Der vorliegende Vertrag dient der Abwicklung der Kosten, die durch die Beauftragung externer Auftragnehmer anfallen.

2 Rahmenbedingungen

Die Durchführung der Vergabe, die Betreuung der Infrastruktur und des externen Auftragnehmers während der Durchführung des Penetrationstests sowie ggf. Nacharbeiten werden über den Betriebsvertrag Zuvex, ggf. über bereits vereinbarte Zusatzkontingente, geregelt.

Der Auftragswert soll [REDACTED] nicht überschreiten.

Es erfolgt im Einklang mit dem Vergaberecht eine freihändige Vergabe.

3 Vorgaben für den Penetrationstest

Der Penetrationstest soll einen Black Box Test und einen White Box Test umfassen. Dadurch soll überprüft werden, welche Gefährdungsszenarien sich unter unterschiedlichen Voraussetzungen ergeben können. [REDACTED]

[REDACTED] Für die Vergabe ist wichtig, dass alle Personen, die für den Auftrag eingesetzt werden sollen, namentlich benannt werden und schriftlich bestätigt wird, dass diese sicherheitsüberprüft sind. Der konkrete Nachweis der Sicherheitsüberprüfung kann im Zuschlagsfall zwischen den entsprechenden Sicherheitsmanagement-Beauftragten erfolgen.

3.1 Black Box Test

Für den Black Box Test erhält der Anbieter eine Auswahl von URLs zu verschiedenen Zuvex-Verfahren. [REDACTED]

[REDACTED]. Wenn der Anbieter mit den üblichen Methoden nicht weiterkommt, bekommt er weitere Informationen für den White Box Test.

3.2 White Box Test

Der Anbieter erhält neben einer Auswahl von URLs zu verschiedenen Zuvex-Verfahren auch Logindaten (Benutzername und Passwort), mit denen er auf die Verfahren zugreifen kann. Dabei gilt es zwei Szenarien zu überprüfen:

- Der Anbieter hat nur die Account-Daten eines Zuvex-Nutzers erhalten, der auf das Verfahren selbst nicht zugelassen ist.
- Der Anbieter hat die Account-Daten eines Zuvex-Nutzers erhalten, der auf das Verfahren zugelassen ist.

In beiden Fällen soll der Anbieter prüfen, ob er in dem jeweiligen Verfahren Schaden anrichten könnte, und ob er von dort aus andere Systeme oder Verfahren erreichen und schädigen könnte.



3.3 Ergebnisbericht

Der Ergebnisbericht soll durch den Anbieter graphisch aufbereitet werden (Ampel-System) mit einem Management-Summary und dann den tabellarischen Testergebnissen und Handlungsempfehlungen, ggf. mit Screenshots aus dem Testverlauf.

4 Kriterien für Auswahl des Anbieters

Für die Auswahl der anzuschreibenden Anbieter gelten folgende Kriterien:

- Der Anbieter ist vom BSI zertifiziert und empfohlen und bietet uns BSI-zertifizierte und sicherheitsüberprüfte (Stufe 1) Mitarbeiter für den Penetrationstest an. Grundlage für die Auswahl der Anbieter ist die entsprechende Übersicht über zertifizierte Dienstleister vom BSI¹. Auf der Seite sind 10 Anbieter vermerkt, von denen 7 Penetrationstests anbieten. Drei dieser Anbieter werden angeschrieben und um ein Angebot gebeten mit Frist.
- Von den angeschriebenen Anbietern gewinnt derjenige mit dem besten Preis-Leistungsverhältnis. Der Preis allein ist also nicht ausschlaggebend, sondern auch die folgenden Faktoren:
 - Qualität und Umfang des Test-Berichts (Beispielbericht bei Vergabe einfordern)
 - Vorhandensein eines Management-Summary mit Ampel-System
 - Test-Umfang (Umfang Methoden)

5 Schlussbestimmungen

Der Vertrag endet mit erbrachter Leistung. Eine Umsetzung der Vergabe und des Penetrationstests ist für das zweite Halbjahr 2017 vorgesehen. Weitere Verabredungen werden nicht getroffen.

¹

https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/IS_REV_PEN/IS_REV_Dienstleister/stellen_zertifizierung_pentester-is-revisoren.html