



POLIZEI
Sachsen

Vergabeverfahren des Polizeiverwaltungsamtes (PVA)

VMware Enterprise License Agreement (ELA) der Polizei Sachsen

Anlage 02.5 - Liefer- und Leistungsbedingungen (LuL)

Vergabe-Nr.: B3970 | Vertrags-Nr.: 19-RAB0004

Inhaltsverzeichnis

1.1	Personaleinsatz und Sicherheitsüberprüfung (SÜ)	3
1.1.1	Auszug § 8 SächsSÜG – Einfache Sicherheitsüberprüfung (Ü 1).....	3
1.1.2	Einstufung von Leistungen	3
1.2	IT-Anbindung des Auftragnehmers.....	5
1.3	Zutritt, (Fern-)Zugang, Zugriff	5
1.4	Ansprechpartner.....	6
1.5	Qualitätsstandards	7
1.6	Reaktion und Benachrichtigung bei sicherheitsrelevanten Vorfällen	7
1.7	Vertraulichkeitsvereinbarung	8
1.8	Anforderungen an die Vertraulichkeit – „No-spy – Garantie“	9
1.9	Audits, Kontrollrechte	9
Anlage 1.a	- Anforderungen an die Vertraulichkeit – „No-spy – Garantie“	10

1.1 Personaleinsatz und Sicherheitsüberprüfung (SÜ)

Der Auftragnehmer erbringt die Leistungen durch Personal, welches entsprechend den vertraglichen Anforderungen für die Erbringung der Leistungen qualifiziert ist. Die Kommunikation mit dem Auftraggeber erfolgt in deutscher Sprache entsprechend der Vereinbarungen in der Leistungsbeschreibung. Zudem sind, je nach Leistungsanforderungen, entsprechende Sicherheitsüberprüfungen des zur Leistungserfüllung eingesetzten Personals des Auftragnehmers nötig.

1.1.1 Auszug § 8 SächsSÜG – Einfache Sicherheitsüberprüfung (Ü 1)

(1) Die einfache Sicherheitsüberprüfung ist für Personen durchzuführen, die

1. Zugang zu **VS-VERTRAULICH** eingestuften Verschlusssachen erhalten sollen oder ihn sich verschaffen können,
2. Tätigkeiten in Bereichen nach § 1 Abs. 2 Nr. 3 wahrnehmen sollen.

1.1.2 Einstufung von Leistungen

Im Zuge der Leistungserbringung ist damit zu rechnen, dass der Auftragnehmer sowohl durch die mit der Umsetzung beauftragten Personen sowie auch als Unternehmen selbst Kenntnis zu Tatsachen, Dokumenten, Konzepten und Planungen mit folgender Einstufung erhalten:

GEHEIM (geh.; auch: Stufe I):

Die Kenntnisnahme durch Unbefugte kann die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen. Häufige Kennzeichnung: Auf Schriftstücken roter Stempelabdruck oder Druck in der Kopf-/Fußzeile.

VERSCHLUSSSACHE – VERTRAULICH (VS-VERTRAULICH, VS-Vertr.):

Die Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein. Häufige Kennzeichnung: Auf Schriftstücken blauer oder schwarzer Stempelabdruck oder Druck in der Kopfzeile.

VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NUR FÜR DEN DIENSTGEBRAUCH, VS-NfD):

Die Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein. Häufige Kennzeichnung: Auf Schriftstücken blauer oder schwarzer Stempelabdruck oder Druck in der Kopfzeile

- Der in den Ausschreibungsunterlagen festgelegte Anteil an eingesetzten Personen muss bereits mit Beginn der Tätigkeit eine erfolgte erweiterte Sicherheitsüberprüfung (SÜ2) oder eine einfache Sicherheitsüberprüfung (SÜ1) nach Sächsischem Sicherheitsprüfungsgesetz (SächsSÜG) vorlegen können. Eine gleichwertige Überprüfung, d.h. nach den Vorgaben anderer deutscher Bundesländer oder der Bundesrepublik Deutschland gilt ebenso.

Dies ist erforderlich da der Einsatz direkt nach Zuschlag des Auftraggebers erfolgen wird.

- Des Weiteren sind vom Auftragnehmer nur Personen einzusetzen, die zum Zeitpunkt der Angebotsabgabe die schriftliche Bereitschaft erklärt haben, sich einer erweiterten Sicherheitsüberprüfung nach SächsSÜG zu unterziehen.

Für diese noch nicht überprüften Personen des Auftragnehmers wird der/die Geheimschutzbeauftragte des Polizeiverwaltungsamtes (PVA) nach Zuschlagserteilung das Sicherheitsüberprüfungsverfahren bei der Landesdirektion Sachsen einleiten. Dazu ist im Rahmen der Angebotsabgabe ein Ansprechpartner (Sicherheitsbevollmächtigte/r des Auftragnehmers) zu benennen.

Die formelle Durchführung des Sicherheitsüberprüfungsverfahrens wird durch die Landesdirektion Sachsen gesteuert. Auf die Zeitdauer des Sicherheitsüberprüfungsverfahrens kann kein Einfluss genommen werden. Das Sicherheitsüberprüfungsverfahren ist kostenfrei. Kosten können in Bezug auf evtl. anfallenden Schriftwechsel (Portokosten) entstehen. Sollte nach Abschluss der behördlichen Sicherheitsüberprüfung keine Berechtigung zur Tätigkeitsaufnahme für den entsprechenden Personen erteilt werden, kann dieser Person nicht (weiter) im vorgesehenen Tätigkeitsfeld eingesetzt werden und ist mit einem gleichwertigen Ersatz durch den Auftragnehmer auszugleichen. Dieses Vorgehen gilt auch im Falle des Austausches von eingesetzten Personen. Der Auftragnehmer darf Personen in vorgesehenen Schlüsselpositionen nur mit Einwilligung des Auftraggebers auswechseln. Der Auftraggeber wird seine Einwilligung unverzüglich erklären, wenn die Ablösung zwingend erforderlich ist und der Auftragnehmer eine qualifizierte Ersatzperson anbietet. Zwingend erforderlich ist die Ablösung insbesondere dann, wenn der weitere Einsatz nicht wie im vereinbarten Leistungsumfang möglich ist. Personal, das nicht auf Schlüsselpositionen eingesetzt ist, darf der Auftragnehmer auch ohne Einwilligung des Auftraggebers auswechseln, sofern das Ersatzpersonal über die vertraglich vorausgesetzte Eignung verfügt. Die Einarbeitung erfolgt auf Kosten des Auftragnehmers.

Der Auftraggeber kann den Austausch einer vom Auftragnehmer zur Vertragserfüllung eingesetzten Person verlangen, wenn diese sich in erheblichem Umfang pflichtwidrig verhält, eine Leistung schlecht erbringt oder die vertraglich vereinbarten persönlichen Voraussetzungen durch die Person nicht mehr erfüllt werden, z. B. wenn Angaben aus einer Sicherheitserklärung nach dem SächsSÜG nicht mehr den Tatsachen entsprechen. Die Einarbeitung des Ersatzpersonals erfolgt auf Kosten des Auftragnehmers. Der Auftraggeber hat das Recht, auch aus anderen Gründen den Austausch der zur Vertragserfüllung eingesetzten Personen zu verlangen. In diesem Fall kann der Auftragnehmer den Ersatz angemessener Kosten verlangen, soweit er diese im Voraus verbindlich mitteilt und der Auftraggeber gleichwohl auf Austausch der Person besteht.

Die vom Auftragnehmer eingesetzten Personen treten in kein Arbeitsverhältnis zum Auftraggeber ein, auch nicht soweit sie Leistungen in dessen Räumen erbringen. Der Auftragnehmer wird durch organisatorische Maßnahmen gewährleisten, dass die jeweils von ihm im Rahmen der Erbringung der Serviceleistungen abgestellten Personen ausschließlich dem Direktionsrecht und der Disziplinargewalt des Arbeitgebers unterstehen. Weisungen erfolgen ausschließlich im Rahmen der vereinbarten Aufgabenverteilung. Die vom Auftragnehmer eingesetzten und in die Geschäftsprozesse des Auftraggebers eingebundenen Personen unterliegen dort in Bezug auf die Informationssicherheit den gleichen Anforderungen wie eigene Mitarbeiter und Mitarbeiterinnen des Auftraggebers.

Bei Beendigung des Auftragsverhältnisses bzw. Ausscheiden einer vom Auftragnehmer eingesetzten Person hat der Auftragnehmer sicherzustellen, dass eine geregelte Übergabe aller Arbeitsergebnisse sowie aller vom Auftraggeber erhaltenen Unterlagen und Betriebsmittel (z.B. mobiles Endgerät, Token, Schlüssel, Ausweise etc.) erfolgt.

1.2 IT-Anbindung des Auftragnehmers

Bei Bedarf stellt der Auftraggeber dem Auftragnehmer für den Zeitraum der Supportarbeiten einen Zugang zum Datennetz des Auftraggebers (Port) zur Verfügung. Seitens des Auftraggebers werden eine entsprechende IP-Adresse sowie die für den Support notwendigen Nutzerkonten mit den dafür notwendigen Berechtigungen zur Verfügung gestellt.

Der Auftraggeber räumt dem Auftragnehmer - soweit für die vereinbarten Leistungen erforderlich – das:

- nicht ausschließliche, nicht übertragbare,
- zeitlich auf die notwendige Dauer der Leistungserbringung, höchstens jedoch auf die Dauer des Vertrages beschränkte, und
- inhaltlich auf den notwendigen Umfang und auf den Zweck der Leistung beschränkte

Recht zur Bearbeitung ein.

Soweit dies zur Erbringung der Leistungen erforderlich ist, räumt der Auftraggeber die vorgenannten Rechte auch für die entsprechenden Quellcodes der jeweiligen Software sowie für der zum IT-System beim Auftraggeber vorhandenen Dokumentation ein.

Der Zugriff wird ausschließlich auf das im abgeschlossenen Vertrag näher bezeichnete IT-System gestattet. Der Auftragnehmer ist nicht berechtigt, die eingeräumten Rechte für andere als die vorgenannten Zwecke zu nutzen oder diese Dritten gegenüber ganz oder teilweise offen zu legen.

Bei einem direkten Anschluss von IT-Systemen des Auftragnehmers an das Datennetz des Auftraggebers sind folgende Einstellungen zwingend einzuhalten:

- Deaktivierung aller drahtlosen (wie bspw. WLAN, Bluetooth, Infrarot) und drahtgebundenen (wie bspw. Modem, Firewire) Kommunikationsschnittstellen,
- permanent aktivierter Virens Scanner mit aktueller Signatur.

In Abweichung der Festlegungen der Vorgaben des Auftraggebers können nach Abstimmung zum Einsatz kommen:

- abweichendes Betriebssystem,
- abweichender Virens Scanner,
- abweichender Browser.

Der Auftraggeber hat das Recht, die Einhaltung der Festlegungen der zuvor genannten Regelungen jederzeit zu überwachen und zu kontrollieren.

1.3 Zutritt, (Fern-)Zugang, Zugriff

Der Auftraggeber wird den eingesetzten Personen des Auftragnehmers Zutritt zu seinen Räumlichkeiten, Zugang zu der dort vorhandenen informationstechnischen Infrastruktur und den Zugriff auf Daten und Anwendungen gewähren, sofern dies jeweils zur Erbringung der Leistung

erforderlich ist und die gesetzlichen und erforderlichen persönlichen Voraussetzungen (wie Sicherheitsüberprüfungen nach dem SächsSÜG -) erfüllt sind.

Es ist eine entsprechende Vereinbarung zwischen Auftraggeber und Auftragnehmer zu treffen die die auftrags- und ordnungsgemäße Durchführung von Wartungs- und Konfigurationsarbeiten sowie Arbeiten zur Störungsbeseitigung durch externe Dienstleister im Datennetz des Polizeivollzugsdienstes des Freistaates Sachsen oder des BOS Leitstellennetzwerkes regelt und dem für den Auftragnehmer vertraglich festgelegten Umfang entspricht.

Bei Ausscheiden einer eingesetzten Person sind durch den Auftragnehmer alle Zutritts-, Zugangs- und/oder Zugriffsmittel des Auftraggebers zurückzufordern und dem Auftraggeber zu übergeben, welche der ausscheidenden Person ausgehändigt wurden.

1.4 Ansprechpartner

Ansprechpartner der Vertragsparteien sind ausschließlich die im Vertrag benannten Personen. Änderungen der Ansprechpartner sind der anderen Partei mit angemessenem Vorlauf schriftlich mitzuteilen. Der Auftraggeber wird Hinweise in Bezug auf die zu erbringenden Leistungen ausschließlich dem vom Auftragnehmer benannten verantwortlichen Ansprechpartner übermitteln und den übrigen vom Auftragnehmer eingesetzten Personen keine Weisungen erteilen.

Anlaufstellen für die Vertragsparteien während der Leistungserbringung.

Als Ansprechpartner beim **Auftraggeber** werden folgende Personen benannt:

- für Informationssicherheit beim Auftraggeber:
 - PVA, Referat 41, Informationssicherheit, is.iuk.pva@polizei.sachsen.de
- für Datenschutz beim Auftraggeber:
 - PVA, Datenschutzbeauftragte(r), dsb.pva@polizei.sachsen.de
- für Geheimschutz/vorbeugenden personellen Sabotageschutz beim Auftraggeber:
 - PVA, Geheimschutzbeauftragte(r), ghs.pva@polizei.sachsen.de

Als Ansprechpartner beim **Auftragnehmer** werden folgende Personen benannt.

- für Informationssicherheit beim Auftragnehmer:
 - Name: Telefon: , E-Mail:
- für Datenschutz beim Auftragnehmer:
 - Name: Telefon: , E-Mail:
- für Geheimschutz/vorbeugenden personellen Sabotageschutz beim Auftragnehmer:
 - Name: Telefon: , E-Mail:

1.5 Qualitätsstandards

Der Auftragnehmer muss Informationssicherheitsmanagementprozesse (ISMS) nach einem in der Industrie anerkannten Standard der Informationssicherheit¹ aufsetzen und einhalten. Er muss Maßnahmen der Informationssicherheit danach planen und umsetzen. Diesbezügliche Vorgaben bzw. Anforderungen des Auftraggebers sind einzuhalten. Die Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

Ebenso sind die Standards und Vorgaben für die vertraglich vereinbarten Lieferungen bzw. Leistungen maßgeblich. Der Auftragnehmer erbringt die Leistungen nach aktuellem Stand der Technik, der zum Zeitpunkt der Leistungserbringung vorherrscht.

Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datenschutz-, Datensicherheits- bzw. Informationssicherheitsmaßnahmen.

1.6 Reaktion und Benachrichtigung bei sicherheitsrelevanten Vorfällen

Der Auftragnehmer ist verpflichtet, alle Sicherheitsvorfälle in seiner Organisation sowie der Organisation involvierter Dritter zu melden, welche potentiell einen negativen Effekt auf materielle oder immaterielle und gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten. Diese Meldung ist umgehend ohne Zeitverzug dem Auftraggeber zunächst mündlich sowie später schriftlich zu übermitteln. Als Beispiele könnten dies auch Fälle von Industriespionage oder eine Sicherheitslücke im Source-Code sein.

Auf Nachfrage des Auftraggebers wird Auftragnehmer im Falle eines Vorfalls entsprechende Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie einen finalen Korrekturbericht bereitstellen.

Für die beim Auftraggeber vor Ort zur Ausführung der Leistung eingesetzten Mitarbeiter gilt die „Richtlinie zur Behandlung von Sicherheitsvorfällen im Polizeivollzugsdienst, im BOS-Digitalfunk und im Leitstellenverbundnetz des Freistaates Sachsen“, wonach folgende allgemein gültige Verhaltensregeln zu beachten sind:

- Ruhe bewahren, keine übereilten Maßnahmen ergreifen,
- bei Ereignissen, die den sofortigen Einsatz von Rettungskräften oder polizeilichen Kräften erfordern (Gefahr für Leib und Leben), diese unverzüglich alarmieren,
- erkannte Sicherheitsvorfälle und (vermutliche) sicherheitsrelevante Unregelmäßigkeiten unverzüglich bei der IuK-Leitstelle (zentraler Meldekopf) anzeigen:

Telefon: 0341 22388 5555 bzw. LIK 727 5555

Fax: 0341 5855 5559

E-Mail: service@bos.sachsen.de

- alle Begleitumstände ungeschönt, offen und transparent erläutern, um damit zur Schadensminderung beizutragen,

¹ BSI-Standards 100-1 bis 100-4 bzw. deren Weiterentwicklungen 200-x und internationale Normen wie der ISO/IEC 27001

- mögliche Schadenshöhen, Folgeschäden, potentiell intern und extern Betroffene und mögliche Konsequenzen vor der Behandlung von Sicherheitsvorfällen beruhend auf den persönlichen Erfahrungen abschätzen und Maßnahmen abwägen,
- Gegenmaßnahmen erst nach Aufforderung durch Berechtigte (Ausnahme bei Gefahr für Leib und Leben, z. B. Erste Hilfe) ergreifen und
- keine unautorisierte Weitergabe von Informationen über Sicherheitsvorfälle an Dritte.

1.7 Vertraulichkeitsvereinbarung

Vertraulich im Sinne dieser Vereinbarung sind Informationen - unabhängig von der Verbreitungsform oder dem vermittelnden Datenträger, insb. auch Softwarecodes -, welche die Parteien ausdrücklich als vertraulich bezeichnen, besonders kennzeichnen oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt.

Die Parteien werden alle geeigneten Vorkehrungen treffen, um die Vertraulichkeit sicherzustellen. Insbesondere werden sie vertrauliche Informationen nur an solche Personen weitergeben, die sie auf Grund ihrer Tätigkeit im Rahmen der Zusammenarbeit erhalten müssen.

Die Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- bzw. Dienstgeheimnissen und Datensicherheitsmaßnahmen, insbesondere die von der jeweils anderen Partei zur Verfügung gestellten Daten und Unterlagen sowie die Arbeitsergebnisse vertraulich zu behandeln, insbesondere allen Unbefugten nicht zugänglich zu machen oder anders als zu dem vertraglich, vorgesehenen Zweck zu verwerten. Die Erfüllung gesetzlicher Pflichten bleibt unbenommen.

Auf Verlangen sind vertrauliche Unterlagen einschließlich aller davon gefertigten Kopien sowie alle gespeicherten Daten inklusive davon gefertigter Datensicherungen, die einer Partei gehören, bei Beendigung der Zusammenarbeit an die jeweils andere Partei auszuhändigen oder zu vernichten. Zurückbehaltungsrechte können nicht geltend gemacht werden.

Die Parteien beachten die international standardisierte Vereinbarung zum Austausch von schutzwürdigen Dokumenten „Traffic Light Protocol“ (TLP). TLP ist für Informationen zu verwenden, die nicht geheimhaltungsbedürftig im Sinne der VSA sind. Informationen, die mit einer entsprechenden Angabe versehen sind, sind wie folgt zu behandeln:

Stufe	Bedeutung	Bestimmung
TLP-White	unbegrenzt (pressefrei)	Informationen und Dokumente dürfen (unter Beachtung des Urheberrechts) uneingeschränkt an jeden einschließlich Massenmedien weitergegeben werden.
TLP-Green	organisationsübergreifend	Informationen und Dokumente dürfen auch an andere Organisationen weitergegeben, aber nicht veröffentlicht oder den Massenmedien zugänglich gemacht werden.
TLP-Amber	organisationsintern	Informationen und Dokumente dürfen auch an Kollegen in der eigenen Organisation oder an andere Organisationen weitergegeben werden (Kenntnis nur wenn nötig).
TLP-Red	persönlich	Informationen und Dokumente dürfen vom Empfänger nur nach Genehmigung durch den Absender weitergegeben werden.

Die Vertraulichkeitsverpflichtung gilt nicht für Informationen:

- welche die jeweilige Partei zum Zeitpunkt der Überlassung ohne Vertraulichkeitsverpflichtung bereits besitzt,
- welche zu dem vorstehend genannten Zeitpunkt bereits veröffentlicht sind oder später ohne Verschulden der Parteien durch Dritte veröffentlicht werden,
- welche den Parteien rechtmäßig von dritter Seite ohne Verpflichtung zur Vertraulichkeit zugegangen sind, oder
- welche die Parteien einander durch schriftliche Erklärung ausdrücklich freigegeben haben.

Die Vertraulichkeitsverpflichtung gilt auch für die Rechtsnachfolger der Parteien.

Sofern es im Rahmen der Zusammenarbeit erforderlich wird, Dritte einzuschalten und vertrauliche Informationen an diese weiterzugeben, werden die Parteien hierzu vorher das ausdrückliche schriftliche Einverständnis der jeweils anderen Vertragspartei einholen und mit dem Dritten entsprechende schriftliche Vereinbarungen treffen, um die Einhaltung der Bestimmungen dieser Vereinbarung sicherzustellen.

Die Vorschriften zum Geheimschutz bleiben davon unberührt.

1.8 Anforderungen an die Vertraulichkeit – „No-spy – Garantie“

Für Vertragsverhältnisse, die besonderer Vertraulichkeit unterliegen ist die **Anlage 1.a** auszufüllen und zu unterschreiben. ²

1.9 Audits, Kontrollrechte

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein anderer beauftragter Dritter im Auftrag des Auftraggebers die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

Der Auftragnehmer verpflichtet sich, die Durchführung von Sicherheits-Audits zu unterstützen. Insbesondere wird für die vom Auftraggeber benannten Personen auch der Zutritt zu Gebäuden und Räumen – im Beisein von Mitarbeitern des AN – gewährt, in denen Technik des Auftragnehmers für den Auftraggeber betrieben wird.

Der Auftragnehmer hat dem Auftraggeber oder einem von ihm beauftragten Dritten die notwendigen Kontrollrechte (inkl. Zutritt, Zugang, Einsicht, Auskunft) zur Prüfung des Datenschutzes, der Informationssicherheit und der Notfallvorsorge einzuräumen. Prüfungen zur Einhaltung des Datenschutzes, der Informationssicherheit und der Notfallvorsorge werden im gegenseitigen Einvernehmen in regelmäßigen Abständen durchgeführt.

² siehe Anlage 1a - Anforderungen an die Vertraulichkeit – „No-spy – Garantie“

Dieses Formblatt ist auszufüllen und zu unterschreiben.

Anlage 1.a - Anforderungen an die Vertraulichkeit – „No-spy – Garantie“

Für Vertragsverhältnisse welcher besonderer Vertraulichkeit unterliegen ist die Anlage 1.a auszufüllen und zu unterschreiben.

Eigenerklärung im Rahmen der Zuverlässigkeitsprüfung

Der Bieter erklärt, dass er rechtlich und tatsächlich in der Lage ist, im Falle eines Zuschlages die dann im Vertrag enthaltene Verpflichtung einzuhalten, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwerten. Insbesondere bestehen zum Zeitpunkt der Abgabe des Angebotes keine Verpflichtungen, Dritten solche Informationen zu offenbaren oder in anderer Weise zugänglich zu machen. Dies gilt nicht, soweit hierfür gesetzliche Offenlegungspflichten bestehen (etwa gegenüber Stellen der Börsenaufsicht, Regulierungsbehörden oder der Finanzverwaltung), es sei denn, solche Offenlegungspflichten bestehen gegenüber ausländischen Sicherheitsbehörden. In Zweifelsfällen hat der Bieter die Vergabestelle auf die gesetzliche(n) Offenlegungspflicht(en) im Rahmen der Abgabe der vorstehenden Erklärung hinzuweisen.

Der Bieter wird die Vergabestelle nach dem Zuschlag des Auftraggebers sofort schriftlich benachrichtigen, wenn sich hinsichtlich des Inhaltes der beauftragten Leistungen eine Änderung ergibt. Dies gilt insbesondere, wenn für ihn eine Notwendigkeit oder Verpflichtung entsteht oder er eine solche hätte erkennen können, die ihn an der Einhaltung der beschriebenen Vertraulichkeit hindern könnte.

Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden. Vertrauliche Informationen dürfen ausschließlich zum Zweck der Erfüllung der Verpflichtungen aus dem Vertrag eingesetzt werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die bereits rechtmäßig bekannt sind oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.

.....
Ort, Datum

.....
Unterschrift / Firmenstempel
Name in Druckbuchstaben



Polizeiverwaltungsamt

Neuländer Str. 60 | 01129 Dresden

Telefon: +49 (0351) 8501 0

Telefax: +49 (0351) 8501 106

E-Mail: pva@polizei.sachsen.de

Internet: www.polizei.sachsen.de