Asseco CEIT, a. s.
info@asseco-ceit.com
Univerzitná 8661/6A, 010 08 Žilina
Slowakische Republik
+421 (0)41 513 7401
+421 (0)41 513 9290

Regeln für sicherheitsrelevante Lieferanten

Mit dem sicherheitsrelevanten Lieferanten muss eine Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) zur Wahrung der Vertraulichkeit und Sicherheit der bereitgestellten Informationen, Dokumente und Geräte abgeschlossen werden. Im Falle eines Verstoßes gegen diesen Vertrag trägt der Lieferant die sich aus diesem Vertrag ergebenden Folgen (Vertragsstrafe, Schadenersatz).
Der Anbieter muss über ein Informationssicherheitsmanagementsystem verfügen (eine Zertifizierung ist nicht erforderlich).

a) Aufstellung und Genehmigung einer Sicherheitspolitik, die die Sicherheit von Daten und Informationen abdeckt, die beim Lieferanten im Zuge der Erbringung des Leistungsgegenstandes erzeugt und verarbeitet werden können. Die Sicherheitspolitik muss die Leitprinzipien, Ziele, Sicherheitsanforderungen, Rechte und Verantwortlichkeiten in Bezug auf das Informationssicherheitsmanagement enthalten.
b) Bewältigung eigener Risiken, die eine Erbringung des Leistungsgegenstands beeinflussen können.
c) Auf der Grundlage des Sicherheitsbedarfs und der Ergebnisse der Risikobewertung geeignete Sicherheitsmaßnahmen im Rahmen des vorgesehenen Leistungsgegenstandes umsetzen, überwachen und deren Wirksamkeit bewerten.
d) Festlegung und Aufrechterhaltung aktueller Sicherheitsmaßnahmen in Form von Verfahren und Technologien, die die Einhaltung der Sicherheitspolitik gewährleisten.
e) Aufzeichnungen über die Erstellung und Verarbeitung von Daten und Informationen im Rahmen des erbrachten Leistungsgegenstandes führen, alle wesentlichen Umstände, die mit der Gewährleistung der Sicherheit dieser Daten und Informationen zusammenhängen, aufzeichnen und diese Aufzeichnungen der Asseco CEIT, a. s. auf Anfrage zur Verfügung stellen.
f) Wenn er sich bei der Erbringung des Leistungsgegenstandes eines Subunternehmers bedient, die angemessene Einhaltung dieser Sicherheitsanforderungen auch in den vertraglichen Beziehungen mit seinen Subunternehmern zu gewährleisten.

1 Sicherheit der Humanressourcen

1.1 Der sicherheitsrelevante Lieferant und dessen eventuelle Subunternehmen sind verpflichtet, die folgenden Maßnahmen in ihren internen Prozessen zu gewährleisten:

a) verfügt über einen Entwicklungsplan für das Sicherheitsbewusstsein, um eine angemessene Fortbildung und Verbesserung des Sicherheitsbewusstseins zu gewährleisten, der einschließt:
    - Unterweisung von Benutzern, Administratoren, Inhabern von Sicherheitsrollen und Subunternehmern in ihren Verantwortlichkeiten und in der Sicherheitspolitik;
    - theoretische und praktische Schulung von Benutzern, Administratoren und Inhabern von Sicherheitsrollen;
b) er hat Personen benannt, die für die Durchführung jeder der im Plan aufgeführten Aktivitäten verantwortlich sind;

c) im Einklang mit dem Entwicklungsplan für das Sicherheitsbewusstsein sicherstellen, dass Benutzer, Administratoren, Inhaber von Sicherheitsrollen und Lieferanten durch anfängliche und regelmäßige Schulungen über ihre Verantwortlichkeiten und die Sicherheitspolitik unterrichtet werden;
d) er führt regelmäßige Schulungen für die Inhaber von Sicherheitsrollen gemäß dem Plan zur Entwicklung des Sicherheitsbewusstseins auf der Grundlage der aktuellen Cybersicherheitserfordernisse durch;
e) er stellt im Einklang mit dem Entwicklungsplan für das Sicherheitsbewusstsein regelmäßige Schulungen und Überprüfungen des Sicherheitsbewusstseins der Mitarbeiter entsprechend ihrer Stellenbeschreibung sicher;
f) er stellt die Einhaltung der Sicherheitsrichtlinien seitens der Benutzer, Administratoren und Inhaber von Sicherheitsrollen sicher;
g) im Falle der Beendigung des Vertragsverhältnisses mit Administratoren und Inhabern von Sicherheitsrollen stellt er die Übertragung der Zuständigkeiten sicher;
h) er legt Regeln und Verfahren für den Umgang mit Verstößen gegen die festgelegten Sicherheitsregeln durch Benutzer, Administratoren und Inhaber von Sicherheitsrollen fest;
i) er führt Aufzeichnungen über die durchgeführten Schulungen, welche den Gegenstand der Schulung und eine Liste der Personen, die an der Schulung teilgenommen haben, enthalten müssen.

1.2 Asseco CEIT, a.s. behält sich das Recht vor, Aufzeichnungen zu führen und die Tätigkeit des Lieferanten zu überprüfen, sowie Aufzeichnungen über Zwischenfälle und unübliche Handlungen von Mitarbeitern und anderen Personen, die für den Lieferanten tätig sind, zu führen. Auf der Grundlage dieser Aufzeichnungen ist das Unternehmen befugt, die Vertrauenswürdigkeit und Zuverlässigkeit der Mitarbeiter des Lieferanten zu beurteilen. Im Falle eines festgestellten Risikos informiert Asseco CEIT, a.s. den Lieferanten über die Nichteinhaltung und beide Parteien nehmen Verhandlungen auf, um die Situation zu lösen.
1.3 Die Qualifikation der Mitarbeiter des Lieferanten muss der Position angemessen sein (ausgeführte Arbeit und Sicherheitsstufe).

2 Physische Sicherheit, Brandschutz und Arbeitsschutz

Der Lieferant ist als Arbeitgeber für die Einhaltung der Arbeitsschutzbestimmungen durch seine Mitarbeiter und andere natürliche Personen, die Arbeiten für den Lieferanten ausführen, sowie für die Einhaltung der Bedingungen für den Zutritt von Personen auf das Gelände von Asseco CEIT, a.s. bei der Ausführung von Arbeiten am Leistungsgegenstand verantwortlich.

3 Management des IS-Betriebs

Der Lieferant verpflichtet sich:

a. Gewährleistung des sicheren Betriebs eines Informationssystems und einer Infrastruktur, die für die Erbringung des Leistungsgegenstands verwendet werden.
b. Auf Anfrage der Asseco CEIT, a.s. einen Überblick über die bei seinem Informationssystem und seiner Infrastruktur (in der sie den Vertragsgegenstand leisten).
c. Sicherstellen, dass für die Erbringung des Leistungsgegenstandes nur Anwendungen und Technologien verwendet werden, die den geltenden slowakischen und europäischen Rechtsvorschriften, insbesondere hinsichtlich der Lizenzbedingungen, des Urheberrechts und der mit dem Urheberrecht verbundenen Rechte sowie der Änderung bestimmter Gesetze (Urheberrechtsgesetz) in der jeweils geltenden Fassung, entsprechen.

4 Zugangskontrolle

4.1 Identifizierung:

a. Jeder Arbeitnehmer des Lieferanten, der an der Erfüllung des Vertrages beteiligt ist und die EDV-Ressourcen des Lieferanten nutzt, muss über ein eigenes, eindeutiges Benutzerkonto verfügen, das in seiner IT-Infrastruktur registriert und gepflegt wird und dem bestimmte Rollen in den einzelnen vorgesehenen Systemen, Modulen oder Anwendungen zugewiesen werden. Jeder Arbeitnehmer des Lieferanten muss mit gültigen Identifikationsdaten und aktuellen Kontaktdaten geführt werden.
b. Jeder Arbeitnehmer des Lieferanten, der auf die internen Systeme der Asseco CEIT, a.s. zugreift, hat ein eindeutiges, bei Asseco CEIT, a.s. angelegtes Benutzerkonto, dem in den einzelnen Systemen, Modulen oder Anwendungen spezifische Rollen zugewiesen sind, die sich ausschließlich auf die Erfüllung des Vertragsgegenstandes beziehen.

4.2 Authentifizierung

4.2.1 Bedingungen für die Authentifizierung bei der Nutzung der ICT-Infrastruktur von Asseco CEIT, a.s.

a. Die Multi-Faktor-Authentifizierung wird zur eindeutigen Identifizierung privilegierter Benutzer bestimmter Systeme verwendet.
b. Passwort-Authentifizierung - wenn es nicht möglich ist, eine eindeutige Identifizierung privilegierter Benutzer durch mehrere Faktoren zu verwenden, wird die Authentifizierung mit kryptografischen Schlüsseln, die ein ähnliches Sicherheitsniveau garantieren, oder die Verwendung eines Passworts mit den erforderlichen Regeln verwendet.

4.2.2 Für den Fernzugriff der Arbeitnehmer des Lieferanten reicht der Lieferant Unterlagen zum Ausfüllen des Fernzugriffsantrags ein, anhand derer dann die Parameter des sicheren Fernzugriffs festgelegt werden.

a. der Antrag wird intern bei Asseco CEIT, a.s. von der verantwortlichen Person des jeweiligen vorgesehenen Systems von Asseco CEIT, a.s. für den Lieferanten ausgefüllt (Auf der Grundlage der Angaben der Kontaktperson des Lieferanten).
b. Nach der Bearbeitung des Antrags wird der Arbeitnehmer des Lieferanten individuell über die Einzelheiten der Fernzugriffsregeln informiert und erhält die Authentifizierungsdaten.

4.2.3 Der Lieferant ist für die Aktivitäten seiner Arbeitnehmer oder anderer zu seinen Gunsten beschäftigter natürlicher Personen verantwortlich, die mit den Sicherheitsvorschriften und anderen klärenden Sicherheitsinformationen, die von Asseco CEIT, a.s. auf Anfrage des Lieferanten nachweislich zur Verfügung gestellt werden, übereinstimmen müssen. Alle Schäden, die sich aus der Verletzung dieser und anderer Sicherheitsinformationen durch die Arbeitnehmer des Lieferanten oder andere Personen, die für den Lieferanten arbeiten, ergeben, gehen zu Lasten des Lieferanten, der verpflichtet ist, die Asseco CEIT, a.s. für diese Schäden vollständig zu entschädigen.

4.3 Autorisierung

4.3.1 Die Arbeitnehmer des Lieferanten sind verpflichtet, privilegierte Berechtigungen in der ICT-Infrastruktur von Asseco CEIT, a.s. nur in angemessenem Umfang und nur für den Zeitraum zu nutzen, der für die Ausübung von Tätigkeiten im Einklang mit der Erfüllung des Vertragsgegenstandes unbedingt erforderlich ist. Weder Benutzer noch Administratoren dürfen Konten mit privilegierten Rechten für Routinearbeiten verwenden, die nichts mit der Verwaltung des betreffenden Systems zu tun haben.

4.3.2 Die Arbeitnehmer des Lieferanten werden von Asseco CEIT, a.s. darüber informiert, zu welchen geschützten Informationen von Asseco CEIT, a.s. sie Zugang haben und wie sie darüber verfügen können. Jegliche Manipulationen und andere Operationen mit geschützten Informationen von Asseco CEIT, a.s., die nicht ausdrücklich in den Anweisungen angegeben sind, sind dem Lieferanten nicht erlaubt.

4.4 Bedingungen für den Fernzugriff

4.4.1 Für den Zugang zu den Informationssystemen von Asseco CEIT, a.s. werden standardgemäß den Mittel von Asseco CEIT, a.s. verwendet (HW, SW). Der Zugang der Computerausrüstung des Lieferanten (PCs, Laptops) zu geschützten internen Informationen und zu Informations- und Telekommunikationssystemen unterliegt der Genehmigung der ICT-Abteilung von Asseco CEIT, a.s. und des zuständigen Systemadministrators (Garantiegebers).

4.4.2 Die Arbeitsstationen der Lieferanten, die über VPN ankommen, müssen:

a. über einen fortschrittlichen funktionalen Virenschutz (mit aktiviertem Echtzeitschutz) verfügen;
b. über eine funktionierende persönliche Firewall verfügen;
c. automatische/verwaltete Aktualisierungen des Betriebssystems eingerichtet haben;
d. über ein Betriebssystem verfügen, für das der Support noch nicht beendet ist;
e. in einer Linux-Umgebung ähnliche Bedingungen haben wie oben für Windows definiert - AV, FW, UPDATE, OS.;
f. in der Endstation die Identifikations- und Autorisierungselemente speichern, die vom festgelegten Mitarbeiter der Asseco CEIT, a.s. bereitgestellt werden;
g. einen VPN-Client installieren, der ausschließlich auf Kosten des Lieferanten installiert wird;
h. über einen zweiten Faktor (HW- oder SMS-Token) für den VPN-Zugang verfügen; dieser wird den festgelegten Mitarbeitern zur Verfügung gestellt;
i. Anwendungen von Drittanbietern aktualisiert haben, ohne das Urheberrecht zu verletzen.

5 ÄNDERUNGSMANAGEMENT

Änderungen auf der Seite des Lieferanten müssen unter Berücksichtigung der Kritikalität von Informationen, Systemen und Prozessen sowie durch eine Neubewertung der Risiken verwaltet werden. Der Lieferant verpflichtet sich:

a) Vertragsveränderungen zu verwalten und zu erfassen.
b) Änderungen bei den erbrachten Dienstleistungen in Übereinstimmung mit den Empfehlungen der Standardregelungen für die Informationssicherheit zu verwalten und zu erfassen.

6 Akquisition, Entwicklung, Wartung

Der Lieferant verpflichtet sich, die sichere Implementierung, Innovation, Aktualisierung und Prüfung der Technologien, die Gegenstand der Leistung sind, zu gewährleisten und der Asseco CEIT, a.s. die Dokumentation des Leistungsgegenstandes mindestens im folgenden Umfang zu liefern:

a) Bestandspläne,
b) die Unterlagen aller Sicherheitseinstellungen, Funktionen und Mechanismen,
c) eine Dokumentation, die eine Beschreibung des Autorisierungskonzepts und der Zulassung enthält,
d) eine Dokumentation mit Sicherungs- und Archivierungsverfahren,
e) eine Dokumentation mit Installations- und Konfigurationsverfahren
f) eine Dokumentation einschließlich Schwachstellentests und Einhaltung der Sicherheitsanforderungen von Asseco CEIT, a.s.
g) eine Dokumentation zur Gewährleistung der Geschäftskontinuität und der Wiederherstellung nach einem Notfall.

Im Falle der Entwicklung von Lösungen verpflichtet sich der Lieferant:

a. zur Einhaltung und Umsetzung der besten Praktiken für die sichere Softwareentwicklung.
b. Ist die Lieferung des Quellcodes der Lösung Teil der vertraglichen Leistung, so ist ein Audit der erbrachten oder zu erbringenden Leistung zu ermöglichen, insbesondere um zu überprüfen, ob die Leistung vertragsgemäß erbracht wurde.
c. Stellen Sie sicher, dass die Leistung nur die Komponenten enthält, die für den ordnungsgemäßen Betrieb der Lösung objektiv erforderlich sind und/oder die im Vertrag ausdrücklich genannt sind (insbesondere, dass die Lösung keine unnötigen Komponenten, keine Softwaremuster usw. enthält).
d. Falls die Leistung auch die Installation eines Betriebssystems oder einer Fremdsoftware umfasst, ist bei der Installation darauf zu achten, dass die vorgeschriebenen Versionen dieser Produkte verwendet werden, die mit der Umgebung von Asseco CEIT, a.s. kompatibel und funktionsfähig sind.
e. zur Gewährleistung der Sicherheit der Testumgebung beim Lieferanten und des Schutzes der von Asseco CEIT, a.s. bereitgestellten Testdaten.

f. zur Sicherstellung, dass nur der im Vertragsgegenstand spezifizierte kompilierte oder ausführbare Code und andere für den Betrieb des Leistungsgegenstandes notwendige Daten in die Produktionsumgebung der Asseco CEIT, a.s. geliefert werden
g. zur Sicherstellung, dass die im Rahmen der Dienstleistung gelieferte Lösung mit den Empfehlungen der Informationssicherheitsstandards übereinstimmt.
h. dem Kunden die notwendige Unterstützung zu gewähren, falls der Kunde Sicherheitstests im Zusammenhang mit dem Leistungsgegenstand verlangt / durchführt. Verlangt der Besteller vom Lieferanten eine Bestätigung über die Durchführung von Sicherheitsprüfungen, so ist dies in einer gesonderten vertraglichen Vereinbarung zu regeln.
i. zur Übergabe des Quellcodes an die Asseco CEIT, a.s., falls im Vertrag festgelegt, in einer sicheren Form mit der Sicherstellung seiner Integrität.
j. zur Sicherstellung der Versionsverwaltung des Quellcodes.
k. zur Sicherstellung, dass der Quellcode gesichert und außerhalb der Produktionsumgebung gespeichert wird.
l. zur Sicherstellung, dass die Quellcodeverteilung eine Datei aus der Entwicklungsumgebung für die kontrollierte Kompilierung dieser Quellcodes enthält
m. in der Umgebung von Asseco CEIT, a.s. keinen Programmcode zu entwickeln, zu kompilieren oder zu verbreiten, der zur illegalen Kontrolle, Beeinträchtigung der Verfügbarkeit, Vertraulichkeit oder Integrität oder zur unbefugten oder illegalen Beschaffung von Daten und Informationen bestimmt ist.

7 Monitoring

a) Der Zugang der Arbeitnehmer des Lieferanten zu ausgewählten geschützten internen Informationen und zu den Informations- und Kommunikationssystemen von Asseco CEIT, a.s. wird kontinuierlich erfasst, überwacht und ausgewertet. Ereignisse in den Systemen werden von Asseco CEIT, a.s. in Logs aufgezeichnet.
b) Der Lieferant ist verpflichtet, seine IKT-Infrastruktur kontinuierlich auf veröffentlichte und bekannte Sicherheitslücken zu überwachen, die den reibungslosen und sicheren Betrieb der Systeme im Zusammenhang mit den von ihm erbrachten Dienstleistungen beeinträchtigen können. Dazu gehören Sicherheitslücken in Betriebssystemen, Software von Drittanbietern, Webkomponenten usw.

8 Schutz von Medien

a. Die Speicherung geschützter Informationen von Asseco CEIT, a.s. auf tragbaren Datenträgern und der Transport von Datenträgern außerhalb der Räumlichkeiten von Asseco CEIT, a.s. bedürfen seiner Zustimmung.
b. Im Falle der Speicherung geschützter Informationen von Asseco CEIT, a.s. auf tragbaren Datenträgern ist der Lieferant verpflichtet, soweit technisch möglich, diese Daten in

verschlüsselter Form zu speichern oder deren Speicherung zu verlangen und Aufzeichnungen über diese Datenträger zu führen.

c. Der Lieferant ist verpflichtet, für die Vernichtung von Betriebsdaten, die geschützte Informationen der Asseco CEIT, a.s. enthalten, unmittelbar nach Ablauf des Zwecks ihrer Verarbeitung und/oder Speicherung zu sorgen. Sind die Daten auf dem elektronischen Datenträger erst einmal zerstört, dürfen die Informationen nicht mehr wiederherstellbar sein. Der Lieferant muss ein Protokoll über die Datenvernichtung führen.

9 Cyber-Vorfälle

Der Lieferant ist verpflichtet, alle vermuteten Cyber-Vorfälle zu melden:

a. dem Verantwortlichen von Asseco CEIT, a.s.
b. innerhalb des Zeitrahmens unmittelbar (ohne Verzögerung) nach der Entdeckung des Cybersicherheitsvorfalls/der Störung.
c. per E-Mail, per Telefon mit Gesprächsaufzeichnung auf beiden Seiten oder persönlich.
d. mit Beschreibung:
    - des Datums und der Uhrzeit, zu der der Vorfall festgestellt wurde;
    - des Charakters des Vorfalls;
    - der Quelle des Vorfalls;
    - der Ziels/der Opfer des Vorfalls;
    - dem potenziellen Einfluss.

10 Kundenprüfung

10.1 Berechtigung zur Durchführung einer Prüfung

a. Asseco CEIT, a.s. behält sich das Recht vor, den Lieferanten zu überprüfen.
b. Asseco CEIT, a.s. informiert den Lieferanten mindestens 5 Arbeitstage im Voraus über seine Absicht, eine Prüfung durchzuführen. Beide Parteien vereinbaren den Inhalt, die notwendige Zusammenarbeit und den Zeitplan der Prüfung, wobei Asseco CEIT, a.s. sich verpflichtet, so vorzugehen, dass die betrieblichen Bedürfnisse des Lieferanten nicht beeinträchtigt werden.
c. Asseco CEIT, a.s. behält sich das Recht vor, bei Vorliegen schwerwiegender Gründe (z.B. Verdacht auf risikoreiches Verhalten des Lieferanten) im Zusammenhang mit der Vertragserfüllung unter Berücksichtigung der betrieblichen Situation des Lieferanten eine unangekündigte Prüfung beim Lieferanten durchzuführen.
d. Wenn Nichtkonformitäten festgestellt werden, legt der Auditor/Inspektor Abhilfemaßnahmen für die festgestellten Mängel und einen Termin für deren Umsetzung fest. Der Lieferant ist verpflichtet, die Abhilfemaßnahmen im Rahmen der festgelegten Maßnahme und innerhalb des geforderten Zeitrahmens durchzuführen.
e. Die Dokumentation der von Asseco CEIT, a.s. durchgeführten Prüfungen wird in der für die Prüfungen zuständigen Abteilung aufbewahrt. Datensätze, die sich auf ein bestimmtes Audit

beziehen, werden immer mit demselben Identifikator gekennzeichnet. Die einzelnen Prüfungsaufzeichnungen bestehen aus:

- dem Prüfungsplan;
- der Prüfungsmitteilung;
- dem Fragebogen zur Prüfung (Liste mit Fragen des Prüfers, wenn es der Prüfung für angemessen hält);
- Prüfungsbericht;
- schriftliche, fotografische oder sonstige Aufzeichnungen von Vorgängen, Verfahren oder Ausrüstungen, die für die Prüfung relevant sind (sofern dies zur Dokumentation der Feststellungen erforderlich ist);
- eine Aufzeichnung der Feststellungen (Abhilfemaßnahmen und einer nachfolgenden Kontrolle).

f. Die geprüfte Partei (Lieferant) erhält einen abschließenden Prüfbericht mit allen eventuellen Feststellungen zur Stellungnahme:
   - Auf der Grundlage der im abschließenden Prüfbericht dargelegten Feststellungen schlägt der Lieferant Maßnahmenentwürfe und Fristen für Lösungen vor und legt der Asseco CEIT, a.s. eine Liste mit diesen Maßnahmen zur Genehmigung vor;
   - Asseco CEIT, a.s. wird seine Zustimmung zu den vorgeschlagenen Maßnahmen bestätigen.

10.2 Abhilfemaßnahmen

a. Die geprüfte Partei (Lieferant) ist verpflichtet, dafür zu sorgen, dass die vereinbarten Abhilfemaßnahmen innerhalb der vorgegebenen Zeit umgesetzt werden.
b. Der Bericht über die durchgeführten Maßnahmen ist vom Lieferanten der Asseco CEIT, a.s. zu übermitteln und vorzulegen.

11 Schutz der Vermögenswerte vor unbefugten Aktivitäten

Der Lieferant darf auf dem Vermögen von Asseco CEIT, a. s. keine Tools installieren oder verwenden, die nicht Teil des Leistungsgegenstandes sind.

12 Bedingungen für die Beendigung des Vertrags

a. Im Falle der Beendigung des Vertragsverhältnisses muss jeglicher Zugang des Lieferanten und seiner Mitarbeiter zu den Vermögenswerten von Asseco CEIT, a.s. (VPN, Systeme, Informationen) spätestens zum Zeitpunkt der Beendigung des Vertragsverhältnisses beendet werden.
b. Wurden den Arbeitnehmern des Lieferanten Vermögenswerte der Asseco CEIT, a.s. zur Verfügung gestellt, so sind diese spätestens zum Zeitpunkt der Beendigung des Vertragsverhältnisses zurückzugeben.

c. Wenn den Lieferanten Informationswerte (Daten) von Asseco CEIT, a.s. bereitgestellt wurden, müssen diese spätestens bis zum Termin der Beendigung des Vertragsverhältnisses zurückgegeben und ohne die Möglichkeit einer Erneuerung restlos aus allen Systemen des Lieferanten und von allen Datenträgern des Lieferanten gelöscht werden.
d. Bei einer vorzeitigen Beendigung des Vertragsverhältnisses auf andere Weise als durch Erfüllung der Verpflichtung (z.B. durch Kündigung, Rücktritt vom Vertrag, Vereinbarung über die Beendigung des Vertrages usw.) können die Zugänge des Lieferanten durch Asseco CEIT, a.s. gegebenenfalls vor Ablauf der Laufzeit des Vertragsverhältnisses beendet werden.