Anlage „Datenschutz, Datensicherheit und Cyber-Security“

1 Datenschutz

Der Auftragnehmer ist verpflichtet, das österreichische Datenschutzgesetz idF BGBl. I Nr. 14/2019 und die Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) und alle sonstigen in Österreich geltenden datenschutzrechtlichen Bestimmungen in der jeweils geltenden Fassung einzuhalten. Dazu gehört auch eine etwaige Verpflichtung zur Bestellung eines Datenschutzbeauftragten.

Der Auftragnehmer verpflichtet sich, Mitarbeiter sowie sämtliche Subunternehmer die mit personenbezogenen Daten, welche der Auftraggeber verarbeitet, in Berührung kommen gemäß § 6 DSG schriftlich zur Einhaltung der vereinbarten Datenschutzmaßnahmen sowie zur Geheimhaltung aller Informationen zu verpflichten.

Der Auftragnehmer wird den Auftraggeber über

- Verstöße des Auftragnehmers bzw seiner Mitarbeiter gegen datenschutzrechtliche Bestimmungen oder in diesem Vertrag definierte Pflichten betreffend den Datenschutz und Datensicherheit,
- den Verdacht auf derartige Verstöße sowie
- Unregelmäßigkeiten und Rechtswidrigkeiten bei der Verwendung personenbezogener Daten im Rahmen dieses Vertragsverhältnisses

unverzüglich schriftlich informieren.

Der Auftragnehmer wird durch entsprechende vertragliche Regelungen Sorge dafür tragen, dass die oben angeführte Geheimhaltungspflicht / Treuepflicht sowie die datenschutzrechtlichen Pflichten von allen seinen Mitarbeitern, einschließlich aller Gehilfen, und allfälligen Subunternehmern erfüllt werden. Diese Verpflichtung gilt örtlich und zeitlich unbeschränkt und auch gegenüber allfälligen mit dem Auftragnehmer verbundenen Unternehmen sowie sämtlichen Gehilfen. Die Haftung des Auftragnehmers für seine Mitarbeiter und allfällige Subunternehmer wird dadurch nicht eingeschränkt.

1.1 Auftragsverarbeitung

Beauftragt der Auftraggeber den Auftragnehmer mit der Verarbeitung personenbezogener Daten (Auftragsverarbeitung), so werden der Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung sowie die Kategorien an verarbeiteten personenbezogenen Daten nach Betroffenen bzw. Betroffenengruppen und Datenarten sowie etwaige dabei eingesetzte Subauftragsverarbeiter gesondert festgelegt und dokumentiert.

Zu diesem Zweck wird der Auftraggeber mit dem Auftragnehmer vor Beginn der jeweiligen Leistungserbringung eine gesonderte Auftragsverarbeitungsvereinbarung abschließen (siehe dazu als Muster Anlage „Muster Auftragsverarbeitung des Auftraggebers“ (AVV) unter dem Link [https://www.apg.at/ueber-uns/die-apg/einkauf/, die aber zu Projektbeginn noch jeweils entsprechend angepasst wird).

Der konkrete Inhalt der AVV wird vor Beginn der Leistungserbringung detailliert. Den Auftragnehmer treffen entsprechende Mitwirkungspflichten (zB Bekanntgabe der konkreten TOMs des Auftragnehmers, Informationen für das Verarbeitungsverzeichnis des Auftraggebers usw), die nicht gesondert vergütet werden.

Insbesondere wird der Auftragnehmer im Rahmen der Auftragsverarbeitung

a) die vom Auftraggeber in Erfüllung des Vertrags zur Verfügung gestellten personenbezogenen Daten nur auf schriftliche Weisung des Auftraggebers und nur in dem Umfang verarbeiten, als die Verarbeitung zum Erreichen des Vertragszweckes erforderlich ist;

b) ein Verzeichnis zu allen Kategorien der von ihm durchgeführten Tätigkeiten gemäß Art 30 Abs 2 DSGVO führen;

c) dem Auftraggeber auf Aufforderung unverzüglich alle Informationen zur Verfügung stellen, damit dieser seiner Rechenschaftspflicht gemäß Art 5 Abs 2 DSGVO, ihren Informationspflichten nach den Art 13 und 14 DSGVO sowie seiner Auskunftspflicht nach Art 15 DSGVO, ihrer Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art 30 Abs 1 DSGVO und gegebenenfalls ihrer Pflicht zur Durchführung einer Datenschutzfolgeabschätzung gemäß Art 35 DSGVO entsprechen kann;

d) auf Aufforderung des Auftraggebers unverzüglich die erforderlichen Schritte im System des Auftragnehmers zur Berichtigung oder Löschung personenbezogener Daten nach den Art 16 und 17 DSGVO oder Einschränkung der Verarbeitung nach Art 18 DSGVO setzen;

e) auf Aufforderung des Auftraggebers unverzüglich eine Übertragung von Daten gemäß Art 20 DSGVO veranlassen;

f) auf Aufforderung des Auftraggebers unverzüglich die Verarbeitung von Daten infolge eines Widerspruches gemäß Art 21 DSGVO einstellen;

g) im Falle einer Verletzung / Verstoßes des Schutzes personenbezogener Daten (sei es durch den Auftragnehmer, seine Mitarbeiter, einschließlich aller Gehilfen) diese / diesen unverzüglich dem Auftraggeber unter Bekanntgabe aller nach Art 33 Abs 3 DSGVO vorgesehener Informationen schriftlich melden.

Eine außerhalb dokumentierter Weisungen des Auftraggebers liegende Verarbeitung personenbezogener Daten oder Offenlegung von Informationen gegenüber Dritten durch den Auftragnehmer ist unzulässig, außer der Auftragnehmer ist aufgrund einer zwingenden gesetzlichen Bestimmung eines EU-Mitgliedstaats über die festgelegten Tätigkeiten hinaus zu einer bestimmten Verarbeitung (insbesondere zur Offenlegung) verpflichtet. In diesem Fall teilt der Auftragnehmer dies dem Auftraggeber zeitgerecht vor Durchführung der Verarbeitung mit. Die Verständigung kann nur dann unterbleiben, wenn das Gesetz des EU-Mitgliedstaats diese aufgrund eines zwingenden öffentlichen Interesses verbietet.

Der Auftragnehmer erklärt, dass er seines Wissens nach keinen Gesetzen aus Drittstaaten unterliegt, die ihm die Befolgung des vorgehenden Absatzes unmöglich machen. Der Auftragnehmer teilt dem Auftraggeber jede Gesetzesänderung, die ihm die Befolgung des vorgehenden Absatzes voraussichtlich unmöglich macht, schriftlich mit.

Der Auftraggeber ist über jede Form der Verlagerung der Datenverarbeitung (dazu zählt auch die Verlegung des Sitzes des Auftragnehmers) in ein Drittland (sohin außerhalb der EU oder des EWR) schriftlich zu informieren (siehe im Detail Punkt 1.2). Davon unabhängig darf eine Verlagerung der Datenverarbeitung nur (i) unter Einhaltung der in Kapitel V der DSGVO festgesetzten Bedingungen und (ii) unter Bestellung eines verantwortlichen Ansprechpartners in der EU gemäß Art 27 DSGVO (wenn der Auftragnehmer seinen Sitz in ein Drittland verlegt) erfolgen.

Wird die Auftragsverarbeitung beendet, ist der Auftragnehmer nach Beendigung der Tätigkeit für den Auftraggeber verpflichtet, sämtliche Informationen einschließlich Unterlagen, die Informationen enthalten, nach freier Wahl des Auftraggebers entweder diesem zur Gänze zu übergeben, oder auftragsgemäß zur Gänze zu löschen, sofern und soweit nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Sowohl die Übergabe wie auch die Löschung hat in einer Weise zu erfolgen, dass eine auch bloß teilweise Wiederherstellung der übergebenen bzw gelöschten Daten nicht oder nur mit technisch und wirtschaftlich unvertretbarem Aufwand möglich ist. Der Auftragnehmer hat dem Auftraggeber die ordnungsgemäße Durchführung der Datenübertragung bzw Datenlöschung schriftlich zu bestätigen und nachzuweisen.

1.1.1 Auftragsverarbeitung unter Einsatz von Subauftragnehmern

Im Fall einer Auftragsverarbeitung unter Einsatz von Subauftragnehmern finden die Bestimmungen über die Auftragsverarbeitung (Punkt 1.1) und den Einsatz von Subunternehmern aus den jeweils anwendbaren AEB mit nachfolgenden Ergänzungen Anwendung:

Der Auftragnehmer wird nur solche Subauftragnehmer auswählen, die aufgrund der von ihnen getroffenen und gegenüber dem Auftraggeber dokumentierten technischen und organisatorischen Maßnahmen dazu geeignet und auch verpflichtet sind, die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der DSGVO und dieser Vereinbarung durchzuführen.

Dazu muss der Auftragnehmer insbesondere auch sicherstellen, dass der Auftraggeber die ihm gegenüber dem Auftragnehmer zustehenden Kontrollrechte und sonstigen Rechte im gleichen Maß auch direkt gegenüber dem Subauftragnehmer sinngemäß ausüben kann, und dass der Subauftragnehmer gegenüber dem Auftraggeber sinngemäß denselben Datenschutzpflichten und sonstigen Pflichten unterliegt, denen der Auftragnehmer nach diesem Vertrag unterliegt.

In diesem Zusammenhang ist der Auftraggeber, bei Vorliegen eines berechtigten Interesses, insbesondere berechtigt, jederzeit Einsicht in die zwischen dem Auftragnehmer und dem Subauftragsnehmer abgeschlossenen Verträge zu nehmen bzw durch vom Auftraggeber bestimmte Dritte nehmen zu lassen und die gegenüber dem Auftragnehmer festgelegten Kontrollrechte sinngemäß auch gegenüber dem Subauftragnehmer auszuüben.

Die Verantwortlichkeiten des Auftragnehmers und des Subauftragnehmers sind eindeutig voneinander abzugrenzen.

Der Auftragnehmer hat die Einhaltung der den/die Subauftragnehmer nach diesem Vertrag treffenden Datenschutz- und Informationssicherheitspflichten vor Beginn der Tätigkeit für den Auftragnehmer und danach regelmäßig zu prüfen. Die Ergebnisse sämtlicher Prüfungen sind nachvollziehbar und vollständig zu dokumentieren und bei Vorliegen eines berechtigten Interesses über Anfrage des Auftraggebers diesem uneingeschränkt vorzulegen. Sollte der Auftragnehmer im Rahmen dieser Prüfung zur Kenntnis gelangen, dass der Subauftragnehmer die ihn nach diesem Vertrag treffenden Datenschutz- und Informationssicherheitspflichten nicht oder nicht ausreichend erfüllt, so hat er den Auftraggeber unaufgefordert und umgehend darüber zu informieren.

Bei Beendigung der Auftragsverarbeitung hat der Auftragnehmer die Löschung oder Übergabe der Daten durch den/die Subauftragnehmer herbeizuführen.

1.2 Datenübermittlung in ein Drittland

Die Speicherung und Verarbeitung personenbezogener Daten hat ausschließlich im EU/EWR-Raum zu erfolgen. Der Auftragnehmer garantiert, dass keine Daten in ein Drittland übermittelt werden. Dies gilt auch für etwaige Dienstleister des Auftragnehmers („onward transfer“).

Eine Datenübermittlung in ein Drittland ist nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers zulässig.

Im Falle einer Datenübermittlung in ein Drittland hat der Auftragnehmer im Sinne der Rechtsprechung des EuGH vom 16.7.2020 zu C-311/18, „Schrems II“, jedenfalls ein angemessenes Datenschutzniveau im Drittland durch den Abschluss von Standarddatenschutzklauseln (im Sinne des Art 46 Abs 2 lit c DSGVO) sowie die Ergreifung „zusätzlicher Maßnahmen“ im Sinne dieser Rechtsprechung sicherzustellen. Dies gilt solange sich keine andere Methodik zur Wahrung der Datenschutzrechte der betroffenen Personen im Drittland etabliert haben. Diese Maßnahmen sind – im Falle der Datenübermittlung in die USA – zusätzlich zum (derzeit) bestehenden EU-US Data Privacy Framework zu ergreifen

1.3 Erzeugte Daten und Informationspflichten bei verbundenen Diensten (sofern im Einzelfall anwendbar)

Die Bestimmungen der „Verordnung über harmonisierte Vorschriften für einen fairen Daten-zugang und eine faire Datennutzung (Datenverordnung)“ (Verordnung (EU) 2023/2854) sind, insoweit zutreffend, auf alle Leistungserbringungen des Auftragnehmers anwendbar, einschließlich vor Geltung der Verordnung am 12.9.2025.

Der Auftragnehmer wird die im Rahmen der Leistungserbringung herzustellenden verbundenen Dienste der Datenverordnung entsprechend konzipieren und herstellen. Verbundene Dienste werden so erbracht, dass die bei ihrer Nutzung erzeugten Daten (einschließlich erforderlicher Metadaten) standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind („data accessibility by design“). Der Auftragnehmer agiert dabei nach dem Stand der Technik und stellt sicher, dass der Auftraggeber, seinen Verpflichtungen, als Dateninhaber im Sinne der Datenverordnung, nachkommen kann.

Ein verbundener Dienst umfasst gemäß der Datenverordnung einen digitalen Dienst, einschließlich Software, der kein elektronischer Kommunikationsdienst ist und der so in ein vernetztes Produkt integriert oder so mit ihm verbunden ist, dass ohne ihn eine oder mehrere seiner Funktionen des vernetzten Produkts nicht ausgeführt werden könnten oder der später mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen.

Ein vernetztes Produkt gemäß der Datenverordnung ist ein körperlicher beweglicher Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist (primär IoT Geräte, die Umgebungs- oder Nutzungsdaten über eine Netzwerkverbindung übertragen können).

1.4 Sichere und datenschutzkonforme Leistungserbringung (sofern im Einzelfall anwendbar)

Bei den eingesetzten IT-Systemen ist auf größtmögliche Sicherheit der Applikationen, der Daten, sowie den Datenschutz Bedacht zu nehmen. Der Datenschutz ist durch Technikgestaltung („privacy by design“) und datenschutzfreundliche Voreinstellungen („privacy by default“) zu gewährleisten. Die individuellen Komponenten der Software sind so zu konzipieren, dass bekannte Angriffsmöglichkeiten ausgeschlossen sind.

Die Speicherung und Übermittlung personenbezogener Daten hat grundsätzlich verschlüsselt zu erfolgen. Weiter hat das System eine den Anforderungen der DSGVO entsprechende und nachweisliche Löschung personenbezogener Daten zu ermöglichen.

Ferner muss es bei Bedarf möglich sein, sämtliche Zugriffe protokollieren zu können; insbesondere muss der Zugriff auf Daten, die besonderen Kategorien personenbezogener Daten nach der DSGVO zuzuordnen sind, lückenlos nachvollziehbar sein.

Grobplanung, Detailplanung und Umsetzung haben unter Berücksichtigung der Einhaltung der datenschutzrechtlichen Grundsätze zu erfolgen; die Software wird gemäß diesen Grundsätzen (Art 25 DSGVO) konzipiert und implementiert. Dies umfasst insbesondere

- die Einhaltung des Grundsatzes der Datenminimierung (es werden nicht mehr Daten verarbeitet, als für die Zwecke der Verarbeitung erforderlich);

- die Sicherstellung, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweils bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden und nur den Personengruppen zugänglich sind, die sie für die Erfüllung ihrer Aufgaben benötigen;

- die Gewährleistung eines dem jeweiligen Grad der Sensibilität der Daten und dem dadurch gebotenen Schutz der Rechte und Freiheiten der Betroffenen entsprechenden Schutzniveaus;

- die Konzipierung der Systeme in einer Weise, die es dem Auftraggeber ermöglicht, seine datenschutzrechtlichen Pflichten (Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Übertragung, Meldung der Verletzung des Schutzes personenbezogener Daten) effizient erfüllen zu können.

- die Darstellung der technischen Sicherheitsmaßnahmen, um den Verlust von Daten bzw unbefugten Zugriff zu vermeiden.

Der Auftragnehmer gewährleistet über die Laufzeit des Vertrages die Einhaltung der Sicherheits- und „secure-coding"-Vorgaben, und üblicher Standards des Qualitätsmanagements, Risikomanagements und IT-Sicherheitsmanagements.

Die Auftraggeberin behält sich vor, Nachweise über das Qualitätsmanagementsystem, das IT-Sicherheitsmanagement sowie das Risikomanagement des Auftragnehmers und die Dokumentation über Qualitätsprüfungen zu verlangen (zB Qualitätsmanagementhandbuch).

1.5 Haftung

Der Auftragnehmer verpflichtet sich weiters, alle sonstigen datenschutzrechtlichen Bestimmungen Österreichs und der DSGVO einzuhalten und den Auftraggeber bei einer allfälligen Verletzung schad- und klaglos zu stellen.

2 Datensicherheit

Der Auftragnehmer verpflichtet sich insbesondere zu folgenden Maßnahmen zur Gewährleistung der Datensicherheit:

- Die Aufgabenverteilung bei der Datenverwendung ist zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen.
- Die Verwendung von Daten ist an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden.
- Jeder Mitarbeiter ist über seine nach dem Datenschutzgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren.
- Die Zutrittsberechtigung zu den Räumlichkeiten des Auftragnehmers ist zu regeln.
- Die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ist zu regeln.
- Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und jedes Gerät ist durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern.
- Es ist Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.
- Es ist eine Dokumentation über die gemäß den oben angeführten Punkten getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.
- Die Festlegung von Passwörtern hat gemäß dem Stand der Technik zu erfolgen; die Festlegung von Standardpasswörtern ist nicht zulässig.
- Sofern Systeme und Services über das Internet zugänglich sind, ist eine phishing-sichere zweistufige Authentifizierung, zumindest jedoch eine Multifaktor-Authentifizierung zu verwenden.

Erhält der Auftragnehmer Zugriff auf IT-Systeme des Auftraggebers, wird er die Nutzungsvereinbarung betreffend die IT des Auftraggebers unterzeichnen und deren Einhaltung gewährleisten.

Der Auftragnehmer verpflichtet sich weiters zur Einhaltung der Hausordnung und allfälliger Zutrittsregelungen des Auftraggebers.

Die Maßnahmen haben während der gesamten Vertragslaufzeit dem Stand der Technik zu entsprechen und im Rahmen der wirtschaftlichen Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger

Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Vom Auftragnehmer ist ein Schutzniveau zu gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Der Auftragnehmer wird dem Auftraggeber vor Projektstart und im Zuge des Projektes alle Informationen und Unterlagen zur Verfügung stellen, die erforderlich sind, um dem Auftraggeber die Prüfung der Gesetzeskonformität und Effektivität der gesetzten Maßnahmen zu ermöglichen und dem Auftraggeber auf Wunsch die Möglichkeit geben, sich vor Ort, im zumutbaren Rahmen, davon zu überzeugen, wobei die betrieblichen Abläufe beim Auftragnehmer möglichst wenig zu stören sind.

3 Cyber-Sicherheit

Der Auftragnehmer wird – soweit es im Einflussbereich des Auftragnehmers liegt – bei Erbringung seiner Leistungen einen „all-hazards approach“ verfolgen. So müssen IT-Systeme des Auftraggebers nicht nur gegen typische IT-bezogene Gefahren, wie Hackerangriffe oder Computerviren geschützt werden, sondern es sind auch ausreichende Vorkehrungen zum Schutz vor anderen Ereignissen, wie zB Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen zu treffen. In letzterem Fall wird der Auftragnehmer den Auftraggeber proaktiv beraten und Vorschläge übermitteln sowie bei der Umsetzung geeigneter Schutzmaßnahmen unterstützen. Erkennt der Auftragnehmer bei Leistungserbringung diesbezügliche Schutzlücken oder Optimierungspotential etc., wird er den Auftraggeber unaufgefordert hierüber nachweislich informieren.

Gleichzeitig muss auch der Auftragnehmer in ihrem Unternehmen diesen Ansatz verfolgen und entsprechende, effektive und zuverlässige Risikomanagementmaßnahmen setzen. Der Auftragnehmer sichert zu, ein ausreichendes Schutzniveau zu etablieren sowie aufrecht zu halten und so eine cybersicherheitsrechtliche Unbedenklichkeit zu gewährleisten.

Der Auftragnehmer ist weiters verpflichtet, die von der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) sowie zukünftig anwendbaren nationalen Umsetzungsgesetzen geforderten Risikomanagementmaßnahmen (Mindestmaßnahmen) auf seiner Ebene zu implementieren, sollten die bezogenen Services in den relevanten Anwendungsbereich fallen. Sofern in begründeten Fällen mit den Mindestmaßnahmen nicht das Auslangen gefunden werden kann, ist der Auftraggeber berechtigt, dem Auftragnehmer weitere Maßnahmen aufzutragen. Der Auftraggeber behält sich vor, die Leistungserbringung durch den Auftragnehmer bei Reduktion/Entfall des Entgeltsanspruchs einzuschränken oder zu unterbrechen, bis die Maßnahmen umgesetzt und ein entsprechendes Schutzniveau erreicht ist (cybersicherheitsrechtliche Unbedenklichkeit). Die Kosten hierfür (insbesondere für Kosten innerhalb der Lieferkette) trägt der Auftragnehmer.

Der Auftraggeber behält sich das Recht vor, einen schriftlichen Nachweis für Sicherheitsmaßnahmen entsprechend gesetzlicher Vorgaben (z.B. NISG) einzufordern, sofern ein entsprechender Anwendungsfall vorliegt.
Dazu werden auch Nachweise und Zertifizierungen basierend auf anerkannten Informationssicherheitsstandards wie z.B. ISO/IEC 27001 und KSÖ Cyber Risk Rating akzeptiert

Ergänzend behält sich der Auftraggeber zudem das Recht vor, Sicherheitsbewertungen und –Überprüfungen (Audits) durchzuführen, um die Einhaltung der voranstehenden Anforderungen an die Informationssicherheit zu überprüfen. Der Auftraggeber benachrichtigt den Lieferanten im Voraus und stellt sicher, dass das Audit während der normalen Geschäftszeiten und mit minimaler Unterbrechung des Geschäftsbetriebs des Lieferanten durchgeführt wird. Auf Anfrage muss der Lieferant die Einhaltung der hier aufgeführten Anforderungen schriftlich bestätigen und alle Fragen des Auftraggebers an den Lieferanten zu seinen Sicherheitsverfahren schriftlich beantworten.

(Vermutete) Cybersecurity-Vorfälle sind direkt unverzüglich an das Security Operation Center des Auftraggebers zu melden (https://www.apg.at/.well-known/security.txt). Weiters ist vom Auftragnehmer selbst eine Kontaktstelle für die Meldung von Cybersecurity-Vorfällen zu benennen.

Anlage:
„Muster Auftragsverarbeitung des Auftraggebers“ (AVV)