Ergänzende Bestimmungen zur Auftragsdatenverarbeitung

betreffend die zum Zeitpunkt der Unterzeichnung dieser Vereinbarung bestehenden Vertragsbeziehungen bzw. abgeschlossenen Produktverträge (einzeln jeweils „Hauptvertrag“) zwischen

_____

(Auftraggeber), Kundennummer **D**_____

und

QENTA Payment CEE GmbH (QENTA Payment CEE) (Auftragnehmer) (gemeinsam „Parteien“ oder jeweils einzeln „Partei“):

1. Allgemeines

1) Diese Vereinbarung wird mit Unterzeichnung integrierender Bestandteil des jeweiligen Hauptvertrages zwischen dem Kunden (Auftraggeber) und QENTA Payment CEE (Auftragnehmer).

2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers iSv Art 4 und Art 28 der EU-DSGVO (EU-Datenschutzgrundverordnung – Verordnung (EU) Nr. 2016/679). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

3) Im Sinne dieser Vereinbarung bezeichnet der Ausdruck

- „Personenbezogene Daten“ alle Informationen, die sich iSv Art 4 Nr. 1 EU-DSGVO auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen und nach Punkt 4 dieser Vereinbarung verarbeitet werden;
- „Datenverarbeitung“ oder „Verarbeitung“ iSv Art 4 Nr. 2 EU-DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- „Auftragsverarbeiter“ die QENTA Payment CEE als Auftragnehmer der Datenverarbeitung iSv Art 4 Nr. 8 EU-DSGVO;
- „Kunde“ den Kunden der QENTA Payment CEE, der als Auftraggeber der Datenverarbeitung ein Verantwortlicher iSv Art 4 Nr. 7 EU-DSGVO ist;
- „Endkunde“ den Kunden des Auftraggebers, der mittels Fernabsatz Produkte oder Dienstleistungen vom Auftraggeber bezieht;
- „Finanzdienstleister“ jeden Herausgeber, Anbieter oder Betreiber samt Lizenznehmern eines Zahlungsmittels oder Zahlungssystems (Kreditkartengesellschaften, Banken u.ä.);
- „Zahlungsdaten“ jene Informationen, die beim Fernabsatz-Kaufvorgang für die Bezahlung eines Produkts oder einer Dienstleistung vom Zahlungsauslösenden (Kunde oder Endkunde) für ein bestimmtes Zahlungsmittel eingegeben werden müssen (z.B. Kreditkartendaten, Bankverbindung);
- „Basislizenz“ die zum Zeitpunkt des Vertragsabschlusses des jeweiligen Hauptvertrages bestehenden Grundfunktionen und Inklusivleistungen des jeweiligen QENTA Produkts;
- „Zahlungsmittel“ ein zum Zeitpunkt des Vertragsabschlusses für das jeweilige QENTA Produkt verfügbares unbares Zahlungsinstrument (z.B. Kreditkarte, Online Banking Verfahren) zur Erteilung eines Zahlungsauftrages zwischen Zahler (Endkunde) und Zahlungsempfänger (Kunde);
- „Zusatzfeature“ eine zum Zeitpunkt des Vertragsabschlusses für das jeweilige QENTA Produkt optional zur Basislizenz verfügbare Zusatzfunktion;
- „Unterauftragsverhältnis“ solche Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung (technische Abwicklung von elektronischen Zahlungstransaktionen) beziehen. Nicht hierzu gehören Dienstleistungen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben (z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Verwaltungsdienstleistungen, Wartung und Benutzerservice, die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen).

2. Gegenstand, Zweck und Dauer der Auftragsdatenverarbeitung

1) Gegenstand der Auftragsdatenverarbeitung ist die technische Abwicklung von elektronischen Zahlungstransaktionen für den jeweils im Hauptvertrag genannten Leistungsumfang. Dazu werden dem Auftragnehmer die nach Punkt 4 näher spezifizierten Daten vom Auftraggeber über eine gesicherte Schnittstelle übergeben, damit der Auftragnehmer die folgenden Arbeiten und Leistungen erbringen kann:

- Zur Einleitung des Fernabsatz-Bezahlprozesses durch Eingabe von Zahlungsdaten die Zurverfügungstellung
  - eines Bezahlfensters für den Endkunden (für die Produkte „QPay Checkout Page“ oder „QMore Checkout Seamless“
  - einer Weboberfläche für den Auftraggeber (für die Produkte „QFile Checkout Automated“ oder „QCall Checkout Terminal“
  - einer Server-to-Server-Schnittstelle für den Auftraggeber (für das Produkt „QTill Checkout Enterprise“;
  - eines Bezahlfensters für den Auftraggeber (für die Produkte „QPay Checkout Page“ oder „QMore Checkout Seamless“ zur Backoffice Nutzung);
- Die Übernahme und Prüfung der eingegebenen Daten auf Richtigkeit und Gültigkeit im Vorfeld für die Abwicklung einer eCommerce-Zahlungstransaktion;
- Die Weiterleitung der Daten an den vertraglich vorgesehenen Finanzdienstleister (abhängig vom im Leistungsumfang enthaltenen Zahlungsmittel) zur Abbuchung des Transaktionsbetrages vom Bankkonto des Endkunden zugunsten des Auftraggebers;
- Die Rückgabe des Ergebnisses der Zahlungstransaktion (z.B. erfolgreiche Zahlung) an den Zahlungsauslösenden (Endkunde oder Auftraggeber);
- Die Generierung von relevanten Informationen zur Analyse von Transaktionsdetails in der Weboberfläche „QENTA Checkout Journal“ sowie zur Verwaltung von erfolgreichen Zahlungstransaktionen in der Weboberfläche „Q-Payment Center“;
- Die Teilnahme am Zahlungsmittelsystem durch Zurverfügungstellung von IT-Infrastruktur und Zahlungsapplikationen für den Zahlungsmittelbetreiber (Finanzdienstleister) und zur Benutzung durch den Zahlungsauslösenden (Endkunde oder Auftraggeber);
- Die Zurverfügungstellung von Sicherheitstechnologien für die sichere Zahlungsabwicklung und zur Einhaltung regulatorischer Anforderungen;
- Die Erbringung von Zusatzleistungen (Zusatzfeatures) wie jeweils im zugrundeliegenden Hauptvertrag vom Auftraggeber beauftragt.

2) Zweck der Verarbeitung personenbezogener Daten ist die Zahlungsabwicklung in Erfüllung des jeweiligen Hauptvertrages gegenüber dem Auftraggeber (für den jeweiligen Leistungsumfang: Basislizenz, 1 bis N Zahlungsmittel, 0 bis N Zusatzfeatures). Durch die Auftragsdatenverarbeitung ermöglicht der Auftragnehmer die Zahlungsabwicklung, die als Teilleistung für den Vertrieb von Produkten oder Dienstleistungen des Auftraggebers gegenüber dess en Endkunden ist. Der Auftragnehmer erbringt die Dienstleistung der Zahlungsabwicklung durch verschiedene technische Dienste,

gelangt dabei jedoch zu keiner Zeit in den Besitz der zu transferierenden Geldbeträge (sogenannter PSP-Vertrag).

3) Die Dauer der Auftragsdatenverarbeitung beginnt mit Unterzeichnung und umfasst die jeweilige Laufzeit des Hauptvertrages im Rahmen dessen diese Vereinbarung getroffen wurde.

3. Kategorien betroffener Personen

Die betroffenen Personen der Auftragsdatenverarbeitung (technische Zahlungsabwicklung) sind der Auftraggeber sowie alle Endkunden des Auftraggebers. Der Auftraggeber ist zudem betroffene Person in Bezug auf die von ihm durch Produktbestellung im Kunden-Registrierungsbeleg angegebenen personenbezogenen Daten.

4. Arten personenbezogener Daten

1) Durch die Bestellung einer Basislizenz (QPay Checkout Page, QMore Checkout Seamless, QFile Checkout Automated, QCall Checkout Terminal, QTill Checkout Enterprise, QPay Checkout Page/QMore Checkout Seamless für Backoffice), optional erweitert um zugehörige Zahlungsmittel (1 bis N Zahlungsmittel) und Zusatzfeatures (0 bis N Zusatzfeatures), erteilt der Auftraggeber dem Auftragnehmer die Weisung, sämtliche hierfür notwendigen Datenkategorien nach den nachfolgenden Bestimmungen zu verarbeiten. Der Auftraggeber nimmt insbesondere zur Kenntnis, dass jedes weitere bestellte Zahlungsmittel und/oder Zusatzfeature die Verarbeitung weiterer personenbezogener Datenkategorien nach sich ziehen kann.

2) Für jeden Verarbeitungszweck (Basislizenz mit/ohne Zahlungsmittel und Zusatzfeatures) ist via https://guides.qenta.com/privacy jederzeit und abschließend ersichtlich, welche Kategorien von übermittelten Daten von welchen betroffenen Personen zum Vertragsabschlusszeitpunkt verarbeitet werden und ob diese als personenbezogene Daten zu qualifizieren sind. Je nach Produktumfang werden vom Endkunden und/oder Auftraggeber unter anderem folgende Datenkategorien an die QENTA Zahlungsschnittstelle übermittelt und gegebenenfalls von dieser wieder an den Auftraggeber retourniert:

- Finanzdaten der Transaktion (z.B. ausgewähltes Zahlungsmittel, Zahlungsbetrag, Buchungsreferenz, Buchungstext);
- Zahlungsdaten des Endkunden (z.B. Kreditkartennummer, Bankverbindung), die beim Kaufvorgang für die Bezahlung des Produkts/der Dienstleistung des Auftraggebers mit einem bestimmten Zahlungsmittel übermittelt werden;
- Personendaten des Endkunden je Zahlungsmittel (z.B. Name, Adresse, Geburtsdatum, E-Mail-Adresse);
- Technische Transaktionsparameter für die Anbindung des Auftraggebers an die QENTA Zahlungsschnittstelle (z.B. Parameter für Konfigurations- und Sicherheitseinstellungen);
- Warenkorbdaten der Transaktion (z.B. für jede Warenkorbposition: Artikel-Nr., Artikelbeschreibung, Artikelpreis);
- Online Daten des Endkunden (z.B. IP-Adresse, Spracheinstellungen) zur Erhöhung der Benutzerfreundlichkeit (z.B. für Sprach- und Währungsvoreinstellungen);
- Zusatzfeature-spezifische Daten (z.B. Rückgabe von Endkundeninformationen an den Auftraggeber für jede erfolgreiche Zahlungstransaktion);
- Custom Parameters (das sind Daten, deren Übermittlung durch den Auftraggeber explizit gewünscht ist und von diesem alleine veranlasst wurde).

3) Allfällig vom Auftraggeber bei Produktbestellung im Kunden-Registrierungsbeleg angegebene personenbezogene Daten (Unternehmensinformationen und Kontaktdaten) werden in der Kundendatei von QENTA gespeichert und nur zum Zwecke der Zurverfügungstellung der gewünschten Produkte oder Dienstleistungen sowie zur Kontaktaufnahme verwendet und verarbeitet. Die Erfassung dieser Daten ist auf das für die Durchführung des Vertragsverhältnisses notwendige Minimum beschränkt. Die Daten des Auftraggebers werden keinesfalls veräußert, noch Dritten unmittelbare Nutzungsrechte daran eingeräumt. Nach Zustimmung des Auftraggebers können die Daten jedoch interessewahrend an Finanzdienstleister weitergegeben werden, sofern dies dazu dient, die Nutzung von QENTA Produkten zu fördern oder zu ermöglichen.

4) Der Auftragnehmer verarbeitet keine besonderen Kategorien von personenbezogenen Daten iSv Art 9 EU-DSGVO.

5. Datensicherheitsmaßnahmen

1) Für die ordnungsgemäße Umsetzung der in vorbezeichneter Vereinbarung zwischen den Parteien geregelten Auftragsdatenverarbeitung hat der Auftragnehmer geeignete technische und organisatorische Maßnahmen im Sinne von Art 32 EU-DSGVO getroffen. Eine Dokumentation der zum Zeitpunkt der Auftragsvergabe getroffenen Maßnahmen wird dem Auftraggeber mit dieser Vereinbarung als Anlage zur Verfügung gestellt.

2) Die Datenverarbeitung wird vom Auftragnehmer in einer Weise vorgenommen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um jene der Datensicherheit sowie zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, getroffene Maßnahmen weiter zu entwickeln oder mit adäquaten Alternativen zu ersetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden und wesentliche Änderungen sind zu dokumentieren.

4) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art 32 EU-DSGVO).

6. Weisungsbefugnis des Auftraggebers

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglich festgelegten und dokumentierten Weisungen des Auftraggebers und unter Einhaltung der gegebenenfalls vom Auftraggeber erteilten ergänzenden Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Ausgenommen hiervon sind nationale oder unionsrechtliche Vorschriften, die den Auftragnehmer gegebenenfalls zu einer anderweitigen Verarbeitung verpflichten.

2) Ist der Auftragnehmer nach Abs 1 der Ansicht, dass eine Weisung des Auftraggebers gegen nationale oder unionsrechtliche Datenschutzvorschriften verstößt oder zu einer Haftung des Auftragnehmers nach Art 82 EU-DSGVO führt, hat er den Auftraggeber unverzüglich vor der Verarbeitung darauf hinzuweisen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3) Aus Gründen der Nachvollziehbarkeit haben sämtliche Weisungen des Auftraggebers schriftlich (Textform) zu erfolgen. Jede

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@qenta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

mündliche Weisung muss unverzüglich schriftlich bestätigt werden.
4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangenden Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber ebenfalls in Textform mitteilen.

7. Berichtigung, Einschränkung und Löschung von Daten

1) Der Auftragnehmer darf die personenbezogenen Daten, die im Auftrag verarbeitet werden sollen, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers sowie soweit gesetzlich dazu verpflichtet verarbeiten, berichtigen, löschen oder sperren. Soweit sich ein Endkunde unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner personenbezogenen Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Einschränkung, Datenübertragbarkeit und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3) Für die Ermöglichung der zuvor genannten Tätigkeiten kann der Auftragnehmer bei Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers entstehen, einen Vergütungsanspruch von € 150,00 pro Stunde geltend machen.

8. Allgemeine Pflichten des Auftragnehmers

1) Der Auftragnehmer verpflichtet sich, dass eine Datenverarbeitung stets im Einklang mit dem Zweck, der Art und dem Umfang dieser Auftragsdatenvereinbarung sowie der Weisungsbefugnis nach Punkt 6 steht. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

2) Der Auftragnehmer verpflichtet sich, die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich in Mitgliedstaaten der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum durchzuführen. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art 44 ff EU-DSGVO erfüllt sind.

3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung nach Art 32 EU-DSGVO ergriffen hat. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist, wie unter Punkt 5 näher ausgeführt, als Anlage diesem Vertrag beigefügt.
5) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Zu diesem Zweck kontrolliert der Auftragnehmer regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

6) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art 37 EU-DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen. Im Übrigen kann mit dem QENTA Payment CEE Datenschutz-Team via privacy@qenta.com Kontakt aufgenommen werden.

9. Mitwirkungspflichten des Auftragnehmers

1) Der Auftraggeber ist als Verantwortlicher iSv Art 4 EU-DSGVO für die Wahrung von Betroffenen Rechte nach Art 12-23 EU-DSGVO – insbesondere für Anträge auf Auskunft, Berichtigung, Sperrung oder Löschung – allein verantwortlich. Der Auftragnehmer wird den Auftraggeber jedoch unverzüglich darüber informieren, wenn Betroffene ihre Rechte gegenüber dem Auftragnehmer geltend machen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

2) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen durch Betroffene nach Abs 1. Der Auftragnehmer trägt insbesondere dafür Sorge, dass alle notwendigen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser seine Pflichten innerhalb der gesetzlichen Fristen erfüllen kann.

3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen und der Art der Verarbeitung zudem bei der Einhaltung der in den Art 32-36 EU-DSGVO Pflichten wie:

- Datensicherheitsmaßnahmen für die sichere Verarbeitung personenbezogener Daten (Art 32 EU-DSGVO);
- Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art 33 EU-DSGVO);
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art 34 EU-DSGVO);
- Datenschutz-Folgeabschätzungen (Art 35 EU-DSGVO);
- Vorherige Konsultationen der Aufsichtsbehörde (Art 36 EU-DSGVO).

4) Für sonstige Unterstützungsleistungen, die nicht in der Leistungsbeschreibung nach Abs 2 und Abs 3 enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung von € 150,00 pro Stunde beanspruchen. Das Gleiche gilt für eine übermäßige Beanspruchung der Unterstützungsleistungen nach Abs 2 und Abs 3 durch den Auftraggeber.

10. Meldepflichten des Auftragnehmers

1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße gegen datenschutzrechtliche Bestimmungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

2) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Insbesondere ist dem Auftragnehmer bekannt, dass für den Auftraggeber eine Meldepflicht nach Art 33-34 EU-DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung dieser Meldepflichten unterstützen. Meldungen für den Auftraggeber kann der Auftragnehmer jedoch nur nach vorheriger Weisung des Auftraggebers durchführen.

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@qenta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

3) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über allfällige Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, sofern sie sich auf diesen Auftrag beziehen. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Soweit der Auftraggeber seinerseits Kontrollen oder Maßnahmen der Aufsichtsbehörde ausgesetzt ist (z.B. Verwaltungs- oder Strafverfahren, Haftungsanspruch eines Betroffenen), hat ihn der Auftragnehmer nach besten Kräften zu unterstützen. Im letzteren Fall kann der Auftragnehmer für die Ermöglichung dieser Tätigkeiten bei Mehraufwänden einen Vergütungsanspruch von € 150,00 pro Stunde geltend machen.

11. Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz – einschließlich der Einhaltung der Pflichten nach Art 28 EU-DSGVO – sowie die Einhaltung dieser Vereinbarung durch den Auftragnehmer jederzeit im angemessenen Umfang zu kontrollieren.

2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Abs 1 zur Verfügung zu stellen. Die Nachweise, die nicht nur den konkreten Auftrag betreffen, können insbesondere erfolgen durch:

- Umsetzung von technischen und organisatorischen Maßnahmen;
- Aktuelle Prüfergebnisse, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Datenschutzbeauftragter, IT-Sicherheitsabteilung, Wirtschaftsprüfer, externe Datenschutzauditoren, Revision);
- Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. PCI DSS, BSI Grundschutz);
- Die Einhaltung genehmigter Verhaltensregeln gemäß Art 40 EU-DSGVO;
- Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art 42 EU-DSGVO.

3) Im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber (Art 58 EU-DSGVO) ist der Auftragnehmer verpflichtet, der zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen und die erforderlichen Auskünfte zu erteilen.

4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer bei Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers entstehen, einen Vergütungsanspruch von € 150,00 pro Stunde geltend machen.

12. Unterauftragsverhältnisse

1) Der Auftragnehmer wird zur Erfüllung der vertraglichen Leistungen Teile der Verarbeitung an Unterauftragnehmer vergeben. Der Auftragnehmer nimmt allerdings keinen weiteren Unterauftragnehmer ohne vorherige gesonderte Genehmigung des Auftraggebers in Anspruch. Zudem bedarf jedes Unterauftragsverhältnis einer Vereinbarung nach Art 28 EU-DSGVO. Ein zustimmungspflichtiges Unterauftragsverhältnis liegt bei der Erbringung von Nebenleistungen nicht vor.

2) Folgende Unterauftragnehmer sind zum Zeitpunkt des Vertragsschlusses mit der Erbringung von vertragsrelevanten Hauptleistungen beauftragt. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung der Einhaltung von Art 28 EU-DSGVO:

Unterauftragnehmer	Anschrift / Land	Leistung
PagoNxt Merchant Solutions SL	Einsteinring 35, 85609 Aschheim, Deutschland	Payment Processing, Technologie-Dienstleistungen
A1 Telekom Austria AG & World-Direct eBusiness Solutions GmbH	Lasallestr. 9, 1020 Wien, Österreich	PCI DSS Compliant Rechenzentrum
Computop Paygate GmbH	Schwarzenbergstraße 4 96050 Bamberg Deutschland	Payment Transaction Processing

3) Die Einbindung weiterer sowie der Wechsel bestehender Unterauftragsnehmer wird dem Auftraggeber durch den Auftragnehmer in angemessener Zeit vorab schriftlich angezeigt. Das Unterauftragsverhältnis gilt als genehmigt, sofern der Auftraggeber nicht bis zu dem in der Anzeigemitteilung genannten Zeitpunkt gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt. Der Auftraggeber kann den Unterauftragnehmer des Auftragnehmers nur dann ablehnen, soweit hierfür ein wichtiger Grund vorliegt und dies unter der zuvor genannten Frist kommuniziert wurde.

4) Der Auftragnehmer sorgt im Rahmen der Unterauftragsverhältnisse als Unterauftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen bei den Unterauftragnehmern. Die Weitergabe von personenbezogenen Daten des Unterauftraggebers an den Unterauftragnehmer sowie dessen erstmaliges Tätigwerden sind überdies erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

13. Übermittlung von Daten an Dritte

1) Zur Abwicklung von elektronischen Zahlungstransaktionen für den Auftraggeber bzw. zur Erfüllung der vertraglich vereinbarten Leistungen müssen die in Punkt 4 beschriebenen Arten von personenbezogenen Daten, oder je nach Zahlungsmittel Teile davon, an Finanzdienstleister übermittelt werden.

2) Der Auftragnehmer übermittelt diese personenbezogenen Daten auf Basis einer gesonderten Weisung des Auftraggebers, um den Zweck des Auftragsgegenstandes erfüllen zu können. Der Auftragnehmer tritt gegenüber dem Finanzdienstleister als bevollmächtigter Vertreter des Auftraggebers auf dessen Rechnung auf. Zu diesem Zweck hat der Auftraggeber mit dem (den) Finanzdienstleistern (einen) separate(n) Akzeptanzvertrag (Akzeptanzverträge) geschlossen, der (die) vom jeweiligen Hauptvertrag über die technische Zahlungsabwicklung (siehe „PSP-Vertrag“ unter Punkt 2) bzw. von der Beauftragung des Auftragnehmers unabhängig ist (sind).

3) Die Übermittlung von personenbezogenen Daten an Finanzdienstleister erfolgt ausschließlich unter Einhaltung der in Punkt 5 genannten Datensicherheitsmaßnahmen.

14. Löschung und Rückgabe von personenbezogenen Daten

1) Der Auftragnehmer verpflichtet sich nach Beendigung des Auftragsverhältnisses alle personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach nationalen oder unionsrechtlichen Rechtsvorschriften eine Verpflichtung zur Speicherung der Daten besteht. Die Löschung ist in geeigneter Weise zu dokumentieren und auf Anforderung vorzulegen.

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@genta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

2) Kopien oder Duplikate von personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Daten, deren Sicherheitskopien in Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten sowie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und können bei Vertragsende vom Auftragnehmer zu dessen Entlastung übergeben werden.

15. Haftung und Schadenersatz

Der Auftragnehmer und der Auftraggeber haften gegenüber betroffenen Personen entsprechend der in Art 82 EU-DSGVO getroffenen Regelungen.

16. Schlussbestimmungen

1) Diese ergänzenden Bestimmungen zur Auftragsdatenverarbeitung werden für den jeweils zugrundeliegenden Hauptvertrag integrierender Vertragsbestandteil.

2) Dieser Vertrag enthält sämtliche Vereinbarungen in Bezug auf den Gegenstand dieses Vertrags und ersetzt diesbezüglich alle bisherigen Vereinbarungen der Parteien. Nebenabreden zu diesem Vertrag sind nicht getroffen worden. Die Vereinbarung ist hinsichtlich der in ihr enthaltenen Regelungen abschließend.

3) Soweit nicht vorstehend anderwärtig geregelt, sind die für den Hauptvertrag geltenden Allgemeinen Geschäftsbedingungen der QENTA Payment CEE in der aktuellen Fassung auf diese ergänzenden Bestimmungen anzuwenden. Dies gilt insbesondere für die Anwendung des Gerichtsstands, Rechtsgeltung, Auslegung, Salvatorische Klausel und Schriftformklausel auf diese Bestimmungen. Im Fall von Widersprüchen haben die Regelungen dieses Vertrages Vorrang gegenüber anderen vertraglichen Vereinbarungen und den Allgemeinen Geschäftsbedingungen der QENTA Payment CEE.

4) Der Auftraggeber erklärt durch seine Unterschrift bereits vorab, dass außer den Unterschriften nach Punkt 17 keine weiteren handschriftlichen Vermerke auf dem Vertragstext zulässig sind. Etwaige nachträglich angebrachten Vermerke erzeugen keine rechtsverbindliche Wirkung zwischen den Parteien.

17. Unterschriften

Dieser Vertrag tritt nach Gegenzeichnung des Auftraggebers und Retournierung an den Auftragnehmer in Kraft. Der Auftraggeber hat diese Vereinbarung gelesen, erklärt sich damit einverstanden und anerkennt, dass diese der Leistungserbringung zugrunde liegt. Der Unterzeichner bestätigt, zur Zeichnung berechtigt zu sein.

Für den Auftraggeber:

_____

Unterschrift

_____

Name, Position

_____

Ort/Datum

Firmenstempel:

Für den Auftragnehmer:

_____

Kerim Chouaibi, Geschäftsführer

Graz, den 17.03.2021

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@genta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

Anhang: Datensicherheitsmaßnahmen

Der Auftragnehmer dokumentiert hiermit nachfolgend getroffene technischen und organisatorischen Maßnahmen zur Datensicherheit gemäß Art 32 EU-DSGVO.

1. Allgemeines

Datensicherheit und Datenschutz sind wichtige Grundsätze der Verarbeitung von Daten bei QENTA. Als Payment Service Provider (PSP) ist sich QENTA bewusst, dass sie eine große Menge personenbezogener Daten verarbeitet und diese Daten als eines ihrer wichtigsten Güter besonders schützen muss.

Neben den Vorgaben der österreichischen und unionsrechtlichen Datenschutzvorschriften unterliegt QENTA den strengen Regelungen des PCI DSS (Payment Card Industry Data Security Standard), im Rahmen dessen jährliche Audits der Datensicherheitsmaßnahmen durchgeführt werden. QENTA erreichte als erster österreichischer PSP eine Zertifizierung nach PCI DSS und ist seit dem Jahre 2007 durchgehend zertifiziert.

QENTA versichert hiermit die Einhaltung aller datenschutzrechtlichen Vorgaben im Rahmen der Auftragsdatenverarbeitung, insbesondere der Datensicherheitsmaßnahmen nach § 54 DSG (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG), BGBl. I Nr.. 2017/120).

Das DSG definiert in § 54 verschiedene Datensicherheitsmaßnahmen, die für eine ordnungsgemäße und sichere Verarbeitung von personenbezogenen Daten getroffen werden müssen. Dabei handelt es sich im Einzelnen um folgende Punkte:

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellung
- Zuverlässigkeit
- Datenintegrität

Die für die Einhaltung der einzelnen Punkte ergriffenen Maßnahmen werden im Folgenden genauer dargelegt.

2. Zugangskontrolle

QENTA gewährleistet zu jedem Zeitpunkt, dass Unbefugten der Zugang zu Datenverarbeitungsanlagen verwehrt wird.
Alle Räumlichkeiten der QENTA verfügen über ein elektronisch gesichertes Türsystem. Sämtliche Mitarbeiter sind in Besitz von elektronischen Schlüsseln mit den für ihre Arbeit erforderlichen Zutrittsrechten. Die zentral von der Verwaltungseinheit erteilten Zutrittsrechte werden dokumentiert und in regelmäßigen Abständen einer Sicherheitsüberprüfung durch die IT Security unterzogen.

Zur Unterscheidung von Mitarbeitern und sonstigen Personen werden von der Verwaltungseinheit in Abstimmung mit der IT Security eigene Besucherausweise ausgehändigt. Besucher und sonstige Nicht-Mitarbeiter dürfen sich in den Räumlichkeiten der QENTA nur in Begleitung eines Mitarbeiters bewegen oder aufhalten.

Die Räumlichkeiten der QENTA sind physisch von der Infrastrukturumgebung für die Datenverarbeitung getrennt. Die Datenverarbeitung wird durch Unterauftragnehmer durchgeführt (siehe Punkt „Unterauftragsverhältnisse“ des Auftragsdatenverarbeitungsvertrages), die Rechenzentren für QENTA betreiben (darunter insbesondere die QENTA Technologies GmbH als zentraler Technologie-Dienstleister der QENTA Gruppe). Die Rechenzentren sind gegen unbefugten Zutritt durch Wachpersonal, das rund um die Uhr vor Ort ist, sowie Videoüberwachung und Alarmanlagen geschützt. Zudem versichert sich QENTA in regelmäßigen Abständen über die Einhaltung der von diesen Dienstleistern getroffenen Datensicherheitsmaßnahmen.

3. Datenträgerkontrolle

QENTA trifft geeignete Datensicherheitsmaßnahmen für die Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern im Rahmen ihrer „Information Security Policy“, die von jedem Mitarbeiter einzuhalten sowie jährlich durch ein eigenes Security Awareness Programm sicherzustellen ist.

Für die Mehrzahl der Datenverarbeitungsvorgänge fungieren die Rechenzentren, die räumlich durch Auslagerung von der Office-Umgebung der QENTA getrennt sind und der Verantwortung der Dienstleister obliegen, mit denen eine datenschutzkonforme Vereinbarung diesbezüglich getroffen wurde. Eine spezielle Zugangskontrolle (siehe Ziffer 2) sorgt dafür, dass sensible Bereiche mit entsprechenden Datenträgern für Unbefugte unerreichbar bleiben.

Eine Clean Desk Policy verhindert die unberechtigte Einsicht und das Entfernen von Datenträgern bzw. unternehmensspezifischer Informationen, die sich auf Hard Copies befinden. Nicht mehr für den unmittelbaren Bearbeitungsvorgang benötigte Hard Copies sind entweder zeitnah zu vernichten oder an einem für jedermann versperrten Ort aufzubewahren (z.B. versperrbare Schränke, Safes). Unsere Drucker in der Office-Umgebung zudem so aufgestellt, dass das Risiko des Lesens, Kopierens oder Entfernens von Hard Copies durch Dritte möglichst ausgeschlossen wird.

Über Media-Inventories erfolgt eine qualifizierte Datenträgerverwaltung, die dokumentiert, wie viele Datenträger gleich welcher Art (magnetisch/optisch/mobil) für welche Aufgaben und Verarbeitungen in Verwendung sind und wo diese gelagert sind. Über den Bestand der Datenträger ist regelmäßig eine Bestandskontrolle durchzuführen und die Lagerung in zutrittsgeschützten bzw. verschließbaren Bereichen vorzunehmen.

Die Sammlung, Vernichtung bzw. Löschung von Datenträgern erfolgt nach einer eigenen „Media Destruction Policy“, die auch Regelungen zu Lagerung, Transport und Entsorgungswegen dieser Datenträger umfasst. Dabei werden die medientypischen Eigenheiten des Datenträgers berücksichtigt und Entsorgungsvorgänge protokolliert.

Die Verwendung von Wechselmedien ist auf das innerhalb der QENTA genehmigte IT Equipment eingeschränkt und muss jeweils vom Vorgesetzten nach internen Sicherheitsrichtlinien genehmigt werden. Die Nutzung von nichtbetrieblicher Soft- und Hardware innerhalb der QENTA Umgebung ist für Mitarbeiter gänzlich untersagt, damit keine Schadprogramme eingeschleust und die Stabilität von IT-Systemen nicht negativ beeinträchtigt werden kann.

Im Übrigen sind für den vertraulichen Umgang mit personenbezogenen Daten entsprechende Vorkehrungen getroffen. Alle Mitarbeiter der QENTA sind auf die Einhaltung des Datengeheimnisses gemäß § 6 DSG verpflichtet und sämtliche Daten werden nach deren Wichtigkeit klassifiziert (Public/Internal/Confidential). Im Zweifelsfall werden Daten zumindest als „Internal“ eingestuft, wobei der Autor bzw. Urheber der Daten für die korrekte Klassifizierung verantwortlich ist.

4. Speicherkontrolle

QENTA verhindert die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@qenta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

Alle Systeme der QENTA sind mit angemessenen Benutzerkontroll- und Zugriffskontrollsystemen (siehe Ziffer 5 und 6) ausgestattet. Damit ist gewährleistet, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung zugeordneten personenbezogenen Daten Zugang haben und der Zugriff auf zentrale und dezentrale Rechner samt den darauf gespeicherten personenbezogenen Daten für Unbefugte ausgeschlossen bzw. ohne Verwendung von Benutzerkennung und Passwort nicht möglich ist.

Jede Eingabe, Veränderung oder Löschung von personenbezogenen Daten ist über ein umfassendes Protokollierungssystem jederzeit nachvollziehbar, weshalb eindeutig zugeordnet werden kann, welche Person zu welchem Zeitpunkt welchen Bearbeitungsvorgang getätigt hat. Gemäß den PCI DSS Regularien ist eine eigene „Audit Trail Policy“ implementiert, die die Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen sicherstellt (davon umfasst sind auch alle erfolgreichen und abgewiesenen Zugangsversuche) sowie entsprechende Stellen bei Verdachtsfällen automatisch informiert.

Authentifizierungsdaten wie Benutzerkennung und Passwort werden niemals ungeschützt über das Netzwerk übertragen. Sämtliche Mitarbeiter sind über das jährliche Security Awareness Programm zudem sensibilisiert, dass diese Daten weder über Formulareingaben (Speicherung im Browser) noch in Niederschriften (z.B. Handzettel, Dateien) gespeichert werden dürfen.

Die Verhinderung des unbefugten Zugriffs auf Daten wird durch das regelmäßige und zeitnahe Einspielen von Sicherheitsupdates für alle genutzten Drittapplikationen gewährleistet. IT Betriebssysteme (OS) werden gemäß den Vorgaben von PCI DSS periodisch mit Sicherheitsupdates versorgt. Die Qualität eigenentwickelter Applikationen wird vor Inbetriebnahme durch einen umfangreichen Qualitätssicherungsprozess sichergestellt.

Monitore sind in der Office-Umgebung so aufgestellt, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird. Es existieren keine frei zugänglichen Netzwerkanschlüsse und das Vorliegen möglicher unautorisierter Wlan Access Points wird vierteljährlich mittels eigenen Security Scans überprüft.

Die Bildschirme aller Arbeitsstationen und alle Services, die personenbezogene Daten verarbeiten oder speichern, werden automatisch nach 15 Minuten Inaktivität gesperrt. Ein Entsperren ist nur mit persönlicher Benutzerkennung und zugehörigen Passwort möglich. Die Sperrung des Arbeitsplatzrechners bei Verlassen des Arbeitsplatzes ist durch interne Richtlinien verbindlich geregelt.

Um Sicherheitsrisiken in Zusammenhang mit mobilen IT-Geräten (wie Smartphones oder Notebooks) zu verringern, unterliegt die Verwendung dieser Geräte speziellen Regelungen. Mobile Rechner (Notebooks) sind mit einer Festplattenverschlüsselung ausgestattet, an die zentrale IT-Infrastruktur mittels Benutzerauthentifizierung angeschlossen, mit einem Firewall- und Virenschutzkonzept geschützt und die Übertragung von Daten erfolgt nur mittels sicheren Fernzugriffs (VPN Client mit PIN und Hardware-Token oder PIN und SMS-Token).

5. Benutzerkontrolle

QENTA trifft geeignete Maßnahmen bzw. hat entsprechende Methoden und Einrichtungen im Einsatz um die unbefugte Nutzung von Daten mit Hilfe von Datenübertragungseinrichtungen zu verhindern.

Sämtliche Systeme bei QENTA sind mit Benutzerkontrollsystemen ausgestattet. Der Zugriff auf verschiedene Dienste kann ohne Benutzerkennung und persönlichen Passwort nicht erfolgen und ist somit vor Unbefugten geschützt. Jeder Mitarbeiter muss verbindlich eine Benutzerkennung haben. Gruppenkonten oder die Weitergabe von Accounts sind nicht erlaubt.

Jeder Mitarbeiter bei QENTA verfügt über einen persönlichen Zugang zu den Systemen, die jeweils nur mit einem ihm bekannten, persönlichen Passwort gesichert sind. Die internen Passwort-Richtlinien sind durch technische Systemeinstellungen konfiguriert und verlangen automatisch eine regelmäßige Veränderung des persönlichen Passworts (systemabhängig sind Zeiträume von 90 Tagen oder kürzer konfiguriert). Die Qualität des Passworts ist anhand von definierten Regeln sichergestellt (z.B. Mindestlänge, Komplexität, Zeichenkategorien, Gültigkeit). Alle Regeln zur Passwortvergabe und -änderung sind in internen Richtlinien dokumentiert und entsprechen den verbindlichen Vorgaben des PCI DSS.

Mit jeder Benutzerkennung ist eine oder mehrere Zugangsberechtigungen zu diversen Systemen verknüpft, die den Rollenbeschreibungen der jeweiligen Stelle und damit der jeweiligen Zugriffskontrolle folgt (siehe Ziffer 6).

Vor Erstellung einer Benutzerkennung ist eine Genehmigung des Security Boards notwendig und die Beantragung erfolgt über das zentrale IT Security System der QENTA. Sämtliche Benutzerprofile sind revisionssicher dokumentiert und Checklisten für die Erstellung bzw. Entfernung von Benutzeraccounts von den Administratoren geführt und archiviert.

Benutzeraccounts von ausgeschiedenen Mitarbeitern müssen nach dem letzten Arbeitstag (Ende des Dienstverhältnisses) deaktiviert werden. Ein eigenes Entry-Exit-Checklisten-System stellt dies über ein Beantragungsverfahren bei der zentralen IT Security der QENTA Gruppe sicher.

Das Benutzermanagement ist durch zentrale Sicherheitssoftware gegen Schadsoftware, Störungen und unberechtigte Zugriffe abgesichert.

6. Zugriffskontrolle

QENTA gewährleistet, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten nur zu den ihrer Zugangsberechtigung zugeordneten personenbezogenen Daten Zugang haben.

Der Zugriffskontrolle liegt ein Berechtigungskonzept zugrunde, mit dem das Need-to-Know Prinzip des Datenzugriffs sichergestellt wird. Über Benutzer- und Administrationsberechtigungen ist der Zugriff auf Systemdaten nur in einem Umfang möglich, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Somit hat jeder Mitarbeiter Zugriff auf genau jene Daten, die er für seine tägliche Arbeit benötigt.

Berechtigungen für bestimmte Systeme und Funktionen werden nur Mitarbeitern gestattet, die diese für die Durchführung ihrer Tätigkeit benötigen. Die Zugriffsrechte bzw. der Umfang der Berechtigungen wird auf das für die Aufgabenerfüllung notwendige Minimum beschränkt. Generell werden Zugriffsberechtigungen technisch soweit wie möglich eingeschränkt und nur im Einzelfall explizit erlaubt (Deny-all Prinzip). Soweit Funktionen ohne Verlust der Qualität der Datenverarbeitung zeitlich beschränkt werden können, sind Zugriffe auf personenbezogene Daten zeitlich zu beschränken.

Die für die jeweilige Stelle des Mitarbeiters notwendigen Rechte sind als Rollen definiert, die dem Mitarbeiter zugewiesen werden. Darüberhinausgehende Einzelberechtigungen werden von der IT Security freigegeben. Die Freigabe erfolgt nach Rücksprache mit dem Information Owner (i.d.R. der Leiter der zuständigen Fachabteilung) und im Rahmen der datenschutzrechtlichen Instruktionen.

Die Rollenbeschreibungen (siehe Ziffer 5) und vergebenen Rechte werden von den zuständigen Abteilungen dokumentiert, gepflegt und in regelmäßigen Abständen (mindestens einmal jährlich) von der IT Security stichprobenartig überprüft. Abhängig von der jeweiligen Rolle sind von jedem Mitarbeiter zudem spezielle Sicherheitsrichtlinien einzuhalten.

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@genta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

Administratorzugänge werden nur nach vorheriger interner Schulung vergeben. Sämtliche Administratorzugriffe auf Systeme werden gemäß den Vorgaben des PCI DSS revisionssicher protokolliert. Ein möglicher Missbrauch von Berechtigungen und deren Veränderungen kann jederzeit durch periodische, stichprobenartige Auswertungen der Logfiles erkannt werden.

7. Übertragungskontrolle

Auf Grund strenger PCI DSS Regularien kann jederzeit überprüft und festgestellt werden, welche Daten zu welcher Zeit durch wen an Einrichtungen zur Datenübertragung übermittelt wurden. Ebenso ist abschließend dokumentiert, an welchen Stellen Input- oder Output-Daten übermittelt werden (bzw. nicht übermittelt werden) und über welche Netzwerke (intern/extern) diese Übermittelung erfolgt.

Jede Datenübermittlung wird durch interne Systeme protokolliert und die Übermittlung selbst mit starker Verschlüsselung und sicherheitsgeprüften Protokollen durchgeführt, die dem Stand der Technik bzw. aktuellen Branchenstandards entsprechen. Eine interne „Firewall and Network Policy“ sorgt für eine sichere interne und externe Datenübermittlung und wird operativ zentral von der IT Security der QENTA Gruppe verwaltet. Eine Datenübermittlung darf zudem nur durchgeführt werden, wenn die Authentizität der Übermittlungsberechtigten geprüft wurde (z.B. durch Zertifikate oder Benutzerkennung).

Die Übermittlungswege sind einerseits durch eine genaue Dokumentation von Datenflüssen und des Netzwerkplans mit verschiedensten Ausprägungen nachvollziehbar. Andererseits werden sämtliche Datenübermittlungen protokolliert, ausgewertet sowie für nicht ordnungsgemäße Übermittlungsvorgänge rechtzeitig Gegenmaßnahmen getroffen. Sämtliche QENTA internen Schnittstellen sind dokumentiert. Die Dokumentationen externer Schnittstellen liegen vor.

8. Eingabekontrolle

Durch eine, höchsten Datenschutzanforderungen entsprechende, Eingabekontrolle gewährleistet QENTA, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind.
Zu diesem Zweck sind einerseits sämtliche Prozesse in einem eigenen Dokumentenmanagement erfasst, um über Datenflüsse den Zeitpunkt und die eingebende Stelle ermitteln zu können. Andererseits kann über interne Protokollierungssysteme jederzeit festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu sind entsprechende Logfiles sämtlicher Systeme bezüglich Zugang, Zugriff, sowie Erfassen, Ändern und Löschen von personenbezogenen Daten auswertbar. Gleichfalls wird durch die sorgfältige Vergabe der Zugriffsrechte sichergestellt, dass alle Daten nur gemäß ihrer Zweckbindung und den Weisungen des Auftraggebers verarbeitet werden.

Alle relevanten Daten werden in den Datenbanken von QENTA unter Angabe einer eindeutigen Mandantenkennung gespeichert, so dass eine eindeutige Zuordnung der Daten zum Betroffenen jederzeit möglich ist. Testdaten sind dabei eindeutig von produktiven Daten getrennt.

Jeder Mitarbeiter hat zum Zweck der Dateneingabe und -änderung eine persönliche Nutzerkennung für das jeweilige System, so dass alle Eingaben einer Person zugeordnet werden können. Die strikte Zweckbindung und Trennung der Verarbeitung wird durch regelmäßige Schulungen der Mitarbeiter sowie durch periodische Prüfungen durch den Bereich Informationssicherheit der QENTA Gruppe sichergestellt.

Bei Administratorzugriffen werden alle Änderungen an personenbezogenen Daten in den Systemen der QENTA durch die jeweilige Software-Applikation protokolliert oder durch entsprechende Prozesse dokumentiert, so dass sämtliche Änderungen jederzeit nachvollzogen werden können.

9. Transportkontrolle

QENTA stellt mit ausreichenden Datensicherheitsmaßnahmen sicher, dass personenbezogene Daten weder bei ihrer Übermittlung noch bei ihrem Transport auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Der Austausch und die Übertragung personenbezogener Daten erfolgt grundsätzlich nur in verschlüsselter Form und im Rahmen einer eigenen „Data Transmission Policy“. Verschlüsselte Verbindungen dürfen nur zu vertrauenswürdigen Systemen aufgebaut werden, deren Zertifikat im Client explizit vertraut wird.

Abhängig von der Art der Weitergabe werden verschlüsselte Übermittlungsverfahren über HTTPS und SFTP verwendet. E-Mails und Dateien können verschlüsselt werden (z.B. PGP-Verschlüsselung für regelmäßigen, verschlüsselten Datenaustausch).

Zur Übertragung von Zahlungsdaten in/aus unsicheren Netzen sind ausschließlich Protokolle mit starker Verschlüsselung wie TLS 1.2 zulässig. Für diese Protokolle dürfen wiederum nur starke Ciphers mit entsprechenden Schlüssellängen verwendet werden. Für die Auswahl von Algorithmen die unter die Kategorie starke Kryptografie fallen werden die Empfehlungen von Branchenstandards herangezogen (z.B. NIST).

Die Übermittlung von Zahlungsdaten über End-User Messaging Systeme ist strengstens untersagt.

Die Verschlüsselung beim Austausch personenbezogener Daten ist ein zentrales Thema der allgemeinen Datenschutzschulungen, die für jeden Mitarbeiter verpflichtend sind. Alle Schnittstellen zu externen Stellen, über die personenbezogene Daten automatisiert übertragen werden, sind nach aktuellen Standards gesichert (z.B. TLS Verschlüsselung) und unterliegen einer laufenden Anpassung an aktuelle technische Standards.

Im Übrigen muss der physische Transport von sensiblen Medien vom Sicherheitsbeauftragen der QENTA genehmigt und protokolliert werden. Der Versand von Medien durch externe Dienstleister ist untersagt.

10. Wiederherstellung

QENTA gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Zu diesem Zweck betreibt QENTA Intrusion Detection Systeme (IDS) und Intrusion Protection Systeme (IPS) und gewährleistet durch 24/7 Bereitschaft eine zeitnahe Alarmierung bei Störungen (Incidents).

Ein nach PCI DSS zertifizierter Vorfallreaktionsplan (Incident Response Plan) dient als Grundlage für die Vorgehensweise bei Störungen im Zusammenhang mit dem Betrieb der QENTA Zahlungsplattform. Dabei werden Kontakte, Kommunikations- und Eskalationsprozesse definiert, um im Bedarfsfall schnell und effektiv auf die Behebung des Fehlers bzw. die Einleitung von entsprechenden Maßnahmen reagieren zu können. Die verantwortlichen Mitarbeiter werden regelmäßig auf den Umgang mit dem Incident Response Plan geschult und bestimmte Tätigkeiten konkreten Mitarbeitern zugeordnet, um einen raschen und reibungslosen Ablauf bei der Wiederherstellung des Systems zu gewährleisten. Außerdem wird der Incident Response Plan mit jedem Incident auf eventuelle Prozesslücken oder Dateninkonsistenzen überprüft und dadurch stetig angepasst und verbessert.

Backups aller Daten werden regelmäßig angefertigt und an einem sicheren, durch bauliche Maßnahmen getrennten Ort aufbewahrt, wobei diesbezüglich die Vorgaben des BSI Grundschutz befolgt werden. In den Rechenzentren erfolgt der Umgang mit Backups

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@qenta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX

darüber hinaus nach einer eigenen „Backup Policy“, die unter anderem Backup-Medien entsprechend klassifiziert und neben den einzelnen Datenbeständen auch Konfigurationsdaten in das Backup-System einschließt, um eine zeitnahe Wiederherstellung zu gewährleisten.

11. Zuverlässigkeit und Datenintegrität

QENTA gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen bewertet und abhängig von deren Auswirkungen als Störfunktion an den Auftraggeber gemeldet werden (z.B. bei Abbrüchen von Zahlungstransaktionen).

Alle Systeme werden rund um die Uhr überwacht, so dass im Fehlerfall umgehend reagiert werden kann, der Auftraggeber rechtzeitig verständigt wird und das System gemäß dem Vorfallreaktionsplan (siehe Ziffer 10) rasch wiederhergestellt werden kann. Sämtliche internen Systeme werden umfassend durch ein Firewall- und Virenschutzkonzept geschützt, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen.

Die Systeme von QENTA sind über ein mehrstufiges Firewall-Konzept gegenüber dem Internet abgesichert. Alle Änderungen an der Firewall Konfiguration unterliegen einem internen Freigabeprozess und werden von der IT Security geprüft. Die Netzwerkkonfiguration und die aus dem Internet erreichbaren Payment Applikationen werden zudem periodisch durch von PCI DSS vorgeschriebenen Schwachstellen-, Web-Applikations-, Netzwerk- sowie Penetrationstests überprüft.

Neben diesen Sicherheitstests auf Infrastruktur- und Applikationsebene wird Software bei QENTA nur nach einer eigens abgenommenen „Software Development Policy“ entwickelt, um Sicherheitslücken möglichst zu vermeiden und eine effiziente Lastenverteilung zu gewährleisten. Dies umfasst u.a. Source-Code-Reviews, Trennung von Entwicklungs- und Produktionsumgebung, Vier-Augen-Prozesse, eine nachgelagerte Qualitätssicherung und Secure-Coding-Verfahren sowie Roll-Back-Verfahren für Releases um Fehlfunktionen zu minimieren oder bereits im Vorfeld zu vermeiden. Software Entwickler von QENTA sind aufgrund der PCI DSS Vorschriften zudem verpflichtet, laufend – mindestens jedoch jährlich – an internen und externen Fortbildungen teilzunehmen, um bezüglich sicherheitsrelevanten Themen auf dem neuesten Stand zu sein.

QENTA arbeitet ausschließlich mit konzerninternen sowie verlässlichen externen Dienstleistern zusammen, die Datenzentren nach gängigen Standards (ISO 27001, ISAE 3404, PCI-DSS) betreiben und zertifizieren. Die wichtigsten Produktivsysteme sind redundant ausgestaltet und automatische Umschaltsysteme sorgen bei Teilausfällen für höchste Zuverlässigkeit der QENTA IT-Systeme.

Die interne „Information Security Policy“ der QENTA stellt angemessene Maßnahmen für Internetverhaltensregelungen und E-Mail-Nutzung auf und schult Mitarbeiter in periodischen Abständen zu sicherheitsrelevanten Themen. Für die Einstellung und das Ausscheiden von Mitarbeitern sind Standardprozesse implementiert, die u.a. Background-Checks (Überprüfung von einschlägigen Vorstrafen mit Relevanz zur Payment Branche) sowie das Zuweisen und Entziehen von Rechten (z.B. physische Zutrittsrechte, IT-Equipment, Account Zugriffsrechte) umfassen.

12. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Datensicherheitsmaßnahmen

QENTA sorgt für die regelmäßige Überprüfung, Bewertung, Evaluierung und Überarbeitung der Datensicherheitsmaßnahmen.

Zur periodischen Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen werden Ereignisse des Incident Response Managements, der im Rahmen von PCI DSS durchgeführten Risikoanalyse, der jährlichen PCI DSS Audits, der Sicherheits- und Schwachstellentests sowie Erkenntnisse des allgemeinen Datenschutzmanagements berücksichtigt. Die technischen und organisatorischen Maßnahmen unterliegen dem ständigen technischen Fortschritt und der Weiterentwicklung wie in Punkt „Datensicherheitsmaßnahmen“ des Auftragsdatenverarbeitungsvertrages ausgeführt.

Sämtliche Datenverarbeitungsvorgänge der QENTA unterliegen einem regelmäßigen Überprüfungsprozess. Neben der Berücksichtigung sämtlicher gesetzlicher Anforderungen und der Einbindung der gesamten QENTA Systemumgebung in das interne Datenschutzmanagement, wird insbesondere darauf Wert gelegt, dass Software laufend auf datenschutzfreundliche Voreinstellungen überprüft wird und die Verarbeitung von personenbezogenen Daten nach dem Grundsatz der Datensparsamkeit (Art 5 EU-DSGVO) durch Mittel wie Pseudoanonymisierung und Anonymisierung eingeschränkt wird.

Im Zuge der internen Auftragskontrolle wird zudem laufend sichergestellt, dass QENTA als Auftragnehmer keine Datenverarbeitungen entgegen den Weisungen des Auftraggebers vornimmt. Dazu stellt QENTA bereits durch die Regelungen im Vertrag mit dem jeweiligen Auftraggeber sicher, dass die rechtlichen Grundlagen der Auftragsdatenverarbeitung beachtet werden. Außerdem achtet QENTA bei der Vergabe von Unterauftragsverhältnissen besonders auf die Einhaltung der datenschutzrechtlichen Vorschriften und überprüft potenzielle Unterauftragnehmer vorab in Hinblick auf technische, finanzielle, datensicherheitsspezifische und rechtliche Aspekte. Alle vertraglichen Regelungen werden vom internen Beauftragten für Datenschutz auf Konformität mit den gesetzlichen Bestimmungen geprüft und alle Mitarbeiter von QENTA regelmäßig zu den aktuellen Regelungen des Datenschutzes geschult.

QENTA Payment CEE GmbH | Taborstraße 1-3/10 | A-1020 Wien I Tel: +43 316 813681 | Fax: +43 316 813681-1203 vertrieb@genta.com I
Geschäftsführer: Kerim Chouaibi I Handelsgericht Wien: FN 539960i | Steuernr.: 09 378/7331 | UID Nr.: ATU75909616 I Erste Group Bank AG |IBAN: AT42 2010 0600 1677 2700| BIC GIBAATWGXX