professionelle netzwerke & computersysteme

Auftragsverarbeiter-Erklärung

der PNC GmbH in Bezug auf die

EU-Datenschutzgrundverordnung (DSGVO)

Version 1.0

Stand: 25.05.2018

Präambel

- Dieses Dokument regelt die Rechte und Pflichten von Auftraggeber (in Folge auch „AG“ genannt) und Auftragnehmer (in Folge auch „AN“ genannt) in Bezug auf die Vereinbarung über die Auftragsverarbeitung personenbezogener Daten.

- Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

- In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden in Schriftform (auf Papier) zu erfolgen haben, können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

- Dieses Dokument bedarf keiner besonderen Zustimmung durch die beteiligten Parteien, sondern tritt durch die Absichtserklärung, gemeinsam Geschäfte abzuwickeln, in Kraft.

Dauer der Vereinbarung

Die Verarbeitung beginnt mit dem ersten Zugriff der PNC auf die Daten des AG und erfolgt auf unbestimmte Zeit bis zur Kündigung dieser Erklärung oder des Hauptvertrags durch eine Partei. Beiderseitige Geheimhaltungsverpflichtungen gelten über eine etwaige Kündigung hinaus.

Gegenstand der Vereinbarung

Gegenstand eines Auftrages kann beispielsweise die Installation, der Betrieb, die Wartung, Parametrierung, Überwachung und Datensicherung von zentralen und clientseitigen IT-Systemen und Telekommunikationsanlagen des Partners, der Support von Benutzern sowie eine Kombination der genannten Tätigkeiten sein. Die Durchführung der Arbeiten erfolgt entweder direkt an den Systemen oder mittels Fernzugriff.

Des Weiteren kann Gegenstand eines Auftrages die Bereitstellung zentraler IT-Systeme in Rechenzentren der PNC oder seiner Partner für die Nutzung durch den Auftraggeber sowie der Betrieb, die Wartung, Parametrierung, Überwachung und Datensicherung dieser Systeme.

Wenn PNC Daten im Auftrag ihrer AG verarbeitet, umfasst dies jene Tätigkeiten, die in den Verträgen zwischen AG und PNC oder in produktspezifischen Bedingungen konkretisiert sind. Der AG ist dabei für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Verarbeitung an sich sowie der Datenweitergabe an PNC als Auftragsverarbeiter allein verantwortlich („Verantwortlicher“ im Sinne des Art 4 Punkt 7 DSGVO). Der AG stellt sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die von PNC als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der

unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen entsprechend DSGVO angemessen sind.

Eine Verwendung personenbezogener Daten über die Produkt- oder Servicebeschreibung hinaus aus dem Datenbestand des AG erfolgt nicht, Gegenstand des Vertrages sind die rein technischen Aspekte der Speicherung, Bereitstellung und Datensicherung der Daten sowie fallweises Auslesen im Rahmen des Supports von Benutzern (Ansicht des Bildschirminhaltes) nach vorheriger Zustimmung des Auftraggebers oder eines berechtigten Vertreters.

Die Art der Daten sowie die Kategorien der Daten werden ausschließlich durch den AG festgelegt, die Erfassung und Speicherung der Daten erfolgt allein durch den AG. Sollen auch personenbezogene Daten besonderer Kategorien nach Art. 9 DSGVO verarbeitet werden, so ist dies in einer gesonderten Vereinbarung explizit zu regeln. Die Verantwortung bezüglich Zulässigkeit der Verarbeitung (insbesondere aber nicht ausschließlich nach Art. 9 DSGVO) liegt beim Auftraggeber, der die für den Betrieb seines Unternehmens erforderlichen Daten festlegt, wie z. B. Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten o. ä..

PNC erlangt allenfalls ausschnittweise Kenntnis der gespeicherten Daten des Auftraggebers im o. a. Rahmen und hat keinerlei eigenständige Entscheidungsbefugnis bezüglich einer weiteren Verarbeitung der gespeicherten Daten.

PNC verarbeitet personenbezogene Daten des Auftraggebers nur insoweit, als sie zur organisatorischen, kaufmännischen oder technischen Erfüllung des Auftrages erforderlich sind (Kontaktdaten des Unternehmens und einzelnen Mitarbeitern des Auftraggebers und vom Auftraggeber beauftragten Unternehmen, Zugangsinformationen für IT-Systeme des Auftraggebers).

Pflichten des Auftragnehmers (PNC)

Der AN verarbeitet personenbezogene Daten ausschließlich wie vereinbart oder wie vom AG angewiesen, es sei denn, der AN ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der AN diese dem AG vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der AN verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

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

Der AN erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO in seinen eigenen Systemen umgesetzt und dem AG selbige empfohlen hat. Die Verantwortung zur Umsetzung verbleibt beim AG.

Der AN ergreift die technischen und organisatorischen Maßnahmen, damit der AG die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem AG alle dafür notwendigen Informationen.

Der AN darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des AG berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den AN gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den AG der von ihm betriebenen Datenanwendung hält, hat der AN den Antrag unverzüglich an den AG weiterzuleiten und dies dem Antragsteller mitzuteilen.

Der AN unterstützt den AG bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation) gegen einen entsprechenden Kostenersatz. Der AG wird darauf hingewiesen, dass er die vorliegende Auftragsverarbeitung in das Verarbeitungsverzeichnis nach Art 30 DSGVO aufzunehmen hat.

Dem AG wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungs-einrichtungen eingeräumt. Der AN verpflichtet sich, dem AG jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Der AN ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der AN die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des AG in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben. Der AN hat den AG unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des AG verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

Rechte und Pflichten des Auftraggebers (AG)

Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der AG verantwortlich.

Der AG erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der AG unverzüglich dokumentiert bestätigen. Der AN behält sich das Recht vor, in heiklen Fällen vorab die Schriftform zu verlangen.

Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der AG ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim AN in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom AN soweit erforderlich Zutritt und Einblick zu ermöglichen. Der AN ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

Kontrollen beim AN haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom AG zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des AN, sowie nicht häufiger als alle 12 Monate statt. Soweit der AN den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

Nutzt der AG Produkte, Services oder Dienstleistungen und stellt sie außerhalb seines eigenen Unternehmens zur Verfügung bzw. beauftragt in fremdem Namen, so gelten verpflichtet er sich, die Datenschutzbestimmungen entsprechend selbst einzuhalten und umzusetzen. PNC schließt jede Haftung Dritten gegenüber aus dieser Konstellation aus.

Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem AN gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Einzelheiten sind dem Anhang zu entnehmen.

Ort der Durchführung der Datenverarbeitung

Systeme des Auftragnehmers (PNC)
Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

Systeme des Auftraggebers (AG)
Der AG führt die beauftragten Tätigkeiten auf Systemen des Kunden durch, unabhängig vom Standort des Systems.
Eine Lokalisierung des Systems durch den AN ist in vielen Fällen nicht möglich, die Zulässigkeit der Verarbeitung der Daten am jeweils aktuellen Standort liegt in der alleinigen Verantwortung des AG (u. a. entsprechend Art 45,49,46,47 DSGVO).

Sub-Auftragsverarbeiter

Der Auftragsnehmer ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuzuziehen:

- UPC (Housing/Hosting)
- IT-Klinik (Web-/Mailhosting, DNS, Domänenverwaltung)
- Cyren (NoSpamProxy – Spam-/AV-Filterung)
- Kaspersky (AV-Scan)
- EDVsolution Andreas Meyer

Der Auftragnehmer kann weitere Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der AN dies dem AG eine Woche vorab schriftlich anzeigt und
- der AG nicht innerhalb einer Woche gegenüber dem AN schriftlich Einspruch gegen die geplante Auslagerung erhebt und
- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.

Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der AN gegenüber dem AG für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Anhang – Technisch-organisatorische Maßnahmen

Vertraulichkeit

Physischer Schutz

Kein unerlaubter Zugriff auf IT-Systeme: Zutrittskontrolle, Versperren, Verschlüsselung – eine oder mehrere dieser Verfahren kommen zur Anwendung.

Zugangskontrolle

Schutz vor unbefugter Systemnutzung: Komplexe Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Sicherungs- und Transport-Datenträgern.
Die zur Authentifizierung eingerichteten und vom Auftragnehmer verwendeten Zugangskennungen und Passwörter der Systeme des Auftraggebers verlassen den Personenkreis der Berechtigten beim AN nicht. Sie werden in gesicherten Bereichen auf IT-Systeme des AN hinterlegt und sind nur dem Personenkreis zugänglich, der diese für die Erbringung der vereinbarten Dienstleistung zwingend benötigt. Der Zugang von außen auf die Netzwerke von AG sowie AN erfolgt ausschließlich über verschlüsselte Verbindungen.

Zugriffskontrolle

Kein unbefugtes Lesen, Ändern oder Löschen von Daten: Benutzerprofile werden mit minimal erforderlichen Berechtigungen versehen, die zugewiesenen Berechtigungen werden periodisch überprüft.

Pseudonymisierung, Klassifikation der Daten

sind entsprechend dem Gegenstand der Verarbeitung nicht möglich: Kontaktinformationen des Partners werden zur Kontaktaufnahme benötigt, die durch den Partner auf seinen Systemen gespeicherten Daten werden durch die PNC nicht verarbeitet.

Integrität

Weitergabekontrolle

Kein unbefugtes Lesen, Ändern oder Löschen von Daten bei elektronischer Übertragung oder Transport: Verwendung von verschlüsselten Verbindungen inkl. VPN, Verschlüsselung von Transportdatenträgern.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

Systeme der PNC

Sicherungskonzept mit Monitoring sowie Auslagerung der Sicherungsdatenträger bzw. Auslagerung auf räumlich getrennte Systeme
Einsatz von Firewalls, Antivirensoftware und USV-Systemen
Dokumentierte Standardprozesse bei Wechsel bzw. Ausscheiden von Mitarbeitern

Systeme des Partners

Alle oben angeführten und auch weitere Maßnahmen im Umfang der Beauftragung durch den Partner

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management
Richtlinien und regelmäßige Schulungen für Mitarbeiter

Incident-Response-Management
Dokumentierte Vorgangsweise

Datenschutzfreundliche Voreinstellungen

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des AG: Verarbeitung von Daten nur mit zugrundeliegendem Verarbeitungsvertrag und schriftlicher Weisung des Auftraggebers.

Anhang – Weisungsberechtigte Personen

Die Weisungsbefugnis eines Auftraggebers ist grundsätzlich von der Geschäftsführung oder einer anderen zur rechtlichen Vertretung des Auftraggebers befugten Person zu erteilen.

Sonstiges

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.

Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

Für Nebenabreden ist die Schriftform erforderlich.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.