## Nutzungs- und Datenschutzbestimmungen für JaOffice

Die BPS International GmbH (im folgenden «BPS» genannt) erbringt ausschließlich für Unternehmen Dienstleistungen und Software-Produkte mit der Bezeichnung JaOffice zu den nachstehenden Nutzungs- und Datenschutzbestimmungen.

Die Nutzung von JaOffice setzt voraus, dass Auftraggeber und Nutzer bzw. der Kunde diesen Nutzungs- und Datenschutzbestimmungen und den AGB zugestimmt haben und diese einhalten.

Der Nutzer bzw. der Kunde benötigt zum Betrieb von JaOffice spezifische Endgeräte, z.B.

seitens des Websystems: Computer mit Internetzugang und Internetbrowser Google Chrome Version 16 oder neuer, Mozilla FireFox Version 3.5 oder neuer, Internet Explorer Version 7 oder neuer, Apple Safari 4 oder neuer, sowie

und ggf. seitens des mobilen Endgerätes: die meisten Smartphones und Tablet PCs mit Android Betriebssystem ab Version 2.2 und iOS Betriebssystem sind für den Betrieb von JaOffice geeignet.

Die Funktionen und Leistungen von JaOffice sind auf die bei der Registrierung verfügbaren Funktionen gemäß den Leistungsinformationen beschränkt.

BPS optimiert bzw. verändert JaOffice fortlaufend. Der Nutzer bzw. der Kunde stimmt zu, dass BPS beispielsweise Funktionen oder Features hinzufügen oder entfernen oder zusätzliche oder neue Bedingungen für JaOffice einführen kann.

BPS erbringt Leistungen im Rahmen der Kapazitäten des JaOffice-Systems und der technischen Anlagen, mittels derer JaOffice betrieben wird, u.U. auch Anlagen Dritter, z.B. bei der Nutzung von JaOffice als Cloud oder als Private Cloud oder bei der Nutzung von JaOffice auf den technischen Anlagen des Kunden. Zeitweilige Störungen, Beschränkungen oder Unterbrechungen der Leistungen können sich auch in Not- und Katastrophenfällen, durch atmosphärische Bedingungen und geographische Gegebenheiten sowie durch funktechnische Hindernisse, Unterbrechung der Stromversorgung oder wegen Änderungen an den Anlagen und Systemen von BPS und / oder Dritten, wegen sonstiger Maßnahmen (z.B. Wartungsarbeiten, Updates), die für die ordnungsgemäße oder verbesserte Erbringung der Leistungen erforderlich sind, oder aus Gründen höherer Gewalt (einschließlich Streiks und Aussperrungen) ergeben. BPS übernimmt keine Haftung und leistet keinen Schadenersatz gegenüber Nutzern bzw. gegenüber des Kunden für jegliche Verspätungen, Störungen, Schäden, entgangene Einnahmen / Gewinne oder für jegliche Verluste, die aufgrund von System- und / oder (Träger)Funktionsstörungen bzw. Abweichungen entstehen, ebenso wenig wie für direkte oder indirekte Schäden, die dem Nutzer bzw. der Kunde aufgrund der genannten Ereignissen oder Umstände entstanden sind.

Im Fall der Nutzung von JaOffice per Private Cloud Server und im Fall der Nutzung von JaOffice auf den technischen Anlagen des Kunden bzw. auf solchen, die der Kunde oder BPS im Auftrag des Kunden bestellt, bedarf es ab Tag der Installation bis zu 10 Arbeitstage, um JaOffice auf diesen Anlagen zu implementieren, zu prüfen und bereitzustellen. Innerhalb dieser Periode kann JaOffice nicht oder nur teilweise bzw. eingeschränkt durch Nutzer bzw. durch den Kunden genutzt werden (Installationsperiode). Der Kunde willigt ein, dass zu Zwecken des Funktionstests innerhalb dieser Installationsperiode Test-Nutzer von BPS das System des Kunden betreten und dort Daten oder Informationen erheben, speichern und verwalten und um ggf. technische Tests hinsichtlich der System-Stabilität durchführen. Nach der Installationsperiode wird JaOffice an den Kunden zur Nutzung übergeben.

JaOffice basiert zum Teil auf der Leistungsfähigkeit, Verfügbarkeit und Genauigkeit von Signalen, Verbindungen, Schnittstellen oder technischen Anlagen bzw. Leistungen und / oder Produkten Dritter, insb.

Hardware-, Software- sowie Mobilfunk-, Internet- bzw. Server-Spezifikation. BPS verantwortet und garantiert nicht die Genauigkeit, Verfügbarkeit, Leistungsfähigkeit, Fehlerfreiheit bzw. Sicherheit und Zugangsmöglichkeit von Endgeräten, Signalen, Verbindungen, Schnittstellen und anderen Leistungen und / oder Produkten Dritter bzw. von Trägerfunktionen, die zum Betrieb von JaOffice erforderlich sind bzw. zu denen JaOffice lediglich den Zugang ermöglicht.

Der Nutzer bzw. der Kunde informiert sich vor Registrierung und vor Vertragszeichnung, falls der Nutzer bzw. der Kunde zugleich Kunde ist, insb. über die ausreichende Serverspezifikation und Internetverbindungen bzw. über die Mobilfunkversorgung an den von ihm bevorzugten Standorten, über die Leistungsfähigkeit und Spezifikationen und Qualitäten der jeweils zur Verwendung von JaOffice gewählten oder in Frage kommenden Endgeräte und technischen Anlagen.

Der Nutzer bzw. der Kunde stellt gegenüber BPS keine Ansprüche, wenn er keine oder nicht alle JaOffice-Leistungen in Anspruch nehmen kann, weil seine Endgeräte, Verbindungen, Schnittstellen, technischen Anlagen und Leistungen Dritter bzw. die Trägerfunktionen technisch, naturgemäß oder aufgrund einer Beschädigung oder Störung nicht oder nicht vollständig für den Betrieb von JaOffice geeignet sind.

Der Nutzer bzw. der Kunde wird nur solche Endgeräte und technische Anlagen funktionsgerecht verwenden, die für die Nutzung von JaOffice ausgestattet sind. Dem Nutzer bzw. der Kunde ist bekannt, dass nicht alle Endgeräte, Server oder weitere technische Anlagen auf dem Markt alle von JaOffice angebotenen Leistungen unterstützen. Die Laufzeit oder Gültigkeit einer Lizenz oder eines JaOffice-Vertrages wird durch eingeschränkte Möglichkeiten zur Nutzung von JaOffice seitens des Nutzer bzw. der Kundes nicht beeinflusst.

Der Nutzer bzw. der Kunde ist sich bewusst, dass auch bedingt durch seine Verbindungen bzw. Tarife oder individuellen Leistungen seines Anlagen- und Netzbetreibers nicht alle Funktionen von JaOffice vollständig genutzt werden können. Der Nutzer bzw. der Kunde prüft vor Registrierung, wie er JaOffice auf Basis seiner technischen Anlagen und Verbindungen verwenden kann. Auch die entgeltfreie Testphase dient dieser Prüfung.

Dem Nutzer bzw. der Kunde ist bewusst und er akzeptiert, dass für oder während des Betriebes von JaOffice weitere Entgelte anfallen können, z.B. durch seine Tarife bzw. Verträge mit seinem Telekommunikationsanbieter, z.B. für GPRS-, GPS-, Sprach-, Nachrichten-, Internet- oder Datenübertragung, Strom zum Betrieb seiner technischen Anlagen und / oder ein Serveraus- oder umbau infolge JaOffice Installation. Der Nutzer bzw. der Kunde informiert sich vor Registrierung über weitere Kosten.

Der Nutzer bzw. der Kunde ist darüber unterrichtet, dass sich nach dem aktuellen Stand der Technik Programm- bzw. Systemfehler trotz größter Gewissenhaftigkeit und Sorgfalt nicht sicher ausschließen lassen. BPS gewährleistet keine absolute Genauigkeit und keine volle Funktion von JaOffice zu jeder Zeit.

Der Nutzer bzw. der Kunde ist damit einverstanden, dass er JaOffice ausschließlich selbst auf Basis der Lizenz nutzt, die durch sein persönliches und geheimes Passwort geschützt ist. Er wird weder sein Gerät, auf dem oder mit Hilfe dessen er JaOffice betreibt, noch seinen Zugang (Login) und / oder seine Lizenz Anderen verfügbar machen, auch nicht unternehmensintern.

Eine mobile Applikation darf niemals ohne das Wissen des Nutzer bzw. der Kundes bzw. Verwenders auf einem mobilen Endgerät bestätigt, installiert bzw. sogar betriebsbereit eingeloggt werden.

Der Nutzer bzw. der Kunde stimmt zu, dass in bzw. durch oder mit Hilfe von JaOffice Signale, Inhalte und Daten erstellt, übertragen, kombiniert, aufgezeichnet, gespeichert und/ oder erkennbar gemacht werden, siehe Datenschutzbestimmungen. Diese Daten werden innerhalb des zentralen und gemeinschaftlich von allen Nutzer bzw. der Kunden verwendetes JaOffice-Netzwerk für ein Unternehmen erstellt bzw. gespeichert und dort für andere Nutzer bzw. der Kunde verfügbar gemacht. Die meisten Daten sind naturgemäß für die

unternehmensinterne Kommunikation und Zusammenarbeit bestimmt und somit unternehmensintern öffentlich, es sei denn, der Nutzer bzw. der Kunde verwendet die Funktion(en) der „persönliche Nachricht“.

Der Nutzer bzw. der Kunde hat die Zugangsdaten für JaOffice sorgfältig aufzubewahren, geheim zu halten und nicht weiterzugeben. Der Nutzer bzw. der Kunde wird die Sicherheit seiner für den Betrieb / für die Verwendung von JaOffice gewählten bzw. verwendeten Geräte und technischen Anlagen selbst gewährleisten.

Die Nutzer bzw. der Kunde werden Inhalte, Informationen, Signale bzw. Daten die sie durch, mit oder in JaOffice aufzeichnen, abspeichern, dokumentieren, veröffentlichen oder hoch- bzw. herunterladen, vertraulich behandeln, zusätzlich außerhalb von JaOffice sichern bzw. aufbewahren und — falls Inhalte, Informationen, Signale bzw. Daten weitergeleitet werden — nur dem Personenkreis zugänglich machen, der nach den Gesetzen, der Organisationsstruktur des Unternehmens bzw. dem Geschäftszweck nach dafür ermächtigt und autorisiert ist.

JaOffice darf nicht in speziellen Risikobereichen oder in solchen genutzt werden, die einen fehlerfreien Betrieb erfordern oder in denen ein Ausfall von JaOffice zu einer unmittelbaren Gefahr für Leib, Leben und Gesundheit oder zu erheblichen Schäden an Eigentum, betriebswirtschaftlichen Ressourcen bzw. Einnahmen und Gewinnen oder der Umgebung führen kann. BPS gewährleistet nicht, dass JaOffice für den Einsatz in speziellen Risiko- oder Berufsbereichen geeignet ist. JaOffice ist kein spezialisiertes Produkt, sondern lediglich ein Kommunikations- und Datenportal für eine universelle, breite Nutzung in vielen Unternehmen.

Der Nutzer bzw. der Kunde verpflichtet sich, JaOffice nicht missbräuchlich zu nutzen, sondern ausschließlich zur Nutzung der auf den Internetseiten von JaOffice erklärten Funktionen, innerhalb der gesetzlich zulässigen Rahmen und als EndNutzer bzw. der Kunde. Der Nutzer bzw. der Kunde darf mit bzw. durch JaOffice keine Aktionen ausführen oder JaOffice in der Art Nutzen, das damit gegen ethische oder moralische Normen und Sitten gehandelt wird bzw. dass die Privatsphäre der Nutzer bzw. der Kunde und / oder Dritter verletzt wird.

BPS übernimmt auch keine Haftung bzw. Gewährleistung und leistet keinen Schadensersatz für bzw. bei Ereignissen bzw. Schäden, die aufgrund der unangemessenen und / oder fahrlässigen Nutzung von JaOffice durch den Nutzer bzw. der Kunde, seiner Erfüllungs- bzw. Verrichtungsgehilfen bzw. durch Dritte entstehen.

Der Nutzer bzw. der Kunde ist verpflichtet, die Hardware, Software, Verbindungen, Schnittstellen und technischen Anlagen bzw. seine Endgeräte vor unberechtigten Zugriffen Dritter zu schützen. Der Nutzer bzw. der Kunde ist verpflichtet, angemessene Maßnahmen zur Schadensabwehr und -minderung zu treffen und seine Pflichten einzuhalten.

Der Nutzer bzw. der Kunde hat BPS den Verlust, Diebstahl, die Manipulation oder die unberechtigte Nutzung des für JaOffice verwendeten Endgerätes, der Lizenz oder des Zugangs (d.h. Login) unverzüglich mitzuteilen.

BPS kann diese Nutzungsbedingungen oder etwaige zusätzliche Bedingungen für JaOffice anpassen, um beispielsweise Änderungen der rechtlichen Rahmenbedingungen oder Änderungen von JaOffice zu berücksichtigen. Änderungen gelten nicht rückwirkend und werden frühestens 14 Tage nach ihrer Veröffentlichung wirksam. Änderungen hinsichtlich einer neuen Funktion für einen Dienst oder Änderungen aus rechtlichen Gründen sind jedoch sofort wirksam. Wenn der Nutzer bzw. der Kunde den geänderten Nutzungsbedingungen nicht zustimmt, muss er die Nutzung von JaOffice einstellen.

BPS lehnt jegliche Gewährleistungen und Bedingungen, einschließlich jeder konkludenten Gewährleistung und anderer Bedingungen, hinsichtlich Tauglichkeit bzw. Eignung für einen bestimmten Zweck ab.

Jegliche Produkte und Dienste zum Download oder zur internetbasierten Nutzung sind das urheberrechtlich geschützte Werk von BPS. Die Reproduktion oder der Vertrieb von JaOffice oder dessen Inhalten oder Funktionen ist ausdrücklich verboten.

Durch die Nutzung von JaOffice erwirbt der Nutzer bzw. der Kunde keinerlei Urheberrechte oder gewerbliche Schutzrechte an JaOffice oder an den Inhalten, auf die er Zugriff hat bzw. haben kann. Diese Nutzungsbedingungen gewähren Nutzer bzw. der Kunde kein Recht zur Nutzung von Marken, Markenelementen oder Logos, die in JaOffice verwendet werden.

Die Elemente von und über JaOffice sind markenrechtlich, wettbewerbsrechtlich sowie durch weitere Gesetze geschützt und dürfen weder ganz noch teilweise kopiert oder imitiert werden. Logos, Grafiken, Sound oder Bilder von BPS bzw. JaOffice Websites dürfen nicht kopiert oder weiterübertragen werden.

Nutzer bzw. der Kunde oder Dritte dürfen nach Einwilligung Inhalte und von JaOffice zu verwenden, sofern der Urheberrechtshinweis sowie dieser Hinweis zur Berechtigung in allen Kopien enthalten ist; die Verwendung der Dokumente von JaOffice ausschließlich zu informatorischen nicht-kommerziellen Zwecken erfolgt und die Dokumente nicht in anderen Medien publiziert werden und keine Veränderungen an den Dokumenten vorgenommen werden.

Sämtliche Informationen werden «wie besehen» und ohne Gewährleistung jeglicher Art zur Verfügung gestellt.

Die auf den Websites veröffentlichten Dokumente, einschließlich der Grafiken, können Ungenauigkeiten und Fehler enthalten.

## Datenschutzerklärung

JaOffice kann auf vielfältige Weise ausschließlich für berufliche Zwecke verwendet werden.

Der Nutzer bzw. der Kunde darf JaOffice nur auf Basis seiner Registrierung bzw. seiner gültigen Lizenzen verwenden.

BPS erhebt Informationen in folgender Art:

Daten, die Nutzer bzw. der Kunde BPS mitteilen: zur Nutzung von JaOffice muss mittels Vor- und Zunamen sowie mittels Eingabe einer offiziell für die betriebliche Kommunikation verwendete eMail-Adresse ein Websystem-Konto zur Verwendung der internetbasierten Softwareplattform erstellt werden und anschließend ein persönliches Passwort erstellt werden. Aus diesen Daten wird ein eigenes, abgeschlossenes, firmeninternes JaOffice-Netzwerk mit einer spezifischen URL erstellt, die den Namen des Unternehmens aus der eMail-Domain enthalten kann.

Informationen, die innerhalb der Nutzung von JaOffice entstehen, wie z.B.

Gerätebezogene Informationen und Verbindungsdaten
z.B. eindeutige Gerätekennungen und Informationen, IP-Adressen etc.

Protokolldaten
z.B. Daten zu Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit Ihrer Anfrage und Referral-URL, Cookies, über die der Browser oder das JaOffice-Nutzer bzw. der Kundekonto eindeutig identifiziert werden können.

Vom Nutzer bzw. der Kunde erstellte, gespeicherte, eingerichtete Elemente sowie Informationen und Inhalte, z.B. Diskussionen, Dateien, Informationen, Bewertungen, anderweitige Texte und weitere Elemente und Funktionen, die der Nutzer bzw. der Kunde individuell für seinen Geschäftsbetrieb anlegen, konfigurieren,

speichern und löschen kann. Sicherheits- und datenschutzbedingt ist dies nur innerhalb des JaOffice-Netzwerks möglich.

Kommunikation
z.B. vom MobilNutzer bzw. der Kunde an das Websystem und vom Websystem an den MobilNutzer bzw. der Kunde (z.B. Nachrichten). JaOffice erfasst nur Nachrichten, die innerhalb von JaOffice erstellt, versendet bzw. empfangen wurden und greift nicht auf Daten zu, die außerhalb der mobilen JaOffice-Applikation auf dem Mobilgerät sind, z.B. Kontaktdaten, Telefonbuch, Bilder etc.; es sei denn, der Nutzer bzw. der Kunde kopiert Daten explizit manuell aus seinem Mobilgerät und verarbeitet diese mittels JaOffice, z.B. das Kopieren einer SMS aus dem Mobilgerät und Einstellen des Textes in JaOffice.

Eindeutige Applikationsnummern
Bestimmte Dienste haben eine eindeutige Anwendungsnummer. Diese Nummer und installationsspezifische Daten, wie zum Beispiel Art des Betriebssystems oder Anwendungsnummer der Version, werden möglicherweise bei der Installation oder Deinstallation des entsprechenden Dienstes an BPS gesendet oder wenn JaOffice zum Beispiel wegen automatischer Updates Kontakt mit dem Server aufnimmt.

Lokale Speicherung
Gegebenenfalls erhebt und speichert BPS Informationen (einschließlich personenbezogene Daten) lokal auf dem Nutzer bzw. der Kundegerät, indem BPS Mechanismen, z.B. den Webspeicher Ihres Browsers und Applikationsdaten-Caches nutzt.

Cookies und anonyme Kennungen
BPS verwendet verschiedene Technologien, um Informationen zu erheben und zu speichern, wenn der Nutzer bzw. der Kunde JaOffice aufruft, darunter auch die Versendung bzw. Speicherung von Cookies oder anonymen Kennungen.

Schriftliche Anfragen bzw. Korrespondenz
Wenn Sie BPS in Schriftform kontaktieren, speichern wir Ihre Kommunikation im gewöhnlichen Rahmen ab, z.B. werden Ihre eMails und z.B. darin enthaltene Kontakte in eMail-Programmen zur Beantwortung bzw. zur Kundenpflege gespeichert.

BPS verwendet diese Daten ausschließlich intern zur Bereitstellung, zur Instandhaltung, zum Schutz sowie zur Verbesserung von JaOffice. Nutzer bzw. der Kundedaten gibt BPS nicht an Dritte weiter, auch nicht anonymisiert zu Marktanalysen oder für sonstige Verwendungen. Ebenso verkauft oder teilt BPS Nutzer bzw. der Kundedaten nicht an oder mit Dritten, in welcher Form auch immer.

Da JaOffice insbesondere seitens mobiler Endgeräte als Applikation des Android oder iOS-Betriebssystems funktioniert, können u.U. Daten, Signale und Inhalte auf der Funktionsebene des mobilen Endgerätes von Dritten anderweitig verwendet werden. Auskunft über diese Datenverwendung geben Nutzungs- und Datenschutzbestimmungen Dritter, z.B. für das Betriebssystem Android und iOS, für die Hardware und Firmware.

BPS stellt Nutzer bzw. der Kunden zum Zwecke der Datentransparenz z.B. innerhalb ihres persönlichen Zugangsbereiches eine Auflistung des erfolgten Austausches ihrer Daten zur Verfügung. Nutzer bzw. der Kunde können damit sehen, wann welche Daten von wem eruiert, eingeholt oder angesehen wurden.

JaOffice ermöglicht, Signale, Daten, Inhalte und Informationen innerhalb des bei der Registrierung und bei Lizenzfreigabe beschränkten Nutzer bzw. der Kundekreises mit anderen zu teilen, Signale, Daten, Inhalte und Informationen, die der Nutzer bzw. der Kunde innerhalb dieses Kreises aufzeichnet bzw. zugänglich macht, werden von JaOffice nur für diesen Nutzer bzw. der Kundekreis verfügbar gemacht.

Der Nutzer bzw. der Kunde des Websystems kann ausgewählte, zusammengefasste Signale, Daten, Inhalte und Informationen aus JaOffice exportieren bzw. weiterleiten bzw. in JaOffice importieren, z.B. Dateien oder Texte.

Im Fall der Nutzung der Cloud-Lösung von JaOffice werden Daten von Auftraggebern und dessen Nutzer bzw. der Kunden ausschließlich in Deutschland verarbeitet und gespeichert, und zwar auf Servern der Strato AG mit Standort in Berlin und Karlsruhe. Die Server sowie Prozesse sind ISO 27001-zertifiziert. Es findet kein Datentransfer, keine Datenverarbeitung- oder speicherung im Ausland statt.

BPS lehnt gegebenenfalls Anfragen ab, die unangemessen oft wiederholt werden, die einen unverhältnismäßigen technischen Aufwand erfordern (beispielsweise die Entwicklung eines neuen Systems oder die grundlegende Änderung einer bestehenden Praxis), die den Schutz personenbezogener Daten — u.a. auch derer Dritter — gefährden oder die nur mit extremen Schwierigkeiten praktisch umsetzbar sind.

Daten, die Nutzer bzw. der Kunde mittels ihrer Bedienoberfläche löschen können, werden zunächst nur gesperrt und dann erst mit zeitlicher Verzögerung endgültig gelöscht, um versehentlichen Löschungen oder evtl. vorsätzlichen Schädigungen vorzubeugen. Wünscht der Nutzer bzw. der Kunde eine sofortige Löschung, gibt er diesen Wunsch formlos und schriftlich an BPS bekannt.

Wünscht der Kunde die Löschung ganzer Netzwerke bzw. Portale oder Extranets, wird dies aus Gründen der Informations- und Datensicherheit üblicherweise durch BPS ausgeführt und nicht durch Nutzer bzw. der Kunde oder den Kunden selbst. Die Löschung von ganzen Netzwerken bzw. Portalen oder Extranets inklusive aller verfügbaren Daten und Informationen wird über eine eMail an den JaOffice Support bekannt gegeben. BPS benennt hieraufhin einen mit der Löschung beauftragten, konkreten Mitarbeiter, sowie Start- und Endzeit des Löschvorgangs. Eine derartige Löschung ist nicht reversibel und wird vom Kunden zwei Mal bestätigt. Alternativ kann BPS dem Kunden entsprechende Skripts bzw. Protokolle zur Verfügung stellen, mittels derer der Kunde direkt oder über eine Beauftragung die Löschung von ganzen Netzwerken bzw. Portalen oder Extranets ohne BPS vornehmen kann. BPS schließt für diesen Fall die Produkthaftung aus, sobald derart gerichtete Skripts bzw. Protokolle durch den Kunden oder im Auftrag des Kunden bereits lediglich auf dem Server installiert werden, auf dem JaOffice betrieben wird.

BPS gibt keine personenbezogenen Daten oder sonstige Informationen bzw. Inhalte an Unternehmen, Organisationen oder Personen außerhalb von BPS weiter, außer es bestehen rechtliche Gründe, um anwendbare Gesetze, Regelungen, oder anwendbares Verfahrensrecht einzuhalten oder einer vollstreckbaren behördlichen Anordnung nachzukommen, Betrug, Sicherheitsmängel oder technische Probleme aufzudecken, zu verhindern oder anderweitig zu bekämpfen, die Rechte, das Eigentum oder die Sicherheit von BPS, unserer Nutzer bzw. der Kunde oder der Öffentlichkeit vor Schaden zu schützen, soweit gesetzlich zulässig oder erforderlich.

Diese Datenschutzerklärung kann sich von Zeit zu Zeit ändern. BPS gibt diese Änderungen bekannt.

## Technische und organisatorische Maßnahmen des Datenschutzes

## ADV – BPS International GmbH

### § 1 Getroffene technische und organisatorische Schutzmaßnahmen

| |
|---|
| (1) Schutzmaßnahmen der **Zutrittskontrolle:** |

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „… Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)“.

Mit dem Begriff „Zutritt“ ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT- Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu.

## 1.1. Grundsätzliche Anforderungen

### 1.1.1. Festlegung von Sicherheitsbereichen

Der Schutzbedarf eines Gebäudes bzw. Raumes ist festzustellen anhand der darin befindlichen DV-Anlagen sowie ggf. sonstiger Unterlagen auf denen personenbezogene Daten verarbeitet bzw. gespeichert werden. BPS International verwendet dreigeteilte Sicherheitsbereiche, von denen der offene durch Mitarbeiter sowie in Begleitung durch Empfangs- und Sicherheitspersonal von Gästen und Lieferanten betreten werden kann. Der Mitarbeiterbereich kann durch elektronische Zugangskontrollen via Chipkarte lediglich von autorisierten Mitarbeitern betreten werden, die in diesen Räumlichkeiten und Sicherheitsbereichen arbeiten (z.B. Stockwerkbeschränkung; Mitarbeiter dürfen mit dem Fahrstuhl unbegleitet nur auf das Stockwerk fahren, auf dem sie tätig sind). Der Hochsicherheitsbereich umfasst Räumlichkeiten, in denen Auftrags- und Kundendaten in Papierform oder in elektronischer Form verarbeitet oder archiviert werden; dieser Bereich kann nur durch einen kleinen Kreis an definierten Mitarbeitern betreten werden und erfolgt ausschließlich durch persönliche Schlüssel- bzw. Zugangsübergabe durch entsprechende Leiter.

Die Erfüllung der Anforderung 1.1.1 wird verpflichtend vereinbart. ☒

### 1.1.2. Realisierung eines wirksamen Zutrittsschutzes

Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Spezialverglasung, Einbruchmeldesystem, Drehkreuz mit Chipkarte, Vereinzelungsanlage, Schließanlage) oder organisatorische (z.B. Pförtner) Maßnahmen abgesichert werden.

Die Erfüllung der Anforderung 1.1.2 wird verpflichtend vereinbart. ☒

### 1.1.3. Festlegung zutrittsberechtigter Personen

Die Voraussetzungen sowie der Kreis der allgemein zutrittsberechtigten Personen müssen festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen, auf das notwendige Minimum beschränkt werden ("Prinzip der minimalen Berechtigung"). Der Zutritt ist bei fehlender Berechtigung zu verwehren. Zutrittsmittel zu Gebäuden bzw. Räumlichkeiten sind grundsätzlich personengebunden zu vergeben und dürfen nicht an Dritte weitergegeben werden. Die Nutzer bzw. der Kunde sind hierfür zu sensibilisieren.

Die Erfüllung der Anforderung 1.1.3 wird verpflichtend vereinbart. ☒

### 1.1.4. Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über

den gesamten Lebenszyklus

Ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten (einschl. Schlüssel-, Sichtausweise, Transponder, Chipkartenverwaltung etc.) ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Sperren von Zutrittsberechtigungen sind zu beschreiben. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zutrittsmittel und -rechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr erforderlichen Räumlichkeiten unverzüglich zu entziehen. Sämtliche mit Sicherheitsaufgaben betraute Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.

Die Erfüllung der Anforderung 1.1.4 wird verpflichtend vereinbart. ☒

### 1.1.5. Begleitung von Besuchern und Fremdpersonal

Es existieren schriftlich fixierte Regelungen zum Zutritt für Firmenfremde, wie Gäste oder Lieferanten. Diese Regelungen beinhalten z.B. die Anforderung, dass Firmenfremde Ihren berechtigten Aufenthalt innerhalb der Gebäude jederzeit nachweisen können, z.B. mittels Gästeausweis, Besucherausweis, oder Lieferantenausweis. Namen und Herkunft (Firmenzugehörigkeit, Geschäftsadresse oder Privatadresse) der Personen sind zu protokollieren. Die stichprobenartige Prüfung des berechtigten Aufenthaltes innerhalb der Gebäude ist obligatorisch. Besteht ein erhöhter Schutzbedarf, sind Personen zu begleiten bzw. während ihrer Tätigkeit zu beaufsichtigen. Dies gilt z.B. ausnahmslos für Hochsicherheitsbereiche.

Die Erfüllung der Anforderung 1.1.5 wird verpflichtend vereinbart. ☒

### 1.1.6. Überwachung der Räume außerhalb der Schließzeiten

Das Gebäude bzw. die Räumlichkeiten, in denen sich DV-Anlagen befinden, auf denen personenbezogene oder personenbeziehbare Daten verarbeitet und/oder gespeichert werden, sind außerhalb der regulären Betriebszeiten zu überwachen. Der Zutritt zu diesen Anlagen darf ausschließlich in Begleitung und niemals von einem Einzelnen erfolgen.

Die Erfüllung der Anforderung 1.1.6 wird verpflichtend vereinbart. ☒

### 1.1.7. Protokollierung des Zutritts

Bei Verwendung von elektronischen Zutrittskontrollanlagen sind die Zutrittsprotokolle 12 Monate revisionssicher aufzubewahren. Zur Missbrauchserkennung sind regelmäßig stichprobenartige Auswertungen vorzunehmen.

Die Erfüllung der Anforderung 1.1.7 wird verpflichtend vereinbart. ☒

(2) Schutzmaßnahmen der **Zugangskontrolle:**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „…zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)...“.

Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden.

## 1.2. Grundsätzliche Anforderungen

### 1.2.1. Zugangsschutz (Authentisierung)

Der Zugang zu DV-Anlagen, auf denen Daten verarbeitet werden, darf erst nach Identifikation und erfolgreicher Authentisierung per Chipkarte der befugten Personen möglich sein. Die Zugangskontrolle erfolgt einmal beim Zutritt zu den zentralen Eingangsbarrieren, gefolgt von einer Zutrittsbeschränkung des Fahrstuhls nur für das Stockwerk, in dem der jeweilige Mitarbeiter arbeitet, gefolgt von einer Zutrittskontrolle an den zentralen Etagentüren der Büroräume sowie eine weitere Zutrittskontrolle für die Räume der technischen Anlagen durch personenbezogene Schlüsselaushändigung und Protollliste inklusive Zeitstempel. Der Zugang ist bei fehlender Berechtigung entsprechend zu verwehren.

Die Erfüllung der Anforderung 2.1.1 wird verpflichtend vereinbart. ☒

### 1.2.2. Starke Authentisierung bei höchstem Schutzniveau

Eine starke Authentisierung erfolgt immer auf Basis mehrerer (mindestens zweier) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer bzw. der Kunde eigenen Eigenschaft (in der Regel biometrische Verfahren). Dies sind:

- Klingel an der Hauptpforte mit Bildkamera bzw. personenbezogene Chipkarte
- Personenbezogene Chipkarte oder geführter Einlass an der Haupteingangstür
- OneTimePassworte (OTP) + Gerät

Die Erfüllung der Anforderung 2.1.2 wird verpflichtend vereinbart. ☒

### 1.2.3. Einfache Authentisierung (per BeNutzer bzw. der Kundename/Passwort) bei hohem Schutzniveau

Passworte müssen angemessenen Mindestregeln entsprechen wie z.B. einer minimalen Passwortlänge und Komplexität. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden. Die Umsetzung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit ist soweit möglich durch technische Einstellungen sicherzustellen.

- Ein Passwort besteht aus mindestens 8 Zeichen.
- Das Passwort setzt sich aus einem Zeichenmix zusammen. Die verfügbaren Zeichen werden in vier Kategorien unterteilt:
  - Kleine Buchstaben z.B. abcdefgh...
  - Große Buchstaben z.B. ABCDEFGH...
  - Ziffern z.B. 123456...
  - Sonderzeichen z.B. !“§$%...
  - Der Zeichenmix muss aus mindestens drei der oben genannten Kategorien bestehen.
- Für das Passwort dürfen keine leicht zu erratenden Begriffe und keine Trivialpasswörter verwendet werden.

- Ein Passwort ist in regelmäßigen Abständen, mindestens jedoch alle 90 Tage zu ändern
- Bei Änderung darf nicht eines der letzten 4 verwendeten Passworte wieder verwendet werden
- Das Passwort darf bei der Eingabe nicht im Klartext auf dem Bildschirm sichtbar wird.
- Das Erstpasswort muss auf sicherem Wege zum Nutzer bzw. der Kunde kommen und/oder dieser mindestens sofort nach erstmaliger Anmeldung aufgefordert werden, dieses zu ändern

Die Erfüllung der Anforderung 2.1.3 wird verpflichtend vereinbart. ☒

### 1.2.4. Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

Das Authentisierungsgeheimnis (z.B. BeNutzer bzw. der Kundekennung und Passwort) darf nie ungeschützt über das Netzwerk übertragen werden.

Die Erfüllung der Anforderung 2.1.4 wird verpflichtend vereinbart. ☒

### 1.2.5. Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen

Nach wiederholter fehlerhafter Authentisierung muss der Zugang gesperrt werden. Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden. BeNutzer bzw. der Kundekennungen, welche über einen längeren Zeitraum nicht genutzt werden (max. 60 Tage), müssen automatisch gesperrt bzw. auf inaktiv gesetzt werden.

Die Erfüllung der Anforderung 2.1.5 wird verpflichtend vereinbart. ☒

### 1.2.6. Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)

Zugriffspasswörter und/oder Formulareingaben dürfen nicht auf dem Client selbst oder in seiner Umgebung abgelegt werden (z.B. Speicherung im Browser, „Passwortdatenbanken“ oder Haftnotizen). Die Nutzer bzw. der Kunde sind hierfür zu sensibilisieren.

Die Erfüllung der Anforderung 2.1.6 wird verpflichtend vereinbart. ☒

### 1.2.7. Festlegung befugter Personen

Der Kreis der Personen, die befugt Zugang zu DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden (können), ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum zu beschränken. Zugänge für temporär beschäftigte Personen (Berater, Praktikanten, Auszubildende) müssen individuell vergeben werden. Wieder verwendbare Kennungen (z.B. Berater1, Azubi1, etc.) dürfen nicht vergeben werden.

Die Erfüllung der Anforderung 2.1.7 wird verpflichtend vereinbart. ☒

### 1.2.8. Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist einzurichten, zu beschreiben und zwingend anzuwenden. Dieser beinhaltet mindestens einen Beantragungs- und Genehmigungsprozess sowie den Prozess zur Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen.

Die Vergabe von Zugangsberechtigungen darf immer nur für diejenigen DV- Anlagen(-typen) erfolgen, zu welchen der Zugang im Rahmen der Aufgabenwahrnehmung notwendig ist ("Prinzip der minimalen Berechtigung"). Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu DV-Anlagen sind

grundsätzlich personengebunden zu vergeben und an ein persönliches Credential (z.B. Passwort, Token, Chipkarte) zu knüpfen (BeNutzer bzw. der Kundekennung). Authentifizierungsmedien und/oder BeNutzer bzw. der Kundekennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden. Die Nutzer bzw. der Kunde sind hierfür zu sensibilisieren.

Regelungen und Verfahren zum Sperren und datenschutzgerechten Löschen von Zugangskennungen müssen beschrieben werden. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Authentifizierungsmedien und Zugangsberechtigungen zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV-Anlagen, unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration).

Die Erfüllung der Anforderung 2.1.8 wird verpflichtend vereinbart. ☒

#### 1.2.9. Protokollierung des Zugangs

Alle erfolgreichen und abgewiesenen Zugangsversuche müssen protokolliert (verwendete Kennung, Rechner, IP-Adresse) und für mindestens 6 Monate revisionssicher archiviert werden. Zur Missbrauchserkennung sind regelmäßig stichprobenartige Auswertungen vorzunehmen.

Die Erfüllung der Anforderung 2.1.9 wird verpflichtend vereinbart. ☒

### 1.3. Maßnahmen am Arbeitsplatz des Anwenders

#### 1.3.1. Automatische Zugangssperre

Bei mehr als fünf Minuten Inaktivität der Arbeitstation bzw. des Terminals muss ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert werden.

Die Erfüllung der Anforderung 2.2.1 wird verpflichtend vereinbart. ☒

#### 1.3.2. Manuelle Zugangssperre

Arbeitsstationen und Terminals sind bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu schützen (z.B. durch manuelle Aktivierung des kennwortgeschützten Bildschirmschoners, durch Sperrung des Systems über den Task- Manager oder Abmeldung). Die Mitarbeiter sind hierfür zu sensibilisieren.

Die Erfüllung der Anforderung 2.2.2 wird verpflichtend vereinbart. ☒

(3) Schutzmaßnahmen der **Zugriffskontrolle:**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „…zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle)“.

Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können.

## 1.4. Grundsätzliche Anforderungen

### 1.4.1. Erstellen eines Berechtigungskonzepts

Ein Berechtigungskonzept (BeNutzer bzw. der Kunde- und Administrationsberechtigungen) stellt sicher, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des BeNutzer bzw. der Kundes erforderlich ist. Regelungen und Verfahren zum Anlegen, Ändern und datenschutzgerechten Löschen von Berechtigungsprofilen bzw. BeNutzer bzw. der Kunderollen sind darin zu beschreiben. Aus dem Berechtigungskonzept muss hervorgehen, welche Aufgabenträger Administrationsaufgaben (System, BeNutzer bzw. der Kunde, Betrieb, Transport) wahrnehmen und welche BeNutzer bzw. der Kundegruppen, welche Aktivitäten im System durchführen können. Verantwortlichkeiten sind geregelt.

Die Erfüllung der Anforderung 3.1.1 wird verpflichtend vereinbart. ☒

### 1.4.2. Umsetzung von Zugriffsbeschränkungen

Mit jeder Zugangsberechtigung muss eine Zugriffsberechtigung verknüpft sein, beispielsweise durch die Verknüpfung mit einer oder mehrere im Berechtigungskonzept definierten Rollen. Jeder Zugangsberechtigte darf nur mit den Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.

Soweit Datenbestände mehrer Auftraggeber in einer Datenbank gespeichert oder mit einer Datenverarbeitungsanlage verarbeitet werden, sind logische Zugriffseinschränkungen vorzusehen, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet sind (Mandantenfähigkeit). Zudem ist die Datenverarbeitung selbst soweit einzuschränken, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Daten verwendet werden können.

Es werden in den Datenverarbeitungsanlagen eindeutige Merkmale eingebaut, die es der zugreifenden Person ermöglicht, zu erkennen, dass es sich um eine authentische Datenverarbeitungsanlage handelt. Zudem muss sich auch der Zugriffsberechtigte gegenüber der Datenverarbeitungsanlage anhand von nachprüfbaren eindeutigen Merkmalen identifizieren und authentisieren lassen, z.B. mittels Ausweislesern an den Terminals.

Die Erfüllung der Anforderung 3.1.2 wird verpflichtend vereinbart. ☒

### 1.4.3. Vergabe minimaler Berechtigungen

Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum zu beschränken. Soweit bestimmte Funktionen ohne Verlust der Qualität der

Datenverarbeitung zeitlich beschränkbar sind, sind Zugriffe auf die personenbezogene Daten und Berechtigungen zeitlich zu begrenzen.

Die Erfüllung der Anforderung 3.1.3 wird verpflichtend vereinbart. ☒

### 1.4.4. Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Erteilen/Entziehen von Berechtigungen bzw. der Zuweisung von BeNutzer bzw. der Kunderollen sind zu beschreiben. Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Berechtigungen sind an eine persönliche BeNutzer bzw. der Kundekennung und an einen Account zu knüpfen. Dies schließt den Einsatz von mehreren Personen genutzten Gruppenkennungen/-passwörtern aus.

Bei der Vergabe der Berechtigungen bzw. Zuweisung von BeNutzer bzw. der Kunderollen dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Dabei ist sicherzustellen, dass die im System abgebildete Funktionstrennung nicht durch kumulierte Berechtigungen aufgehoben wird.

Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zugriffsrechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV- Anlagen und Speicherbereichen unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration). Die Dokumentationen sind 12 Monate aufzubewahren.

Die Erfüllung der Anforderung 3.1.4 wird verpflichtend vereinbart. ☒

### 1.4.5. Vermeidung der Konzentration von Funktionen

Sowohl in Applikationen als auch im administrativen Bereich ist eine Konzentration von Funktionen zu vermeiden. Es ist zu vermeiden, dass durch eine geeignete Konzentration von verschiedenen Rollen bzw. Zugriffsrechten auf eine Person diese in der Kombination eine übermächtige Gesamtrolle erhalten kann und dadurch Kontrollmöglichkeiten ausgeschaltet werden. Beispielsweise kann ein Datenbank-Administrator, der gleichzeitig Anwender der Applikation ist, Transaktionen durch direkte Zugriffe auf das Datenbankmanagementsystem manipulieren oder Daten einsehen, die nicht seiner Rolle entsprechen. Insbesondere gilt dies für die Protokollierungstechniken für die Zugriffe auf personenbezogene Daten. Hier dürfen nicht dieselben Personen das Protokollierungssystem administrieren, deren unerlaubte Zugriffe ggf. erkannt werden sollen.

Die Erfüllung der Anforderung 3.1.5 wird verpflichtend vereinbart. ☒

### 1.4.6. Protokollierung des Datenzugriffs

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen müssen protokolliert (BeNutzer bzw. der Kundekennung, Transaktionsdetails) werden. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 6 Monaten auszugehen. Geeignete Verfahren zu Missbrauchserkennung und zur anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren. Backend-Zugriffe auf Daten oder Informationen des Kunden und / oder seiner Nutzer bzw. der Kunde erfolgen ausschließlich auf schriftlich dokumentierten Wunsch des Kunden und nach seiner Einwilligung, in der Art, dass BPS Start- und Endzeitpunkt des Zugriffs, den Umfang des Zugriffs auf Backend-Daten sowie den damit betrauten

Mitarbeiter benennt sowie der Person, die den Vorgang nach dem 4-Augen-Prinzip überwacht.

Die Erfüllung der Anforderung 3.1.6 wird verpflichtend vereinbart. ☒

(4) Schutzmaßnahmen der **Weitergabekontrolle:**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „…zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)".

## 1.5. Allgemeine Anforderungen

### 1.5.1. Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl

Für jedes IT-/NT-System, in dem personenbezogene Daten übermittelt werden, ist eine Protokollierung der Übermittlung notwendig. In welcher Form (vollständig oder beispielweise beschreibend nach Art der Daten/ Sender und Empfänger) hängt im Einzelfall davon ab, ob die Protokollierung in einem vertretbaren Aufwand möglich ist, wer die Daten mit wem (Übermittlung zwischen zwei vertrauenswürdigen Instanzen?) austauscht und wie die Übermittlung stattfindet (verschlüsselt/unverschlüsselt). Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 6 Monaten auszugehen. Geeignete Verfahren zu Missbrauchserkennung und zur Anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren.

Die Erfüllung der Anforderung 4.1.1 wird verpflichtend vereinbart. ☒

### 1.5.2. Rechtmäßigkeit der Weitergabe ins Ausland

Die Erhebung bzw. die Verarbeitung und Speicherung von Daten findet ausschließlich in Deutschland statt. Hierfür verwendet BPS ISO 27001-zertifizierte Server der Strato AG mit Standort Berlin und Karlsruhe oder den Server des Auftraggebers. Eine Erhebung bzw. Verarbeitung von Daten im Geltungsbereich des Telekommunikationsgesetzes in Nicht-EU-Staaten ist grundsätzlich unzulässig.

Die Erfüllung der Anforderung 4.1.2. wird verpflichtend vereinbart. ☒

## 1.6. Transport über Netze

Daten werden überwiegend in Netzen mit entsprechenden Protokollen ausgetauscht. Authentisierung und Verschlüsselung sowie eine geeignete Netzarchitektur sind die Maßnahmen, um das Risiko des unbefugten Kopierens und Änderns personenbezogener Daten zu reduzieren.

### 1.6.1. Sichere Datenübertragung zwischen Server und Client

Die Datenübertragungen zwischen Clients und Servern wird generell verschlüsselt und zwar wie folgt:

- Secure Socket Layer/Transport Layer Security (SSL/TLS) in Verbindung mit validen Zertifikaten

bei Web-Anwendungen (auch als https bekannt)

- Secure Shell
- Secure Network Communication (SNC) bei der Kommunikation zwischen SAP-GUI und SAP ERP oder R/3
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC mit Verschlüsselungsoption RC4
- SFTP
- SQLNet mit Advanced Security Option (ASO).
- XML Dateien verschlüsseln mit XML Encryption bei SOAP-Protokollen

Die Erfüllung der Anforderung 4.2.1 wird verpflichtend vereinbart. ☒

### 1.6.2. Sicherung der Übertragung im Backend

Werden personenbezogene Daten innerhalb des Backends zwischen einzelnen Systemen ausgetauscht, so ist genau zu betrachten, wie die einzelnen Verbindungen gegen unbefugten Zugriff geschützt sind. Verlassen die Daten nicht den gesicherten Bereich des Rechenzentrums und kann ausgeschlossen werden, dass beispielsweise die Administratoren der Netzkomponenten die Daten abfangen können, dann kann auf die Verschlüsselung der Übertragungsstrecke bei geringem und mittlerem Schutzbedarf verzichtet werden. Daten mit hohem Schutzbedarf sind beim Transport zu verschlüsseln. Sobald die Daten über längere Strecken (beispielsweise zu einem anderen Rechenzentrum) übertragen werden, ist die Verschlüsselung des Transports zwingend notwendig.

Die Erfüllung der Anforderung 4.2.2 wird verpflichtend vereinbart. ☒

### 1.6.3. Übertragung zu externen Systemen

Werden personenbezogene Daten zu externen Systemen übertragen, ist eine Verschlüsselung zwingend erforderlich.

Die Erfüllung der Anforderung 4.2.3 wird verpflichtend vereinbart. ☒

## 1.7. Logischer Zugang zu Systemen

Um unbefugte Zugriffe auf Systeme zu minimieren, muss der logische Zugang zu den Systemen begrenzt werden. Das bedeutet, dass die möglichen Kommunikationsbeziehungen auf das notwendige Maß reduziert und kontrolliert werden müssen.

### 1.7.1. Risikominimierung durch Netzseparierung

Um das Risiko zu mindern, dass personenbezogene Daten, die zwischen IT-Systemen weitergegeben werden, auf dem Netz mitgelesen werden, müssen für diese IT-Systeme Netzsegmente gebaut werden. Solche Netzsegmente können mit Hilfe von Switches und Routern konfiguriert werden. Datenpakete, egal auf welcher Ebene, verlassen und erreichen die IT-Systeme in diesen Segmenten nur über definierte Schnittstellen, an denen weitere Maßnahmen der Weitergabekontrolle ergriffen werden können. Diese Segmentierung muss mindestens eine Trennung zwischen Frontend- und Backendsystemen vorsehen. Innerhalb des Backends wird eine sinnvolle Segmentierung ebenfalls dringend empfohlen.

Die Erfüllung der Anforderung 4.3.1 wird verpflichtend vereinbart. ☒

### 1.7.2. Implementation von Sicherheitsgateways an den Netzübergabepunkten

Die IT-/NT-Systeme, auf denen personenbezogene Daten verarbeitet werden, sind durch dem aktuellen Stand der Technik entsprechende Maßnahmen (i.d.R. Firewalls) vor unerwünschten Zugriffen oder Datenströme sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen. Unabhängig davon, ob es sich um Netzwerk-/Hardware-Firewalls oder ergänzend dazu um hostbasierte Firewalls handelt, müssen diese dauerhaft aktiviert sein. Jedwede Deaktivierung oder Umgehung der Funktionen durch den Anwender muss dabei wirksam ausgeschlossen werden. Das Regelwerk muss so augesetzt werden, dass alle Kommunikationsbeziehungen außer den notwendigen automatisch geblockt werden.

Die Erfüllung der Anforderung 4.3.2 wird verpflichtend vereinbart. ☒

### 1.7.3. Härtung der Backendsysteme

Die Backendsysteme müssen nach dem Stand der Technik gehärtet werden, damit sich ein Angreifer nicht aufgrund von Schwachstellen unbefugt Zugriff auf die Systeme und Daten verschaffen kann.

Die Erfüllung der Anforderung 4.3.3 wird verpflichtend vereinbart. ☒

## 1.8. Schnittstellen

### 1.8.1. Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder

Alle Schnittstellen zu anderen IV-Verfahren sind zu dokumentieren. Diese Dokumentation muss die folgenden Informationen beinhalten:

- alle personenbezogenen Datenfelder
- Richtung der Übermittlung (Import/ Export)
- der jeweilige Verwendungszweck für die Übermittlung
- das IV-Verfahren/ die Schnittstelle, an das die Daten exportiert werden
- Art der Authentisierung der Schnittstelle
- Schutz der Übertragung (z.B. Verschlüsselung)

Insbesondere sind auch Import- und Exportschnittstellen aus bzw. in Dateien zu beschreiben, und wie deren Verwendung technisch oder organisatorisch geschützt wird. Auch Datenmigrationen sind entsprechend als Schnittstelle zu beschreiben.

Die Erfüllung der Anforderung 4.4.1 wird verpflichtend vereinbart. ☒

### 1.8.2. Umsetzung einer Maschine-Maschine- Authentisierung

Werden personenbezogene Daten zwischen IT-/NT-Systemen ausgetauscht, dann sollte jedes System über eine eindeutige und verifizierbare elektronische Identität verfügen. Damit kann das Risiko begrenzt werden, dass nicht autorisierte Systeme stellvertretend agieren und personenbezogene Daten empfangen bzw. einen autorisierten Empfänger vortäuschen können.

Die Erfüllung der Anforderung 4.4.2 wird verpflichtend vereinbart. ☒

## 1.9. Speicherung/Aufbewahrung

### 1.9.1. Sichere Ablage von Daten

Zur sicheren Ablage personenbezogener Daten mit höchstem Schutzniveau ist eine verschlüsselte Datenablage vorzusehen. Dies gilt auch für etwaige Backups. Für JaOffice ist diese SSL-verschlüsselt.

Die Erfüllung der Anforderung 4.5.1 wird verpflichtend vereinbart. ☒

### 1.9.2. Automatisierte Löschung temporärer Zwischenspeicher

Temporäre Zwischenspeicher (z.B. der Browsercache oder der TEMP-Ordner des Betriebssystems) sind so zu konfigurieren, dass Ihre Inhalte sofern möglich unmittelbar bei jedem Beenden oder aber spätestens beim Start der Anwendung (z.B. des Browsers) bzw. des Betriebssystems automatisiert gelöscht werden.

Die Erfüllung der Anforderung 4.5.2 wird verpflichtend vereinbart. ☒

### 1.9.3. Zugriff auf lokale Zwischenspeicher

Jeder Zugriff auf etwaige lokal abgelegte Zwischenspeicher oder Datenbanken, die Kundendaten des Auftraggebers enthalten, zu Zwecken bzw. mit Anwendungen, die der Auftraggeber nicht freigegeben (resp. - sofern einschlägig - bereitgestellt) hat, ist unzulässig und sofern möglich technisch zu verhindern.

Die Erfüllung der Anforderung 4.5.3 wird verpflichtend vereinbart. ☒

### 1.9.4. Gesicherte Speicherung auf mobilen Datenträgern

Die Speicherung auf mobilen Datenträgern ist aufgrund des hohen Verlustrisikos zu vermeiden. Sollte eine Speicherung dennoch unumgänglich sein, so sind die darauf gespeicherten Daten zu verschlüsseln. Nicht mehr benötigte Daten sind umgehend datenschutzgerecht zu löschen.

Die verwendete Hardware ist zudem gegen Verlust/Diebstahl zu schützen (Nutzung von Kabelschlössern, geeignete verschließbare Transportbehältnisse,…)

Die Erfüllung der Anforderung 4.5.4 wird verpflichtend vereinbart. ☒

### 1.9.5. Einführung eines Prozesses zur Datenträgerverwaltungen

Es muss eine qualifizierte Datenträgerverwaltung existieren. Die Verwaltung der Datenträger muss dokumentieren, wie viele Datenträger mit personenbezogenen Daten für welche Aufgaben und Verarbeitungen erstellt wurden und wo diese bis zur Vernichtung gelagert werden. Über den Bestand der Datenträger ist regelmäßig eine Bestandskontrolle durchzuführen. Eine Lagerung der erstellten Datenträger in einem kontrollierten Sicherheitsbereich ist bei personenbezogenen Daten obligatorisch. Darüber hinaus wird die Anfertigung von Kopien von Datenträgern dokumentiert und für einen Zeitraum von 12 Monate ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Die Erfüllung der Anforderung 4.5.5 wird verpflichtend vereinbart. ☒

### 1.9.6. Sichere Datenträgeraufbewahrung

Die bereitgestellten oder abgerufenen personenbezogenen Daten sind in Sicherheitsschränken, z.B. Datasafes aufzubewahren, soweit der Auftrag oder die Datenverarbeitung an sich eine Gewährleistung der Verfügbarkeit erfordert.

Die Erfüllung der Anforderung 4.5.6 wird verpflichtend vereinbart. ☒

## 1.10. Sicherer Versand von Daten

### 1.10.1. Einführung und Umsetzung von Versandvorschriften

Es existieren Verpackungs- und Versandvorschriften für den Transport von personenbezogenen Daten mittels Datenträgern. Diese Versandvorschriften orientieren sich an dem Schutzbedarf der zu übermittelnden personenbezogenen Daten. Für personenbezogene Daten ist eine Verschlüsselung der

personenbezogenen Daten vor der Übermittlung obligatorisch. Ferner wird durch Arbeitsanweisung festgelegt, welche Personen befugt sind, personenbezogene Daten zu übermitteln. Die eigentliche Übermittlung wird dann im Vier-Augen-Prinzip veranlasst und dokumentiert.

Soweit Datenträger durch Transportunternehmen übermittelt werden, werden die Datenträger nur nach vorheriger Authentisierung des Transportunternehmens (Post, Spediteur, Kurierdienst, Taxifahrer, etc.), notfalls durch telefonische Rückversicherung beim Transportunternehmen, herausgegeben. Soweit sehr große Datenbestände transportiert werden (>250.000 Datensätze) ist eine Begleitung des Transportes obligatorisch. Die Herausgabe der Datenträger an das Transportunternehmen ist zu dokumentieren. Nach jeder Übermittlung und nach jedem Transport sind die übermittelten Datenmengen zu plausibilisieren. Zudem werden die Vollständigkeit der Datenmengen und die Integrität geprüft.

Die Erfüllung der Anforderung 4.6.1 wird verpflichtend vereinbart. ☒

## 1.11. Sichere Löschung, Entsorgung und Vernichtung

### 1.11.1. Prozess zur Sammlung und Entsorgung

Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern in Papierform ist einzurichten und zu beschreiben. Dabei werden Regelungen und Verfahren zur sicheren Sammlung und internen Weitergabe sowie zu Lagerung, Transport und Vernichtung unter Berücksichtigung medientypischer Eigenarten in einer Organisationsrichtlinie/Verfahrensanweisung beschrieben. Das datenschutzgerechte Vernichten bzw. Löschen ist arbeitsplatz- und zeitnah durchzuführen, um ein Zwischenlagern der Datenträger weitgehend zu vermeiden. Dadurch wird auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht. Alternative Entsorgungswege sind organisatorisch auszuschließen. Die Mitarbeiter sind hierfür regelmäßig zu sensibilisieren.

Die Erfüllung der Anforderung 4.7.1 wird verpflichtend vereinbart. ☒

### 1.11.2. Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des HauptNutzer bzw. der Kundes) oder Weitergabe an externe Stellen datenschutzgerecht gelöscht werden (siehe Annex 4). Die Formatierung ist als sicheres Löschverfahren ungeeignet. Es müssen andere sichere Lösch-/ Zerstörungsverfahren gewählt werden, die eine Rekonstruktion der Daten nur mit hohem Aufwand erlauben.

Die Erfüllung der Anforderung 4.7.2 wird verpflichtend vereinbart. ☒

### 1.11.3. Führung von Löschprotokollen

Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten ist zu protokollieren. Die Protokolle sind mindestens 12 Monate revisionssicher zu archivieren.

Die Erfüllung der Anforderung 4.7.3 wird verpflichtend vereinbart. ☒

(5) Schutzmaßnahmen der **Eingabekontrolle::**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: "… zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)".

### 1.12. Grundsätzliche Anforderungen

#### 1.12.1. Dokumentation der Eingabeberechtigungen

Es existiert eine Dokumentation, welche Person aufgrund ihrer Aufgabenstellung befugt und verantwortlich ist, Eingaben in der Datenverarbeitungsanlage vorzunehmen.

Die Erfüllung der Anforderung 5.1.1 wird verpflichtend vereinbart. ☒

#### 1.12.2. Protokollierung der Eingaben

Die Eingaben in die Datenverarbeitungsanlage werden protokolliert. Die Protokolle sind für einen Zeitraum von 12 Monaten aufzubewahren.

Die Erfüllung der Anforderung 5.1.2 wird verpflichtend vereinbart. ☒

(6) Schutzmaßnahmen der **Verfügbarkeitskontrolle:**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „…zu gewährleisten, dass personen-bezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)".

### 1.13. Backup-Konzept

#### 1.13.1. Backup-Konzept

Um die Verfügbarkeit der Daten auch im Notfall sicherzustellen, müssen die Daten regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept erstellt werden, dass einen befugten Mitarbeiter in die Lage versetzt, sämtliche Mittel für die Wiederherstellung der Daten so zu nutzen, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung stehen.

Die Erfüllung der Anforderung 7.1.1 wird verpflichtend vereinbart. ☒

### 1.14. Disaster-Recovery

#### 1.14.1. Notfallplan

Der Auftraggeber ist über jede Störung (z.B. vorsätzlicher Angriff intern/extern) und Außerbetriebnahme der Datenverarbeitung schnellstmöglich zu informieren. Liegen Anzeichen für eine Störung vor, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Notfallplan zu erstellen, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche

Personen, insb. auch auf Seite des Auftraggebers, über den Vorfall zu unterrichten sind.

Die Erfüllung der Anforderung 7.1.2 wird verpflichtend vereinbart. ☒

### 1.14.2. Aufbewahrung der Backups

Eine Lagerung von Datensicherungen hat in feuer- und wassergeschützten Datensicherheitsschränken stattzufinden.

Die Erfüllung der Anforderung 7.2.2 wird verpflichtend vereinbart. ☒

### 1.14.3. Prüfung der Notfalleinrichtungen

Es hat eine regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter stattzufinden.

Die Erfüllung der Anforderung 7.2.3 wird verpflichtend vereinbart. ☒

(7) Schutzmaßnahmen der **Trennungskontrolle:**

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „… zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“.

## 1.15. Grundsätzliche Anforderungen

### 1.15.1. Sparsamkeit bei der Datenerhebung

Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses mindestens notwendig sind.

Die Erfüllung der Anforderung 8.1.1 wird verpflichtend vereinbart. ☒

### 1.15.2. Getrennte Verarbeitung

Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.

Wünscht ein Auftraggeber die Verarbeitung seiner Daten auf einer separaten, physisch getrennten und abgeschirmten Anlage, gibt er dies vor Angebotslegung und Vertragsunterzeichnung bekannt. Für den Auftraggeber wird hieraufhin eine solche DV-Anlage bereitgestellt, u.U. gegen Aufpreis.

Die Erfüllung der Anforderung 8.1.2 wird verpflichtend vereinbart. ☒

## 1.16. Grundsätzliche Anforderungen

### 1.16.1. Prozessdefinition /-kontrolle

Für die Verarbeitung von Daten im Unternehmen müssen Prozesse und Arbeitsabläufe definiert sein. Die Umsetzung und Einhaltung der Prozesse ist zu kontrollieren. Hierzu zählen vor allem die physische und organisationsbedingte Trennung von Entwicklungs-, Test- und Produktionsbetrieb.

Die Erfüllung der Anforderung 9.1.1 wird verpflichtend vereinbart. ☒

### 1.16.2. Funktionstrennung und -zuordnung

Im nächsten Schritt ist die Funktionstrennung festzulegen, zu dokumentieren und zu begründen, d.h. welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür ergeben sich aus den Aufgaben selbst, den Anforderungen dieser Vereinbarung (insb. dem Katalog der Mindestvorgaben sowie ergänzender Standards) und aus gesetzlichen Bestimmungen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar. Nach der Festlegung der einzuhaltenden Funktionstrennung erfolgt Zuordnung der Funktionen zu Personen.

Die Erfüllung der Anforderung 9.1.5 wird verpflichtend vereinbart. ☒

(8) Maßnahmen zur **Datenlöschung:**

## 1.17. Sichere Löschung, Entsorgung und Vernichtung

### 1.17.1. Prozess zur Sammlung und Entsorgung

Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern in Papierform ist einzurichten und zu beschreiben. Das datenschutzgerechte Vernichten bzw. Löschen von Daten ist arbeitsplatz- und zeitnah durchzuführen, um ein Zwischenlagern der Datenträger weitgehend zu vermeiden. Dadurch wird auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht. Alternative Entsorgungswege sind organisatorisch auszuschließen. Die Mitarbeiter sind hierfür regelmäßig zu sensibilisieren.

Gelöschte Daten sind nicht wiederherstellbar und die Löschung kann, sofern sie einmal initialisiert ist, nicht rückgängig gemacht werden. Daten in bzw. aus Datenbanken werden ebenso derartig aus den Strukturen gelöscht, dass die Löschung nicht rückgängig gemacht werden kann.

Die Löschung findet von Daten findet bei BPS International mittels Software und turnusmäßig nach den gesetzlichen Anforderungen statt. Sofern ein Auftraggeber bekannt gibt, dass etwaige Daten umgehend zu löschen sind, z.B. bei erkanntem Datenmissbrauch durch Personal des Auftraggebers, erfolgt dies durch manuelle Tätigkeit eines konkreten, zuzuweisenden BPS-Mitarbeiters, der die Löschung protokolliert und bestätigt.

Datenträger, deren Daten gelöscht wurden, werden zusätzlich physikalisch zerstört.

Daten und Informationen in Papierform (hard copy) werden durch DIN 32757-1 zertifizierte Shredder vernichtet.

Die Erfüllung der Anforderung 4.7.1 wird verpflichtend vereinbart. ☒

### 1.17.2. Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des HauptNutzer bzw. der Kundes) oder Weitergabe an externe Stellen datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet. Es müssen andere sichere Lösch-/ Zerstörungsverfahren gewählt werden, die eine Rekonstruktion der Daten nur mit hohem Aufwand erlauben.

Die Erfüllung der Anforderung 4.7.2 wird verpflichtend vereinbart. ☒

### 1.17.3. Führung von Löschprotokollen

Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten ist zu protokollieren. Die Protokolle sind mindestens 12 Monate revisionssicher zu archivieren.

Die Erfüllung der Anforderung 4.7.3 wird verpflichtend vereinbart. ☒

(9) Schutzmaßnahmen für sichere **Softwareentwicklung: (optional)**

BPS International hat sich verpflichtet, durch die grundlegenden Verträge mit seinen wichtigsten Kunden und Partnern Swisscom, Deutsche Telekom sowie für MTS GSM und staatliche Organe, auf externes Personal sowie auf Outsourcing zu verzichten. Alle Entwicklungs-, Projekt- und Integrationsaufgaben werden ausschließlich intern und durch internes Personal abgewickelt und zwar in der Art, dass Mitarbeiter, die mit Entwicklungsaufgaben betraut sind, nicht und nicht zusätzlich für Aufgaben in bzw. an Produktivanlagen eingesetzt werden.

Die Entwicklung von Systemen findet ortsgetrennt und Barriere-geschützt von Produktivanlagen statt und auch von Prozessen, die Systeme oder Vorgänge von Auftraggebern betreffen.

Programmänderungen und anderweitige Arbeiten an Systemen oder Anlagen werden elektronisch mit Personal-, Zeit- und Ortsstempeln protokolliert.

Zur internen Kommunikation während der Software-Entwicklung werden ausschließlich abgeschirmte und geschützte Systeme verwendet.

Während der Software-Entwicklung werden Test- und Probationsserver (IIS7) eingesetzt, die ausschließlich in den Räumlichkeiten der BPS International GmbH stehen und nicht einen auswärtigen Standort oder Verarbeitungsort haben, wobei diese Anlagen sowohl physisch wie auch organisationsbedingt von Produktivsystemen- und anlagen sowie von deren Arbeitsprozessen getrennt sind.

Bei BPS International gilt die physische und organisationsbedingte Trennung von Entwicklungs-, Test- und

Produktionsbetrieb.

Zur Entwicklung von Software verwendet BPS International ausschließlich zertifizierte und geschützte Plattformen, wie Microsoft Visual Studio 2013 und Microsoft SQL Server 2008 r2.

BPS International GmbH, München
Letzte Aktualisierung: 01.08.2015, 17:50 MEZ