Technische und Organisatorische Maßnahmen Gemäß Art. 32 DSGVO

Anhang 1 zur Vereinbarung über Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: 21.03.202418
Version: 1.00
Dokumenten-Verantwortlicher: IPAX Geschäftsführung

IPAX GmbH
Donaustraße 106
3400 Klosterneuburg
Österreich
Telefon: +43 1 3670030
E-Mail: office@ipax.at
Web: www.ipax.at

Inhaltsverzeichnis

Einleitung

DGSVO bezeichnet die VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

In weiterer Folge wird der Auftraggeber für die Auftragsverarbeitung (Vertragspartner des Auftragsverarbeitungs-Vertrages) als **Kunde** und die IPAX GmbH als Auftragsverarbeiter als **IPAX** bezeichnet.

Diese Dokument beschreibt die Technischen und Organisatorischen Maßnahmen die IPAX im Zuge eines Auftragsverarbeitungs-Vertrages (gem. Art. 28 DSGVO) mit dem Kunden ergreift. IPAX behält sich das Recht vor dieses Dokument regelmäßig zu ändern und zu aktualisieren. Es gilt die zum Abschluss des Auftragsverarbeitungs-Vertrages gültige Fassung als vereinbart. IPAX behält sich weiters das Recht vor vereinbarte technischen und organisatorischen Maßnahmen jederzeit zu ändern, solange sie den gleichen oder besseren Schutz von personenbezogenen Daten bewirken – insbesondere wenn dies aufgrund des technischen Fortschrittes erforderlich ist.

Äquivalenzlisten Produktgruppen

Die konkreten technischen und organisatorischen Maßnahmen sind vom dem jeweiligen von IPAX bezogenen Produkt abhängig und in den folgenden Punkten nach Produktgruppen zusammengefasst. Die Nachfolgende Tabelle gibt Aufschluss welches Produkt unter welche Produktgruppe fällt. Für das jeweilige Produkt gelten nur die unter der zugehörigen Produktgruppe explizit angeführten technischen und organisatorischen Maßnahmen. Manche Maßnahmen sind zudem von dem Bestehen von Zusatzverträgen abhängig.

Produkt Produktbezeichnung lt. Homepage/Vertrag/Rechnung	**Produktgruppe** im Sinne dieses Dokuments	**Standort**
VIRTUAL line	V-Server	INTERXION Wien
VIRTUAL line Performance SSD	V-Server	INTERXION Wien
VIRTUAL line Windows	V-Server	INTERXION Wien
VIRTUAL line High Availability	V-Server	INTERXION Wien
HYBRID line	V-Server	INTERXION Wien
Managed Webserver	V-Server	INTERXION Wien
POWER line	Rootserver	INTERXION Wien, IP.ONE Wien
PROFESSIONAL line	Rootserver	INTERXION Wien, IP.ONE Wien
BUSINESS line	Rootserver	INTERXION Wien
Rootserver Sonderangebote, sonstige Rootserver, legacy Rootserver Produkte, individuell konfigurierte dedizierte Server, Basic Server, Medium Server, Cluster Server	Rootserver	INTERXION Wien, IP.ONE Wien
Für jedes Rootserver Produkt mit Zusatzvertag Managed Virtualization (Host-Virtualisierung)	V-Server	INTERXION Wien, IP.ONE Wien
Backup Storage	Backupspeicherplatz	INTERXION Wien, IP.ONE Wien
Backupspace	Backupspeicherplatz	INTERXION Wien, IP.ONE Wien
Cloud Backup	Cloud-Speicher	INTERXION Wien
Cloud Workspace	Cloud-Speicher	INTERXION Wien
Webhost Plus	Webhosting & Mailhosting	INTERXION Wien
Business Host	Webhosting & Mailhosting	INTERXION Wien
Managed Wordpress	Webhosting & Mailhosting	INTERXION Wien
Serverhousing*	Server- und Rackhousing*	INTERXION Wien, IP.ONE Wien
Rackhousing*	Server- und Rackhousing*	INTERXION Wien, IP.ONE Wien

*Bei diesen Produkten liegt keine Verarbeitungstätigkeit im Sinne der DSGVO durch IPAX vor. Die für diese Produkte vorgesehenen technischen und organisatorischen Maßnahmen (i.d.R. reine Infrastruktur-Bereitstellung) sind nur aufgeführt, um es unseren Kunden zu ermöglichen, Ihre eigenen Verzeichnisse gemäß Art. 32 DSGVO zu erstellen.

Technische und Organisatorische Maßnahmen Gemäß Art. 32 DSGVO

1. Vertraulichkeit

1.1. Zutrittskontrolle

1.1.1. Für Verträge über ***Webhosting***, ***Mailhosting***, ***Cloud-Speicher***, ***V-Server***, ***Rootserver mit Standort INTERXION Wien***, ***Backupspeicherplatz mit Standort INTERXION Wien***, ***Server- und Rackhousing mit Standort INTERXION Wien***, sowie alle IPAX Control Panel Dienste:

- Biometrisches Zutrittskontrollsystem (mittels Fingerabdruck)
- Kontaktlose Schlüsselkarte
- Vereinzelungsanlage
- Einzeln versperrte Serverschränke (dokumentierte Schlüsselvergabe an Mitarbeiter und Serverhousing-Kunden)
- Sicherheitszonen und räumliche Trennung (Rechenzentrum > Raum > Cage im Raum > Serverschrank)
- 24/7 Videoüberwachung
- 24/7 Sicherheitspersonal im Rechenzentrum
- Rechenzentrum ist ISO27001 zertifiziert
- Rechenzentrum ist ISO9001 zertifiziert

1.1.2. Für Verträge über ***Rootserver mit Standort IP.ONE Wien***, ***Backupspeicherplatz mit Standort IP.ONE Wien Server- und Rackhousing mit Standort IP.ONE Wien***

- Biometrisches Zutrittskontrollsystem (mittels Fingerabdruck)
- Einzeln versperrte Serverschränke (dokumentierte Schlüsselvergabe an Mitarbeiter und Serverhousing-Kunden)
- Sicherheitszonen und räumliche Trennung (Rechenzentrum > Raum > Serverschrank)
- 24/7 Videoüberwachung
- Gebäude Wachdienst
- Rechenzentrum ist ISO27001 zertifiziert

1.2. Zugangskontrolle

1.2.1. Für IPAX Control Panel Dienste

- Verschlüsselt gespeicherte Kennwörter welche vom Kunden selbst gesetzt werden können.
- Passwort Policy obliegt dem Kunden, eine entsprechende Information zur Stärke des Kennworts wird beim Setzen angezeigt.
- Server-Backend für Administration ist nicht öffentlich erreichbar, Login nur für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Server-Backend, ein um unberechtigte Zugriffe zu verhindern.

1.2.2. Für Verträge über ***Rootserver***

- Server werden mit Server-Passwort übergeben, Passwort muss vom Kunden geändert werden und ist IPAX nicht bekannt. Für die Passwort Policy ist der Kunde verantwortlich.
- Das Updaten des Betriebssystem und der auf dem Betriebssystem installierten Software obliegt dem Kunden.
- NUR bei Zusatzverträgen Servermanagement Advanced und Servermanagement Basic: Administrationszugang für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- NUR bei Zusatzverträgen Servermanagement Advanced und Servermanagement Basic: IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Server, ein um unberechtigte Zugriffe zu verhindern. Die Softwareupdates betreffen das Betriebssystem und mit dem Betriebssystem ausgelieferte Standard Server Software. Für das updaten von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware ist der Kunde verantwortlich.

1.2.3. Für Verträge über ***V-Server***

- Server-Hostsystem für Administration ist nicht öffentlich erreichbar, Login nur für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Host-System ein um unberechtigte Zugriffe zu verhindern.
- Server Gastsysteme werden mit Server-Passwort übergeben, Passwort muss vom Kunden geändert werden und ist IPAX nicht bekannt. Für die Passwort Policy ist der Kunde verantwortlich.
- Für Software-Updates auf dem Gast-System ist einzig und allein der Kunde verantwortlich.
- **NUR** bei ***Managed Webserver*** und Zusatzverträgen Servermanagement Advanced und Servermanagement Basic: Administrationszugang für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- **NUR** bei ***Managed Webserver*** und Zusatzverträgen Servermanagement Advanced und Servermanagement Basic: IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Server, ein um unberechtigte Zugriffe zu verhindern. Die Softwareupdates betreffen das Betriebssystem und mit dem Betriebssystem ausgelieferte Standard Server Software. Für das Updaten von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware ist der Kunde verantwortlich.

1.2.4. Für Verträge über ***Webhosting***, ***Mailhosting***, ***Cloud-Speicher***

- Server-Backend für Administration ist nicht öffentlich erreichbar, Login nur für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Backend und Applikationsservern ein, um unberechtigte Zugriffe zu verhindern.
- Front-End-, Applikations- bzw. Produktzugänge werden mit Passwörtern geschützt. Die Passwörter werden vom Kunden gesetzt und verschlüsselt gespeichert und sind IPAX nicht bekannt. Die Passwort Policy für diese Kennwörter obliegt dem Kunden.
- Für Software-Updates von vom Kunden auf den Server aufgespielter, installierter oder betriebener Software (z.B. Content Management Systeme und sonstige PHP, SQL und Web-programmierungen) ist einzig und allein der Kunde verantwortlich.
- Für die Sicherheit und Update von Client-Software und der Client-Software Umgebung zur Produktnutzung ist einzig und allein der Kunde verantwortlich.

1.2.5. Für Verträge über ***Backupspeicherplatz***

- Server-Backend für Administration ist nicht öffentlich erreichbar, Login nur für autorisierte IPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. IPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- Produktzugänge sind mit Benutzername und Passwort gesichert und auf IPAX-Interne Netze beschränkt.

1.3. Zugriffskontrolle

1.3.1. Für Verträge über ***Webhosting***

- Nur autorisierte IPAX Mitarbeiter haben Backend-Server Zugriff. Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.
- FTP-Verbindungen und von FTP-Benutzern durchgeführte Veränderungen an Dateien werden protokolliert. Löschen, Anlegen und Bearbeiten von Datenbanken wird protokolliert.
- Für die Zugriffskontrolle auf die vom Kunden auf aufgespielte, installierte oder betriebene Software (z.B. Content Management Systeme und sonstige PHP, SQL und Web-programmierungen) bzw. der vom Kunden vorgenommen Datenverarbeitung ist einzig und allein der Kunde verantwortlich.

1.3.2. Für Verträge über ***Mailhosting***

- Nur autorisierte IPAX Mitarbeiter haben Backend-Server Zugriff. Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.
- Verbindungsdaten werden nur im gesetzlich zulässigen Rahmen Protokolliert. Inhaltsdaten werden durch Unternehmensinterne Zugriffsrichtlinie zusätzlich geschützt.

1.3.3. Für Verträge über ***Rootserver***

- Die Zugriffskontrolle auf den Server unterliegt einzig und allein dem Kunden.
- Die Zugriffskontrolle auf die am Server vom Kunden aufgespielte, installierte oder betriebene Software bzw. vom Kunden vorgenommen Datenverarbeitung unterliegt einzig und allein dem Kunden.

- **NUR** bei Zusatzverträgen Servermanagement Basic und Servermanagement Advanced: Nur autorisierte IPAX Mitarbeiter haben Zugriff auf den Server. Der Zugriff der Mitarbeiter auf den Server wird protokolliert. Getrennte Kunden-Benutzer werden nur auf Anfrage eingerichtet. Der Zugriff dieser Nutzer auf den Server wird ebenso protokolliert. Benutzermanagement und -Policy für diese Zugänge obliegt dem Kunden.

1.3.4. Für Verträge über ***V-Server***

- Nur autorisierte IPAX Mitarbeiter haben Zugriff auf den Hosting-Server (Backend-Server). Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.
- Die Zugriffskontrolle der Gast-systeme obliegt einzig und allein dem Kunden
- Die Zugriffskontrolle auf die am Gast-System vom Kunden aufgespielte, installierte oder betriebene Software bzw. vom Kunden vorgenommen Datenverarbeitung unterliegt einzig und allein dem Kunden.
- **NUR** bei ***Managed Webserver*** und Zusatzverträgen Servermanagement Basic und Servermanagement Advanced: Nur autorisierte IPAX Mitarbeiter haben Zugriff auf den Gast-Server. Der Zugriff der Mitarbeiter auf den Gast-Server wird protokolliert. Getrennte Kunden-Benutzer werden nur auf Anfrage eingerichtet. Der Zugriff dieser Nutzer auf den Server wird ebenso protokolliert. Benutzermanagement und -Policy für diese Zugänge obliegt dem Kunden.

1.3.5. Für Verträge über ***Backupspeicherplatz***

- Nur autorisierte IPAX Mitarbeiter haben Backend-Server Zugriff. Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.
- Protokollierungen von Änderungen am Backupdatenbestand selbst richten sich nach der vom Kunden verwendeten Backupmethode, Backuptechnologie und eingesetzter Backupsoftware und werden nicht von IPAX gespeichert.

1.3.6. Für Verträge über ***Cloud-Speicher***

- Nur autorisierte IPAX Mitarbeiter haben Zugriff auf den Hosting-Server (Backend-Server). Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.
- Die von IPAX bereitgestellte Open-Source Software bietet, abhängig vom jeweiligen Produkt, eine Benutzerverwaltung welche Änderungen an Dateien vom jeweiligen Benutzer nachvollziehbar macht.

1.3.7. Für IPAX Control Panel Dienste

- Nur autorisierte IPAX Mitarbeiter haben Backend-Server Zugriff. Der Zugriff der Mitarbeiter auf die Backend-Server wird protokolliert.

1.4 Pseudonymisierung

1.4.1. Für alle IPAX Produkte

- Der Kunde bestimmt Zweck und Mittel der Datenverarbeitung und wie die Daten auf den IPAX Systemen gespeichert werden. Für eine Pseudonymisierung ist somit einzig und allein der Kunde verantwortlich.

1.5. Datenträger Handling und Verschlüsselung

1.5.1. Für alle IPAX Produkte

- Das Handling und der Verbleib aller Datenträger werden dokumentiert.
- Festplatten werden nach Beendigung des Vertrages mittels definierter Verfahren durch mehrfaches überschreiben sicher gelöscht (z.B. gemäß Department of Defence Standard zur Datenlöschung (DoD 5220.22-M) oder vergleichbare). Funktionierende Festplatten werden nach einer Überprüfung wieder eingesetzt. Defekte Festplatten werden gelöscht und zur Garantieabwicklung eingesendet. Kann bei defekten Festplatten in Garantie eine sichere Löschung nicht gewährleistet werden, stimmt IPAX das Vorgehen mit dem Kunden ab. Defekte Festplatten außerhalb der Garantie, für welche eine sichere Löschung nicht gewährleistet werden kann, werden mechanisch unbrauchbar gemacht/ zerstört.
- Da Serversysteme in der Regel 24 Stunden am Tag in Betrieb sind und während des Betriebes Zugriff auf die Datenträger benötigt wird, werden die Datenträger - wenn nicht individuell und explizit vereinbart - von IPAX nicht verschlüsselt. Der direkte Zugriff auf die Datenträger durch Unbefugte wird mittels der unter Zutrittskontrolle genannten Maßnahmen effektiv verhindert.
- Es steht dem Kunden aber frei und obliegt seiner Verantwortung und Entscheidung mittels Einsatz entsprechender Software die Daten verschlüsselt auf den Datenträgern abzulegen. Installation und Konfiguration der Software obliegt dem Kunden. Auf die mit der Verschlüsselung verbundenen Risiken für die Systemverfügbarkeit (Server oder Dienste mit verschlüsselten Datenträgern starten unter Umständen nicht automatisch neu, da eine manuelle Passworteingabe erforderlich ist) und für die

Datenverfügbarkeit (Verlust des Schlüssels kann zum Komplettverlust der Daten führen) sei hingewiesen.

2. Integrität

2.1. Weitergabekontrolle und Transportverschlüsselung

2.1.1. Für Verträge über ***Webhosting***

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Für den Datenzugriff werden dem Kunden verschlüsselte Kommunikationsmethoden zur Verfügung gestellt. Die Wahl und Verwendung der richtigen Verbindung obliegt dem Kunden: FTP: FTPs, phpmyAdmin: SSL verschlüsselt, Direkter externer Datenbank Zugriff wird nicht zugelassen.
- Für den Frontend-Zugriff auf Webseiten die der Kunde auf IPAX Server hochgeladen hat und dort betreibt, bietet IPAX je nach Produkt inkludiert und/oder aufpreispflichtige Technologien um den Datenverkehr zwischen Dritten und der Website des Kunden zu verschlüsseln (kostenlose und kostenpflichtige SSL-Zertifikate). Die Auswahl, Verwendung und Implementierung der Kommunikationsverschlüsselung obliegt einzig und allein dem Kunden.

2.1.2. Für Verträge über ***Mailhosting***

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Das IPAX Webmail ist ausschließlich über SSL-gesicherte Verbindungen erreichbar.
- Für die Kommunikation der Kundenanwendungsprogramme (Mail-Clients) mit dem IPAX Mail-Server wird sowohl für das Senden (SMTP) als auch für das Empfangen (IMAP/POP) eine SSL verschlüsselte Verbindung angeboten. Die Auswahl, Verwendung und Konfiguration (im E-mail Client) der Verschlüsslung obliegt einzig und allein dem Kunden.

2.1.3. Für Verträge über ***Cloud-Speicher***

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Die Administrationsoberfläche des Produktes wird mittels SSL-Verschlüsselung abgesichert.
- Für die Frontend-Anwendung des Produktes wird Verschlüsselung unterstützt. Die Auswahl, Verwendung und Konfiguration (im Client) der Verschlüsslung obliegt einzig und allein dem Kunden.

2.1.4. Für Verträge über ***V-Server***

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Die Administrationsoberfläche des Produktes wird mittels SSL-Verschlüsselung abgesichert.
- Für die Verschlüsselte Verbindung zum Gast-System und der darauf installierten Software bzw. der darauf betriebenen Datenverarbeitung ist einzig und allein der Kunde verantwortlich.
- **NUR** bei ***Managed Webserver*** und Zusatzvertrag ***Servermanagement Basic*** und ***Servermanagement Advanced***: Der IPAX Administrationszugriff erfolgt ausschließlich über verschlüsselte Verbindungen.

2.1.5. Für Verträge über ***Rootserver***

- Für die Verschlüsselte Verbindung zum Server und der darauf installierten Software bzw. der darauf betriebenen Datenverarbeitung ist einzig und allein der Kunde verantwortlich.
- **NUR** bei Zusatzvertrag Servermanagement Basic und Servermanagement Advanced: Der IPAX Administrationszugriff erfolgt ausschließlich über verschlüsselte Verbindungen.

2.1.6. Für Verträge über ***Backupspeicherplatz***

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Die Transportverschlüsselung ist abhängig von der vom Kunden eingesetzten Backupmethode, Technologie und Backupsoftware.
- Für die Absicherung der Daten während des Transportes vom Kundenserver zum Backupserver erfolgt der Transport ausschließlich über ein privates Netzwerk. Das Backup Netzwerk ist nicht von außen erreichbar.

2.1.7. Für IPAX Control Panel Dienste

- Der Backend-Server Zugriff durch die IPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Der Front-End Zugriff zum IPAX Control Panel ist mittels SSL-Verschlüsselung abgesichert.

2.2. Eingabekontrolle

2.2.1. Bei IPAX Control Panel Diensten

- Die Daten werden über die Weboberfläche direkt vom Kunden eingegeben oder geändert. Datenänderungen werden protokolliert.
- Alle von IPAX am Datenbestand und Konfiguration vorgenommen Änderungen müssen vom Kunden über das IPAX Ticket System beauftragt werden. Die von IPAX Mitarbeitern vorgenommenen Änderungen werden hier zusätzlich dokumentiert.

2.2.2. Bei ***Mailhosting***, ***V-Server***, ***Rootserver*** und ***Backupspeicherplatz***

- Der Kunde bestimmt die einzugebenden oder zu erfassenden Daten und konfiguriert seine Anwendung entsprechend.
- Die Daten werden vom Kunden in seiner Datenverarbeitungsanwendung selbst erfasst oder eingegeben. Die Verantwortung der Eingabekontrolle liegt einzig und allein beim Kunden.

2.2.3. Bei ***Webhosting***

- Der Kunde bestimmt die einzugebenden oder zu erfassenden Daten und konfiguriert seine Anwendung entsprechend.
- Die Daten werden vom Kunden in seiner Datenverarbeitungsanwendung selbst erfasst oder eingegeben. Die Verantwortung der Eingabekontrolle liegt einzig und allein beim Kunden.
- Die von IPAX auf den IPAX Hosting Servern erfassten Zugriffe, welche als Grundlage für die IPAX-Besucherstatistik der Kundenwebseite dienen enthalten auch die IP-Adressen Dritter mit denen Personen potentiell identifiziert werden könnten. Diese IP-Adressen werden umgehend nach der Erfassung umgeschrieben sodass die Identifizierung einer Person nicht mehr möglich ist und kein persönliches Datum mehr vorliegt (Anonymisierung durch Umschreibung mit Zufallswerten ohne Möglichkeit zur Ent-Pseudonymisierung).
- Für die vom Kunden auf anderem Wege erfassten IP-Adressen (z.B. mittels am IPAX Server durch den Kunden installierter oder ausgeführter Software) ist der Kunde selbst verantwortlich.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

3.1.1. Für IPAX Control Panel Dienste

- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Der Backend-Server ist mit einer Firewall gesichert.
- IPAX spielt regelmäßige Software Updates (gem. IPAX Update Policy) ein um die Sicherheit, Verfügbarkeit und Belastbarkeit der Serversysteme zu gewährleisten.
- Die Daten werden auf einem geographisch unabhängigen Backupserver gemäß der IPAX Backupstrategie für interne Systeme gesichert. ACHTUNG dieses Backup dient zur IPAX-Internen Desaster-Recovery und zur Erfüllung der Maßnahmen für die IPAX direkter Verantwortlicher i.S.d. DSGVO ist. Ohne gesonderte Vereinbarung besteht kein Anspruch auf das individuelle Rückspielen von ausgewählten Kundendaten (Daten einzelner, spezifischer Kundenaccounts) durch einzelne Kunden.
- Die IPAX Systeme für das Control Panel sind als redundanter Server-Cluster aufgebaut um die Datenverfügbarkeit bei Ausfall eines kompletten Server-Systems zu gewährleisten und die Belastbarkeit des Gesamtsystems sicherzustellen.
- Die Server werden von einer unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die IPAX internen Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die IPAX internen Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO) wird durch das Clustering von Serversystemen sowie das Vorhalten von entsprechender Ersatzhardware in Kombination mit der Backupstrategie (in ein geographisch unabhängiges Rechenzentrum) sichergestellt.
- IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.

3.1.2. Für Verträge über IPAX ***Webhosting*** und ***Mailhosting***

- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Die Backend-Server sind mit Firewalls gesichert.
- IPAX spielt regelmäßige Software Updates (gem. IPAX Update Policy) ein um die Sicherheit, Verfügbarkeit und Belastbarkeit der Serversysteme zu gewährleisten. Die Softwareupdates betreffen das Betriebssystem und mit dem Betriebssystem ausgelieferte Standard Server Software. Für das Updaten von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware (insbesondere Content Management Systeme) ist der Kunde verantwortlich.
    - **NUR** bei ***Managed Wordpress***: IPAX spielt regelmäßig Updates für das Content Management System Wordpress gemäß Leistungsbeschreibung ein.
- Bei IPAX Mailhosting werden E-Mails bei aktivierten Spam Schutz auch einer Viren-Prüfung (Anti-Virus) unterzogen. Dies ist eine zusätzliche Sicherheitsmaßnahme und kann ein Anti-Virus Programm auf dem Client-Rechner des Kunden nicht ersetzen.
- Bei IPAX Webhosting ist der Kunde selbst für die Überprüfung und Entfernung von Schadsoftware auf dem Ihm bereitgestellten Speicherplatz, bzw. in den auf IPAX Servern durch den Kunden hochgeladenen, betriebenen oder ausgeführten Softwareanwendungen verantwortlich.
- Die Daten werden auf einem geographisch unabhängigen Backupserver gemäß der IPAX Backupstrategie für interne Systeme gesichert. Die Vorhalte-Dauer des Backups richtet sich nach der Leistungsbeschreibung des jeweiligen Produktes. Die Möglichkeit für das Rückspielen von einzelnen Kundendaten (Daten einzelner, spezifischer Kundenaccounts), sowie die Entgelte dafür richten sich nach der Leistungsbeschreibung des jeweiligen Webhosting / Mailhosting Produktes.

- Die IPAX Systeme für Webhosting und Mailhosting Produkte sind als redundanter Server-Cluster aufgebaut um die Datenverfügbarkeit bei Ausfall eines kompletten Server-Systems zu gewährleisten und die Belastbarkeit des Gesamtsystems sicherzustellen.
- Die Server werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die IPAX internen Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die IPAX internen Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO), wird durch das Clustering von Serversystemen sowie das Vorhalten von entsprechender Ersatzhardware in Kombination mit der Backupstrategie (in ein geographisch unabhängiges Rechenzentrum) sichergestellt.
- IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.

3.1.3. Für Verträge über IPAX ***Cloud-Speicher***

- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Die Cloudspeicher-Server sind mit Firewalls gesichert.
- IPAX spielt regelmäßige Software Updates (gem. IPAX Update Policy) ein um die Sicherheit, Verfügbarkeit und Belastbarkeit der Serversysteme zu gewährleisten.
- Die Daten werden auf einem geographisch unabhängigen Backupserver gemäß der IPAX Backupstrategie für interne Systeme gesichert. ACHTUNG dieses Backup dient zur IPAX-Internen Desaster-Recovery. Ohne gesonderte Vereinbarung besteht kein Anspruch auf das individuelle Rückspielen von ausgewählten Kundendaten (Daten einzelner, spezifischer Kundenaccounts) durch einzelne Kunden.
- Die im Zuge des Produktes bereitgestellte Open-Source Software bietet Möglichkeiten zur Wiederherstellung gelöschter Dateien. Die Funktionalität dieser Software wird von IPAX aber nicht garantiert und die genaue Konfiguration dieser Funktionalität obliegt dem Kunden.
- Die Server werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die IPAX internen Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die IPAX internen Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO), wird durch das Vorhalten von entsprechender Ersatzhardware in Kombination mit der Backupstrategie (in ein geographisch unabhängiges Rechenzentrum) sichergestellt.
- IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.

3.1.4 Für Verträge über ***V-Server***

- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Das Betriebssystem und die Konfigurationsdateien des Hosts-Systems werden von IPAX auf einem geographisch unabhängigen Backupserver gemäß der IPAX Backupstrategie für Interne Systeme gesichert.

- Für die Sicherung der am Gast-System gespeicherten Daten ist einzig und allein der Kunde verantwortlich.
    - **NUR** bei Zusatzverträgen über Servermanagement Basic und Servermanagement Advanced: IPAX konfiguriert ein lokales Datei-Backup. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltedauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
    - **NUR** bei Zusatzverträgen über Servermanagement Basic und Servermanagement Advanced in Verbindung mit Zusatzvertrag über ***IPAX Backupspeicherplatz***: IPAX konfiguriert statt einem lokalem Backup ein Datei-Backup auf dem IPAX Backupspeicherplatz. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltedauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
    - **NUR** bei ***Managed Webserver***: IPAX konfiguriert ein tägliches inkrementelles Backup auf einen IPAX Backup-Server (siehe IPAX Backupspeicherplatz) die Vorhaltedauer wird von Kunden bei der Bestellung ausgewählt.
- IPAX spielt regelmäßige Software Updates (gem. IPAX Update Policy) auf dem Host-System ein um die Sicherheit, Verfügbarkeit und Belastbarkeit der Host-Serversysteme zu gewährleisten. Für das Updaten der Software auf dem Gast-System ist einzig und allein der Kunde verantwortlich.
    - **NUR** bei ***Managed Webserver*** und Zusatzverträgen Servermanagement Basic und Servermanagement Advanced: IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Server ein um Sicherheit, Verfügbarkeit und Belastbarkeit des Systems zu gewährleisten. Die Softwareupdates betreffen das Betriebssystem und mit dem Betriebssystem ausgelieferte Standard Server Software. Für das Updaten von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware ist der Kunde verantwortlich.
- Nur für IPAX HA-V-Server: Die Gast-Systeme werden auf einem Cluster-System aus mehreren physischen Servern betrieben. Dadurch wird die Verfügbarkeit der Kundenanwendung bei Ausfall eines physischen Server-Systems gewährleistet und die Belastbarkeit des Gesamtsystems erhöht.
- Die Hosting-Server werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die Hosting-Serversysteme sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die Hosting-Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Hosting-Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Hosting-Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO) wird durch das Vorhalten von entsprechender Ersatzhardware ermöglicht. Für die Wiederherstellung der Sicherungen ist der Kunde verantwortlich. Bei IPAX HA-V-Servern erfolgt zusätzlich das Clustering der Host-Systeme.
- Nur bei Zusatzverträgen Servermanagement Advanced: IPAX konfiguriert eine lokale Firewall auf dem Server-Betriebssystem.
- IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting auf dem Host-System, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte des Host-Systems laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter des Host-Systems steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt. Für Monitoring, Alerting, Fehlersuche und Fehlerbehebung bei Gast-Systemen ist einzig und allein der Kunde verantwortlich.
    - **NUR** bei Zusatzverträgen Servermanagement Advanced: IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte des Gast-Systems laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter des Gast-Systems steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.

3.1.5 Für Verträge über ***Rootserver***

- Die IPAX Rootserver werden wenn nicht anders vereinbart mit mindestens 2 Festplatten ausgeliefert welche als RAID-Array konfiguriert sind. Dadurch wird sichergestellt, dass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann. Die Beibehaltung, laufende Überwachung und Wiederherstellung dieser RAID Konfiguration obliegt einzig und allein dem Kunden. Defekte Datenträger müssen vom Kunden an IPAX gemeldet werden und werden im Rahmen der Service Level Agreements des Servers getauscht.

    - **NUR** bei Zusatzverträgen über Servermanagement Advanced: IPAX konfiguriert ein 24/7 Servermonitoring und Alerting. Bei Defekt eines Datenträgers nimmt IPAX den tausch des defekten Datenträgers selbstständig im Rahmen der Service Level Agreements des Servers vor.
- Die Sicherung der am Rootserver durch den Kunden gespeicherten Daten obliegt einzig und allein dem Kunden.
    - **NUR** bei Zusatzverträgen über Servermanagement Basic und Servermanagement Advanced: IPAX konfiguriert ein lokales Datei-Backup. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltedauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
    - **NUR** bei Zusatzverträgen über Servermanagement Basic und Servermanagement Advanced in Verbindung mit Zusatzvertrag über IPAX Backupspeicherplatz: IPAX konfiguriert statt einem lokalem Backup ein Datei-Backup auf dem IPAX Backupspeicherplatz. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltedauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
- Für das Einspielen von Software Updates für das Betriebssystem und die auf dem Server hochgeladene, installierte oder betriebene Software ist einzig und allein der Kunde verantwortlich.
    - **NUR** bei Zusatzverträgen Servermanagement Basic und Servermanagement Advanced: IPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Server ein um Sicherheit, Verfügbarkeit und Belastbarkeit des Systems zu gewährleisten. Die Softwareupdates betreffen das Betriebssystem und mit dem Betriebssystem ausgelieferte Standard Server Software. Für das Updaten von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware ist der Kunde verantwortlich.
- Die Hosting-Server werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- **NUR** für ***BUSINESS line Rootserver*** und ***PROFESSIONAL line Rootserver*** mit HA-Package: Die Hosting-Serversysteme sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- **NUR** für ***BUSINESS line Rootserver*** und ***PROFESSIONAL line Rootserver*** mit HA-Package: Die Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Für die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO) ist der Kunde verantwortlich. Wir unterstützen den Kunden durch das Vorhalten von Ersatz Hardware. Diese wird gemäß der vom Kunden gebuchten oder beim Produkt enthaltenen Service Levels in einem wohl definierten Zeitfenster bereitgestellt. Für die Wiederherstellung der Sicherungen selbst ist der Kunde verantwortlich.
    - **NUR** bei Zusatzverträgen Servermanagement Advanced: Nach erfolgtem Hardwaretausch erfolgt die Wiederherstellung der Sicherung bzw. das Rückspielen des Backups durch IPAX.
- **NUR** bei Zusatzverträgen Cluster-Server, Server Clustering oder Cluster Management: Die Server-Systeme sind als redundanter Server-Cluster aufgebaut um die Datenverfügbarkeit bei Ausfall eines kompletten Server-Systems zu gewährleisten und die Belastbarkeit des Gesamtsystems sicherzustellen.
- **NUR** bei Zusatzverträgen Servermanagement Advanced: IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.
- **NUR** bei Zusatzverträgen Servermanagement Advanced: IPAX konfiguriert eine lokale Firewall auf dem Server-Betriebssystem.

3.1.6. Für Verträge über IPAX ***Backupspeicherplatz***

- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Da es sich bei dem Produkt schon um Backup-Datenspeicher handelt wird von IPAX KEIN nochmaliges Backup dieser Daten angefertigt. Vielmehr ist der Kunde Verantwortlich dafür Sorge zu tragen, dass von allen am Backupspeicher abgelegten Daten eine Kopie (idealerweise am Produktivsystem) existiert.

- Die Server werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die Backup-Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die Backup-Server sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Serversysteme sind mittels einer Gas-Löschanlage gegen Brände geschützt.
- Die Fähigkeit die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit c DSGVO) wird durch das Vorhalten von entsprechender Ersatzhardware ermöglicht. Für die Wiederherstellung der Sicherungen ist der Kunde verantwortlich.
- IPAX konfiguriert und betreibt ein 24/7 Servermonitoring und Alerting, welches den ordnungsgemäßen Betrieb sowie kritische Auslastungswerte laufend überwacht. Bei Beeinträchtigung des Betriebes oder überschreiten kritischer Parameter steht Rund um die Uhr ein Bereitschaftstechniker bereit, der mit der Fehlersucher und Fehlerbehebung selbstständig beginnt.

3.1.7. Für Verträge über ***Server- und Rackhousing****

- Die Server/Geräte des Kunden werden von einer Unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- **NUR** bei Zusatzvertrag Hochverfügbarkeits-Package: Die Server/Geräte des Kunden sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- **NUR** bei Zusatzvertrag Hochverfügbarkeits-Package: Die Server/Geräte des Kunden sind über eine redundante Netzwerkverbindung angebunden um dem Ausfall einer Netzwerkkomponente vorzubeugen.
- Die Server/Geräte des Kunden werden unter kontrollierten Umgebungsbedingungen mit redundanter Klimatisierung, Brandfrüherkennungssystemen, Leckage-Warnsystemen betrieben.
- Die Server/Geräte des Kunden sind mittels einer Gas-Löschanlage gegen Brände geschützt.










4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Überprüfung, Bewertung und Evaluierung des Gesamtsystems der Datenverarbeitung

4.1.1. Gilt für Alle Produkte:

IPAX stellt standardisierte technische Dienstleistungen, wie beschrieben, in Form von standardisierten Produkt Paketen bereit. Diese stellen in der Regel nur einzelne, begrenzte, technische Teilaspekte der Datenverarbeitungsanwendungen des Kunden (z.B. Logische Speicherung von Daten) dar und sind somit ein Baustein der Datenverarbeitungsanwendung des Kunden. Der Kunde ist allein verantwortlich und verpflichtet regelmäßig sein Gesamtsystem der Datenverarbeitung zu überprüfen und zu evaluieren ob dieses den Bestimmungen der DSGVO entspricht und somit ein angemessenes Schutzniveau für seine Datenverarbeitung

bietet. IPAX stellt dem Kunden für diesen Zweck Leistungsbeschreibung und Beschreibung der technischen und organisatorischen Schutzmaßnahmen des jeweiligen Produktes bereit. Es obliegt der alleinigen Verantwortung des Kunden zu beurteilen und zu entscheiden, ob das jeweilige IPAX Produkt das für die Datenverarbeitung des Kunden angemessene Schutzniveau aufweist. IPAX ist nicht in die Evaluierung, Bewertung oder Überprüfung der Datenverarbeitungsanwendung des Kunden eingebunden oder dafür verantwortlich. Für eine Risikoanalyse oder eine Datenschutz-Folgenabschätzung des Kunden Gesamtsystems und der im Zuge dessen von IPAX im Auftrag des Kunden verarbeiteten Daten ist der Kunde verantwortlich.

4.2. Überprüfung, Bewertung und Evaluierung der technischen Betriebssicherheit der IPAX Systeme und Produkte

4.2.1. Gilt für Verträge über ***Webhosting***, ***Mailhosting***, ***Cloud-Speicher***, ***V-Server***, ***Backup-Speicherplatz*** und Control Panel Dienste.

- IPAX überprüft im Zuge des Produktmanagements in regelmäßigen Abständen, ob die technischen und organisatorischen Schutzmaßnahmen der IPAX internen Server und Hosting Produkte ein zeitgemäßes Schutzniveau bieten bzw. dem Stand der Technik entsprechen und eine dem Produktpreis und der Produkt-Leistungsbeschreibung angemessene Betriebssicherheit gewährleisten.
- Dies gilt insbesondere für die physische Sicherheit und die logische Sicherheit für Zugang und Zugriff auf IPAX-Backend oder Hosting Server und der darauf von IPAX betriebenen Software.
- IPAX führt für die IPAX Hosting Systeme ein Software Inventar, welches zusammen mit dem Produkt-Lifecycle-Management sicherstellt, dass alle IPAX Hosting Server über Betriebssystem-Software verfügen, welche vom Herausgeber mit aktuellen Sicherheitsupdates versorgt werden.
- Von IPAX selbst entwickelte Software welche dem Kunden bereitgestellt wird, wird gemäß der OWASP Richtlinien für Anwendungssicherheit evaluiert und es wird bei der Anwendungsentwicklung auf Datenschutzfreundliche Voreinstellungen geachtet.
- Bei Produkten bei denen der Kunde auf IPAX Server hochgeladene, installierte oder ausgeführte Software betreibt obliegt die Überprüfung, Bewertung und Evaluierung dieser Software und der damit einhergehenden Sicherheitsrisiken einzig und allein dem Kunden.

4.3. Überprüfung, Bewertung und Evaluierung des IPAX internen Datenschutzes

- IPAX führt ein aktuelles Verarbeitungsverzeichnis aller Verarbeitungstätigkeiten von Kundendaten für die IPAX Verantwortlicher im Sinne der DSGVO ist. Dieses enthält auch ein eigenes Verzeichnis von allen gemäß Art. 32 ergriffenen Maßnahmen zur sicheren Datenverarbeitung. IPAX evaluiert diese technischen und Organisatorischen Maßnahmen in regelmäßigen Intervallen.

- Alle IPAX Mitarbeiter haben sich zur entsprechenden Verschwiegenheit und Geheimhaltung von Kundendaten vertraglich verpflichtet. Dies umfasst sowohl Geheimhaltung von Daten für die IPAX Verantwortlicher im Sinne der DSGVO, ist als auch Daten für die IPAX Auftragsverarbeiter im Sinne der DSGVO ist.

- IPAX schult und unterweist seine Mitarbeiter in regelmäßigen Intervallen im Datenschutz. Dies Umfasst sowohl Schulung und Unterweisung im Umgang mit Daten für die IPAX Verantwortlicher im Sinne der DSGVO ist als auch Daten für die IPAX Auftragsverarbeiter im Sinne der DSGVO ist.

- Von IPAX selbst entwickelte Software für den internen Gebrauch wird gemäß der OWASP Richtlinien für Anwendungssicherheit evaluiert. Es wird bei der Anwendungsentwicklung auf Datenschutzfreundliche Voreinstellungen, sowie auf Dokumentationserfordernisse nach dem DSG geachtet.