



Technische und Organisatorische Maßnahmen Gemäß Art. 32 DSGVO

Anhang 1 zur Vereinbarung über Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: 28.05.2018

Version: 1.00

Dokumenten-Verantwortlicher: XPAX Geschäftsführung



XPAX

XPAX GmbH
Donaustraße 106/9
3400 Klosterneuburg
Österreich

Telefon: +43 1 3110111

E-Mail: office@xpax.at

Web: www.xpax.at

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Einleitung	3
Äquivalenzlisten Produktgruppen	3
1. Vertraulichkeit	4
1.1. Zutrittskontrolle.....	4
1.2. Zugangskontrolle	4
1.3. Zugriffskontrolle	5
1.4. Pseudonymisierung	6
1.5. Datenträger Handling und Verschlüsselung	6
2. Integrität	6
2.1. Weitergabekontrolle und Transportverschlüsselung	6
2.2. Eingabekontrolle.....	7
3. Verfügbarkeit und Belastbarkeit	8
3.1. Verfügbarkeitskontrolle.....	8
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	11
4.1. Überprüfung, Bewertung und Evaluierung des Gesamtsystems der Datenverarbeitung.....	11
4.2. Überprüfung, Bewertung und Evaluierung der technischen Betriebssicherheit der XPAX Systeme und Produkte	12
4.3. Überprüfung, Bewertung und Evaluierung des XPAX internen Datenschutzes	12

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 XPAX GmbH als Auftragsverarbeiter als **XPAX** bezeichnet.

Diese Dokument beschreibt die Technischen und Organisatorischen Maßnahmen die XPAX im Zuge eines Auftragsverarbeitungs-Vertrages (gem. Art. 28 DSGVO) mit dem Kunden ergreift. XPAX 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. XPAX 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 XPAX 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 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
Webhosting Wordpress Starter Hosting Shared Klein Hosting Shared Groß Hosting Shared HTML	Webhosting	INTERXION Wien
Mailhosting Wordpress Starter Hosting Shared Klein Hosting Shared Groß Hosting Shared HTML Mailhosting	Mailhosting	INTERXION Wien
Web und Mailhosting zusammen	Hosting	INTERXION Wien
Virtuelle Server	V-Server	INTERXION Wien, IP.ONE Wien
Dedizierte Rootserver	Rootserver	INTERXION Wien, IP.ONE Wien
Backup-Speicherplatz	Backup-Speicherplatz	INTERXION Wien, IP.ONE Wien
IP-Transit*	IP-Transit*	INTERXION Wien, IP.ONE 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 XPAX 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 **Hosting, V-Server und Rootserver mit Standort INTERXION Wien**
- Biometrisches Zutrittskontrollsystem (mittels Fingerabdruck)
 - Kontaktlose Schlüsselkarte
 - Vereinzelnungsanlage
 - Einzel verscherrte Serverschränke (dokumentierte Schlüsselübergabe 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 **V-Server und Rootserver mit Standort IP.ONE Wien**
- Biometrisches Zutrittskontrollsystem (mittels Fingerabdruck)
 - Einzel verscherrte Serverschränke (dokumentierte Schlüsselübergabe 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 XPAX Verwaltungsoberfläche
- 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 XPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. XPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
 - XPAX 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 XPAX nicht bekannt. Für die Passwort Policy ist der Kunde verantwortlich.
 - Das Updaten des Betriebssystems und der auf dem Betriebssystem installierten Software obliegt dem Kunden.
 - NUR bei Zusatzverträgen Servermanagement: Administrationszugang für autorisierte XPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. XPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
 - NUR bei Zusatzverträgen über Servermanagement: XPAX 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 XPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. XPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
 - XPAX spielt regelmäßig Software-Updates gemäß Update-Policy auf dem Host-System ein um unberechtigte Zugriffe zu verhindern.
 - Server Gastssysteme werden mit Server-Passwort übergeben, Passwort muss vom Kunden geändert werden und ist XPAX 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 Zusatzverträgen über Servermanagement: Administrationszugang für autorisierte XPAX Mitarbeiter über mehrstufiges System mittels Kennwörter (gem. XPAX Passwort Policy) und Kryptographischer-Schlüssel, zusätzlich Firewall und automatische Sperrmechanismen.
- NUR bei Zusatzverträgen über Servermanagement: XPAX 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 **Hosting**

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

1.3. Zugriffskontrolle

1.3.1. Für Verträge über **Webhosting**

- Nur autorisierte XPAX 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
- 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 XPAX 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 über Servermanagement: Nur autorisierte XPAX 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 XPAX 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 Zusatzverträgen über Servermanagement: Nur autorisierte XPAX 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 XPAX 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 XPAX gespeichert.

1.3.7. Für XPAX Verwaltungsoberfläche:

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

1.4 Pseudonymisierung

1.4.1. Für alle XPAX Produkte

- Der Kunde bestimmt Zweck und Mittel der Datenverarbeitung und wie die Daten auf den XPAX 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 XPAX 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 eingeschickt. Kann bei defekten Festplatten in Garantie eine sichere Löschung nicht gewährleistet werden, stimmt XPAX 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 XPAX 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 Kompletverlust 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 XPAX 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 XPAX Server hochgeladen hat und dort betreibt, bietet XPAX 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 XPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Das XPAX Webmail ist ausschließlich über SSL-gesicherte Verbindungen erreichbar.
- Für die Kommunikation der Kundenanwendungsprogramme (Mail-Clients) mit dem XPAX 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 Verschlüsselung obliegt einzig und allein dem Kunden.

2.1.4. Für Verträge über **V-Server**

- Der Backend-Server Zugriff durch die XPAX 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 Zusatzvertrag *Servermanagement*: Der XPAX 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 über *Servermanagement*: Der XPAX Administrationszugriff erfolgt ausschließlich über verschlüsselte Verbindungen.

2.1.6. Für Verträge über **Backupspeicherplatz**

- Der Backend-Server Zugriff durch die XPAX 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 XPAX Verwaltungsoberfläche

- Der Backend-Server Zugriff durch die XPAX Administration erfolgt ausschließlich über verschlüsselte Verbindungen.
- Der Front-End Zugriff zur XPAX Verwaltungsoberfläche ist mittels SSL-Verschlüsselung abgesichert.

2.2. Eingabekontrolle

2.2.1. Bei XPAX Verwaltungsoberfläche

- Alle von XPAX am Datenbestand und Konfiguration vorgenommenen Änderungen müssen vom Kunden über das XPAX Ticket System beauftragt werden. Die von XPAX 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 XPAX auf den XPAX Hosting Servern erfassten Zugriffe, welche als Grundlage für die XPAX-Besucherstatistik der Kundenwebseite dienen, enthalten auch die IP-Adressen Dritter mit denen Personen potentiell identifiziert werden könnten. Diese IP-Adressen werden einmal täglich 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 XPAX Server durch den Kunden installierter oder ausgeführter Software) ist der Kunde selbst verantwortlich.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

3.1.1. Für XPAX Verwaltungsoberfläche

- 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.
- XPAX spielt regelmäßige Software Updates (gem. XPAX Update Policy) ein um die Sicherheit, Verfügbarkeit und Belastbarkeit der Serversysteme zu gewährleisten.
- Die Daten werden auf einem geographisch unabhängigen Backupserver gemäß der XPAX Backupstrategie für interne Systeme gesichert. ACHTUNG dieses Backup dient zur XPAX-Internen Disaster-Recovery und zur Erfüllung der Maßnahmen für die XPAX 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 Server werden von einer unterbrechungsfreien Stromversorgung (USV-Anlage) mit Dieselgenerator Backup gespeist um einen Ausfall der großräumigen Stromversorgung vorzubeugen.
- Die XPAX internen Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die XPAX 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.
- XPAX 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 XPAX **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.
- XPAX spielt regelmäßige Software Updates (gem. XPAX 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 Updates von, vom Kunden auf den Server hochgeladene, installierte oder ausgeführte Drittsoftware (insbesondere Content Management Systeme) ist der Kunde verantwortlich.
- Bei XPAX 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 XPAX Webhosting ist der Kunde selbst für die Überprüfung und Entfernung von Schadsoftware auf dem ihm bereitgestellten Speicherplatz, bzw. in den auf XPAX Servern durch den Kunden hochgeladenen, betriebenen oder ausgeführten Softwareanwendungen verantwortlich.
- Die Daten werden auf einem geographisch unabhängigen Backupserver gemäß der XPAX 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.
- 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 XPAX internen Server sind mit redundanten Netzteilen an unterschiedliche Stromkreise angebunden um einen Ausfall eines lokalen Stromkreises vorzubeugen.
- Die XPAX 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.
- XPAX 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 XPAX auf einem geographisch unabhängigen Backupserver gemäß der XPAX 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: XPAX konfiguriert ein lokales Datei-Backup. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltdauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
 - NUR bei Zusatzverträgen über Servermanagement: in Verbindung mit Zusatzvertrag über **XPAX Backupspeicherplatz**: XPAX konfiguriert statt einem lokalem Backup ein Datei-Backup auf dem XPAX Backupspeicherplatz. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltdauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
- XPAX spielt regelmäßige Software Updates (gem. XPAX 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 Zusatzverträgen über Servermanagement: XPAX 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.
- 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.
- Nur bei Zusatzverträgen Servermanagement Advanced: XPAX konfiguriert eine lokale Firewall auf dem Server-Betriebssystem.
- XPAX 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 über Servermanagement: XPAX 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 XPAX 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 XPAX gemeldet werden und werden im Rahmen der Service Level Agreements des Servers getauscht.
 - NUR bei Zusatzverträgen über Servermanagement: XPAX konfiguriert ein 24/7 Servermonitoring und Alerting. Bei Defekt eines Datenträgers nimmt XPAX 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: XPAX konfiguriert ein lokales Datei-Backup. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltdauer richtet sich nach Kundenwunsch und verfügbaren Speicherplatz.
 - NUR bei Zusatzverträgen über Servermanagement: in Verbindung mit Zusatzvertrag über XPAX Backupspeicherplatz: XPAX konfiguriert statt einem lokalem Backup ein Datei-Backup auf dem XPAX Backupspeicherplatz. Sofern nicht anders vereinbart: Tägliches, inkrementelles Backup. Vorhaltdauer 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 über Servermanagement: XPAX 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.
- 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 über Servermanagement: Nach erfolgtem Hardwaretausch erfolgt die Wiederherstellung der Sicherung bzw. das Rückspielen des Backups durch XPAX.
- NUR bei Zusatzverträgen über Servermanagement: XPAX 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 über Servermanagement: XPAX konfiguriert eine lokale Firewall auf dem Server-Betriebssystem.

3.1.6. Für Verträge über XPAX **Backupspeicherplatz**

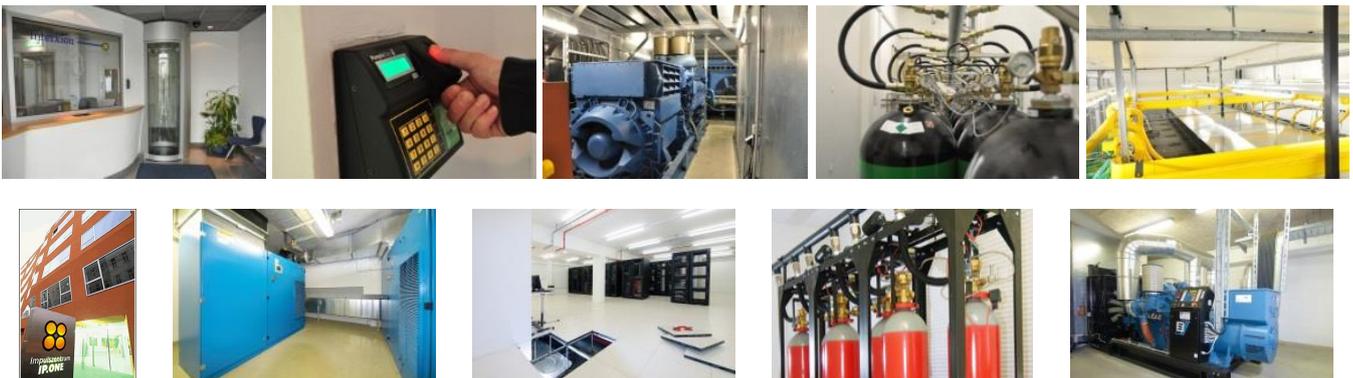
- Die Daten werden auf dem Speicherserver in einem RAID Verbund gespeichert, sodass der Defekt eines einzelnen Datenträgers nicht zum Datenverlust führen kann.
- Da es sich bei dem Produkt schon um Backup-Datenspeicher handelt wird von XPAX KEIN nochmaliges Backup dieser Daten angefertigt. Vielmehr ist 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.
- XPAX 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:

XPAX 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. XPAX 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 XPAX Produkt das für die Datenverarbeitung des Kunden angemessene Schutzniveau aufweist. XPAX 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 XPAX im Auftrag des Kunden verarbeiteten Daten ist der Kunde verantwortlich.

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

4.2.1. Gilt für Verträge über **Webhosting, Mailhosting, V-Server, Backup-Speicherplatz** und die XPAX Verwaltungsoberfläche..

- XPAX überprüft im Zuge des Produktmanagements in regelmäßigen Abständen, ob die technischen und organisatorischen Schutzmaßnahmen der XPAX 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 XPAX-Backend oder Hosting Server und der darauf von XPAX betriebenen Software.
- XPAX führt für die XPAX Hosting Systeme ein Software Inventar, welches zusammen mit dem Produkt-Lifecycle-Management sicherstellt, dass alle XPAX Hosting Server über Betriebssystem-Software verfügen, welche vom Herausgeber mit aktuellen Sicherheitsupdates versorgt werden.
- Von XPAX 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 XPAX 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 XPAX internen Datenschutzes

- XPAX führt ein aktuelles Verzeichnis aller Verarbeitungstätigkeiten von Kundendaten für die XPAX Verantwortlicher im Sinne der DSGVO ist. Dieses enthält auch ein eigenes Verzeichnis von allen gemäß Art. 32 ergriffenen Maßnahmen zur sicheren Datenverarbeitung. XPAX evaluiert diese technischen und Organisatorischen Maßnahmen in regelmäßigen Intervallen.
- Alle XPAX Mitarbeiter haben sich zur entsprechenden Verschwiegenheit und Geheimhaltung von Kundendaten vertraglich verpflichtet. Dies umfasst sowohl Geheimhaltung von Daten für die XPAX Verantwortlicher im Sinne der DSGVO, ist als auch Daten für die XPAX Auftragsverarbeiter im Sinne der DSGVO ist.
- XPAX schult und unterweist seine Mitarbeiter in regelmäßigen Intervallen im Datenschutz. Dies umfasst sowohl Schulung und Unterweisung im Umgang mit Daten für die XPAX Verantwortlicher im Sinne der DSGVO ist als auch Daten für die XPAX Auftragsverarbeiter im Sinne der DSGVO ist.
- Von XPAX 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 Dokumentationsanforderungen nach dem DSG geachtet.