EUGH KIPPT EU-US-PRIVACY SHIELD

Was müssen Sie bei der Provider-Auswahl beachten?

Allgemeine Angaben zum Anbieter

1.) Ihr Cloud-Anbieter hat seinen rechtlichen Sitz in Deutschland bzw. der EU.
Die Vorstellungen von Datenschutz in den USA, Asien und Europa unterscheiden sich maßgebend. Während das deutsche Recht der Allgemeinen Geschäftsbedingungen sehr streng ist, wird in US-Cloud-Verträgen von „Common Law" und in der asiatischen Rechtskultur von „Üblichkeiten" gesprochen.

2.) Ihr Cloud-Anbieter ist NICHT Teil eines US-Konzerns oder Tochtergesellschaft.
Durch den im März 2018 unterzeichneten CLOUD Act müssen US-amerikanische Unternehmen alle Daten in ihrem Besitz, ihrer Obhut oder ihre Kontrolle auf Verlangen an bevollmächtigte US-Behörden herausgeben – sogar teils auch ohne richterlichen Beschluss. Dies gilt auch für europäische Tochtergesellschaften oder Ländzentralen von US-Konzernen.

3.) Ihre Daten werden ausschließlich in deutschen bzw. europäischen Rechenzentren gehostet.
Sofern Sie einen Cloud-Anbieter mit einem rechtlichen Sitz und Rechenzentren in Deutschland oder der EU haben, müssen Sie sich keine Sorgen machen. Achten Sie jedoch auf den Rechenzentrum-Betreiber, dass dieser auch einen rechtlichen Sitz in Deutschland bzw. der EU aufweist und nicht Teil eines US-Unternehmens ist.

4.) Sie haben einen Vertrag zur Auftragsverarbeitung mit Ihrem Cloud-Anbieter geschlossen.
Die DSGVO regelt die Verarbeitung personenbezogener Daten und verpflichtet u. a. Cloud-Anbieter und ihre Kunden, einen Vertrag zur Auftragsverarbeitung zu schließen.

5.) Der mit dem Cloud-Anbieter geschlossene Vertrag zur Auftragsverarbeitung benennt konkrete technische und organisatorische Maßnahmen.
Mit den technischen und organisatorischen Maßnahmen werden tiefergreifenden Datenschutz und -sicherheitsmaßnahmen festgehalten. Da technische Pannen nicht zu 100 % ausgeschlossen werden können, bedarf es eines doppelten Bodens. In den Maßnahmen werden u.a. folgende Dinge festgehalten: Überwachung von Systemressourcen und Log-Files, Kontrolle von Cloud-Umgebungen, Risiken von Cyberangriffen etc. Tiefere Einblicke erhalten Sie weiter unten.

Für eigene Notizen:

Maßnahmen zur Sicherung der Vertraulichkeit und Integrität

1.) Sie kennen die Zutrittskontrollmaßnahmen zu den Serverräumen Ihres Cloud-Anbieters.

Wichtige Fragen dazu sind:

- Sind die personenbezogenen Daten auf mehr als einen Server- bzw. Rechenzentrumstandort verteilt?
- Welche Zugriffmaßnahmen für alle im Einsatz befindlichen Server- bzw. Rechenzentrum-Standorte werden ergriffen?
- Wie viele Personen haben Zutritt und wird dieser protokolliert?
- Ist der Rechenzentrumsbetreiber ISO27001 zertifiziert und werden interne sowie externe Audits durchgeführt?

2.) Sie kennen die Zutrittskontrollmaßnahmen zu den Büroräumen Ihres Cloud-Anbieters.

Wichtige Fragen dazu sind:

- Ist das Gebäude bzw. sind die Büroräume mittels Einbruchmeldeanlage und Videoüberwachung geschützt?
- Werden Zugriffsrechte personifiziert vergeben und wird die Schlüsselausgabe protokolliert?
- Existieren verbindlichen Passwortparameter und zwingt das interne IT-System die Nutzer zur Einhaltung der Passwortparameter?
- Erfolgt die Administration der Systeme durch mehrschichtige Authentifizierungsvorgehen, VPN-Zugang und SSH?

3.) Sie kennen die Maßnahmen zur Sicherung von Papierunterlagen, mobilen Datenträgern und mobilen Endgeräten Ihres Cloud-Anbieters.

Wichtigen Fragen dazu sind:

- Wie werden nicht mehr benötigte Papierunterlagen mit personenbezogenen Daten entsorgt?
- Wie werden nicht mehr benötigte Datenträger, auf der personenbezogenen Daten gespeichert sind, entsorgt?
- Dürfen mobile Datenträger verwendet werden?
- Verarbeiten Mitarbeiter personenbezogene Daten auf privaten Geräten?

4.) Sie kennen die Maßnahmen zur sicheren Datenübertragung.

Wichtige Fragen dazu sind:

- Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?
- Wer verwaltet die Schlüssel bzw. die Zertifikate?
- Werden die Übertragungsvorgänge protokolliert?
- Wie lange werden die Daten aufbewahrt?

Für eigene Notizen:

Maßnahmen zur Sicherstellung der Verfügbarkeiten von ...

1.) Serverräumen

Wichtige Fragen dazu sind:

- Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Tür, Brandmelder, Brandmeldezentrale und Löschsysteme?
- Ist der Standort bzw. das Rechenzentrum klimatisiert?
- Verfügt der Standort bzw. das Rechenzentrum über eine unterbrechungsfreie Stromversorgung und ein zusätzliches Dieselaggregat?
- Werden die Funktionen regelmäßig getestet?

2.) Backup- und Notfall-Konzept, Virenschutz

Wichtige Fragen dazu sind:

- Existiert ein Backup-Konzept?
- Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?
- Existiert ein Notfallkonzept bzw. existieren Notfallmaßnahmen bei Hardwaredefekten, Brand, Totalverlust etc?
- Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich?

3.) Netzanbindung

Wichtige Fragen dazu sind:

- Verfügt das Unternehmen über eine redundante Anbindung, bestenfalls über eine eigene redundante Anbindung (Glasfaserring)?
- Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden, bestenfalls über eine eigene redundante Anbindung (Glasfaserring)?
- Wer ist für die Netzanbindung des Unternehmens verantwortlich?

Pseudonymisierung / Verschlüsselung nach Artikel 32 Abs. 1 (DSGVO)

1.) Einsatz nach Pseudonymisierung

Wichtige Fragen dazu sind:

- Werden verarbeitete personenbezogenen Daten pseudonymisiert?
- Werden Algorithmen zur Pseudonymisierung eingesetzt?
- Erfolgt eine Trennung der Zuordnungsdaten und eine Aufbewahrung in getrennten Systemen?
- Wie kann die Pseudonymisierung bei Bedarf rückgängig gemacht werden?

2.) Einsatz von Verschlüsselung

Wichtige Fragen dazu sind:

- Werden verarbeitete, personenbezogenen Daten über bereits beschriebene Maßnahmen hinaus verschlüsselt?
- Welche Arten der Verschlüsselung werden eingesetzt?
- Welche kryptografischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z.B. Hashen von Passwörtern) eingesetzt?
- Wer hat Zugriff auf verschlüsselte Daten?

Für eigene Notizen:

Sonstige Maßnahmen nach Artikel 32 Abs. 1 (DSGVO)

1.) Belastbarkeit

Wichtige Fragen dazu sind:

- Existieren Maßnahmen, die die Fähigkeit gewährleisten, die Belastbarkeit der Systeme und Dienste in Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen?

2.) Wiederherstellbarkeit

Wichtige Fragen dazu sind:

- Existieren Notfall- oder Recovery-Konzepte und Maßnahmen?
- Gewährleisten die Konzepte, die Verfügbarkeit der personenbezogenen Daten und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?

3.) Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen

Wichtige Fragen dazu sind:

- Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung?
- In welchen Abständen finden die Überprüfungen statt?
- Wie werden die Ergebnisse protokolliert?
- Sind weitere Prozesse des Business Continuity Managements, Capacity Managements und Informations Security Managements etabliert?

Für eigene Notizen: