Technische und organisatorische Maßnahmen – Cloud Services –

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, muss der Auftragsverarbeiter die nachfolgend genannten technischen und organisatorischen Maßnahmen treffen, die der Verantwortliche als geeignet bestätigt hat, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus berücksichtigt der Verantwortliche insbesondere die Risiken, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von, beziehungsweise unbefugten Zugang zu, personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

1 Vertraulichkeit (ART. 32 ABS.1 (B) DSGVO)

1.1 **Zutrittskontrolle zu Verarbeitungsbereichen**: Der Auftragsverarbeiter trifft geeignete Maßnahmen, um zu verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsanlagen erhalten, in denen die personenbezogenen Daten verarbeitet werden. Dies wird auf folgende Weise erreicht:

(a) Der Zugang zu den Räumlichkeiten wird durch Sicherheitspersonal, Zugangskarten und (elektronische) Türschlösser kontrolliert.

(b) Zutrittsrechte zu den Räumlichkeiten werden nur denjenigen Mitarbeitern und Auftragnehmern gewährt, die einen legitimen geschäftlichen Grund für diesen Zutritt haben. Wenn ein Angestellter oder Auftragnehmer die zugewiesenen Zutrittsrechte nicht mehr benötigt, werden diese unverzüglich entzogen.

(c) Die Rechenzentren, in denen personenbezogene Daten gehostet werden, sind durch angemessene Sicherheitsmaßnahmen geschützt. Die vom Auftragsverarbeiter betriebenen Datenzentren befinden sich in der höchsten Sicherheitszone gemäß der Richtlinie für den physischen Zutritt. Die Rechenzentren von Dienstleistern gewährleisten angemessene Sicherheitsvorkehrungen, um nur befugtem Personal Zutritt zu den Räumlichkeiten zu gewähren.

(d) Der im Bestellformular für Cloud-Dienste angegebene Infrastructure-as-a-Service-Unterprozessor (IaaS-Anbieter) unterhält eine physische Zugangskontrolle für die Datenverarbeitungsgeräte der Cloud-Dienste. Unabhängige externe Audits überprüfen die jeweiligen physischen Sicherheitsmechanismen des IaaS-Anbieters im Hinblick auf die Einhaltung von ISO/IEC 27001.

(e) Besucher werden registriert, müssen einen Besucherausweis tragen und müssen während ihres Besuchs von Mitarbeitern des Auftragsverarbeiters begleitet werden.

1.2 **Zugangskontrolle zu Datenverarbeitungssystemen**: Der Auftragsverarbeiter ergreift geeignete Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden. Dies wird auf folgende Weise erreicht:

(a) Je nach den beauftragten Cloud-Diensten: Authentifizierung über Passwörter und/oder Multi-Faktor-Authentifizierung, dokumentierte Autorisierungsprozesse, dokumentierte Änderungsmanagementprozesse und Protokollierung des Zugriffs auf mehreren Ebenen.

(b) Der Zugang zu den Daten und Systemen der verantwortlichen Stelle wird gemäß der Zugangskontrollrichtlinie des Auftragsverarbeiters im Einklang mit der Norm ISO/IEC 27001 kontrolliert.

(c) Die Mitarbeiter des Auftragsverarbeiters erhalten ihre eigenen Anmeldedaten. Die Passwörter müssen den bewährten Praktiken der Branche entsprechen und mit der Anmelde- und Passwortrichtlinie des Auftragsverarbeiters übereinstimmen (z. B. Länge und Komplexität).

(d) Automatische Zeitüberschreitung der Arbeitsstationen, wenn sie nicht genutzt werden; zum erneuten Öffnen ist eine Authentifizierung erforderlich.

(e) Personalrichtlinien in Bezug auf die Zugriffsrechte des Personals auf personenbezogene Daten (falls vorhanden), Information des Personals über seine Pflichten und die Folgen von Verstößen gegen diese Pflichten, um sicherzustellen, dass das Personal nur auf personenbezogene Daten und Ressourcen zugreift, die für die Erfüllung seiner Aufgaben erforderlich sind, sowie Schulung des Personals in Bezug auf die geltenden Datenschutzpflichten und -pflichten.

(f) Einsatz modernster Verschlüsselungstechnologien für Daten bei der Übertragung („in transit") und bei der Speicherung der Daten („at rest").

1.3 **Zugriffskontrolle zu Datenverarbeitungssystemen**: Der Auftragsverarbeiter verpflichtet sich sicherzustellen, dass die zur Nutzung seines Datenverarbeitungssystems berechtigten Personen nur

im Rahmen und im Umfang ihrer jeweiligen Zugriffsberechtigung auf die Daten zugreifen und dass personenbezogene Daten nicht unbefugt gelesen, vervielfältigt, verändert oder gelöscht werden können. Dies wird auf folgende Weise erreicht:

(a) Den Mitarbeitern des Auftragsverarbeiters wird der Zugriff nach dem Prinzip der geringsten Berechtigung gewährt. Zu den anzuwendenden Zugriffskontrollen gehören ein dokumentiertes Änderungsverwaltungsverfahren sowie eine mehrstufige Authentifizierung und Verschlüsselung. Dieser Zugriff wird in Übereinstimmung mit der Cloud-Zugriffskontrollrichtlinie des Auftragsverarbeiters, der Clear Desk and Clear Screen Policy, der Encryption Policy und der Customer Cloud Data Privacy Policy kontrolliert.

(b) Die Anforderungen an die Datenübertragung in der Cloud-Kommunikationssicherheitsrichtlinie des Auftragsverarbeiters sind in Einklang mit der Norm ISO/IEC 27001.

(c) Einsatz modernster Verschlüsselungstechnologien für Daten bei der Übertragung („in transit") und bei der Speicherung der Daten („at rest").

1.4 **Trennung der Verarbeitung für unterschiedliche Zwecke**: Der Auftragsverarbeiter ergreift Maßnahmen, um sicherzustellen, dass für verschiedene Zwecke erhobene Daten getrennt voneinander verarbeitet werden können. Dies wird auf folgende Weise erreicht:

(a) Die Verarbeitung von Mandanteninhalten wird direkt in der Cloud-Anwendung gekapselt, auf die über den Cloud Service zugegriffen wird. Die Kontrolle des Zugriffs auf die Mandantenanwendung unterliegt dem Verantwortlichen. Alle Mandanteninhalte des Verantwortlichen werden direkt in der logisch getrennten Mandantendatenbank gekapselt.

1.5 **Pseudonymisierung**: Zur Erreichung der Zwecke der Auftragsdatenverarbeitung ist es nicht möglich, personenbezogene Daten zu pseudonymisieren. Ist eine Pseudonymisierung seitens des Verantwortlichen erforderlich, müssen die Daten innerhalb des Cloud-Dienstes in einem pseudonymisierten Format verarbeitet werden.

1.6 **Verschlüsselung**: Alle relevanten Daten werden gemäß den in der Verschlüsselungsrichtlinie festgelegten höchsten Standards unter Verwendung modernster Verschlüsselungsalgorithmen übertragen und gespeichert.

2 Integrität (ART. 32 ABS.1 (B) DSGVO)

2.1 **Eingabekontrolle**: Der Auftragsverarbeiter ergreift geeignete Maßnahmen, um zu kontrollieren, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, geändert oder aus ihnen entfernt wurden. Dies wird auf folgende Weise erreicht:

(a) Die Quelle der personenbezogenen Daten unterliegt der Kontrolle des Verantwortlichen, und die in den Cloud-Dienst eingegebenen personenbezogenen Daten werden durch gesicherte Datenübertragung (d. h. über Webdienste oder Eingabe in die Anwendung) von dem Verantwortlichen verwaltet. Hinweis: Bestimmte Cloud-Dienste können es dem Verantwortlichen gestatten, unverschlüsselte Datenübertragungsprotokolle zu verwenden. In solchen Fällen ist der Verantwortliche allein für ihre Entscheidung verantwortlich, solche unverschlüsselten Datenübertragungsprotokolle zu verwenden.

(b) Nur autorisiertes Personal kann auf die Produktions-Cloud-Infrastruktur der Datenverarbeitung des Verantwortlichen zugreifen, und zwar ausschließlich zum Zweck der Verwaltung und Wartung. Alle Mitarbeiter verfügen über eine eindeutige Benutzerkennung und verwenden sichere Passwörter gemäß der Anmelde- und Passwortrichtlinie, und alle diese Aktivitäten werden überwacht und protokolliert.

(c) Authentifizierung des autorisierten Personals; individuelle Benutzerkennungen, die, sobald sie einmal zugewiesen wurden, nicht erneut einer anderen Person zugewiesen werden können.

2.2 **Weitergabekontrolle**: Der Auftragsverarbeiter ergreift geeignete Maßnahmen, um zu verhindern, dass personenbezogene Daten während der Übermittlung von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können. Dies wird auf folgende Weise erreicht:

(a) Für alle Produktions-Cloud-Umgebungen bieten die Sicherheitsmechanismen des IaaS-Anbieters private, isolierte Bereiche für die vom Auftragsverarbeiter genutzte Cloud, in denen die jeweiligen Cloud-Ressourcen in einem definierten virtuellen Netzwerk gestartet werden. Alle erfassten Daten werden in einer virtuellen Cloud-Umgebung gespeichert und über HTTPS mit aktuellen Verschlüsselungscodes übertragen.

(b) Controller-Tenant-Daten im Ruhezustand für Cloud-Dienste sind verschlüsselt. Sofern für die Cloud-Dienste nicht anders angegeben (einschließlich des Bestelldokuments oder der geltenden

Leistungsbeschreibung), werden Datenübertragungen außerhalb der Cloud-Dienstumgebung verschlüsselt.

(c) Die Anforderungen an die Datenübertragung gemäß den Sicherheitsrichtlinien für die Cloud-Kommunikation des Auftragsverarbeiters schützen die Übertragung von Daten des Verantwortlichen bei der Verwendung aller Arten von Kommunikationseinrichtungen.

(d) Einsatz geeigneter Firewall- und Verschlüsselungstechnologien für Daten während der Übertragung.

(e) Die Datenübertragungen werden protokolliert und überwacht.

3 Verfügbarkeit (ART. 32 ABS.1 (B) DSGVO)

3.1 **Verfügbarkeitskontrolle**: Der Auftragsverarbeiter ergreift geeignete Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor versehentlicher oder unbefugter Änderung, Verlust oder Zerstörung geschützt werden. Dies wird durch die folgenden Maßnahmen erreicht:

(a) Alle Änderungen an den Produktionsumgebungen werden vollständig überwacht. Der Prozessor führt regelmäßige Tenant-Backups durch, um die Images virtueller Maschinen und Tenant-Daten wiederherstellen zu können.

(b) Die Verfügbarkeitskontrolle für Cloud-Dienste wird im Rahmen des Information Security Continuity Management und der Backup- und Wiederherstellungskontrollen für Cloud-Dienste gewährleistet, die mit der Norm ISO/IEC 27001 in Einklang sind.

(c) Die IaaS-Anbieter Dienste des Auftragsverarbeiters sind vor Ausfällen von Versorgungsdiensten gemäß der Norm ISO/IEC 27001 geschützt, die von einem unabhängigen Prüfer validiert und zertifiziert wurde.

(d) Die Sicherung von Steuerungsdaten und der Schutz von Protokolldateien werden in Übereinstimmung mit der Norm ISO/IEC 27001 kontrolliert. Die Aufbewahrung der Sicherungskopien wird durch entsprechende Richtlinien geregelt.

(e) Jeder festgestellte Sicherheitsvorfall wird zusammen mit den befolgten Datenwiederherstellungsverfahren aufgezeichnet.

3.2 **Belastbarkeit**: Firewalls schützen den externen Zugang zu allen Cloud-Produktionsnetzen und -systemen, und Intrusion Detection Prevention Systeme werden zur Begrenzung/Filterung des Netzverkehrs eingesetzt. Die Notfallwiederherstellung von Cloud-Diensten wird jährlich getestet und überprüft.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (ART. 32 ABS. 1 LIT. D DSGVO)

4.1 **Datenschutzmanagement**: Der Auftragsverarbeiter hat ein Datenschutzmanagementsystem eingeführt, das dokumentierte Datenschutzprozesse enthält, wie z. B. den Umgang mit Datenschutzverletzungen, die Führung von Verzeichnissen von Verarbeitungstätigkeiten und die Unterstützung des Verantwortlichen bei der Bearbeitung von Anfragen der betroffenen Personen. Das Datenschutzmanagementsystem unterliegt einer regelmäßigen Überprüfung und Kontrolle.

4.2 **Incident-Response-Management**: Der Auftragsverarbeiter verfügt über klar definierte Prozesse zur Behandlung von IT-Sicherheitsvorfällen und Datenschutzverletzungen im Rahmen des Qualitätsmanagement- und Datenschutzmanagementsystems, das der Norm ISO/IEC 27001 entspricht. Sicherheitsvorfälle werden mit dem Incident Management Tool des Auftragsverarbeiters verfolgt. Das Incident-Response-Programm des IaaS-Anbieters (Erkennung, Untersuchung und Reaktion auf Vorfälle) wurde im Einklang mit den ISO 27001-Standards entwickelt, und die Systemfunktionen werden angemessen eingeschränkt und überwacht.

4.3 **Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**: Der Auftragsverarbeiter verfügt über Datenschutzrichtlinien und -kontrollen, die es den Mitarbeitern von Cloud Services untersagen, auf Tenantdaten zuzugreifen, es sei denn, sie wurden vom Tenantadministrator des Verantwortlichen ausdrücklich autorisiert und zugelassen. Alle Mandanteninhalte des Verantwortlichen werden direkt in der logisch getrennten Mandantendatenbank gekapselt. Personenbezogene Daten sind ausschließlich berechtigten Personen zugänglich und können nur von diesen verwaltet werden. Der direkte Datenbankzugriff ist eingeschränkt; für den Zugriff auf Anwendungen sind Rechte festgelegt und werden durchgesetzt. Standardkonfigurationen von Cloud Services sind so eingestellt, dass nur solche personenbezogenen Daten verarbeitet werden,

die notwendig sind, um die Cloud Services zu erbringen.

4.4 **Auftragskontrolle**: Der Auftragsverarbeiter ergreift geeignete Maßnahmen, um sicherzustellen, dass die personenbezogenen Daten gemäß den Anweisungen des Verantwortlichen verarbeitet werden. Der Auftragsverarbeiter stellt sicher, dass er eine schriftliche Beschreibung der Sicherheitsmaßnahmen seiner Unterauftragsverarbeiter erhält, wenn diese für die Erbringung von Unterstützungsleistungen zuständig sind. Darüber hinaus hat der Auftragsverarbeiter die Einhaltung dieser Maßnahmen durch die Unterauftragsverarbeiter regelmäßig zu überwachen. Dies wird auf folgende Weise erreicht:

(a) Die Kontrolle über die personenbezogenen Daten verbleibt bei dem Verantwortlichen. Zwischen dem Verantwortlichen und dem Auftragsverarbeiter bleibt der Verantwortliche zu jeder Zeit der für die Zwecke der Cloud-Dienste, des Cloud-Dienste-Vertrags und des Datenverarbeitungs-Vertrags Verantwortliche. Der Verantwortliche ist für die Einhaltung seiner Pflichten als Verantwortlicher gemäß den Datenschutzgesetzen verantwortlich, insbesondere für die Rechtfertigung der Übermittlung personenbezogener Daten an den Auftragsverarbeiter (einschließlich der Bereitstellung aller erforderlichen Mitteilungen und der Einholung aller erforderlichen Zustimmungen) sowie für seine Entscheidungen und Maßnahmen in Bezug auf die Verarbeitung und Nutzung der Daten.

(b) Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich für die Erbringung der Cloud-Dienste verarbeiten und (i) personenbezogene Daten nicht für andere Zwecke als die in der Cloud-Dienste-Vereinbarung genannten oder vom Verantwortlichen angewiesenen Zwecken verarbeiten oder nutzen oder (ii) solche personenbezogenen Daten an Dritte weitergeben, die nicht Unterauftragsverarbeiter für die oben genannten Zwecke oder gesetzlich vorgeschrieben sind.

(c) Der Zugang zu den Daten und Systemen des Verantwortlichen wird gemäß den Richtlinien für die Zugangskontrolle zu den Cloud-Diensten und den Sicherheitskontrollen für den Betrieb kontrolliert, die mit der Norm ISO 27001 übereinstimmen.

4.5 **Auftragskontrolle – Systemadministratoren**: Des Weiteren implementiert der Auftragsverarbeiter angemessene Maßnahmen zur Überwachung seiner Cloud Dienste und um sicherzustellen, dass diese mit den erhaltenen Anweisungen und den entsprechenden ISO/IEC-27001-Kontrollen übereinstimmen. Dies wird durch folgende Maßnahmen erreicht:

(a) Individuelle Ernennung von Systemadministratoren;

(b) Regelmäßige Überprüfung der Systemadministratoren, um zu beurteilen, ob sie die ihnen zugewiesene Rolle erfüllen;

(c) Führen einer aktualisierten Liste mit den Identifikationsdaten der Systemadministratoren;

(d) Bewertung der technischen und organisatorischen Maßnahmen der Unterauftragsverarbeiter vor deren Beauftragung und regelmäßige Überwachung der Einhaltung dieser Maßnahmen.

Zusätzliche länderspezifische Maßnahmen

Folgende Maßnahmen gelten, soweit sich der Verantwortliche in dem jeweiligen Land befindet:

I. Belgien

1. Es wird vereinbart, dass jeder Auftragsverarbeiter diese AVV für seine eigenen Zwecke und seine eigene Datenverarbeitung abschließt, ohne mit den anderen gesamtschuldnerisch oder gesamtschuldnerisch ("solidairement ou indivisiblement") verbunden zu sein.
2. In ausdrücklicher Abweichung von Artikel 1325 des belgischen Zivilgesetzbuches kann dieser DPA von jedem Unterzeichner separat gültig unterzeichnet werden und muss durch die Vorlage einer Original- oder Nicht-Originalkopie zusammen mit den Unterschriftsseiten (oder Kopien davon) der anderen relevanten Parteien ordnungsgemäß nachgewiesen werden. Die Parteien verzichten auf alle Beweis- und/oder sonstigen Anforderungen an die Ausführung dieses DPA, die nicht in diesem Abschnitt für Belgien festgelegt sind.

II. Luxemburg

1. Es wird vereinbart, dass jeder Auftragsverarbeiter diese AVV für seine eigenen Zwecke und seine eigene Datenverarbeitung abschließt, ohne mit den anderen gesamtschuldnerisch oder gesamtschuldnerisch ("solidairement ou indivisiblement") verbunden zu sein.
2. Erfolgt in [zwei] Urschriften, wobei jede Vertragspartei den Empfang eines ordnungsgemäß unterzeichneten Originals bestätigt.

III. Australien

Die folgenden Änderungen gelten nur in Bezug auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag eines Verantwortlichen, der eine australische Verbindung in Bezug auf diese

personenbezogenen Daten im Sinne des Privacy Act 1988 (Cth) ("**australische Daten**") hat, unabhängig davon, ob das Land, in dem der Unterauftragsverarbeiter ansässig ist, von der Europäischen Kommission als Land benannt wurde, das ein angemessenes Schutzniveau gemäß Artikel 45 Absatz 1 gewährleistet. Datenschutzverordnung:

1. In dieser DPA werden Verweise auf
    - ein "Mitgliedstaat" schließt Australien ein;
    - die "Datenschutz-Grundverordnung", die "DSGVO", die "anwendbaren Datenschutzgesetze" ("**EU-Datenschutzgesetze**") und alle Bestimmungen, Abschnitte, Kapitel oder Artikel dieser EU-Datenschutzgesetze in der Vereinbarung werden durch den Begriff "Privacy Act 1988 (Cth) und alle anwendbaren bundesstaatlichen und territorialen Datenschutzgesetze sowie alle damit verbundenen Gesetze und Vorschriften" ("**Australische Datenschutzgesetze**") ersetzt;
    - "personenbezogene Daten" sind so zu verstehen, dass sie personenbezogene Daten im Sinne der australischen Datenschutzgesetze umfassen;
    - der Begriff "Aufsichtsbehörde" ist als Verweis auf die zuständige Regulierungsbehörde gemäß den australischen Datenschutzgesetzen zu verstehen; und
    - "besondere Datenkategorien" und "sensible Daten" sind so zu verstehen, dass sie sensible Informationen im Sinne der australischen Datenschutzgesetze umfassen;
2. Der Auftragsverarbeiter wird angemessene Schritte unternehmen, um die von ihm verarbeiteten australischen Daten vor Missbrauch, Beeinträchtigung und Verlust sowie vor unbefugtem Zugriff, Änderung oder Offenlegung zu schützen;
3. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Folgendes informieren: (i) jeden bekannten oder vernünftigen Grund zu der Annahme, dass der Auftragsverarbeiter oder seine Mitarbeiter die gesetzlichen Bestimmungen zum Schutz australischer Daten nicht einhalten, und (ii) jeden bekannten oder vernünftigen Grund zu der Annahme, dass die Bestimmungen dieses DPA nicht eingehalten werden. Der Auftragsverarbeiter wird den Verantwortlichen ferner unverzüglich benachrichtigen, wenn er der Ansicht ist, dass eine Anweisung gegen geltendes Recht verstößt. Nach Abgabe einer solchen Benachrichtigung ist der Auftragsverarbeiter nicht verpflichtet, der Anweisung Folge zu leisten, es sei denn, der Verantwortliche hat sie bestätigt oder geändert. Der Auftragsverarbeiter informiert den Verantwortlichen über Beschwerden und Anträge betroffener Personen (z. B. in Bezug auf die Berichtigung, Löschung und Sperrung von Daten) und Anordnungen von Gerichten und zuständigen Aufsichtsbehörden sowie über alle anderen vom Auftragsverarbeiter festgestellten Gefährdungen oder Bedrohungen in Bezug auf die Einhaltung des Datenschutzes und leistet dem Verantwortlichen angemessene Unterstützung, um rechtzeitig auf solche Beschwerden oder Anfragen zu reagieren. Ungeachtet der vorstehenden Punkte (i) und (ii) wird der Auftragsverarbeiter den Verantwortlichen unverzüglich über eine Datenschutzverletzung informieren, wenn der Auftragsverarbeiter berechtigten Grund zu der Annahme hat, dass ein Sicherheitsvorfall aufgetreten ist, der sich wahrscheinlich auf die Verfügbarkeit, Integrität und/oder Vertraulichkeit der vom Auftragsverarbeiter verarbeiteten australischen Daten auswirkt (z. B. Entdeckung einer unbeabsichtigten Datenlöschung, Entdeckung von Daten, die für Ressourcen zugänglich sind, die nicht oder nicht mehr autorisiert waren, Entdeckung von unbeabsichtigter Offenlegung oder Daten, die möglicherweise durch einen Hackerangriff oder eine andere externe Sicherheitsbedrohung kompromittiert wurden). Die Benachrichtigung über Datenschutzverletzungen muss mindestens den Umfang der betroffenen australischen Daten, den Umfang und die Anzahl der betroffenen Personen, den Zeitpunkt, zu dem die Datenschutzverletzung stattgefunden hat, die Umstände und die Auswirkungen der Datenschutzverletzung sowie die Maßnahmen, die ergriffen wurden, um die Folgen der Verletzung zu beseitigen, sowie weitere Informationen enthalten, die der für die Verarbeitung Verantwortliche möglicherweise benötigt, um die australischen Datenschutzgesetze einzuhalten;
4. Australische Daten müssen vernichtet oder dauerhaft anonymisiert werden, nachdem sie für einen von dieser DPA zugelassenen Zweck nicht mehr benötigt werden. Der Auftragsverarbeiter muss eine schriftliche Bestätigung des Verantwortlichen einholen, dass australische Daten nicht mehr benötigt werden, bevor er diese australischen Daten vernichtet oder anonymisiert.
5. Australische Daten dürfen nur dann für Direktmarketing verarbeitet werden, wenn die betroffene Person einer solchen Verarbeitung ausdrücklich zugestimmt hat oder der für die Verarbeitung Verantwortliche etwas anderes schriftlich vereinbart hat;
6. Identifikatoren betroffener Personen, die von oder im Namen einer australischen Regierungsorganisation zugewiesen wurden, dürfen nicht verwendet oder weitergegeben werden, es sei denn, dies ist nach australischem Recht erforderlich oder zulässig. und
7. Sensible Daten dürfen nur mit Zustimmung der betroffenen Person verarbeitet werden, es sei denn, der für die Verarbeitung Verantwortliche stimmt schriftlich etwas anderem zu.

IV. Malaysia

Auftragsverarbeiter ergreift die folgenden Sicherheitsmaßnahmen in Übereinstimmung mit den Anforderungen des Standards zum Schutz personenbezogener Daten 2015 und des Gesetzes zum Schutz personenbezogener Daten von 2010:

1. ein Verzeichnis aller Mitarbeiter zu führen, die an der Verarbeitung personenbezogener Daten beteiligt sind;
2. die Rechte seiner Mitarbeiter nach Beendigung der Betriebszugehörigkeit, Kündigung und Ende der Vertrags-/Vertragslaufzeit oder aufgrund organisatorischer Änderungen einzustellen;

3. Kontrolle und Einschränkung des Umfangs des Rechts seiner Mitarbeiter auf Zugang zu personenbezogenen Daten;
4. die Aus- und Ein- und Ausreise in Bezug auf die Datenspeicherorte zu kontrollieren;
5. Aktualisieren Sie alle Sicherungs-/Wiederherstellungssysteme und Antivirensoftware, um persönliche Daten vor Invasionen zu schützen;
6. Computersysteme vor Malware-Bedrohungen für personenbezogene Daten zu schützen;
7. sicherzustellen, dass die Übertragung personenbezogener Daten über Wechseldatenträger und Cloud-Computing-Dienste nur mit schriftlicher Genehmigung der Geschäftsleitung des Auftragsverarbeiters erfolgt;
8. alle Übertragungen personenbezogener Daten aufzuzeichnen, bei denen ein Wechseldatenträger und ein Cloud-Computing-Dienst verwendet werden; und
9. ein genaues, regelmäßiges Protokoll über den Zugriff auf personenbezogene Daten zu führen und die Aufzeichnungen offenzulegen, wenn dies von der malaysischen Abteilung für den Schutz personenbezogener Daten verlangt wird.

V. Mexiko

Für Verantwortliche mit Sitz in Mexiko gelten das Bundesgesetz über den Schutz personenbezogener Daten im Besitz natürlicher Personen von 2010 und die folgenden zusätzlichen Maßnahmen:

1. Der Auftragsverarbeiter legt die Aufgaben und Pflichten fest, die für die für den Schutz personenbezogener Daten zuständigen Beamten gelten;
2. Der Unterauftragsverarbeiter implementiert in seiner Organisation ein angemessenes Datenschutzmanagement, einschließlich der folgenden Beispiele:
    - Erstellung und Pflege von Verzeichnissen von: (i) personenbezogenen Daten, die von betroffenen Personen erhoben wurden; (ii) Sicherheitssysteme und Speicherinfrastrukturen, die für die Verarbeitung personenbezogener Daten verwendet werden;
    - Durchführung von Sicherheitsmaßnahmen, Lückenanalysen und Durchführung regelmäßiger Audits und Bewertungen von Sicherheitsrisiken, um mögliche Risiken und Verbesserungsbereiche zu identifizieren und zu bewerten;
    - Entwicklung und Umsetzung von Aktionsplänen, um alle bei solchen Bewertungen und Audits festgestellten Probleme anzugehen;
    - Angemessene Schulung des Personals, das an der Datenverarbeitung beteiligt ist;
    - Aktualisieren Sie die Sicherheitsmaßnahmen entsprechend, um diese Maßnahmen zu verbessern, entweder als Ergebnis von Empfehlungen, die sich aus Audits oder Bewertungen ergeben, oder nach Bestätigung eines unbefugten Zugriffs oder einer unbefugten Offenlegung personenbezogener Daten.

VI. Indien

Der Digital Personal Data Protection Act 2023 gilt für den Schutz personenbezogener Daten und wird voraussichtlich 2024 in Kraft treten. Zusätzliche Maßnahmen für Verantwortliche, die in Indien ansässig sind: Der Auftragsverarbeiter muss das gleiche oder ein höheres Datenschutzniveau gewährleisten, das vom Verantwortlichen gemäß dem Informationstechnologiegesetz von 2000 und den Regeln für Informationstechnologie (angemessene Sicherheitspraktiken und -verfahren und sensible personenbezogene Daten oder Informationen) von 2011 eingehalten wird.

VII. Israel

1. Der Verantwortliche und der Auftragsverarbeiter halten die geltenden Datenschutzgesetze ein, einschließlich des Gesetzes zum Schutz der Privatsphäre von 1981 und aller Aktualisierungen zur Anpassung an die EU-DSGVO.
2. Der Auftragsverarbeiter wird dem Verantwortlichen mindestens einmal jährlich einen Bericht über die Art und Weise vorlegen, in der er seine Pflichten gemäß den israelischen Informationssicherheitsvorschriften und diesem DPA erfüllt, und den Verantwortlichen über das Auftreten eines Sicherheitsereignisses informieren, an dem die personenbezogenen Daten beteiligt sind.
3. Der Auftragsverarbeiter verpflichtet sich, dafür zu sorgen, dass die befugten Personen in seinem Namen alle erforderlichen Sicherheitsmaßnahmen ergreifen, die in Übereinstimmung mit den geltenden Gesetzen in Bezug auf die personenbezogenen Daten erforderlich sind, einschließlich aller Anforderungen zum Schutz der Integrität dieser personenbezogenen Daten und zum Schutz vor unrechtmäßiger Offenlegung, Verwendung oder Vervielfältigung davon.
4. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen begründetes Verlangen Berichte über die von ihm ergriffenen Sicherheitsmaßnahmen zur Verfügung zu stellen, und wird es dem Verantwortlichen und/oder einer in seinem Namen handelnden Person ermöglichen, dies zu tun.
5. Der Auftragsverarbeiter verpflichtet sich, von Zeit zu Zeit und in jedem Fall nicht weniger als einmal im Jahr jedem, der in seinem Namen im Zusammenhang mit den Verpflichtungen aus diesem DPA handelt, Tutorials zur Verfügung zu stellen, einschließlich der Pflicht, die personenbezogenen Daten streng vertraulich zu behandeln.
6. Der Auftragsverarbeiter wird alle Anforderungen des Verantwortlichen an die Datensicherheit einhalten, die nach den geltenden Datenschutzgesetzen erforderlich sind und die dem Auftragsverarbeiter von Zeit zu Zeit mitgeteilt werden. Der Auftragsverarbeiter schränkt die Möglichkeit

ein, tragbare Geräte an die Systeme anzuschließen, in denen die personenbezogenen Daten gespeichert sind, oder verhindert sie.
7. Der Auftragsverarbeiter stellt sicher, dass die Datenbanksysteme, in denen die personenbezogenen Daten gespeichert sind, laufend aktualisiert werden.
8. Gegebenenfalls sollte der Auftragsverarbeiter gemäß den israelischen Vorschriften zur Informationssicherheit Maßnahmen ergreifen, um den Ein- und Austritt aus den Orten, an denen sich die Systeme, in denen die personenbezogenen Daten verarbeitet werden, befinden, sowie das Ein- und Ausbringen von Geräten in und von solchen Standorten zu kontrollieren und zu dokumentieren.
9. Der Auftragsverarbeiter erteilt die Erlaubnis zum Zugriff auf die personenbezogenen Daten oder zur Änderung ihres Umfangs, nachdem er angemessene Maßnahmen ergriffen hat. Die Zugriffsberechtigungen auf die personenbezogenen Daten werden gemäß den Stellendefinitionen festgelegt.
10. Der Auftragsverarbeiter verpflichtet sich, dass die Personen, die zur Nutzung seines Datenverarbeitungssystems berechtigt sind, geltende Vertraulichkeitsverpflichtungen unterzeichnen, wonach sie die Informationen vertraulich behandeln und die Informationen nur zum Zwecke der Erbringung der Dienstleistungen für den Kunden verwenden werden.
11. Der Auftragsverarbeiter hat geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass er überprüfen und feststellen kann, wann ein Zugriff auf die personenbezogenen Daten erfolgte.
12. Der Auftragsverarbeiter entzieht die Berechtigungen einer bevollmächtigten Person, die ihre Rolle beendet hat. und, soweit möglich, sofort nach Beendigung der Rolle der berechtigten Person die Passwörter ändern, die der berechtigten Person möglicherweise bekannt waren.
13. Die Systeme, in denen die personenbezogenen Daten gespeichert sind, dürfen nicht mit dem Internet oder einem anderen öffentlichen Netzwerk verbunden werden, ohne dass geeignete Mittel zum Schutz vor unbefugtem Eindringen oder vor Programmen installiert wurden, die in der Lage sind, den Computer oder das Computermaterial zu beschädigen oder zu stören (einschließlich der Verwendung akzeptierter Verschlüsselungsmittel). In Bezug auf ein System, auf das aus der Ferne über das Internet oder ein anderes öffentliches Netz zugegriffen werden kann, sind zusätzliche Sicherheitsmaßnahmen zu ergreifen, die darauf abzielen, die Partei, die die Verbindung herstellt, zu identifizieren und ihre Berechtigung zur Durchführung der Vorgänge aus der Ferne und deren Umfang zu überprüfen.