

	Anforderungen an die Sicherheitsorganisation des Dienstleisters bei Verarbeitung von Informationen mit normalem Schutzbedarf (keine besondere Kategorien personenbezogener Daten, vertrauliche Geschäftsgeheimnisse werden nicht verarbeitet) - Ausführungsbedingungen (Anlage 2 zum Vertrag)	MUSS
E-Mail-Gateway	Abgleich ankommender E-Mails mit global gültigen SPAM-Listen (z. B. von Spamhaus, EasyList) am E-Mail-Gateway des Dienstleisters.	MUSS
	Blockierung ausführbarer Dateien im E-Mail-Anhang (z. B. „.bat, .exe, .cmd, .docxm, .zip, .ps1“) und in E-Mails befindlicher, potenziell bösartiger Hyperlinks am E-Mail-Gateway des Dienstleisters.	MUSS
Anti-Malware-Software	Sicherstellung des flächendeckenden Einsatzes einer Anti-Malware-Software nach dem Stand der Technik (z. B. Advanced Detection and Response) und Gewährleistung, dass die Anti-Malware-Software und ihre Signaturen automatisiert auf jedem System auf dem aktuellen Stand gehalten werden.	MUSS
Benutzerrechte	Sicherstellung, dass alle „normalen“ Nutzer*innen des Dienstleisters keinesfalls Administratorrechte besitzen.	MUSS
	Gewährleistung, dass lediglich Administrator*innen die Möglichkeit besitzen, Software, Apps und Add-Ins auf informationsverarbeitenden Systemen zu installieren und zu deinstallieren.	MUSS
	Stellung von höheren, angemessenen Anforderungen an Passwörter von Administrator*innen in Bezug auf die Komplexität (z. B. mindestens 20 Zeichen, ein Sonderzeichen, eine Zahl sowie ein Groß- sowie Kleinbuchstabe).	MUSS
Backups	Erstellung und Einhaltung eines angemessenen Backup-Konzeptes, in dem alle informationsverarbeitenden Systeme berücksichtigt werden, die für die Erbringung aller wesentlichen Prozesse beim Dienstleister erforderlich sind.	MUSS
	Regelmäßige Durchführung von Backups und stichprobenartige Überprüfung auf ihre Funktion auf allen Systemen, die für die Erbringung aller wesentlichen Prozesse beim Dienstleister erforderlich sind,	MUSS
	Vorhaltung dieser Backups auf mehreren Systemen und Einhaltung insbesondere der 3-2-1- Backup-Regel (Erstellen von drei Datenkopien, auf mindestens zwei unterschiedlichen Medien, wovon mindestens ein Backup sicher in Bezug auf das Netz, den Raum und die Domäne getrennt gelagert werden sollte).	MUSS
IP-Netzwerke	Gewährleistung, dass eingesetzte Netzwerke, die für die Erbringung aller wesentlichen Prozesse erforderlich sind, weitestgehend in Bezug auf den Zweck voneinander getrennt sind.	MUSS
	Flächendeckende Definition restriktiver Firewall-Regeln gem. Minimalprinzip. Restriktive Vergabe insbesondere von RDP-, VNC- und SMB-Verbindungsmöglichkeiten.	MUSS
Schulungen	Regelmäßige - zumindest zweijährliche - und flächendeckende Durchführung von Awareness-Schulungen in Kontext Datenschutz und Informationssicherheit - insb. zum Thema Ransomware - für Beschäftigte des Dienstleisters.	MUSS
Updates	Unmittelbare und flächendeckende Durchführung von System- und Softwareaktualisierungen – je nach Kritikalität.	MUSS
	Unmittelbarer und flächendeckender Austausch veralteter Betriebssysteme und Software, welche nicht mehr mit regelmäßigen bzw. aktuellen Updates versorgt werden können.	MUSS
Standards	Durchführung von standardisierten Sicherheitskonfigurationen für informationsverarbeitende Systeme, die für die Erbringung aller wesentlichen Prozesse erforderlich sind, insbesondere bei Neueinführungen und Änderungen an diesen Systemen.	MUSS
	Ausschließliche Installation von Software auf allen informationsverarbeitenden Systemen, die tatsächlich für die benötigte Dienstleistung bzw. -nutzung erforderlich ist.	MUSS
Lieferketten	Vertragliche Regelung, dass die vom Dienstleister beauftragten Subdienstleister mindestens dieselben Sicherheitsstandards erfüllen, wie die beauftragende Organisation sowie regelmäßige Überprüfung dessen.	MUSS
	Zusicherung der Offenlegung aller Betriebsstätten und verbundenen Unternehmen des Dienstleisters sowie seine dbzgl. Subdienstleister inkl. Leistungserbringungsorte.	MUSS
	Zusicherung der Bereitstellung eines Transfer Impact Assessments für Datenverarbeitungen in Drittländern ohne Angemessenheitsbeschluss i. S. d. Art. 45 DSGVO.	MUSS
	Zusicherung, dass keine Datenverarbeitungen aller Betriebsstätten und verbundenen Unternehmen des Dienstleisters sowie seine dbzgl. Subdienstleister in Ländern erfolgen, die in der Staatenliste des BMI gem. § 13 Abs. 1 Nr. 17 SÜG aufgeführt sind.	MUSS
Fernzugänge	Lediglich Einrichtung von Möglichkeiten für den Fernzugriff auf Systeme des Dienstleisters von Subdienstleistern, die dem aktuellen Stand der Technik entsprechen (z. B. über angemessen verschlüsselte VPN-Tunnel, Einsatz eines Jump-Servers, Multifaktor-Authentifikation).	MUSS
Security Operations Center	Dauerhafte Überwachung aller Systeme, die für die Erbringung aller wesentlichen Prozesse erforderlich sind, sowie unmittelbare Reaktion bei Sicherheitsvorfällen.	MUSS
Rechenzentrum	Zusicherung, dass alle wesentlichen Versorgungskomponenten redundant ausgelegt sind (z. B. Strom, Klimatisierung der RZ, Internetanbindung, Verkabelung).	MUSS
	Zusicherung, dass die Überwachung des Zutritts der Rechenzentrumsstellflächen stattfindet (z. B. über Zutrittskontrollsystem, Videoüberwachungssystem, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme).	MUSS
	Zusicherung des angemessenen Brandschutzes (z. B. Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmäßige Brandschutzübungen).	MUSS
	Zusicherung der robusten Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet.	MUSS
	Zusicherung einer 2-Faktor-Authentisierung für den Zutritt auf die Rechenzentrumsstellflächen des Dienstleisters oder beim Provider, der die Bereitstellung übernimmt.	MUSS