Checkliste IT Dienstleister
checklist IT service providers

Klassifizierung: vertraulich
classifiaction: confidential

Englisch

Dienstleister: *service provider:*	Datum: *date:*

Kriterium ***criterion***	**Dienstleisterhinweis** ***Service Provider Note***	**ja** ***yes***	**nein** ***no***	**Bemerkung** ***Comment***
Organisation ***organization***				
Die Auswahl der technischen Sicherungsverfahren und die Organisation der IT-Sicherheit werden in Abstimmung mit dem Kunden auf der Basis der Best Practices der **ISO 27002** (oder vergleichbar) abgestimmt. *The selection of technical security procedures and the organization of IT security are coordinated with the customer on the basis of the best practices of ISO 27002 (or comparable).*	Es geht dabei darum, die Kronjuwelen des Anwenders zu identifizieren und mit ihm gemeinsam passende Maßnahmen auszusuchen. *The aim is to identify the user's crown jewels and work with him to select suitable measures.*	☐	☐	
Der Dienstleister **berichtet** monatlich über den sicherheitsrelevanten Status der Kundensysteme und gibt **Handlungsempfehlungen.** *The service provider reports monthly on the security-relevant status of customer systems and provides recommendations for action.*	Es geht dabei darum, die Kronjuwelen des Anwenders zu identifizieren und mit ihm gemeinsam passende Maßnahmen auszusuchen. *The aim is to identify the user's crown jewels and work with him to select suitable measures.*	☐	☐	
Der Dienstleister erklärt sich bereit, **Security Audits** durch geeignete Dritte mit einer angemessenen Vorlaufzeit zu akzeptieren. *The Service Provider agrees to accept security audits by suitable third parties with a reasonable lead time.*	Geben Sie den Stab weiter - auch Dritte können riskant handeln. *Pass the baton - third parties can also act riskily.*	☐	☐	

Prävention
prevention

Der Dienstleister gewähreistet eine definierte **Mindestverfügbarkeit** pro Monat für alle für den Kunden relevanten Systeme (Service Level Agreement - „SLA“). *The service provider guarantees a defined minimum availability per month for all systems relevant to the customer (Service Level Agreement - "SLA").*	Die Mindestverfügbarkeit muss Ihrem Kunden passen. Richten Sie Ihre internen Dienste darauf aus. *The minimum availability must suit your customer. Align your internal services with it.*	☐	☐	
Der Dienstleister bietet an, für alle für den Kunden relevante Systeme **Backups nach Stand der Technik** durchzuführen und auf Anforderung des Kunden testweise rückzusichern. *The service provider offers to perform state-of-the-art backups for all systems relevant to the customer and to restore them on a test basis at the customer's request.*	Sehen Sie geeignete Prozesse für das Rückspielen vor. *Provide appropriate processes for replay.*	☐	☐	
Der Dienstleister ist in der Lage, eine **Inventarisierung** aller für den Auftraggeber relevanten Anwendungen und Systeme zu dokumentieren. *The service provider is able to document an inventory of all applications and systems relevant to the client.*	Eine kundenspezifische CMDB sollte Pflicht sein, wenn Sie IT-Sicherheitsaufgaben für Kunden übernehmen. *A customer-specific CMDB should be mandatory if you perform IT security tasks for customers.*	☐	☐	
Es gibt einen **dokumentierten Prozess**, um Änderungen an Systemen zu erfassen und die Sicherheitsauswirkungen bewerten zu können, bevor die Änderungen durchgeführt werden. *There is a documented process to capture changes to systems and assess the safety impact before the changes are implemented.*	Der Prozess sollte durch Sie definiert, dokumentiert und gesteuert werden. *The process should be defined, documented and controlled by you.*	☐	☐	

Eine Fernwartung geschieht ausschließlich über nach dem Stand der Technik **verschlüsselte Leitungen** mit angemessen starker **Authentifizierung.** *Remote maintenance is performed exclusively via state-of-the-art encrypted lines with appropriately strong authentication.*	Verwenden Sie für verschiedene Kunden niemald identische Passwörter! *Never use identical passwords for different customers!*	☐	☐	

Reaktion
reaction

Der Dienstleister bietet an, Vorkehrungen zu treffen, um **Hacker-Angriffe** auf alle für den Kunden relevanten Systeme zu erkennen. *The service provider offers to take precautions to detect hacker attacks on all systems relevant to the customer.*	Dies kann manuell geschehen (z.B. Logfile-Analyse) oder automatisch (z.B. Einsatz von SIEM-Lösungen). *This can be done manually (e.g. log file analysis) or automatically (e.g. use of SIEM solutions).*	☐	☐	
Sicherheitswarnungen/-meldungen zu allen mit dem Kunden vereinbarten Betriebssystemen, IT-Systemen und Software-Anwendungen werden **beobachtet.** *Security alerts/messages on all operating systems, IT systems and software applications agreed with the customer are monitored.*	Dafür gibt es standartisierte Informationsangebote. Voraussetzung ist in der Regel eine aktuelle CMDB. *There are standardized information offerings for this purpose. The prerequisite is usually an up-to-date CMDB.*	☐	☐	
Sicherheitsvorfälle und -warnungen mit **hoher Kritikalität** werden sofort an den Kunden kommuniziert und es wird unverzüglich (entsprechend der vereinbarten SLAs) in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt. *Security incidents and alerts with high criticality are immediately communicated to the customer and a secure state is immediately restored (according to the agreed SLAs) in coordination with the customer.*	Etablieren Sie einen Notfall-Prozess zur Information der Kunden bei kritischen Vorfällen und Warnungen! *Establish an emergency process to inform customers of critical incidents and warnings!*	☐	☐	

Sicherheitsvorfälle und –warnungen mit **normaler Kritikalität** werden am gleichen Tag an den Kunden kommuniziert und in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt. *Security incidents and alerts with normal criticality are communicated to the customer on the same day and a secure state is restored in coordination with the customer.*	Seien Sie transparent bei der Festlegung der Kriterien für Kritikalität. *Be transparent in setting criteria for criticality.*	☐	☐	
Der Dienstleister bietet **IT-Notfall-Dienstleistungen** an. *The service provider offers emergency IT services.*	Die sollte auch für alle Systeme angeboten werden, für die nicht im SLA benannt *This should also be offered for all systems that are not named in*	☐	☐	

Lieferant
supplier

Der Dienstleister führt bzgl. seines eigenen Geschäftes und seiner Infrastruktur regelmäßig eine **Risikoanalyse** durch und hat geeignete Notfallpläne und **risikosenkende Maßnahmen** im Einsatz. *The service provider regularly conducts a risk analysis of its own business and infrastructure and has appropriate emergency plans and risk-reducing measures in place.*	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden ausrichten. *Your internal processes must be aligned with the protection needs of your customers.*	☐	☐	
Die **Mitarbeiter** des Dienstleisters sind nachweislich angemessen zu Sicherheitsthemen **qualifiziert.** *The service provider's employees are demonstrably appropriately qualified on safety topics.*	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden *Your internal processes must be aligned with the protection needs of your customers.*	☐	☐	

Auch bei Sicherheitsvorfällen ist eine ausreichende personelle Ausstattung mit **nachgewiesener Kompetenz** (z.B. Herstellerzertifikat ISO 27001, TISAX, BSI-Grundschutz oder andere international anerkannte Zertifikate) für alle für den Kunden relevante Systeme gegeben. *Even in the event of security incidents, there is sufficient staffing with proven competence* *(e.g. manufacturer certificate ISO 27001, TISAX, BSI-Grundschutz or other internationally recognized certificates) for all systems relevant to the customer.*	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden ausrichten. *Your internal processes must be aligned with the protection needs of your customers.*	☐	☐	
Der Dienstleister ist GPDR compliant. *The service provider is GPDR compliant.*	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden ausrichten *Your internal processes must be aligned with the protection needs of your customers.*	☐	☐	
Der Dienstleister dokumentiert seine regelmäßigen **Sicherheits-Sensibilisierungen und -Schulungen** bei seinen Mitarbeitern. *The service provider shall document its regular security awareness and training sessions with its employees.*	Die Sensibilisierungen Ihrer Mitarbeiter sollte den Schutzbedarf der Kunden berücksichtigen. *Awareness training for your employees should take into account the protection needs of customers.*	☐	☐	
Auf **Ausscheiden eines Mitarbeiters** des Dienstleisters wird das Benutzerkonto deaktiviert, Passwörter geändert und alle Unterlagen, die den Kunden *In case of thIn the event of the departure of an employee of the Service Provider, the user account will be deactivated, passwords will be changed and all documents concerning the Client will be confiscated.*	Es empfiehlt sich für Dienstleister aus Selbstschutz ein Privileged Access Management einzusetzen. *It is recommended that service providers implement privileged access management for self-protection.*	☐	☐	
Personenbezogene Daten von Mitarbeitern des Kunden werden in die Schadenspotenzialanalyse im Rahmen des **Datenschutzmanagements** des Dienstleisters mit einbezogen. *Personal data of the customer's employees is included in the damage potential analysis as part of the service provider's data protection management.*	Es empfiehlt sich für Dienstleister aus Selbstschutz ein Privileged Access Management einzusetzen. *It is recommended that service providers implement privileged access management for self-protection.*	☐	☐	