Technische und organisatorische Maßnahmen (TOM) der CONCEPTNET GmbH

- Stand 18.03.2018 -

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Externer Datenschutzbeauftragter, Dienstanweisungen, regelmäßige Schulungen, technisch organisatorische Maßnahmen, Notfallpläne
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Christian Volkmer Projekt 29 GmbH & Co. KG Trothengasse 5 93047 Regensburg Tel. 0941-2986930 Fax 0941-2986939 Mail c.volkmer@projekt29.de Web www.projekt29.de
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Bestellung eines externen Datenschutzbeauftragten, Dienstanweisungen, regelmäßige Schulungen, technische Maßnahmen
	Wie stellen Sie sicher, dass die internen Prozesse gemäß den aktuellen Datenschutzbestimmungen ablaufen und wird des regelmäßig geprüft?	Regelmäßige Prüfungen durch den Datenschutzbeauftragten
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Schulungen durch den Datenschutzbeauftragten, Schulungen durch fachlich geeignete eigene Mitarbeiter
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Ja, im Verfahrensverzeichnis
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Schlüssel, Werkschutz, Überwachungseinrichtungen, Alarmanlage
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Festlegung von zutrittsberechtigten Mitarbeitern

Nr.	Gebiet	Beschreibung
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Clients in verschlossenen Räumen, Regelung für Fremdpersonal, Pförtnerdienst, Richtlinie zur Begleitung von Personen in Gebäuden
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Videoüberwachung mit Aufzeichnung, DSB
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerauthentifizierung via Standardprozess (Active Directory und lokale Betriebssysteme)
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Standardprozess (Active Directory und lokale Betriebssysteme)
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Standardprozess (Active Directory und lokale Betriebssysteme)
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Standardprozess (Active Directory und lokale Betriebssysteme), Dienstanweisungen
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Zugang ausschließlich per VPN oder spezielle Anwendungen; Steuerung über Firewall und Server
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Standardprozess (Active Directory und lokale Betriebssysteme)
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Zeichenmix, mind. 8 Zeichen, Passworthistorie
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Standardprozess (Active Directory und lokale Betriebssysteme, Gruppenrichtlinie)
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Zugriffsberechtigungen auf Basis des Betriebssystems, Protokollierung, Dienstanweisungen, Schulungen

Nr.	Gebiet	Beschreibung
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Zugriffsberechtigungen auf Basis des Betriebssystems
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Standardprozess (Active Directory und lokale Betriebssysteme in Verbindung mit Zugriffsberechtigungen auf Basis des Betriebssystems)
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Protokollierung, Dienstanweisung
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Auswertung stichprobenartig und bei Veranlassung
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Getrennte Systeme, Dienstanweisungen
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch regelmäßige Schulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten. Auf die Besonderheiten im Umgang mit pseudonymisierten Daten wurde hingewiesen.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Je nach Anforderung (Verschlüsselung, verschlüsselte Datenleitung, postalisches Einschreiben, etc.)

Nr.	Gebiet	Beschreibung
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Ja, diverse (z. B. VPN, SSL, bilaterale Zertifikate, etc.)
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Nach Anforderung
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Zugriffskontrolle, technisch-organisatorische Maßnahmen
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Protokollierung, Differenzierte Zugriffsberechtigungen
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Protokollierung
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Protokollierung, Differenzierte Zugriffsberechtigungen
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	Protokollierung, Differenzierte Zugriffsberechtigungen
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Kontrolle durch den DSB, Vertragsgestaltung, Vereinbarungen zur Auftragsdatenverarbeitung
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Kontrolle durch den DSB, Vertragsgestaltung, Vereinbarungen zur Auftragsdatenverarbeitung
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Entsprechende Aufbewahrungseinrichtungen und -orte

Nr.	Gebiet	Beschreibung
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Firewalls, Virenscanner, Filter, Verschlüsselungsprogramme, getrennte Systeme; Regelmäßige und größtenteils automatisierte Aktualisierungen
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Datenschutz- und datensicherheitsgerechte Vernichtung von von elektron. Datenträgern
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Backups, Ersatzsysteme, Notfallpläne, Verfügbarkeit eines Ersatzstandortes
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems (Basis OTRS) zweistufig (1st und 2nd Level); zusätzlich Telefonhotline und automatisierte Überwachung und Alarmierung (Nagios)
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.