Sicherheitskonzept kidit.ch

KiDiT ist eine webbasierte Applikation und als Extension innerhalb einer TYPO3-Umgebung realisiert. Mit dem Benutzeraccount verknüpfte personenbezogene Daten sind über TYPO3 nicht zugänglich. Es sind keine Third-party Extensions installiert.

Zugangskontrolle	
Welche Maßnahmen werden ergriffen, um zu gewährleisten, dass nur befugte Personen Zutritt zu den Datenverarbeitungsanlagen erhalten (z.B. Schließsysteme, speziell abgesicherte Räume, organisatorische Regelungen für den Umgang mit Besuchern)?	• Der Webserver steht in einem TÜV geprüften Rechenzentrum der Hetzner AG. • Details zu den einzelnen Massnahmen können unter http://www.hetzner.de/hosting/unternehmen/rechenzentrum (vgl. Sicherheit) eingesehen werden.
Zutrittskontrolle	
Welche Maßnahmen werden ergriffen, um zu gewährleisten, dass nur befugte Personen Datenverarbeitungssysteme nutzen können (z.B. Nutzerkonten, Passwortrichtlinie (komplexe Passwörter, kontinuierliche Passwortänderungen etc.))?	• Zutritt ist nur mit persönlichem Login möglich, Sessions laufen bei Inaktivität automatisch ab • Passwortrichtlinie: 6-stellige Passwörter • Serverzugriff ist nur über SSH mittels eines private Keys seitens der Future Connection AG möglich
Zugriffskontrolle	
Welche Maßnahmen werden ergriffen, um zu gewährleisten, dass Personen nur Informationen bearbeiten können, für deren Bearbeitung sie tatsächlich auch berechtigt sind (z.B. Abgrenzung Administratoren, Berechtigungskonzept der Anwendung, Abgrenzung zwischen den verschiedenen Systemnutzern/Kunden))?	• Benutzer können nur jeweils auf die eigenen Daten zugreifen (Berechtigungsstufe Kunden) • TYPO3-Administratoren können nicht auf personenbezogene Daten zugreifen • Die Zugangsberechtigung wird mittels TYPO3 ermittelt • Alle Aufrufe innerhalb der KiDiT Applikation benötigen einen gültig eingeloggten TYPO3 Benutzer (*fe_user*)
Weitergabekontrolle	
Welche Maßnahmen werden ergriffen, um zu gewährleisten, dass personenbezogene Daten während ihres Transportes oder ihrer Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können (z.B. Virenschutz, Firewall, Verschlüsselung, kontinuierliche Systemaktualisierungen (Patchmanagement))?	• Als Betriebssystem wird Ubuntu LTS 12.04 eingesetzt • Systemaktualisierungen (security updates) auf Server- und TYPO3-Ebene werden automatisch geprüft und bei Bedarf installiert • Zugriff auf KiDiT erfolgt über eine SSL-verschlüsselte Verbindung
Eingabekontrolle	
Welche Maßnahmen werden ergriffen, um zu prüfen, ob und durch wen personenbezogene Daten eingegeben, verändert und entfernt worden sind (z.B. Protokollierungsmaßnahmen (Webserver, Datenbanksystem etc.))?	• Logfiles auf dem Webserver • Timestamp-Updates in entsprechenden Datenbank-Tabellen • TYPO3 Log-Einträge
Auftragskontrolle	

Wie wird sichergestellt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, entsprechend der Weisung des Auftraggebers verarbeitet werden (z.B. Vertragsgestaltung mit Hosting-Partner, Entwicklungsfirma sowie andere Unterauftragnehmer)	• Geheimhaltungsvereinbarung mit Future Connection, keine weiteren Unterauftragnehmer
Verfügbarkeitskontrolle	
Wie wird sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung und Verlust geschützt sind (z.B. Datensicherungskonzept).	• Daten sind auf einem RAID abgelegt • Es werden zeitlich gestaffelte Snapshots auf dem Server erstellt
Kontrolle der Zwecktrennung	
Wie wird sichergestellt, dass die zu unterschiedlichen Zwecken erhobenen Daten, auch getrennt voneinander verwendet werden können (z.B. Abgrenzung zwischen Administration und Kundenfunktionen, Abgrenzung zwischen dem Datenbestand mehrerer Kunden, Vermeidung Datennutzung für andere Zwecke (z.B. Werbung)).	• Benutzerverwaltung und Speicherung der personenbezogenen Daten erfolgt getrennt • Innerhalb der Berechtigungsstufe 'Kunden' gibt es keine Hierarchie
Eingabevalidierung	
Wie überprüft das System Benutzereingaben bzw. welche Schutzmaßnahmen werden bezüglich XSS-Attacken angewandt?	• Applikatorische Werte werden gegenüber einer Whitelist geprüft • Apache filtert mittels des *mod_security* Modules
Datenbankoperationen	
Welche Maßnahmen werden getroffen, um SQL Injection-Attacken vorzubeugen?	• Datenbank Abfragen verwenden den Abstraktions-Layer von TYPO3
Angriffe und Manipulation	
Wie wird auf Angriffe des Systems von außen reagiert? Gab es bereits derartige Angriffe und wenn ja, wurden in diesem Zusammenhang personenbezogene Daten entwendet?	• SSH Login Versuche werden überwacht, nach 3 fehlgeschlagenen Versuchen wird ein Login dieser IP mittels IP-Tables für 30min unterbunden • Apache DDoS Attacken werden mittels *Varnish* ab gewehrt • Es gab bisher keine erfolgreichen Angriffe

Bei Fragen wenden Sie sich bitte an Future Connection AG, Kilian Hann, Merkurstrasse 51, 8032 Zürich, Schweiz, khann@fconnection.com, +41 44 265 30 92