TECHNISCHE UND ORGANISATORISCHE STANDARDMAßNAHMEN ZUM SCHUTZ VON DATEN GEMÄß DSGVO

der **Elements-Gruppe**, dazu gehören die **elements.at New Media Solutions GmbH**, die **Punkt & Komma GmbH** und die **Pimcore GmbH**, im Folgenden alle kurz ELEMENTS genannt.

Alle technisch-organisatorischen Maßnahmen werden kontinuierlich auf Aktualität und Stand der Technik evaluiert und aktualisiert.

1. Interne Verarbeitungstätigkeiten

- Zutrittskontrolle
  Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, in jedem Fall durch Schlüssel oder elektrische Türöffner (Transponder) und Alarmanlagen. Die Serverräume, Netzverteiler und TK-Anlagen befinden sich in einem Sperrbereich mit eingeschränktem Zugang und werden ausschließlich von ELEMENTS genutzt. Zusätzliche Schutzeinrichtungen: Generalschlüsselanlage; Schlüsselregelung; Kundenabfertigung; Zutrittskontrollsystem; Anwesenheitskontrolle / Zeiterfassungssystem angeschlossen; Protokollierung; Kontrolle von Remote-/Heimarbeitern; Kontrolle von Reinigungs- und Wartungsarbeiten
- Zugangskontrolle
  Schutz vor unbefugter Systembenutzung durch Benutzerkennung und Passwortverfahren mit aktuellen Standards entsprechender und validierter Policy (Zeichenzusammensetzung, Länge, regelmäßiger Wechsel, Passworthistorie) oder durch aktuellen Sicherheitsstandards entsprechenden Public-Keys (SSH-Zugänge). Weitere Maßnahmen: Zwei-Faktor-Authentifizierung bei administrativen Benutzerkonten; Bildschirmsperre bei Pausen mit Passwort-Aktivierung; Erstanmeldeprozedur; geregelte und gesicherte Aufbewahrung von Administrator-Passwörtern; Single-Sign-On; nur personalisierte Zugangskennungen; Protokollierung des Zugangs; zwingende Verschlüsselung von mobilen Datenträgern; Direktanbindung Internet-Serviceprovider (Glasfaser); Zugriffsberechtigungskonzepte; Hardware-Firewalls; Laufende manuelle/teilw. automatisierte und zentrale Installation von Updates und Sicherheitspatches; zentrale Verwaltung der Konfigurationen; hauptamtliche Systemadministratoren; Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren; getrennte Benutzerkonten für Systemadministratoren; Anwendung des 4-Augen-Prinzips bei kritischen Systemänderungen; Protokollierung der Administrationsarbeit
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Systeme. Es gibt Standard-Berechtigungsprofile auf „need to know-Basis“, einen Standardprozess für Berechtigungsvergabe, periodische Überprüfung der vergebenen Berechtigungen. Administrative Benutzerkonten sind auf den kleinstmöglichen Kreis an Administratoren begrenzt und werden mit besonderer Sorgfalt regelmäßig geprüft.
  Weitere Maßnahmen: Berechtigungskonzepte für Daten, Anwendungen und Betriebssysteme; Protokollierung von Dateizugriffen, Programmausführungen und Richtlinienverstößen; Aufbewahrung der Protokolle für einen angemessenen Zeitraum; Synchronisierung der Uhren zur Auswertung von Protokollen; Keine Administrationsrechte für Nutzer auf Endgeräten; Prozesse zur Erlangung / Veränderung von Berechtigungen (Neuanlage, Aufgabenänderung, Austritt); Regelmäßige Überprüfung, ob vergebene Berechtigungen noch notwendig sind; Berechtigungen gehören wenn immer möglich nicht zu Personen sondern zu Rollen; Datenträgerverwaltung; Zugriffsschutz durch automatische oder über Funktionstasten ausgelöste Bildschirmsperre mit ausschließlicher passwortgestützter oder biometrischer Verfahren verifizierter Aufhebung; Regelungen und Kontrolle von externer Wartung und Fernwartung; nur unternehmenseigene Geräte dürfen mit dem internen Netzwerk verbunden werden; Offene oder nicht ausschließlich intern verwendete WLAN-Segmente sind mit einer Firewall vom internen Netz getrennt; die Kommunikation in drahtlosen Netzen erfolgt verschlüsselt; Mobile Endgeräte sind verschlüsselt; Bei Internet-Anwendungen werden Anmeldedaten ausschließlich verschlüsselt übertragen; öffentlich zugängliche IT Systeme befinden sich in einem abgeschotteten DMZ;

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung und Transport ausschließlich über verschlüsselte Verbindungen (z.B. HTTPS, SFTP, VPN). Weitere Maßnahmen: Festplattenverschlüsselung bei mobilen Endgeräten; Protokollierung der Übermittlung; Regelungen für Remotearbeiter und Fernwartung (Software, Zugriffsrechte, Zugriffsweg, Freischaltung / Freigabeverfahren, Verschlüsselung, Zugangskontrolle, Monitoring & Protokollierung);
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch entsprechende Protokollierung.
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch formalisierte Auftragserteilung oder gesonderter Vereinbarung. Kontrolliert und dokumentiert werden in jedem Fall: Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen. Alle Mitarbeiter und Sub-Auftragnehmer sind zur Vertraulichkeit verpflichtet.
- Verfügbarkeitskontrolle
  Brandschutzeinrichtungen (Rauch- oder Brandmelder); Feuerlöscher im Serverraum und in den Arbeitsräumen; Rauchverbot in Server- und PC-Arbeiträumen; USV und Überspannungsschutz für kritische IT-Infrastruktur; Redundante Klimaversorgung im Serverraum; firmenweites Datensicherungskonzept für alle relevanten IT-Komponenten (Speicher-/Löschfristen, standortunabhängige Replikation, manuelle und automatische Integrationskontrolle, rasche Wiederherstellbarkeit); zentrale Festplattensysteme mit Reservekapazitäten (RAID); zentral verwaltete und automatisch aktualisierte Virenschutz / Schutz vor Schadsoftware; Spamfilter; zentrale IDS und IPS Systeme; Notfallpläne für unterschiedliche Szenarien

2. Webserver

Sofern die Einrichtung des Webservers ausschließlich durch ELEMENTS erfolgt werden initial die folgenden Maßnahmen ergriffen: Zugriff nur durch berechtigtes und geschultes Personal (Rollenkonzept); Software-Firewall (nur unbedingt notwendige Ports werden geöffnet); Shell-/Administrationszugang nur für eingeschränkten IP Bereich und Personenkreis(Systemadministratoren); Protokollierung der Zugriffe (7 Tage Speicherdauer); Serverbetrieb ausschließlich für die beauftragte Software; Datenübertragung ausschließlich über verschlüsselte Verbindungen;

Auf ausdrücklichen Wunsch des Auftragsgebers können auftragsbedingt oder anlassbezogen Änderungen an den Maßnahmen notwendig sein. Es erfolgt keine laufende Wartung der einmalig eingerichteten Maßnahmen, sofern dies nicht gesondert vertraglich geregelt ist (Wartungsvertrag).

3. Web-Applikationen

Die durch ELEMENTS erstellten Web-Applikationen werden an den Auftraggeber mit folgenden Schutzmaßnahmen initial übergeben (bei Erstellung der Applikation): Standard-Berechtigungskonzept auf Rollenbasis, passwortauthentifizierte Benutzeraccounts, personalisierte Benutzeraccounts für alle ELEMENTS-Mitarbeiter inkl. SSO-Login, Werkzeug zur Kontrolle der Zugriffsrechte, Schutz gegen Brute-Force Attacken, Standardmechanismen zum Schutz vor ungewollten Zugriff

4. Online-Kampagnen, Targeted Advertising, Newsletter / E-Mail Direktmarketing

Die Übermittlung von personenbezogenen Daten vom Auftraggeber zu ELEMENTS darf nur über verschlüsselte Übertragungsarten stattfinden. Die Daten werden bei ELEMENTS nach Abschluss des Auftrags gelöscht. Der Auftraggeber wird über die Weitergabe an zertifizierte Subauftragsverarbeiter in jedem Fall in Kenntnis gesetzt.