SLW Altötting

Technische und organisatorische Maßnahme zur Einhaltung des Datenschutzes (gemäß §6 KDO)

für die Einrichtung **……..**

1. Zutrittskontrolle

2. Zugangskontrolle

3. Zugriffskontrolle

4. Weitergabekontrolle

5. Eingabekontrolle

6. Auftragskontrolle

7. Verfügbarkeitskontrolle

8. Trennungskontrolle

1. Zutrittskontrolle

Technische und organisatorische Maßnahmen, um Unbefugten in räumlicher Hinsicht den Zugang zu verwehren

- Der Zugang zur Einrichtung während der Öffnungszeiten muss beschränkt und entsprechend kontrolliert sein, z.B. durch Pforte oder Verwaltung bzw. darf kein ungehinderter / unbeaufsichtigter Zugang für Dritte außerhalb von Wartebereichen bestehen.
  ……
- Der Zugang zu Zimmern, in denen sich schützenswerte Daten befinden, muss kontrolliert sein, z.B. durch Vorzimmer. Die Zimmer müssen auch bei kurzzeitigem Verlassen verschlossen werden.
  ……
- Schützenswerte Daten dürfen nicht für Dritte einsehbar ausgehängt werden, z.B. keine Listen mit Klientendaten wie Namen und Arztterminen außerhalb der Räume, die ausschließlich diesen als Wohnraum zugeordnet werden.
  ……
- Der Zugang von Gästen muss geregelt sein.
  ……
- Archive müssen in gesonderten, stabilen und verschlossenen Räumlichkeiten (Schränken) untergebracht sein.
  ……
- Server müssen in abschließbaren Serverschränken, mindestens aber in gesonderten nur für berechtigtes Personal zugänglichen Räumen untergebracht sein.
  ……
- Datenträger und Akten müssen unter Verschluss bzw. in abschließbaren Räumen verwahrt sein.
  ……
- Notebooks, USB-Sticks und Tablets müssen unter Verschluss sein.
  ……
- Datensicherungen müssen in zutrittsgesicherten Safes lagern.
  ……
- Die Ausgabe von Schlüsseln muss geregelt und dokumentiert sein.
  ……
- Für Fremdpersonal (Reinigung, Lieferanten, externe EDV-Diensleister u.a). müssen Regelungen erstellt sein.
  ……

2. Zugangskontrolle

Nur Befugte haben Zugang in das EDV-System bzw. zu Datenträgern

- Aufbewahrungsorte für Datenträger (Akten, USB-Sticks, Notebooks etc.) müssen festgelegt sein.
  ……
- Der zugangsberechtigte Personenkreis zu diesen Datenträgern muss festgelegt sein.
  ……
- Ein Verfahren zur ordnungsgemäßen Verwaltung der Datenträger (Kennzeichnung, Bestandsführung, Rückgabekontrolle, Aufbewahrungsfristen,…) muss vorhanden sein.
  ……
- Unbefugte müssen bei Zugriff auf die EDV automatisch abgewiesen werden.
  ……
- Datenträger müssen datenschutzrechtlich sachgerecht vernichtet werden.
  ……
- Bei der Wiederverwendung von Aktenordnern müssen alle auch auf dem Aktenordner befindlichen Daten entfernt werden (z.B. Aktenrückenschilder).
  ……
- Es muss eine Firewall vorhanden sein.
  ……
- Daten auf mobilen Datenträgern (USB-Sticks,…) müssen verschlüsselt sein.
  ……
- Persönliche Daten dürfen nicht per E-Mail versandt werden.
  ……
- Die Installation / Nutzung von Whatsapp u.ä. Anwendungen ist nicht erlaubt.
  ……
- Das Verfahren zu Passwörtern muss geregelt sein
  (Buchstaben und Ziffern, mind. 8 Zeichen, regelmäßiger Wechsel, Dokumentation der Passworthistorie, keine Gruppenpasswörter bei Zugang zu persönlichen Daten, verbindliche Bildschirmsperre bei Pausen bzw. Verlassen des Arbeitsplatzes, Verfahren zur Passwortrücksetzung und Aufbewahrung des Admin-Passworts).
  ……
- Es muss ein verbindliches Verfahren zur Vergabe von Berechtigungen geben.
  ……

3. Zugriffskontrolle

Verhinderung von Tätigkeiten außerhalb der jeweils eingeräumten Berechtigung

- Es müssen in allen IT-Systemen Berechtigungen festgelegt sein.
  ……
- Die Berechtigungen müssen differenziert sein, wer welche Daten lesen, ändern, löschen darf.
  ……
- Die Berechtigungen für den Zugriff auf Daten, Anwendungen und Betriebssystem müssen differenziert sein.
  ……
- Die organisatorische Bewilligung der Berechtigung soll von der techn. Vergabe der Berechtigung getrennt sein.
  ……
- Es muss geregelt sein, wer wann auf wessen Anforderung Daten aus einem Backup einspielen darf.
  ……
- Die Programm- und Dateibenutzung muss so protokolliert werden, dass sie im Bedarfsfall ausgewertet werden kann.
  ……
- Es muss geregelt sein, wer wann in welchen Akten Eintragungen vornehmen oder Bestandteile von Akten herausgeben darf.
  ……
- Es muss geregelt sein, dass jeder Eintrag in einer Akte mit Datum und Handzeichen zu versehen ist.
  ……
- Die Zuordnung des Handzeichens zur konkreten Person muss dokumentiert sein.
  ……
- Die Mitarbeiter müssen angehalten sein, auf mehreren Personen zugänglichen Kopierern / Druckern / Faxgeräten keine Unterlagen mit schützenswerten Daten liegen zu lassen.
  ……
- Kopierer / Drucker / Faxgeräte müssen so aufgestellt sein, dass Externen der unbeaufsichtigte Zugang nicht möglich ist.
  ……

4. Weitergabekontrolle

Die technische / organisatorische Sicherstellung des Datenschutzes bei der Weitergabe von Daten

- Es muss geregelt sein, welche Akten / Datenträger auf welchem Weg übermittelt werden dürfen, z.B. welche Datenträger / Akten nur durch persönlich bekannten Boten oder Aufgabe zur Post.
  ……
- Datenträger/ Akten dürfen nur auf sicherem Weg transportiert werden (Zuverlässigkeit des Postdienstes, Boten…).
  ……
- Klientenakten dürfen bei Aufgabe zur Post nur per Einschreiben mit Rückschein versandt werden.
  ……
- E-Mails mit geschützten Daten dürfen nur verschlüsselt versandt werden.
  ……
- Bei einer Übertragung von persönlichen Daten per EDV muss die Verbindung auf dem jeweils aktuellsten technischen Stand verschlüsselt sein.
  ……
- Beim Versand von Akten / Datenträgern muss mit dem Empfänger eine Rückmeldung vereinbart sein, dass die Daten / Akten vollständig eingegangen sind.
  ……
- Es muss dokumentiert sein, wann genau die Datenträger / Akten versandt wurden.
  ……
- Es muss festgelegt sein, wer berechtigt ist, über die Weitergabe / Versendung von Daten / Akten zu entscheiden.
  ……
- Die Weitergabe / Versendung von Akten / Datenträgern dürfen nur Berechtigte veranlassen.
  ……

5. Eingabekontrolle

Die Datenpflege muss dokumentiert und damit nachvollziehbar sein.

- Es müssen Benutzerberechtigungen festgelegt sein.
  ……
- Die Berechtigungen müssen differenziert sein (wer hat Zugriff auf welche Daten bzw. Teile von Daten / wer darf was lesen, ändern, löschen).
  ……
- Es muss protokolliert werden, wer was wann eingegeben / verändert / gelöscht hat (maschinell bei Eingaben in der EDV, manuell mit Datum und Handzeichen bei Akten).
  ……
- Es muss eine Protokollierung von Administratorentätigkeiten erfolgen (wer hat wann welchen Benutzer festgelegt oder Benutzerrechte geändert / gelöscht).
  ……
- Es müssen Aufbewahrungs-/Löschfristen festgelegt sein.
  ……
- Passwortrücksetzungen müssen archiviert werden.
  ……
- Alle Mitarbeiter, insbesondere Verwaltungskräfte / Pfortenpersonal sind angewiesen, Notizen an die Mitarbeiter mit Datum und Handzeichen zu versehen.
  ……

6. Auftragskontrolle

Sicherstellung des Datenschutzes, wenn Dritte mit der Verarbeitung von geschützten Daten beauftragt werden

- Der Auftraggeber muss sicherstellen, dass seine Weisungen vom Auftragnehmer zweifelsfrei, uneingeschränkt und präzise eingehalten und umgesetzt werden.
  ……
- Es müssen technische und organisatorische Maßnahmen ergriffen werden, welche die lückenlose Einhaltung des Weisungsprinzips in der Praxis gewährleisten.
  ……
- Der Auftragnehmer darf die Daten nicht duplizieren, verändern oder außerhalb des Auftragsrahmens übermitteln.
  ……
- Es müssen Anweisungen erfolgt oder Verträge vereinbart sein, in denen sich der Auftragsnehmer verpflichtet hat, die Datenschutzbestimmungen zu beachten.
  ……

7. Verfügbarkeitskontrolle

Daten / Akten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Es dürfen keine Räume für Archive genutzt werden, die wasser- und / oder Schimmelbefall-gefährdet sind.

  ……

- Die Mitarbeiter sind angehalten, Akten / Daten nur im von der Leitung genehmigten Ausnahmefall mit nachhause zu nehmen.

  ……

- Es ist ein Backup- und Recoverkonzept mit täglicher Sicherung von EDV-Daten vorhanden.

  ……

- Redundante Serversysteme müssen vorhanden sein.

  ……

- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung müssen vorhanden sein.

  ……

- Datenträger / Archive sind katastrophensicher (Wasser, Feuer,…) aufzubewahren.

  ……

- Es ist Sicherheitssoftware einzusetzen:
  - Virenscanner
  - Firewall
  - Spam-Filter
  - Verschlüsselungsprogramme zur Versendung persönlicher Daten per EDV

  ……

8. Trennungskontrolle (Zweckbindung)

Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen auch getrennt verarbeitet werden.

- Mitarbeiter- und Klientendaten werden auf physikalisch getrennten Systemen verarbeitet.
  ……
- Klientendaten werden in nach dem jeweiligen Klienten getrennten Ordnern erfasst, insbes. auch bei Geschwistern. Die das Geschwisterkind betreffenden Informationen werden unkenntlich gemacht (geschwärzt / gelöscht).
  ……
- Soweit in einer Einrichtung gleichzeitig medizinische und / oder therapeutische Leistungen erbracht werden, müssen die dazugehörigen Daten getrennt von den Daten der anderen Leistungseinheiten (z.B. stationäre Jugendhilfe) erfasst werden.
  ……
- Bei der Weitergabe von Daten an den Kostenträger ist sichergestellt, dass der Kostenträger keine Daten erhält, die nicht erforderlich sind (z.B. Ausschneiden von Spalten in Excel-Tabellen, die für den Kostenträger nicht erforderlich sind).
  ……

Besprochen am …….

……. …….

(Einrichtungsleitung) (Datenschutzbeauftragter)