PDS-Merkblatt: DSGVO – Technische und Organisatorische Maßnahmen
Stand: 19. April 2018 – V1.3

Die Datenschutz-Grundverordnung (DSGVO) verlangt technische und organisatorische Maßnahmen zum Datenschutz auf dem Stand der Technik.
Die folgenden Anleitungen sollen Ihnen helfen, Ihr EDV-System diesem Stand anzupassen.

1. Mitarbeitervereinbarungen

Über Mitarbeitervereinbarungen werden Maßnahmen geregelt, welche technisch gar nicht oder nur unter zu großem Aufwand realisierbar wären.

- Verschwiegenheitsverpflichtung
  Sie sollten von jedem Mitarbeiter eine schriftliche Verschwiegenheitserklärung unterfertigen lassen und in Ihrer DSGVO-Mappe vorhalten
- Verbot der Internetnutzung
  (ausgenommen explizit vereinbarter Web-Sites)
- Verbot der lokalen Datenablage an den Arbeitsplätzen
  (Ablage z.B. nur unter P:\Dokumente)
- Verbot der Nutzung von Datenträgern
  (zB. USB-Stick)

2. Arbeitsplatzrechner

2.1 Bildschirmsperre

Der Datenzugriff auf einen nicht besetzen Arbeitsplatz muss durch eine Bildschirmsperre nach maximal 10 Minuten verhindert werden. Zur Reaktivierung muss ein Kennwort eingegeben werden. So stellen Sie diese Funktion ein:

Windows 10
- Klicken Sie unten links auf das Windows- und anschließend das Zahnrad-Symbol
- Wählen Sie die Kategorie "Personalisierung"
- Wechseln Sie links in den Abschnitt "Sperrbildschirm".
- Klicken Sie nun die Option "Einstellungen für Bildschirmschoner"
- Wählen Sie unter „Bildschirmschoner" „Mystify"
- Stellen Sie "Wartezeit" auf 10 Minuten
- Aktivieren Sie das Häkchen bei „Anmeldung bei der Reaktivierung"
- Abschließend speichern Sie Ihre Einstellungen über "OK".

Windows 7
- Klicken Sie unten links auf das Windows-Symbol
- Wählen Sie „Systemsteuerung"
- Wählen oben rechts unter „Anzeige:" „kleine Symbole"
- Wählen Sie „Anpassung "
- Klicken Sie unten rechts „Bildschirmschoner"
- Wählen Sie unter Bildschirmschoner „Mystify"
- Stellen Sie "Wartezeit" auf 10 Minuten
- Aktivieren Sie das Häkchen "Anmeldeseite bei Reaktivierung"
- Abschließend speichern Sie Ihre Einstellungen über "OK".

2.2 Mikrofone und Kameras deaktivieren

Mikrofone und Kameras gibt es bei Notebooks und All-In-One-Rechner
- Kamera und Mikrofon mit einem Pickerl abkleben

2.3 Windows Updates aktivieren

Bitte führen Sie diese Einstellung nur an einem Rechner pro Tag aus.
Ihre Internetverbindung wird ansonst stark belastet!
So erfolgt die Aktivierung der Windows-Updates:

Windows 10
- Unter Windows 10 sind die Updates automatisch aktiv.
- Es sind aktuell keine Einstellungen erforderlich

Windows 7
- Klicken Sie unten links auf das Windows-Symbol
- Wählen Sie „Systemsteuerung"
- Wählen oben rechts unter „Anzeige:" „kleine Symbole"
- Wählen Sie "Windows Update "
- Wählen Sie links oben "Einstellungen ändern"
- Wählen Sie in der Auswahlbox "Automatisch installieren (empfohlen)

***Vorsicht**: Bitte führen Sie diese Einstellung nur an einem Rechner pro Woche aus. Ihre Internetverbindung wird ansonst stark belastet!*

***Vorsicht**: Das Einspielen von Windows-Updates kann zur zeitweisen Funktionsunfähigkeit Ihres PCs führen. Spezielle Treiber oder spezielle angeschlossene Geräte könnten beim Windows-Update zu Problemen führen. Aus diesem Grund wurden in der Vergangenheit die Windows-Updates nicht automatisch aktiviert. Diese empfohlene Maßnahme müssen Sie daher in eigenem Ermessen durchführen.*

2.4 Virenschutz periodisch kontrollieren

Computer mit Verbindung zum Internet müssen über einen Virenschutz verfügen.

Windows 10
- Unter Windows 10 ist der Virenschutz „Defender" automatisch aktiv.
- Es sind aktuell keine Einstellungen erforderlich

Windows 7
- Unter Windows 7 kann der Virenscanner „MS Essentials" verwendet werden
- Prüfen Sie, ob Sie in der Taskleiste das Symbol „Haus mit Fahne am Dach" sehen
- Dieses Symbol sollte grün sein.
- Sollte dieses Symbol nicht vorhanden sein, nehmen Sie bitte mit uns Kontakt auf.

3. Hauptrechner

3.1 Schutz gegen Diebstahl sicherstellen

Ihr Hauptrechner muss mit einer Sicherung gegen Diebstahl ausgestattet sein. Wenn Sie einen eigenen EDV-Raum oder einen Standard-19" - EDV-Schrank haben, dann versperren Sie diese.

Sollten Sie keine sperrbare Aufbewahrung haben, so müssen Sie den Server mit einer Kabelsicherung ausstatten. Diese Sicherung wird auch als „Kensington-Lock" bezeichnet. Die erforderlichen Stahlseile und Wandanker können Sie über uns beziehen. Siehe Bestellformular am Ende des Dokumentes.
Die Montage bitte durch Ihren Elektriker oder Tischler durchführen lassen.

3.2 Sicherungsdatenträger

Sicherungsdatenträger, welche außerhalb der Ordination bewegt werden, müssen verschlüsselt werden. Sollte ein Sicherungsdatenträger ohne Verschlüsselung verloren gehen, so könnte der Finder unter Umständen auf die Daten zugreifen.

Die Verschlüsselung erfolgt automatisch beim Erstellen der Tagessicherung.

Bitte vereinbaren Sie mit uns einen Termin zur Aktivierung der Verschlüsselung. Da hierbei alle Datenträger neu formatiert werden müssen, benötigen Sie zu diesem Termin alle Sicherungsdatenträger vor Ort. Zur Installation des Verschlüsselungsprogrammes benötigen wir einen Tag Vorlauf, da der Server neu gestartet werden muss.

4. Ausfüllhinweise

Nachfolgend finden Sie Vorschläge zur Beantwortung bestimmter Fragestellungen in Bezug auf den Prototypen „DOKUMENTATIONSPFLICHTEN DATENSCHUTZ-GRUNDVERORDNUNG" der Ärztekammer.

III. Technische und organisatorische Maßnahmen

1.1.1. Bildschirmsperre
>> siehe Tätigkeiten unter Punkt 2.1

1.1.4. Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern
…
Folgende technische Maßnahmen werden je Arbeitsplatzrechner ergriffen:
- Zugangssicherung mit Kennwort
- Kamera und Mikrofon sind verschlossen
- Windows Updates werden periodisch eingespielt
- Virenscanner ist aktiv

1.1.5. Datensicherung der Clients:
…
Die Rechner werden wie folgt gesichert:
Auf den Clients werden keine Daten abgelegt. Eine Sicherung ist daher nicht erforderlich.

2.1.5. Softwaresicherheitsmaßnahmen:
…
Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist, wobei Passwörter folgende Kriterien erfüllen müssen (Passwortrichtlinie):
Das Kennwort für den Zugang zum Endgerät entspricht folgenden Kriterien: Buchstaben, Ziffern, Sonderzeichen

Der Verantwortliche stellt sicher, dass Backups der Datenbestände in folgenden Abständen erstellt werden:
Tägliche Sicherung

2.1.6. Sicherung von Telekommunikationseinrichtungen:
Zugangssicherung mit Kennwort

2.2.2 Dokumentation der technischen Infrastruktur:
Die Dokumentation des installierten EDV-Systems befindet sich bei Fa. Lobmaier Datentechnik GmbH.

4.2. Behandlung von Sicherheitsvorfällen:
- Dokumentation Zeitpunkt, betroffene Daten, beteiligte Personen
- Meldung an die Datenschutzbehörde

5. Bestellung Diebstahlsicherung für Server

Bestellung

Ordination: _____

Wir bestellen folgende Artikel:

Stk.	Benennung	Preis exkl. USt.
1	Diebstahlsicherung für Server Stahlkabelsicherung inkl. Wandanker Zur Montage Elektriker bzw. Tischler beauftragen!  *Wird durch Fa. Lobmaier ausgefüllt:* ☐ Servermodell Fujitsu TX100, TX1310 (KensLock) ☐ Servermodell Fujitsu TX120, TX1320 (Öse) ☐ Servermodell HP NL40/52 (KensLock) ☐ Servermodell HP Gen 8 (KensLock) ☐ Sondermodell: _____	€ 78,00
1	Versand	€ 8,00

_____ _____

Datum: Unterschrift:

Bitte per Fax an Fa. Lobmaier senden (07754 7003 18)