Hinweise zum Datenschutz für die tägliche Arbeit

Allgemeines:

Mit der von Ihnen unterzeichneten **Schweigepflichterklärung** haben Sie sich verpflichtet, Daten, die im Dienst bekannt werden, nicht an Dritte weiterzugeben. Mit Daten sind hierbei personenbezogene Daten (also mit Bezug zu einer natürlichen Person) oder interne Daten (z.B. Geschäftsgeheimnisse, interne Abläufe) gemeint. Über diese Daten darf auch nicht mit engen Freunden / Partnern / Familie gesprochen werden.

Selbst **Kolleg*innen,** die ja ebenfalls eine solche Schweigepflichterklärung unterzeichnet haben, gelten **als „Dritte"!**
Es gilt der Grundsatz, dass jede/r nur auf die Daten Zugriff haben soll, die er / sie für seine tägliche Arbeit benötigt, aber eben auch nicht mehr!

Bei einem **Verstoß** gegen diese Vorschriften können arbeitsrechtliche oder sogar strafrechtliche Konsequenzen drohen.

Sie dürfen nur die personenbezogenen Daten verarbeiten (also erheben, speichern, nutzen), die Sie für Ihr Aufgabengebiet benötigen. Nicht mehr benötigte Daten müssen regelmäßig gelöscht werden.

Informationsquellen:

Informieren Sie sich bitte an Ihrer Dienststelle über vorhandene Regelungen zum Datenschutz und zur Nutzung der IT / PCs (z.B. Dienstanweisungen).

Im Büro:

- Beim **Verlassen** das Büro verschließen.
- **Schlüssel** (Bürotür, Schränke u. Schreibtischschubladen) sicher verwahren. **Keineswegs** jedoch in der „Standard-Ablage" f. Schlüssel (obere, flache Schublade des Bürocontainers)!
- **Unterlagen** mit personenbezogenem Inhalt bei Abwesenheit unter Verschluss halten (z.B. in einem abschließbaren Aktenschrank / Bürocontainer).
- darauf achten, dass bei **Gesprächen** keine vertraulichen Informationen von anderen mitgehört werden können, z.B. bei Telefonaten im Beisein v. BürgerInnen.
- **Papiergut** mit personenbezogenen Inhalten datenschutzgerecht entsorgen, z.B. in dafür bereitgestellte, datenschutzgerechte Tonnen oder im Papierschredder.
  Insbesondere am Kopierer darauf achten, dass Fehlkopien ebenso entsorgt werden (und nicht z.B. im offenen Papierkorb neben dem Kopierer).

- Dokumente aus **Druckern** nach dem Ausdruck entfernen, der Druckvorgang darf bei Druckern / Kopierern auf dem Gang erst nach Authentifizierung am Gerät (PIN, Karte) starten.
- sicherstellen, dass sich **Besucher** nur im Beisein eines Mitarbeiters im Büro aufhalten.
- personenbezogenen Daten dürfen nicht außerhalb der dienstlichen Räumlichkeiten verarbeitet werden. Somit dürfen keine entsprechenden Unterlagen mit nach Hause genommen oder per E-Mail zugesandt werden. Ist dies unumgänglich, sind geeignete Sicherheitsmaßnahmen abzuklären, z.B. für Tele- bzw. **Heimarbeitsplätze**.

PC:

- den Monitor so positionieren, dass Unbefugte (z.B. Besucher*innen) keinen Einblick darauf haben.
- Beim **Verlassen** des Arbeitsplatzes den PC sperren (Bildschirmsperre, z.B. mittels Windows-Taste + L) bzw. bei längerer Abwesenheit abmelden.
- Das **Passwort** ist sorgfältig auszuwählen und darf nicht aufgeschrieben werden (nicht unter die Tastatur legen!).
  Das Passwort geheim halten und auch nicht Kolleg*innen für eine Vertretung geben.
  Ein zugeteiltes Kennwort umgehend in ein persönliches Passwort ändern.
- keinem Unbefugten **Zugang** zu dem PC und den Fachanwendungen gewähren.
- personenbezogenen Daten nur an den dafür vorgesehenen Speicherpfaden ablegen (und nicht z.B. auf der lokalen Festplatte).
- die dienstliche IT darf aus Sicherheitsgründen nicht für private Zwecke genutzt werden. Es dürfen keine private Hard- oder Software verwendet werden. Ausnahmen sind ggf. in einer IT-Dienstanweisung geregelt.
- Die Nutzung von Diensten wie Whats App oder Facebook ist für die dienstliche Kommunikation aus Datenschutzgründen generell unzulässig. Dies gilt auch für die Kommunikation unter Kolleg*innen.

Mail / Post:

- Unterlagen mit schützenswerten personenbezogenen Daten auch im internen Postgang nur im verschlossenen Umschlag versenden
- vor dem Versand von personenbezogenen Daten per E-Mail prüfen, ob dieser Weg zulässig ist (z.B. bei internen Mails oder zu besonders geschützten externen Mailadressaten, die sich auch im sog. Landesnetz befinden oder verschlüsselt erreicht werden können). Informieren Sie sich hierzu ggf. bei der IT-Abteilung.

Vertretung:

- für den Fall einer Abwesenheit den **Zugriff** auf Informationen (z.B. E-Mail Posteingang, Kalender) für die Vertretung einrichten.
- als Vertretung auch **nur im Vertretungsfall** personenbezogene Daten der Kollegen zur Kenntnis nehmen bzw. bearbeiten.

Bei Fragen stehen wir jederzeit gern zur Verfügung:
Gemeinsame Datenschutzbeauftragte im Kreis Segeberg,
E-Mail: datenschutz@segeberg.de
Tel.: 04551 / 951-9851

Link zu unserem Datenschutz-Infoportal:
https://www.segeberg.de/index.php?object=tx|3466.12014.1