

**Allgemeine
Tipps und Hinweise
des Datenschutzgremiums
für Landtagsabgeordnete zum Umgang mit personenbezogenen Daten**

Landtagsabgeordnete haben aus datenschutzrechtlicher Sicht zwei Rollen: 1. Als Mitglieder des Landtages und als Angehörige einer Fraktion bzw. Gruppe haben sie eine öffentlichrechtliche Funktion, 2. Als Mitglieder einer politischen Partei und als Privatperson haben sie einen nicht-öffentlichen Status. In der Funktion als Mitglieder von Landtagsgremien und von Fraktionen haben Abgeordnete die Datenschutzordnung des Schleswig-Holsteinischen Landtages (DSO LT) zu beachten, soweit „die Daten Gegenstand parlamentarischer Beratungen oder Initiativen im Parlament, in seinen Gremien oder in den Fraktionen und ihren Arbeitskreisen sind oder waren,“ (§ 1 DSO LT). Als Angehörige einer Partei oder Privatperson (bei geschäftsmäßiger Datenverarbeitung) unterliegen Abgeordnete den allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG, insbes. die §§ 27 ff. BDSG).

Abgeordnete haben nach Art. 24 Abs. 3 Landesverfassung Schleswig-Holstein ein Zeugnisverweigerungsrecht bzgl. der ihnen in ihrer Funktion anvertrauten Tatsachen. Dem entspricht ein Beschlagnahmeverbot bzgl. solche Daten enthaltender Schriftstücke. Voraussetzung für diesen gesetzlichen **Vertrauensschutz** ist es, dass Abgeordnete die ihnen anvertrauten Informationen und Unterlagen auch vertraulich behandeln. Im Folgenden werden einige Tipps und Hinweise gegeben, wie aus technischer und organisatorischer Sicht durch Abgeordnete diese Vertraulichkeit gewährleistet werden kann.

Beim **Posteingang** sollte darauf geachtet werden, dass auf die eingehenden Unterlagen nicht über allgemein zugängliche Postfächer zugegriffen werden kann. Persönlich an Abgeordnete adressierte Schreiben dürfen nur von diesen oder von diesen ausdrücklich befugten Personen geöffnet werden.

Bei der konventionellen **Aktenorganisation** sollte unterschieden werden zwischen Sachakten und einer bestimmten Person zuzuordnenden oder besonders sensibel zu bewertenden Akten. Akten der zweitgenannten Kategorie sollten ebenso wie Unterlagen aus nicht-öffentlichen Sitzungen in abschließbaren Schränken abgelegt werden. Entsprechendes gilt für Petitionsakten und Kopien hieraus (vgl. § 13 Geheimschutzordnung des Landtags).

Nicht mehr benötigte **Landtagsunterlagen** mit personenbezogenen Daten oder mit sonst vertraulich zu behandelndem Inhalt sollten nicht im Papierkorb entsorgt, sondern sicher vernichtet werden. Denn der Inhalt der Papierkörbe wird zu Recyclingzwecken zentral in Papiercontainern gesammelt, die nicht über besondere Sicherheitsvorkehrungen gegen unbefugte Einsichtnahme verfügen. Im Zweifelsfall sollte deshalb immer der Papierschredder benutzt werden. Selbstverständlich können die Unterlagen auch an die Landtagsverwaltung zurück gegeben und von dieser entsorgt werden. Größere Mengen können mit der Unterstützung eines Hausarbeiters im Landtag (Mitarbeiter der GMSH) mit einem Aktenvernichter im Keller datenschutzgerecht beseitigt werden. Ansprechpartner ist Herr Grages, Tel. 1041.

Dasselbe gilt auch für **Fehlkopien**.

Der Zugang zum PC sollte durch ein **Passwort** gesichert sein. Das Passwort sollte mindestens 8 alphanumerische und Sonder-Zeichen enthalten. Bei der/dem Administrator/in des Fraktionsnetzes sollte man sich vergewissern, dass das Passwort bei dem eingesetzten Betriebssystem nicht umgangen werden kann. Wird der PC für eine gewisse Zeit (z.B. 5 Minuten) nicht mehr genutzt, so sollte sich der Bildschirm automatisch verdunkeln. Die erneute Bildschirmfreigabe sollte nur nach Eingabe des Passwortes erfolgen.

Auf der Festplatte gespeicherte „sensible,, Daten sollten **verschlüsselt** werden (Ablage in speziellen Dateien). Dies gilt in jedem Fall bei der Verwendung von mobilen Geräten (Lap-Tops). Es empfiehlt sich Programme einzusetzen, die ganze Verzeichnisse bzw. Datenträger verschlüsseln, so dass nach Passwordeingabe auf den Gesamtdatenbestand zugegriffen werden kann.

Das Überspielen von Disketten oder die Übernahme von Emails sollte erst erfolgen, nachdem diese mit einem gängigen **Virensuchprogramm** auf Virenbefall hin geprüft worden sind. Es sollte solchen Virensuchprogrammen der Vorzug gegeben werden, die eingehende Emails automatisch prüfen, bevor sie im Briefkasten abgelegt werden. Das Virensuchprogramm sollte so oft wie möglich aktualisiert werden. Entsprechende Virensuchprogramme werden von der/dem Administrator/in des Fraktionsnetzes zur Verfügung gestellt.

Emails oder eigene Dokumente mit „sensiblen,, Inhalt sollten ausgedruckt und danach sofort gelöscht (der „Papierkorb“ sollte deaktiviert oder sofort geleert werden), alternativ verschlüsselt abgelegt werden. Sollen elektronische Dokumente verfügbar bleiben, ohne dass es auf die gespeicherten personenbezogenen Daten ankommt, empfiehlt sich die Anonymisierung bzw. Pseudonymisierung der Dokumente (z.B. durch Löschung von Adressfeldern und Namen).

Nicht beaufsichtigte **Büros** sind beim Verlassen abzuschließen. Der Schlüssel sollte abgezogen werden. Unterlagen mit personenbezogenen Daten oder mit sonst vertraulich zu behandelndem Inhalt sollten nach Gebrauch unter Verschluss genommen werden.

Werden sensible (personenbezogene) Daten aus dem Parlamentsbereich **zu Hause** genutzt, so sollten sie dort verschlossenen aufbewahrt werden. Abgeordnetenpost sollte auf dem privaten PC getrennt von sonstigen Dokumenten abgelegt werden. Zumindest für diesen Bereich ist eine Zugriffssicherung (z.B. per Passwort, s.o.) geboten.

Bei **Fragen und Anregungen** zum Thema Datenschutz können sich Abgeordnete an das Datenschutzgremium des Landtags wenden. Ansprechpartnerin ist Frau Simonsmeier-Schriewer, Tel.: 1020.

Auskünfte erteilt auch gerne das **Unabhängige Landeszentrum für Datenschutz** (ULD). Der Landesbeauftragte für den Datenschutz, Herr Dr. Weichert, ist unter Tel. 1200 zu erreichen.