Merkblatt Datenschutz für Mandatsträger

Als Mandatsträgerin/Mandatsträger benötigen Sie Zugang zu den Daten der von Ihnen repräsentierten oder betreuten Mitglieder. Damit dies ermöglicht wird, haben Sie sich auf die Wahrung des Datengeheimnisses nach dem Bundesdatenschutzgesetz (BDSG) verpflichtet.

Verstöße dagegen sind neben Schadenersatz auch mit Bußgeldern – die Sie persönlich treffen können – von bis zu 300.000 € bedroht, bei Vorsatz und finanziellem Vorteil auch Haft. Versicherungen schützen bei Schadenersatzforderungen, aber nicht bei Bußgeldern und Unterhaltungen mit dem Staatsanwalt führt man – wenn überhaupt – lieber privat, als dienstlich.

Worauf müssen Sie also achten?

Mindestens auf die folgenden Grundsätze:

1. **Datenerhebung beim Betroffenen**. Wenn Sie personenbezogene Daten benötigen, die noch nicht im System sind, fragen Sie den Betroffenen direkt – und lassen Sie sich die Speicherung genehmigen (Einwilligung).
2. **Zweckbindung.** Daten die zu einem bestimmten Zweck erhoben worden sind, dürfen auch nur zu diesem Zweck verwendet werden. Beispiel: Hinterlegte Bankdaten für die Beitragszahlung dürfen ohne Nachfrage nicht zum Überweisen von Kostenerstattungen oder Reisekosten verwendet werden (und umgekehrt).
3. **Vertraulichkeit.** Personenbezogene Daten sollen nicht ohne triftigen Grund an andere Personen weitergegeben werden. Beispiel: Mail-Versand an eine Gruppe grundsätzlich nur in bcc (Blindkopie).
4. Bei jeder Verwendung personenbezogener Daten außerhalb des ursprünglich vorgesehenen Zwecks müssen Sie überlegen und abwägen, ob **schutzwürdige Interessen des Betroffenen** eine Rolle spielen. Beispiel Auslandsanschriften: In einigen Fällen hat die Verwendung von Dienstgradangaben auf Adressaufklebern im Auslandsversand dazu geführt, dass die Betroffenen aus Angst vor Terrorakten gegen ihre Familien umgezogen sind.
5. **Datensparsamkeit.** Beschränken Sie sich auf die Daten, die Sie wirklich benötigen. Was nicht mehr benötigt wird und keiner gesetzlichen Aufbewahrungspflicht unterlegt → löschen!
6. Alle Verletzungen des Schutzes personenbezogener Daten – z.B. Verlust eines mobilen Datenträgers (CD, USB-Stick) mit personenbezogenen Daten → melden! Ihr Datenschutzbeauftragter (w/m) prüft, ob **Meldepflichten** an die Betroffenen oder bestimmte Behörden gesetzlich vorgesehen sind.
7. In allen Zweifelsfällen wenden Sie sich bitte an die **Datenschutzbeauftragte** des Verbandes, zur Zeit Herr Heinz-Josef Enders, datenschutz@reservistenverband.de, +49 228 25909 73.

Daneben fordert das Bundesdatenschutzgesetz in der Anlage zu § 9 BDSG bestimmte technische Mindeststandards um personenbezogene Daten angemessen, aber wirkungsvoll zu schützen. Dazu gehören:

1. **Zutrittskontrolle.** Während der Arbeit am PC, oder wenn Sie Ausdrucke mit personenbezogenen Daten nicht immer verschlossenen haben, dürfen Dritte (das sind auch Ihr Familienangehörigen) keinen Zutritt in dieses Zimmer haben.
2. **Zugangskontrolle.** Verhindern Sie, dass nicht ermächtigte Personen Zugang zu Ihrem mobilen PC oder zu Datenträgern mit personenbezogenen Daten bekommen.
3. **Zugriffskontrolle.** Schützen Sie Ihren Computer und Ihre mobilen Endgeräte und Datenträger mit starken Passwörtern, die auch in Ihrer Familie nicht bekannt sind.
4. **Weitergabekontrolle.** Lassen Sie mobile Datenträger mit personenbezogenen Daten niemals unbeaufsichtigt und nutzen Sie Verschlüsselungen, besonders, wenn Sie in unsicherem Umfeld (z.B. Hotel-WLAN) kommunizieren.