



Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2018

Die Verwendung der Drohbriefe ist ein besonders schwerwiegender Vorfall. Sie stellt nicht nur eine Straftat dar, sondern beschädigt darüber hinaus das Vertrauen der Öffentlichkeit in die Sicherheitsorgane, deren Aufgabe insbesondere die Verhütung von Straftaten ist.

3.2 Verarbeitung personengebundener Hinweise in polizeilichen Datenbanken

Seit einigen Jahren erstellt und nutzt die Berliner Polizei wieder bestimmte polizeiliche Bewertungen von Personen, sog. personengebundene Hinweise (PHW), nachdem sie diese zuvor über zwanzig Jahre lang aufgrund von Kritik der Konferenz der Datenschutzbeauftragten des Bundes und Länder nicht für ihre Arbeit verwendet hatte.¹⁰⁴ Der Wiedereinführung der Hinweise haben wir erfolglos widersprochen.

Aus der Praxis

Zu den personengebundenen Hinweisen, die bundeseinheitlich verwendet werden, gehört die Angabe „Psychische und Verhaltensstörungen“ (PSYV), die bis zu einem entsprechenden Beschluss der Innenministerkonferenz im Jahr 2015 noch „geisteskrank“ hieß.¹⁰⁵ Solche personengebundenen Hinweise sollen insbesondere dem Schutz der betroffenen Person bzw. der Eigensicherung von Polizeibeamtinnen und -beamten dienen.¹⁰⁶

Aufgrund von Anfragen von Bürgerinnen und Bürgern zur Speicherung personengebundener Hinweise in polizeilichen Datenbanken haben wir die Senatsverwaltung für Inneres und Sport nun erneut zu dieser Thematik angeschrieben und darauf hingewiesen, dass wir weiterhin erhebliche Zweifel an der Rechtmäßigkeit der Speicherung des Hinweises „Psychische und Verhaltensstörungen“ haben. Ein solcher Hinweis ist aus unserer Sicht nicht für polizeiliche Zwecke erforderlich und für die Betroffenen äußerst stigmatisierend.

104 JB 2012, 3.8

105 Siehe Drs. 17/2406 des Abgeordnetenhauses Berlin

106 Siehe § 16 Abs. 6 Nr. 1 Bundeskriminalamtgesetz (BKAG)

Insbesondere ist nicht ersichtlich, weshalb die Aufnahme eines solchen Hinweises zur Gefahrenabwehr oder Eigensicherung durch die Polizei notwendig sein soll. Im Regelfall gehen von psychisch erkrankten Personen keine Gefahren aufgrund ihrer Erkrankung aus, die es polizeilich abzuwehren gilt. Soweit im Einzelfall solche Gefahren dennoch bekannt sein sollten, wäre zudem die Aufnahme des ebenfalls möglichen personengebundenen Hinweises „gewalttätig“ denkbar und ausreichend.

Der personengebundene Hinweis „Psychische und Verhaltensstörungen“ sollte mangels Erforderlichkeit aus der Liste der Hinweise, die in polizeilichen Datenbanken durch die Berliner Polizei zu ihrer Aufgabenerfüllung vergeben werden können, herausgenommen werden.

3.3 Sicherheitslücke bei der polizeilichen Datenbank POLIKS?

Ein Polizist beschwerte sich bei uns darüber, dass unbefugte Zugriffe auf die polizeiliche Datenbank POLIKS aufgrund nicht ausreichender Sicherheitsvorgaben möglich seien. Man könne durch mehrfache Eingabe eines falschen Kennworts einen beliebigen Zugang zu POLIKS sperren und sodann über eine telefonische Hotline ohne weitere Hürden diesen Zugang wieder entsperren und sich ein neues Kennwort geben lassen.

In der daraufhin eingeleiteten Prüfung wurde uns bestätigt, dass ein Zugang zu POLIKS gesperrt werde, wenn mehrfach ein falsches Passwort eingegeben werde. Zur Entsperrung könnten sich die betroffenen Nutzerinnen und Nutzer dann an die zentrale IT-Administration wenden. Diese hebe eine Kontensperrung auf, wenn die Meldung durch die Vorgesetzte oder den Vorgesetzten der oder des Betroffenen bestätigt werde. Nach Aufhebung der Sperre sei das Kennwort unverändert; es werde kein neues vergeben. Gegen dieses Verfahren haben wir keine datenschutzrechtlichen Bedenken.

Benötigt die Nutzerin oder der Nutzer nach einer Kontensperrung hingegen ein neues Kennwort, muss sie oder er sich nach Auskunft der Polizei an die jeweils

zuständige örtliche IT-Administration wenden, die nach einer Identifikation der betroffenen Person ein neues Kennwort vergebe. Das konkrete Identifikationsverfahren sei dabei nicht berlinweit einheitlich geregelt. Die polizeiinterne Passwortrichtlinie enthält nach unserer Feststellung hierzu ebenfalls keine konkreten Angaben, sondern lediglich das allgemeine Erfordernis eines Identitätsnachweises. Dieser erfolgt nach Aussage der Polizei entweder durch Vorlage des Dienstausweises, Verifizierung durch den Vorgesetzten oder persönliche Bekanntheit der oder des Betroffenen.

Wir forderten daraufhin, dass eine behördenweit einheitliche Regelung geschaffen und durchgesetzt werden muss, die eine sichere Identifikation der oder des jeweils Betroffenen garantiert. Insbesondere sollte genau festgelegt sein, wann welche der beschriebenen Mittel zur Identitätsprüfung bei einer Passwortneuvergabe Anwendung finden und wie diese jeweils konkret erfolgen soll. Um spätere Überprüfungen – insbesondere im Fall eines Missbrauchsverdachts – zu ermöglichen, sollte die Vergabe von neuen Passwörtern sowie die Art der Identitätsprüfung zudem bei den jeweiligen örtlichen IT-Administrationen dokumentiert werden. Weiterhin haben wir empfohlen, regelmäßig stichprobenartig Kontrollen der örtlichen Passwortneuvergaben vorzunehmen.

Die Polizei hat die Überarbeitung ihrer Passwortrichtlinie zugesagt.

Der unbefugte Zugang zu Daten in POLIKS ist bußgeldbewehrt und stellt sogar eine Straftat dar, wenn er mit Schädigungs- oder Bereicherungsabsicht erfolgt.¹⁰⁷ Die Polizei ist als Verantwortliche verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen im Hinblick auf eine Passwortneuvergabe zu treffen, um bei der Verarbeitung personenbezogener Daten in POLIKS ein dem Risiko angemessenes Schutzniveau zu gewährleisten.¹⁰⁸ Hierdurch wird auch Ordnungswidrigkeiten und Straftaten vorgebeugt.

107 §§ 70, 29 BlnDSG

108 § 50 Abs. 1 BlnDSG