Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 06.04.2021

Positionspapier

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum

Grundsatz der Zweckbindung in polizeilichen Informationssystemen

Graurheindorfer Str. 153
53117 Bonn

FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550

E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Im Rahmen ihrer Aufgabenerfüllung erfasst die Polizei auf vielfältige Art und Weise personenbezogene Daten von Bürgerinnen und Bürgern. Davon betroffen sind aber nicht nur Personen, die durch ihr Verhalten Anlass hierzu gegeben haben. Denn Polizeibehörden erfassen auch solche Menschen, die sich zufällig an einem bestimmten Ort zu einer bestimmten Zeit aufgehalten haben oder die Zeugen oder Geschädigte sind. Einmal erfasst, können die personenbezogenen Daten der Betroffenen mit weiteren Daten verknüpft und zeitlich unbegrenzt abgerufen werden.

Der technische Fortschritt in der elektronischen Datenverarbeitung hat dazu geführt, dass die Möglichkeiten zur Verarbeitung und Auswertung von Informationen in den letzten Jahren exponentiell gewachsen sind. Dies gilt insbesondere mit Blick auf Methoden und Systeme, die große Datenmengen mit Algorithmen oder sogenannter Künstlicher Intelligenz (KI) abgleichen, analysieren und weiterverarbeiten können. Diese Entwicklung hat auch Auswirkungen auf die Arbeit der Polizeibehörden. Diese arbeiten derzeit mit hohem Aufwand daran, ihre Systeme entsprechend zu modernisieren. Die Folgen für die informationelle Selbstbestimmung der betroffenen Personen können gravierend sein. Dies gilt insbesondere dann, wenn informationstechnische Einrichtungen des Bundes und der Länder in einem Verbund zusammenwirken. Werden verschiedene Daten miteinander verknüpft, besteht die Gefahr, dass die Daten von Betroffenen in neuen, vorher nicht relevanten Zusammenhängen verarbeitet werden. Dabei sind aber nicht nur neue Technologien relevant. Besonders wichtig ist die Frage, auf welche Datenbestände die Behörden zugreifen, ob sie gegebenenfalls verschiedene Datenbestände zusammenführen und zu welchen Zwecken die Datenbestände befüllt und gespeichert wurden. Die Einhaltung der datenschutzrechtlich gebotenen Zweckbindung der Datenverarbeitung ist vor diesem Hintergrund für den Schutz der Grundrechte von elementarer Bedeutung.

A. Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz ist ein Grundpfeiler des deutschen und europäischen Datenschutzrechts. Er dient dazu, die Verhältnismäßigkeit staatlichen Handelns sicherzustellen, und hat damit eine wichtige Schutzfunktion für die Grundrechte der betroffenen Bürgerinnen und Bürger. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts dürfen personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie ursprünglich erhoben worden sind. Datenverarbeitungen zu einem anderen Zweck sind nur auf der Grundlage entsprechender Vorschriften zulässig, die wiederum spezifischen verfassungsrechtlichen Anforderungen genügen müssen[1].

[1] Vgl. nur BVerfGE 141, 220 (324 f.).

Damit sichergestellt ist, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen, dürfen die Daten von vornherein nur zu bestimmten, präzise und normenklar festgelegten Zwecken gespeichert werden[2].

Der verfassungsrechtliche Zweckbindungsgrundsatz kommt in zahlreichen einfachgesetzlichen Regelungen zum Ausdruck. So bestimmt § 47 Nr. 2 Bundesdatenschutzgesetz, der der Umsetzung des Art. 4 Abs. 1 Buchst. b) der RL 2016/680/EU dient, dass personenbezogene Daten (nur) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden dürfen. Die zulässige Reichweite zweckändernder Nutzungen richtet sich dabei nach der Ermächtigung für die Datenerhebung[3].

B. Schlussfolgerungen im Hinblick auf polizeiliche Informationssysteme

Die rechtlichen Anforderungen an die Zweckbindung sind bei der technischen Ausgestaltung und der fachlichen Einrichtung polizeilicher Informationssysteme zu berücksichtigen. Dies betrifft insbesondere die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (vgl. § 71 Abs. 2 S. 1 und 2 BDSG).

Aus Sicht des BfDI sind aus den rechtlichen Vorgaben hinsichtlich der Zweckbindung im Hinblick auf die Verarbeitung von personenbezogenen Daten in polizeilichen Informationssystemen folgende Schlussfolgerungen zu ziehen:

- **Zweckfestlegung**

Erhebt eine Polizeibehörde personenbezogene Daten oder speichert sie diese in einem Informationssystem, muss der Zweck der Verarbeitung unverzüglich eindeutig festlegt werden. Es muss stets erkennbar sein, zu welchem Zweck die Polizei ein bestimmtes Datum verarbeitet. Den Korridor der im Rahmen der Zweckbindung zulässigen Datenverarbeitung markieren vor alle die konkrete Aufgabe, die mit der Verarbeitung bestimmter personenbezogener Daten erfüllt werden soll, und die Rechtsgüter, für deren Schutz diese Daten verarbeitet werden sollen[4].

Die möglichen Zwecke der Datenverarbeitung ergeben sich aus den gesetzlichen Aufgabenzuweisungen und ggfls. konkretisierend aus Verwaltungsvorschriften und Ver-

---

[2] Vgl. BVerfGE 65, 1, (46); 118, 168, (187 f.).

[3] BVerfGE 141, 220 (324).

[4] Vgl. Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschn. G., Rn. 516.

fahrensdokumentationen wie Errichtungsanordnungen, Verfahrensverzeichnissen, Datenschutzfolgeabschätzungen. Die Polizeigesetze sehen übereinstimmend folgende grundlegende Zweckbestimmungen vor:

- Aufgabenerfüllung,
- Vorgangsverwaltung,
- Dokumentation,
- Gefahrenvorsorge bzw. Strafverfolgungsvorsorge.

Diese lassen sich – je nach den einschlägigen gesetzlichen Bestimmungen – in Unterzwecke einteilen, die ebenfalls strikt voneinander abzugrenzen sind.

- **Zwecktrennung**

Die zu unterschiedlichen Zwecken in einem Informationssystem gespeicherten Daten müssen physikalisch oder logisch voneinander getrennt sein. Ein solches Trennungsgebot ist Ausfluss des Zweckbindungsgrundsatzes. Es handelt sich um eine technisch-organisatorische Maßnahme, die dazu dient, die gesetzlich vorgesehene Zweckbindung sowie die Kontrolle ihrer Einhaltung auf organisatorischer und technischer Ebene sicherzustellen. Gleichzeitig trägt das Trennungsgebot dazu bei, die Datenverarbeitung auf das zur Erfüllung der jeweiligen Aufgabe erforderliche Maß zu beschränken.

- **Funktionsgerechte Vergabe von Zugriffsrechten**

Bei der Vergabe von Zugriffsrechten ist auf den jeweiligen Verarbeitungszweck zu achten. So ist z.B. der Abruf personenbezogener Daten aus einem polizeilichen Recherchesystem nur zulässig, wenn aus der Sicht des handelnden Polizeibeamten deren Kenntnis zur Erfüllung einer konkreten polizeilichen Aufgabe erforderlich ist[5]. Die Vergabe von Zugriffsrechten erfolgt – denklogisch zwingend – gestuft je nach dem einschlägigen Verarbeitungszweck. Der Kreis der potenziell Zugriffsberechtigten bei Vorsorgezwecken dienenden Datenbeständen ist weiter als im Falle der Aufgabenerfüllung, die sich auf bestimmte Verfahren und damit auf die für die Bearbeitung z.B. einer bestimmten Strafanzeige zuständigen Beamtinnen und Beamten beschränkt. Der Zugriff auf Dokumentationsdaten ist auf den Zweck der Kontrolle der Rechtmäßigkeit des behördlichen Handelns zu begrenzen. Damit hat die Behörde die Möglichkeit, insbesondere in gerichtlichen Verfahren und auch in der Datenschutzkontrolle darzulegen, dass sie ordnungsgemäß gehandelt hat. Sie dürfen nicht pauschal im operativen Bereich genutzt werden.

[5] Vgl. nur OLG Bamberg, ZD 2019, 465 (466).

- **Recherchemöglichkeiten**

Die Recherchemöglichkeiten in einem Informationssystem dürfen nicht weiter reichen als dies erforderlich ist. Insofern besteht ein enger Zusammenhang mit der funktionsgerechten Vergabe von Zugriffsrechten. Nach Daten, die z.B. zum Zweck der Dokumentation des polizeilichen Handelns gespeichert sind, darf in Ermangelung einer entsprechenden gesetzlichen Grundlage nicht zu einem anderen Zweck recherchiert werden. Dies gilt unabhängig davon, ob das einschlägige Fachrecht die Verarbeitung der zur Vorgangsverwaltung oder zur Dokumentation polizeilichen Handelns gespeicherten Daten ausdrücklich nur zu diesem Zweck erlaubt. Vorschriften wie § 22 Abs. 2 BKAG haben angesichts der oben dargelegten verfassungsrechtlichen Vorgaben nur einen klarstellenden Charakter.

Ebenso darf der Abgleich der in einem Informationssystem gespeicherten personenbezogenen Daten mit anderen polizeilichen Datenbeständen nur innerhalb der jeweiligen Zwecke dieser Daten erfolgen[6]. Dies gilt erst recht, wenn die Polizeibehörden Daten mit Methoden der KI abgleichen. Dementsprechend dürfen die zu Zwecken der Strafverfolgung gespeicherten Daten – vorbehaltlich einer Spezialvorschrift – nicht mit den Daten abgeglichen werden, die zu Zwecken der Gefahrenabwehr gespeichert wurden[7]. Die Vorschrift des § 481 Abs. 1 S. 1 Strafprozessordnung, die die Polizeibehörden zur Verwendung personenbezogener Daten aus Strafverfahren nach Maßgabe der Polizeigesetze ermächtigt, bezieht sich auf einzelne Verfahren und kann eine gemischte Speicherung in einem Informationssystem nicht legitimieren[8].

Die verschiedenen Aufgaben der Polizei und folglich die verschiedenen Zwecke der Datenverarbeitung können sich in der Praxis überschneiden. Die Einhaltung der Zweckbestimmung bei der Verarbeitung personenbezogener Daten in polizeilichen Informationssystemen erfordert deshalb ein planvolles Vorgehen bei der Konzeption der entsprechenden Informationssysteme und eine fortwährende Evaluierung durch die verantwortlichen Stellen.

---

[6] Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschn. G., Rn. 1045 ff.

[7] Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschn. G., Rn. 1054.

[8] Singelnstein, in: Münchener Kommentar zur StPO, 1. Aufl. 2019, § 481 Rn. 5; vgl. Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschn. B., Rn. 199 ff.

- **Hypothetische Datenneuerhebung als Spezialfall der Zweckbindung**

Der vom Bundesverfassungsgericht entwickelte Grundsatz der hypothetischen Datenneuerhebung konkretisiert den Verhältnismäßigkeitsgrundsatz. Er formuliert verfassungsrechtliche Anforderungen, die der Gesetzgeber zu beachten hat, wenn er es den Sicherheitsbehörden ermöglicht, bereits erhobene Daten zweckändernd zu nutzen. Diese Rechtsfigur darf nicht dahingehend missverstanden werden, dass sie eine eindeutige Festlegung der Verarbeitungszwecke entbehrlich machen würde. Ebenso wenig ist die pauschale Heranziehung des Grundsatzes der hypothetischen Datenneuerhebung als Begründung für die Schaffung eines Verbundinformationssystems mit weitreichenden Abfrage- und Recherchemöglichkeiten sachgerecht[9].

- **Kennzeichnungs- und Protokollierungspflichten**

Um eine zweckentsprechende Verarbeitung von Daten sicherzustellen, fordert das Grundgesetz Kennzeichnungs- und Protokollierungspflichten[10].

Daten, die aus qualifizierten Grundrechtseingriffen, insbesondere aus Eingriffen in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG, stammen, müssen entsprechend gekennzeichnet sein[11]. Eine ausreichende Kennzeichnung liegt beispielsweise vor, wenn in dem Informationssystem ein besonderes Feld vorgesehen ist, um Datensätze entsprechend kennzeichnen zu können. Ein Vermerk in einem allgemeinen Freitextfeld wird den Anforderungen an eine Kennzeichnung nicht gerecht. Die relevante Information kann im letztgenannten Fall durch andere Hinweise im allgemeinen Freitextfeld „überschattet“ und der Aufmerksamkeit des Sachbearbeiters entzogen werden. Ein besonderes Kennzeichnungsfeld erfüllt daher besser die Warnfunktion der Kennzeichnung.

[9] Vgl. aber BT-Drs. 18/11163, S. 75 ff.

[10] Vgl. nur BVerfG, NJW 2013, 1499 (1503).

[11] Vgl. BVerfGE 100, 313 (395f.); 125, 260 [333]; § 101 Abs. 3 S. 1 StPO.