Hinweise
zu den datenschutzrechtlichen Anforderungen
an die Protokollierung nach § 76 Bundesdatenschutzgesetz

Inhalt

I. Was ist Protokollierung?

Automatisierte Verarbeitungssysteme müssen so gestaltet werden, dass zu allen Datenverarbeitungsvorgängen systemseitig im Hintergrund bestimmte Transaktionsdaten in Form sogenannter Protokolldaten mitgeschrieben werden. Hierbei sind zwei Protokollierungsebenen zu unterscheiden.

Erste Ebene ist die sog. technische Protokollierung von Systemereignissen für **Zwecke der IT-Sicherheit in der IT-Infrastruktur** (z.B. auf Basis des § 64 BDSG, Infrastrukturebene). Die Datensicherheit, insbesondere die Anforderungen nach § 64 BDSG sind Bestandteil des Datenschutzes und unterliegen der Kontrolle der Datenschutzaufsicht. Hierzu können auch die entsprechenden Protokolldaten der ersten Ebene herangezogen werden.

Zweite Ebene ist die durch **materiell-rechtliche datenschutzrechtliche Vorschriften vorgegebene sog. fachliche Protokollierung** (insbesondere § 76 Abs. 1 BDSG, Fachanwendungsebene). Sie dient insbesondere dem Ziel, in dem besonders sensiblen Bereich der Verhütung, Ermittlung, Aufdeckung, Verfolgung und Ahndung von Straftaten bzw. von Ordnungswidrigkeiten eine wirkungsvolle Kontrollmöglichkeit zu implementieren. Darüber hinaus ermöglicht sie den verantwortlichen Stellen die regelmäßig durchzuführende Eigenkontrolle.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.datenschutz.bund.de

Aus den gemäß § 76 Abs. 1 Nr. 1 bis 6 BDSG mindestens zu protokollierenden Verarbeitungsvorgängen entsteht ein System von Spuren über die Historie (Erhebung, Veränderung, Kombination, Löschung) und die Verwendung (Abfrage, Offenlegung einschließlich Übermittlung) eines einzelnen Datums innerhalb eines automatisierten Verarbeitungssystems.

Die Fachanwendungsebene einschließlich ihrer (Fach-)Protokollierung muss auf einer sicheren IT Infrastruktur (erste Ebene) einschließlich deren Protokollierung aufbauen. Dies ist eine Voraussetzung, um die Integrität der Protokolldaten auf der Fachanwendungsebene zu gewährleisten.

Es sind immer zwei zumindest logisch getrennte Datenbestände zu führen, da die Löschfristen bzw. -pflichten sowie Rechte- und Rollenkonzepte voneinander unabhängig sein können (Protokolldaten zur Fachanwendung und Protokolldaten auf der Ebene der IT-Infrastruktur).

II. Wozu dient Protokollierung?

Die Protokollierung nach § 76 BDSG hat den Zweck, eine Kontrolle zu ermöglichen, ob die verantwortliche Stelle personenbezogene Daten innerhalb der materiell-rechtlich zulässigen Grenzen bzw. Zwecke verarbeitet. Verarbeiten Polizei- und Strafverfolgungsbehörden personenbezogene Daten, ist nach den Vorgaben der JI-Richtlinie bzw. des Bundesverfassungsgerichts eine Kontrolle durch unabhängige Datenschutzaufsichtsbehörden zwingend vorzusehen. Diese Kontrolle ist nur möglich, wenn die Datenverarbeitung revisionssicher protokolliert wird. Die Protokolldaten müssen darüber Auskunft geben können, wer (oder was) wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Nur auf diese Weise ist es möglich, im Rahmen einer Datenschutzkontrolle den Weg der Daten nachzuvollziehen. Ebenfalls kann nur auf diese Weise sichergestellt werden, dass Datenlöschungen nachvollzogen werden können.

Verarbeitet eine Sicherheitsbehörde personenbezogene Daten, greift dies in die Grundrechte der betroffenen Personen ein. Protokollierung soll diesen Grundrechtseingriff abmildern und ist deshalb eine verfahrenssichernde Maßnahme. Sie darf deshalb nicht in ihr Gegenteil verkehrt werden und ihrerseits zu zusätzlichen Grundrechtseingriffen gegenüber den betroffenen Personen führen (Zweckbindung). Dies schließt eine Zweckänderung wie etwa die Nutzung für fachliche Zwecke, insbesondere die Verwertung der fraglichen Daten für die allgemeine Strafverfolgung aus. Um eine rechtswidrige Nutzung von Protokolldaten zu verhindern, sind besondere Maßnahmen zu ergreifen (siehe unten Ziff. V). Davon zu unterscheiden ist die Frage, ob Protokolldaten gegenüber Bediensteten der verantwortlichen Stelle zu Zwecken der Strafverfolgung genutzt werden dürfen.

Soweit nach der JI-Richtlinie bzw. § 76 Abs. 3 BDSG Protokolldaten „für Strafverfahren“ verwendet werden dürfen, ist dies restriktiv auszulegen. Danach dürfen die Protokolldaten in Strafverfahren nur verwendet werden, solange das jeweilige Strafverfahren im Zusammenhang mit den Verwendungszwecken Kontrolle der Rechtmäßigkeit der Verarbeitung, Eigenüberwachung oder

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.datenschutz.bund.de

Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten steht (vgl. Empfehlung der Artikel 29-Gruppe in ihrer Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680) vom 29. November 2017, WP 258). Strafverfahren im Sinne des § 76 Abs. 3 BDSG meint dementsprechend nur solche, die sich gegen eine missbräuchliche Nutzung der Datenverarbeitung richten. Das schließt die Verfolgung von Ordnungswidrigkeiten oder die Durchführung entsprechender Disziplinarverfahren gegen Mitarbeitende der Sicherheitsbehörde ein. Ausgeschlossen ist dagegen eine Verwendung der Protokolldaten gegen davon selbst (Haupt-)Betroffene, deren Daten von der Sicherheitsbehörde verarbeitet werden.

III. Wie ergänzen sich Protokollierung und Dokumentation?

Diejenigen Tatsachen, die die rechtliche Zulässigkeit von Verarbeitungsvorgängen begründen, sind nicht Teil der Protokollierung, sondern der (fachlichen) Dokumentation. Die Behörden unterliegen einer Pflicht zur ordnungsgemäßen Aktenführung mit dem Ziel der vollständigen Dokumentation des Verwaltungshandelns. Das schließt alle aus datenschutzrechtlicher Perspektive relevanten Tatsachen (Lebenssachverhalt) und Wertungen (z.B. Ermessensausübung, Prognoseentscheidung) ein, die zu einem der gemäß § 76 Abs. 1 BDSG protokollierungspflichtigen Verarbeitungsvorgänge führen. Die datenschutzrechtlich relevante Dokumentation muss in dem zum betreffenden Verarbeitungsvorgang gehörenden Aktenrückhalt niedergelegt sein.

IV. Wann ist zu protokollieren?

Gemäß § 76 BDSG muss die verantwortliche Stelle in allen „automatisierten Verarbeitungssystemen“ protokollieren. Weitere Pflichten können sich aus spezielleren Rechtsgrundlagen ergeben. Der Begriff der „automatisierten Verarbeitung“ ist weit zu verstehen. Nicht erfasst ist die rein manuelle Erfassung von Daten, etwa in Akten.[1] Bei der elektronischen Aktenführung hingegen handelt es sich um automatisierte Verarbeitungssysteme. Beeinflussen technische Vorgänge die Daten, werden diese stets „automatisiert“ verarbeitet. Dies ist insbesondere der Fall, wenn mit Hilfe des Systems Daten sortiert oder recherchiert werden können. Daher liegt beim Einsatz von Arbeitsplatzcomputern, vernetzten Systemen, Smartphones oder digitalen Kommunikationsmitteln stets eine automatisierte Verarbeitung vor.

Hierbei kommt es nicht auf das Stadium der Datenverarbeitung an. Die Vorgaben gelten ebenso für Datenerfassungssysteme (z.B. Video-Systeme, GPS-Tracker, IMSI-Catcher, Smartphone-Apps)

[1] BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 76 Rn. 7-10.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.datenschutz.bund.de

wie für fachliche Anwendungen (z.B. Vorgangs- und Fallbearbeitungssysteme, Fahndungsdateien). Insoweit gilt:

- Bei Erfassungen mittels Smartphone-App sind mindestens folgende Protokolldaten vorzusehen: Geräte-ID, durchgeführte Aktion (z.B. Kameraerfassung, Chip auslesen), Datum und Uhrzeit, Benutzeridentifikation (ggf. inkl. Standortdaten), ggf. Empfänger / empfangendes System bei Übermittlungen, ggf. Absender / absendendes System bei Eingängen.
- Bei Kennzeichenerfassungssystemen sind mindesten folgende Protokolldaten erforderlich: Geräte-ID, Art der Verarbeitung (z.B. Aufzeichnung, Abgleich), Datum und Uhrzeit, im Trefferfall zusätzlich das Bild, das den Treffer ausgelöst hat, das ausgelesene Kennzeichen, das Abgleichergebnis, ggf. Empfänger / empfangendes System bei Übermittlungen.
- Bei einer einfachen Videoaufzeichnung sind pro Erfassungsgerät mindestens folgende Protokolldaten vorzusehen: Geräte-ID, Standort, Winkel / Bildausschnitt, Beginn und Ende der Aufzeichnung (Datum und Uhrzeit), ggf. Beginn und Ende der Speicherung, ggf. Empfänger / empfangendes System bei Übermittlungen.

V. In welcher Form ist zu protokollieren?

Nach der Rechtsprechung des Bundesverfassungsgerichts muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzaufsichtsbehörden in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält.[2]

Hieraus sind folgende Anforderungen abzuleiten:

- Die Protokolldaten müssen in einem strukturierten, gängigen, maschinenlesbaren und maschinenauswertbaren Format vorliegen oder in ein entsprechendes Format exportierbar sein (z.B. JSON-, CSV-Format). Die verantwortliche Stelle muss die Daten in diesem Format der Datenschutzaufsichtsbehörde vorlegen können (ggf. einschließlich des Auswertungstools). Die Protokolldaten müssen zeitnah zur Verfügung gestellt werden können.
- Es muss möglich sein, die Protokolldaten für Zwecke der Datenschutzkontrolle auszuwerten und in ihnen zu recherchieren. Auf ein entsprechendes Auswertungstool muss die Datenschutzaufsichtsbehörde vor Ort zugreifen können. Hierfür muss gegebenenfalls ein entsprechender temporärer Account eingerichtet werden können und es muss eine Suchmaske vorhanden sein, die ähnlich der Suche in den Echtdaten funktioniert (u.a. Sortierfunktionen, Filter, Aggregation).

[2] NJW 2016, 1781 Abs. Nr. 141; NJW 2013, 1499 Abs. Nr. 215.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.datenschutz.bund.de

Darüber hinaus sind für die Verarbeitung von Protokolldaten angemessene technisch-organisatorische Maßnahmen im Sinne des § 64 BDSG zu treffen. Hierzu gehören neben einem Backup-Konzept insbesondere ein spezifisches Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (z.B. Zugriffsrecht beschränkt auf die/den Datenschutzbeauftragte/n, Admin-Zugriffe nur nach Vier-Augen-Prinzip, förmliches Antragsverfahren) sowie technische Maßnahmen zur Gewährleistung der Revisionssicherheit. Insbesondere Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden. Protokolldaten sollten nicht auf den Produktivsystemen, sondern auf eigens hierfür vorgehaltenen zugriffsbeschränkten zentralen Protokollservern gespeichert werden. Die zu protokollierenden Ereignisse sollten in Echtzeit über ein sicheres Protokoll auf die Protokollserver übertragen werden.

Zugriffe auf Protokolldaten sind ebenfalls zu protokollieren.

VI. Welche Inhalte gehören in die Protokolldaten nach § 76 BDSG?

Inhaltliche Vorgaben enthält § 76 Abs. 2 BDSG lediglich für die Ereignisse der Abfrage (§ 76 Abs. 1 Nr. 3 BDSG) und Offenlegung (§ 76 Abs. 1 Nr. 4 BDSG). Diese Protokolle müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und soweit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Zur Sicherstellung einer effizienten Datenschutzkontrolle sollten die gleichen Protokollinhalte auch bei allen anderen Ereignissen i.S.d. § 76 Abs. 1 BDSG verfügbar sein.

Die Einschränkung „soweit wie möglich“ in Bezug auf die Identität der abfragenden oder offenlegenden Person ist beim heutigen Stand der Technik nicht mehr nachvollziehbar. Schließlich dürfte jeder mit einer speziellen Nutzerkennung o.ä. individualisierbar im System angemeldet sein. Die eindeutige Identifizierbarkeit über personalisierte Nutzerkennungen dient nicht nur einer umfassenden datenschutzrechtlichen Kontrollierbarkeit, sondern auch dem Schutz aller korrekten Anwender.

Die erforderliche „Begründung“ darf nicht nur eine Formalie sein, sondern muss einen effektiven Nutzen für die Datenschutzkontrolle haben. An die Begründungstiefe sind kontextabhängige abgestufte Anforderungen zu stellen. Hierbei ist zu beachten, dass die Protokollierung automatisiert erfolgen soll. Je nach Art der Maßnahme kann z.B. eine Statusangabe wie „Verkehrskontrolle am [Datum] in [Straße, Ort]“ ausreichen. Bei Ermittlungsverfahren muss grundsätzlich mindestens eine Referenz auf die Dokumentation (Vorgangszeichen) und im Idealfall ein Hinweis auf den konkreten Anlass der Abfrage vorhanden sein. Erforderlichenfalls sind die Voraussetzungen einer entsprechenden Dokumentation im Prozess der Abfrage / Eingabe zu schaffen.

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.datenschutz.bund.de

Darüber hinaus muss der Unterschied zwischen verschiedenen Transaktionen wie Abfrage („pull“) und Offenlegung („push“) in der Protokollierung klar erkennbar sein, weil hier ggf. völlig verschiedene Rechtsgrundlagen einschlägig sind, anhand derer die Rechtmäßigkeit des Vorgangs zu beurteilen ist.

Im Ergebnis sollte jeder Protokolldatensatz zu einem Verarbeitungsschritt folgende Angaben enthalten:

- Identifizierungsmerkmal des betreffenden Datums,
- Art der Transaktion (zutreffende Bezeichnung der Tätigkeit oder des Ereignisses),
- Datum und Uhrzeit bzw. Zeitstempel,
- Personenbezogene Benutzeridentifikation (bei Bedarf weitere Daten, wie z.B. Standortdaten) oder bei automatisierten Verarbeitungsschritten Angabe zu Mechanismus und Regeln, die diese auslösen (z.B. automatisierte Löschroutinen oder Abgleiche),
- Begründung/Zweck (bei Abfrage und Offenlegung),
- Empfänger (bei Offenlegung),
- Kombinationsergebnis (bei Kombination),
- Versuchte/fehlgeschlagene Aktionen.

Bereits bei der Planung der Protokollinhalte sind typische Szenarien zur Auswertung mit zu bedenken. Die häufigsten Auswertungen sollten auch für die Eigenkontrolle durch den Datenschutzbeauftragten vorgesehen werden.

Je nach Eingriffsintensität können sich im Einzelfall zusätzliche Anforderungen an die Protokollierung ergeben. Dies gilt ebenso für spezielle gesetzliche Vorschriften. Dies kann bis hin zum Erfordernis einer Inhaltsvollprotokollierung reichen. Die verantwortliche Stelle ist in der Pflicht, die Protokollierung bei jeder spezifischen Anwendung so zu gestalten, dass sie aus Sicht eines verständigen Dritten den Weg und die Entwicklung eines Datums mit allen Stationen von der Erhebung bis zur Löschung nachvollziehbar und mit Blick auf Grundrechtseingriffe kontrollierbar macht.

Falls sich die Verarbeitung eines Datums über verschiedene Systeme oder Systemteile mit verschiedenen Protokolldaten erstreckt, so muss eine automatisierte Verknüpfung der Protokolleinträge gewährleistet werden. Dies kann z.B. bei einer Übermittlung durch Protokollierung einer Transaktions-ID auf Seiten sowohl des Absenders als auch des Empfängers erreicht werden.

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.datenschutz.bund.de

VII. Welche Ereignisse sind nach § 76 BDSG zu protokollieren?

Nach § 76 Abs. 1 BDSG sind die folgenden sechs Ereignisse zu protokollieren:

- **Erhebung** (Nr. 1): Erhebung im Sinne dieser Vorschrift bezeichnet den Zeitpunkt, in dem die (zuvor oder zugleich) aufgenommenen Daten in ein automatisiertes Datenverarbeitungssystem eingespeichert werden. Im System wird ein „neues“ Datum generiert.
- **Veränderung** (Nr. 2) erfasst jedes Hinzufügen, Ändern, Überschreiben eines bereits existierenden Datums. Ein bereits im System vorhandenes Ausgangsdatum wird verändert (Bestandsveränderung). Die geänderte Teilmenge muss eindeutig benannt sein. Bei einem ändernden bzw. überschreibenden Zugriff sollten die Daten vor und nach der Änderung protokolliert werden, damit die Änderung bzw. die Überschreibung erkannt wird.
- **Abfrage** (Nr. 3) ist im Sinne eines „lesenden Zugriffs“ oder „Anschauens“ des Originaldatums zu verstehen. Es handelt sich um eine „pull“-Konstellation im Sinne eines eigenständigen aktiven Zugriffs. Bei Abfragen in Systemen anderer verantwortlicher Stellen ist ebenfalls eine geeignete Protokollierung vorzunehmen.
- **Offenlegung** (Nr. 4) bezeichnet als „push“-Konstellation den Vorgang, Dritten Kenntnis oder die Möglichkeit der Kenntnisnahme zu verschaffen.[3] Dies findet durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung statt.[4] Das schließt manuelle und automatisierte Übermittlungen an und in andere Systeme ein. Diese sind regelmäßig an der entsprechenden Schnittstelle protokollierungsfähig und stets protokollierungspflichtig. Zu protokollieren sind die Bezeichnungen der offengelegten Datenfelder, sowie der Grund der Offenlegung und der Empfänger.
- **Kombination** (Nr. 5) ist kein Spezialfall der Veränderung. Hierbei ändert sich das Ausgangsdatum nicht. Vielmehr wird es zu einem anderen Datum in Beziehung gesetzt, verknüpft, ausgewertet o.ä. Der Begriff der Kombination ist weit auszulegen. Erfasst sind die Anwendung von Auswerte- oder Prognosetools sowie Data-Mining-Techniken und Algorithmen. (Näheres hierzu vgl. unten Ziff. VIII.)

  Eine Kombination liegt auch vor, wenn Daten nach bestimmten Kriterien als Teilmenge einer Datenbank oder mehrerer Datenbanken angezeigt werden. Eine langfristige und dauerhafte Kombination i.S. einer Veränderung ist nach dem Wortlaut nicht erforderlich. Auch die nur vorübergehende Verknüpfung (z.B. in einem Auswertechart) kann zu einer Belastung für betroffene Personen führen, weil mit dem entsprechenden Ergebnis weitergearbeitet wird bzw. daraus neue (Ermittlungs-) Vorgänge generiert werden können. Ohne Protokollierung des

[3] Reimer in: Sydow, Europäische Datenschutzgrundverordnung, 1. Auflage 2017, Art. 4 Rn. 68.
[4] Ernst in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 4 Rn. 30; Reimer a.a.O.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.datenschutz.bund.de

Kombinationsergebnisses wäre hier nicht nachvollziehbar, woher neue Ermittlungsansätze zu bestimmten Personen resultieren. Wird das Kombinationsergebnis in den Originaldatensatz integriert, handelt es sich bei diesem Vorgang um eine Veränderung des Originaldatensatzes. Diese ist gesondert zu protokollieren. Dasselbe gilt auch für die Zusammenführung verschiedener Datensätze zu einem Datensatz. Beide Transaktionen sind zu protokollieren.

- **Löschen** (Nr. 6) meint das spurenlose endgültige Beseitigen im Sinne von Nicht-Wiederherstellbarkeit. Im Protokolleintrag zur Löschung sind jedoch, soweit erforderlich, auch Meta- und Inhaltsdaten des zu löschenden Datums aufzunehmen.

Jede **Verarbeitungsbeschränkung** ist ebenfalls zu protokollieren, da sie – je nachdem, wie sie technisch ausgestaltet ist – unter eine der vorgenannten Fallgruppen fällt. Da gemäß § 58 Abs. 4 BDSG technisch sicherzustellen ist, dass die Einschränkung der Verarbeitung eindeutig erkennbar ist, liegt in der Regel eine Veränderung des Datensatzes vor (Nr. 2).

Darüber hinaus ist eine **Protokollierung administrativer Zugriffe** erforderlich, um Kontrolllücken zu vermeiden. Dies dient auch dem Schutz der Administratoren vor unberechtigten Vorwürfen.

Das umfasst zum einen eine **Protokollierung administrativer Zugriffe auf der Ebene des Betriebssystems**, etwa wenn ein/e Systemadministrator/in die gesamte Datenbank der Fachanwendung kopiert.

Zum anderen umfasst das die **Administration auf Fachebene**. Hier ist insbesondere eine Protokollierung von Zugriffsrechten vorzunehmen (z.B. wann wurde welche Benutzerkennung erstellt/entfernt, wann hatte wer welche Berechtigung). Dies betrifft etwa den Fall, dass jemand zu privaten Zwecken in einer polizeilichen Datenbank überprüft wurde und die abrufende Person die/den Administrator/in um Löschung oder Änderung der Nutzerkennung bittet, so dass der Abruf nicht mehr zugeordnet werden kann. Ohne Protokollierung des Zugriffs auf die Nutzerkennungsverwaltung wäre ein derartiger Datenschutzverstoß nicht erkennbar.

VIII. Besonderheiten bei der Kombination von Daten

Wenn personenbezogene Daten in Beziehung gesetzt und daraus Schlussfolgerungen gezogen werden, müssen alle Verarbeitungsschritte, die hierzu geführt haben, und das Kombinationsergebnis protokolliert werden. Zudem muss nachvollziehbar sein, wie es zu der Kombination kam. Hier zeigt sich wieder, dass neben der Protokollierung eine entsprechende Dokumentation zwingend erforderlich ist.

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.datenschutz.bund.de

Werden Daten (teil-)automatisiert miteinander verknüpft, müssen bei allen Zusammenführungen (**Merging**) und Verknüpfungen (**Linking**) mindestens der Ursprung, das Ziel, der Bearbeiter und der Zeitpunkt protokolliert werden.

Ein Anwendungsbeispiel der Kombination ist die Verknüpfung von personenbezogenen Daten zu sogenannten **Beziehungsnetzwerken** und deren Darstellung als Beziehungsgraph. Bei solchen Formen der Kombination sind besondere Anforderungen an die Protokollierung zu richten, damit diese für die Datenschutzkontrolle nachvollziehbar bleibt. Den wenigsten Anwendern ist wohl bewusst, dass sich beispielsweise hinter der mit einem einfachen Mausklick erzielten Erweiterung eines Beziehungsgraphen auf weitere Darstellungsebenen komplexe Datenverarbeitungsoperationen in Form von Abrufen und Kombinationen im Hintergrund ergeben. Dabei wird eine unüberschaubare Anzahl von Protokolleinträgen generiert, die den ursprünglichen Zweck der Aktion nicht mehr erkennen lässt. Die Nachvollziehbarkeit einer solchen Protokollierung lässt sich nur mit einem geeigneten graphischen Auswertungstool erreichen. Dieses sollte unter anderem Unterschiede in verschiedenen Versionen von Netzwerken visuell darstellen können (z.B. durch Rollbacks).

Allgemein gilt, dass die in Protokolldaten aufgeführten Aktionen so zu aggregieren sind, dass sie der kontrollierenden Instanz helfen, einen Sachverhalt zu rekonstruieren und zu bewerten.

Einen besonderen Fall der Datenkombination stellt die Nutzung **algorithmischer Systeme** dar, bei denen verschiedene Daten miteinander in Beziehung gesetzt werden. In welcher Form solche Algorithmen überhaupt datenschutzrechtlich zulässig eingesetzt werden dürfen, ist im Einzelfall zu klären. Unabhängig von dieser Frage ist es im Hinblick auf die Protokollierung beim Einsatz algorithmischer Systeme wichtig festzuhalten, dass es sich dabei um eine besonders eingriffsintensive Form der Datenverarbeitung handeln kann. Dies gilt insbesondere für die Fälle, in denen es sich um sog. selbstlernende Algorithmen handelt oder Daten mit eine großen Streubreite verknüpft werden. Eingriffsintensive Datenverarbeitungen sind an besondere Eingriffsschwellen und Bedingungen zu binden. Zu diesen Bedingungen zählt auch eine der besonderen Eingriffsintensität gerecht werdende Protokollierung.

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.datenschutz.bund.de