Empfehlungen zur Erstellung von Löschkonzepten

I. Rechtslage

Zu den elementaren, aber oft übersehenen oder als nachrangig bewerteten datenschutzrechtlichen Pflichten gehört die Löschung personenbezogener Daten. Gemäß Art. 5 Abs 1 lit. e DSGVO dürfen personenbezogene Daten nicht länger gespeichert werden, als es für die Zwecke ihrer Verarbeitung erforderlich ist.[1] Dies zu gewährleisten, erfordert eine ebenso umfassende wie langfristige Planung wie nachhaltige Umsetzung.

Neben der rechtlichen Verpflichtung nach Art. 5 Abs. 1 lit e DSGVO reduziert das regelmäßige Löschen nicht mehr benötigter personenbezogener Daten das Risiko einer versehentlichen oder absichtlichen Weiterverarbeitung dieser Daten zu anderen Zwecken ebenso wie das Risiko unberechtigter Zugriffe, etwa durch Cyberkriminelle. Jede zweckwidrige Verarbeitung ist gem. Art. 5 Abs. 1 lit. b DSGVO verboten. Wirksame Löschroutinen und deren Dokumentation sind außerdem erforderlich, um den Informations- und Dokumentationspflichten nach Artt. 12-14 und 30 DSGVO nachkommen sowie Anträge betroffener Personen auf Löschung oder Sperrung gem. Artt. 17-18 DSGVO bearbeiten zu können.

Die Rundfunkanstalten, ihre Gemeinschaftseinrichtungen und Beteiligungsgesellschaften – kurz: die Verantwortlichen im öffentlich-rechtlichen Rundfunk - sind gem. Art. 5 Abs. 2 DSGVO verpflichtet, nachweisen zu können, dass sie personenbezogene Daten im Einklang mit dem Prinzip der Speicherbegrenzung löschen. Voraussetzung dafür ist ein wirksames Datenschutzmanagement auch in Bezug auf die Löschverpflichtung.

II. Handlungsempfehlungen

Um die Einhaltung der datenschutzrechtlichen Anforderungen im öffentlich-rechtlichen Rundfunk zu gewährleisten, empfehlen sich insbesondere folgende Maßnahmen:[2]

1. Erarbeitung gemeinsamer Vorgaben und Standards im öffentlich-rechtlichen Rundfunk

Die Datenverarbeitungsprozesse und die damit verbundenen datenschutzrechtlichen Löschverpflichtungen sind im öffentlich-rechtlichen Rundfunk weitgehend identisch. Daher liegt es nahe, dass die Verantwortlichen des öffentlich-rechtlichen Rundfunks zumindest zu zentralen Aspekten eines Löschkonzepts übergreifende bzw. gemeinsame Vorgaben und Standards verabreden und sich über Best Practices austauschen.

---

[1] Um diese Vorgabe zu erfüllen, können die Verantwortlichen personenbezogene Daten grundsätzlich sowohl löschen als auch anonymisieren. Da die Anonymisierung mit einem hohen Aufwand verbunden ist und deshalb nur im Einzelfall eine Rolle spielen wird, ist hier nur von Löschen die Rede. Die meisten der Handlungsempfehlungen gelten auch dann, wenn personenbezogene Daten anonymisiert werden.

[2] Die folgende Liste von Empfehlungen ist aus einer Prüfung der Löschkonzepte von BR, SR, WDR, Deutschlandradio und ZDF im Jahr 2022 hervorgegangen und erhebt keinen Anspruch auf Vollständigkeit.

2. Zuständigkeiten für Querschnittsaufgaben klären

Da das Löschen personenbezogener Daten häufig eine Querschnittsaufgabe ist, welche die Mitwirkung verschiedener Bereiche erfordert, sollten die Zuständigkeiten in Bezug auf die Zusammenarbeit so weit wie möglich festgelegt werden. Neben der IT-Abteilung können auch Bereiche, die für die Archivierung oder für die zentrale Entsorgung von Papierakten oder Datenträgern zuständig sind, eine Rolle spielen. Die Abgrenzung der Zuständigkeiten dieser Bereiche und die Klärung der Modalitäten der Zusammenarbeit mit ihnen können zusätzlich auch zu Synergieeffekten zwischen Datenschutz und IT-Sicherheit bzw. Archivierung führen.[3] Außerdem müssen Zuständigkeiten im Verhältnis zu Auftragsverarbeitern definiert sein. Das gilt insbesondere dann, wenn es um die Gewährleistung des Rechts auf Löschung geht.

3. Zuständigkeiten für bereichsübergreifende Vorgaben umfassend festlegen

Um sicherzustellen, dass bereichsübergreifende Vorgaben für das Löschen personenbezogener Daten wirksam und in ausreichendem Umfang vorhanden sind, sollten die Zuständigkeiten für deren Entwicklung umfassend geregelt sein. Dazu gehören die Zuständigkeiten für die Entwicklung neuer Vorgaben, deren Implementation, die Überprüfung der Einhaltung sowie Weiterentwicklung bestehender Vorgaben.[4]

Da diese Aufgaben neben dem Wissen über datenschutzrechtliche Vorgaben Kenntnisse der spezifischen Datenverarbeitungstätigkeiten und damit verbundene Unterstützung erfordern, liegt es nahe, für die relevanten Bereiche die Funktion einer Datenschutzkoordination einzurichten und die jeweiligen Personen an der Entwicklung bereichsübergreifender Vorgaben zu beteiligen.

4. Umsetzungsvorgaben für Softwaresysteme, manuelle Prozesse und Auftragsverarbeiter

Aufgrund der sehr unterschiedlichen Anforderungen an die Löschung von personenbezogenen Daten, die über Softwaresysteme, in Papierform und durch Auftragsverarbeiter verarbeitet werden, sollten die Umsetzungsvorgaben zwischen diesen drei Bereichen unterscheiden.[5]

5. Einbindung der Löschvorgaben in regelmäßige Informations- und Schulungsverfahren

Damit das Löschen personenbezogener Daten als Teil des Regelgeschäfts begriffen und umgesetzt wird und alle zuständigen Personen in der Lage sind, die für sie relevanten Informationen zu finden, sollten alle Vorgaben in regelmäßige Informations- bzw. Schulungsverfahren eingebunden werden.

---

[3] Siehe dazu auch Hammer, Volker (2022). Das große Reinemachen: Standards für Löschkonzepte und ihr Nutzen für die Informationssicherheit, <kes> 02/2022, S. 16-24, https://www.kes.info/archiv/heft-archiv/jahrgang-2022/ausgabe-20222/.

[4] Siehe dazu auch Hammer, Volker; Schuler, Karin (2022). DIN „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten", Version 1.0.4, S. 39f. https://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler.pdf.

[5] Hammer & Schuler (2022), S. 31-38.

6. Aufbau von bzw. Einbindung in bestehende Review- und Monitoring-Prozesse

Für ein kontinuierliches Monitoring bzw. regelmäßige Reviews der Löschvorgaben ist die Vorgabe entsprechender Prozesse und Zuständigkeiten sinnvoll. Nach Möglichkeit bietet es sich außerdem an, bestehende Review- und Monitoring-Prozesse (z. B. für das Verzeichnis von Verarbeitungstätigkeiten) zu erweitern.

7. Vorgabe von Standardlöschfristen für verschiedene Datenkategorien

Um die zuständigen Personen beim Festlegen konkreter Löschfristen für die von ihnen verwalteten Daten zu unterstützen, empfiehlt es sich, einen Katalog von technikunabhängigen Löschregeln für verschiedene Datenkategorien anzulegen.[6]

8. Vorgaben und Standards für die Verwendung von Zeitstempeln

Damit insbesondere bei manuell verarbeiteten Daten erkennbar ist, wann der Start- und Endzeitpunkt der Löschperiode erreicht ist, sollten die Verantwortlichen des öffentlich-rechtlichen Rundfunks die Verwendung von automatisiert oder manuell vergebenen Zeitstempeln vorsehen sowie ggf. die zuständigen Mitarbeiter*innen dazu auffordern, diese zu vergeben.[7]

9. Vorgaben und Standards für wirksame Löschmethoden und Berechtigungskonzepte

Die Verantwortlichen des öffentlich-rechtlichen Rundfunks sollten Vorgaben zu Löschmethoden und Berechtigungskonzepten entwickeln. Um die Notwendigkeit dieser Schritte zu verdeutlichen, ist es sinnvoll, in Vorlagen für die Erfassung von Löschkonzepten bzw. das Verarbeitungsverzeichnis Informationen zu Löschmethoden und -berechtigungen abzufragen.

Um die zuständigen Personen bei der Auswahl einer geeigneten Löschmethode und bei der Bestimmung geeigneter Löschberechtigungen zu unterstützen, sollten die Verantwortlichen zudem Standards bestimmen. Beispielsweise sollten Löschungen möglichst automatisiert erfolgen. Weitere Standards könnten sich auf erforderliche Funktionen technischer Systeme beziehen, die etwa bei deren Einführung zu berücksichtigen sind.[8] Dazu zählt z. B., dass technische Systeme beim Löschen die Integrität des verbleibenden Datenbestandes gewährleisten und das gezielte Aussetzen und Unterbrechen von Löschungen ermöglichen sollten. Berechtigungssysteme sollten unbefugte Löschvorgänge verhindern, und dokumentieren, wer eine Löschung durchgeführt hat.

10. Vorgaben und Standards für die Prüfung und Dokumentation von Löschungen

Die Verantwortlichen des öffentlich-rechtlichen Rundfunks sollten Vorgaben zur Prüfung und Dokumentation von Löschvorgängen machen. Um die Notwendigkeit dieser Schritte zu verdeutlichen, ist es sinnvoll, in Vorlagen für die Erfassung von Löschkonzepten Informationen zu Prüf- und Dokumentationsverfahren abzufragen.

---

[6] Hammer & Schuler (2022), S. 13-30.
[7] Baustein 60 „Löschen und Vernichten“ des Standard-Datenschutzmodells (SDM), Version V1.0a, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf, M60.S07.
[8] SDM M60.S04-5, M60.S09-10, M60.P06 und M60.P08.

Darüber hinaus können die Verantwortlichen Standards für wirksame Prüfmethoden festlegen und Best Practices – wie z. B. Löschung ausschließlich gemäß dem Vier-Augen-Prinzip oder regelmäßige Erinnerungen an erforderliche Prüfungen durch automatisierte Wiedervorlagen – kommunizieren.[9] Für die Dokumentation von Löschvorgängen sollten sie ebenfalls Standards festlegen, die sicherstellen, dass Löschbelege datensparsam, vollständig, für Dritte nachvollziehbar und bei Bedarf verfügbar sind.[10] Dazu ist u. a. zu klären, wie sichergestellt ist, dass die Löschung auch Kopien und Backups umfasst, welche Angaben die Dokumentation zu enthalten hat, wie sichergestellt ist, dass Löschprotokolle keine löschpflichtigen Daten enthalten, sowie wo und für wie lange Löschbelege gesammelt werden. Insbesondere für manuelle Löschungen bieten sich Löschbelegvorlagen für die Dokumentation an.

11. Vorgaben für Weisungen an und Prüfung von Auftragsverarbeitern bzgl. des Löschens

Um sicherzustellen, dass Auftragsverarbeiter vertragliche Vereinbarungen auch tatsächlich umsetzen, sind zusätzliche Weisungen und Prüfungen sinnvoll. Die Rundfunkanstalten und ihre Beteiligungsgesellschaften können zuständige Personen unterstützen, indem sie z. B. in einer Checkliste vorgeben, welche Weisungen – etwa zur Festlegung der Löschfristen – erteilt werden sollten und was bei Vor-Ort-Prüfungen zu beachten ist.

November 2022
Dr. Reinhart Binder

[9] SDM M60.S.07-8.
[10] SDM M60.S05-6.