4.19 Dienstanweisung zum Schutz personenbezogener Daten im NDR (Dienstanweisung Datenschutz)

Norddeutscher Rundfunk
Der Intendant

1 Zielsetzung

Alle Beschäftigten des NDR haben im Zusammenhang mit dienstlichen Tätigkeiten Zugang zu und Umgang mit personenbezogenen Daten. Personenbezogene Daten werden an verschiedenen Stellen des NDR stationär oder mobil verarbeitet. Der sorgfältige Umgang mit allen personenbezogenen Daten, sei es zum Beispiel im Rahmen der schriftlichen, telefonischen oder elektronischen Korrespondenz, in der Aktenführung oder in der sonstigen elektronischen Verarbeitung personenbezogener Daten liegt daher im Interesse aller Beschäftigten.

Ziel des Datenschutzes ist es, das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Diese Dienstanweisung dient der praktischen Umsetzung der für den Norddeutschen Rundfunk maßgeblichen datenschutzrechtlichen Vorschriften. Diese ergeben sich vor allem aus dem Rundfunkstaatsvertrag, spezifischen Vorgaben der NDR-Staatsvertragsländer (NDR-Staatsverträgen) und der Datenschutzgrundverordnung(Verordnung /EU) 2016/679-DSGVO).

Zweck der Dienstanweisung ist, die schutzwürdigen Interessen der Betroffenen (z.B. feste und freie MItarbeiter*innen, Leiharbeiter*innen, Auszubildene, Volontär*innen, Praktikant*innen, ehmalige Beschäftigte, Versorgungsempfänger*innen, Bewerber*innen) bei der Verarbeitung ihrer personenbezogenen Daten zu wahren. Die Dienstanweisung gilt für alle Beschäftigten des NDR.

Sofern diese Dienstanweisung das Verarbeiten personenbezogener Daten regelt, gilt sie als Erlaubsnisvorschrift gemäß Art. 88 Abs. 1 DSGVO i.V.m. Erwägungsgrund 155.

2 Begriffsbestimmungen

2.1 Personenbezogene Daten

sind gemäß Art. 4 Ziffer 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar kann eine natürliche Person sein, wenn sie direkt oder indirekt insbesondere aufgrund Zuordnung zu einer Kennung

- wie einen Namen
- zu einer Kennnummer (z.B. Personalnummer, Rundfunkbeitragsnummer, Telefon- oder Telefaxnummern)
- zu Standortdaten (z.B. eine Anschrift)
- zu einem oder mehreren besonderen Merkmalen, die Ausdruck der pysischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (z.B. ein Geburtsdatum),

identifiziert werden kann. Dazu können z. B. auch Personal- oder Gehaltsdaten und Arbeitszeiten gehören.

2.2 Verarbeitung personenbezogener Daten

ist gemäß Art. 2 Ziffer 1 DSGVO jeder elektronische oder nichtelektronische, mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation,

das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

2.3 Befugte

sind Personen, zu deren dienstlichen Aufgaben die Verarbeitung personenbezogener Daten im jeweils erforderlichen Umfang gehört. Unbefugt ist, wer die Daten nicht aus dienstlichen oder sonstigen (z. B. gesetzlich vorgeschriebenen) Gründen zulässigerweise verarbeiten darf. Unbefugt können daher auch Berechtigte sein, die bspw. andere oder mehr personenbezogene Daten verarbeiten als dienstlich veranlasst ist, diese Daten länger als dienstlich erforderlich speichern oder nicht-berechtigten Dritten Kenntnis verschaffen.

2.4 Verarbeitende Stelle

ist im Außenverhältnis zu Dritten der NDR insgesamt, im Innenverhältnis die jeweils zuständige Fachabteilung bzw. Redaktion. Die persönliche Verantwortlichkeit jeder Mitarbeiterin/jedes Mitarbeiters für die ordnungsgemäße Verarbeitung personenbezogener Daten bleibt hiervon unberührt.

2.5 Dritte

ist jede Person oder Stelle außerhalb des NDR, ausgenommen die/der jeweils betroffene Beschäftigte sowie diejenige Person oder Stelle, die personenbezogene Daten im Auftrag des NDR verarbeitet.

2.6 Maßnahmen der Rechtsmäßigkeit der Datenverarbeitung

sind alle technischen und organisatorischen Maßnahmen, die die Nutzenden ergreifen müssen, um die Grundsätze für die Verarbeitung personenbezogener Daten zu gewährleisten. Die Anforderungen sind in Ziffer 3.1 dieser Dienstanweisung beschrieben

3 Zulässigkeit der Verarbeitung personenbezogener Daten

3.1 Grundsätze

Jede Verarbeitung von personenbezogenen Daten im NDR hat sich nach folgenden Maßgaben zu richten:

- **Rechtmäßigkeit**: Für jede Datenverarbeitung ist eine Rechtsgrundlage oder Einwilligung erforderlich. Die Verarbeitung personenbezogener Daten ist verboten, es sei denn, die/der Betroffene wurde informiert und hat wirksam eingewilligt oder eine Rechtsvorschrift gestattet sie. Dabei kann es sich z. B. um eine der Erlaubnisvorschriften der DSGVO, aber auch der sonstigen gesetzlichen, tarifvertraglichen oder hausinternen Bestimmungen (bspw. Dienstvereinbarungen oder Dienstanweisungen) handeln.

- Verarbeitung nach **Treu und Glauben**: Personenbezogene Daten dürfen nicht treuwidrig verarbeitet werden, d. h. Betroffene müssen hinreichende Kenntnis von der Verarbeitung und Art und Umfang dieser erlangen können.

- **Transparenz**: Informationen und Mitteilungen zur Verarbeitung von personenbezogenen Daten sollen leicht zugänglich sowie möglichst verständlich und klar abgefasst sein.

- **Zweckbindung**: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Um dies zu gewährleisten ist z. B. vor Einführung eines IT-Systems stets von der verantwortlichen Stelle zu bestimmen und zu dokumentieren, zu

welchen Zwecken die jeweilige Verarbeitung von personenbezogenen Daten erfolgen soll. Dienstliche Unterlagen mit personenbezogenen Daten dürfen nur für dienstliche Zwecke genutzt und Dritten innerhalb oder außerhalb des Hauses auch nur insoweit zur Kenntnis gebracht bzw. zugänglich gemacht werden. Die Verarbeitung muss somit zur Erfüllung der Aufgaben der verarbeitenden Stelle erforderlich sein und sie darf nur den Zwecken dienen, für die die Daten erhoben bzw. für die sie erstmals gespeichert wurden. Personenbezogene Daten dürfen nicht unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck verarbeitet, bekanntgegeben oder zugänglich gemacht werden. Ausnahmen der Zulässigkeit der Datenübermittlung an Dritte richten sich nach den gesetzlichen Vorschriften und nach Ziffer 4 dieser Dienstanweisung.

- **Datenminimierung**: jede Verarbeitung personenbezogener Daten muss dem Zweck angemessen und auf das für diesen Zweck der Verarbeitung notwendige Maß beschränkt sein. Die Verarbeitung von personenbezogenen Daten ist daher z. B. auf das für die Zweckerfüllung einer IT-Anwendung notwendige Maß zu begrenzen. Es sind so wenige personenbezogene Daten zu verarbeiten, wie zur Durchführung des konkreten Verfahrens erforderlich. Dies gilt auch für automatisierte Datenverarbeitungen.

- **Richtigkeit**: personenbezogene Daten müssen sachlich richtig und gegebenenfalls berichtigt und auf dem neuesten Stand sein.

- **Begrenzung der Speicherdauer**: Die Identifizierung der betroffenen Person darf nur so lange möglich sein, wie es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist. Speicherfristen werden vorab festgelegt und auf das unbedingt erforderliche Mindestmaß beschränkt. Für dienstliche Zwecke nicht mehr benötigte Unterlagen mit personenbezogenen Daten sind qualifiziert zu vernichten und löschen. Löschfristen ergeben sich insbesondere aus gesetzlichen Vorgaben (z. B. der Abgabenordnung, dem HGB). Der Datenbestand ist durch die/den jeweilige/n Nutzer/in regelmäßig daraufhin zu überprüfen, ob er für dienstliche Zwecke noch erforderlich ist. Anderenfalls muss er gelöscht bzw. qualifiziert vernichtet oder für den aktuellen Zugriff bzw. die weitere Verarbeitung gesperrt werden. In Zweifelsfällen ist die/der jeweilige Vorgesetzte oder die/der Rundfunkdatenschutzbeauftragte zu kontaktieren.

- **Integrität und Vertraulichkeit**: Die Sicherheit der Daten ist zu gewährleisten. Schutzwürdige personenbezogene Daten sind gegen unbefugte Einsichtnahme oder Entwendung zu schützen. Vor Verlassen des Arbeitsplatzes müssen sie angemessen gesichert, d. h. verschlossen aufbewahrt werden. Schlüssel dürfen nicht frei zugänglich, sondern müssen ihrerseits gesichert verwahrt werden. Vor Verlassen des Arbeitsplatzes muss der Computer gesperrt oder der Bildschirmschoner (mit Passwortabfrage) aktiviert werden.

- **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** (Privacy by Design and by Default): Zum effektiven Schutz personenbezogener Daten ist bereits bei der Entwicklung, Planung und Einführung von IT-Systemen durch technische und organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten nur in zulässiger Weise verarbeitet werden. Dazu sind die entsprechenden Maßnahmen für das jeweilige technische System anzuführen und die Umsetzungen sicherzustellen, z. B. durch Pseudonymisierung und Konzepte zur Datenminimierung. Soweit ein System unterschiedliche Einstellungsmöglichkeiten bietet, sind diese standardmäßig auf die datenschutzfreundlichsten Voreinstellungen zu setzen.

Zum Nachweis der Einhaltung dieser Grundsätze ist u. a. ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen. Verantwortlich dafür sind die jeweiligen Informationsverantwortlichen gemäß der Dienstanweisung zur IT-Sicherheit im NDR. Für die Erstellung des Verzeichnisses ist das von der/dem Rundfunkdatenschutzbeauftragten zur Verfügung gestellte Formular zu verwenden.

Sofern eine Datenverarbeitung aufgrund ihrer Art, des Umfangs, der besonderen Umstände oder der Zwecke der Verarbeitung hohe Risiken für die Rechte und Freiheiten der Betroffenen zur Folge haben können, ist vor Aufnahme der Verarbeitung eine Datenschutzfolgeabschätzung durchzuführen und zu dokumentieren (Art. 35 DSGVO). Zu bewerten sind die Eintrittswahrscheinlichkeit und die Schwere des Risikos. Bei der Datenschutzfolgenabschätzung sind Maßnahmen, Garantien und Verfahren zu entwickeln, durch die Risiken eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen datenschutzrechtlicher Vorschiften nachgewiesen werden. Dies ist regelmäßig der Fall, wenn nach Maßgabe der IT-Sicherheit ein hoher Schutzbedarf festgestellt wird. Die/der Rundfunkdatenschutzbeauftragte ist einzubeziehen.

3.2 Berechtigungskonzept/Verpflichtung auf die Vertraulichkeit

Personenbezogene Daten dürfen ausschließlich im Rahmen der übertragenen Aufgaben verarbeitet werden. Berechtigungsprofile/Benutzerschlüssel mit Berechtigungsumfang und Zugriffsrechten sind in den jeweiligen Fachbereichen zu erstellen und zu dokumentieren.

Alle Beschäftigten sind zur vertraulichen Behandlung personenbezogener Daten verpflichtet. Die entsprechenden Verpflichtungen sind zu dokumentieren. Die Verpflichtung auf die Vertraulichkeit gilt auch nach Beendigung der Tätigkeit fort.

3.3 Verarbeitung personenbezogener Daten zu journalistischen Zwecken/Medienprivileg

Soweit personenbezogene Daten ausschließlich zu journalistisch-redaktionellen Zwecken verarbeitet werden, ist grundsätzlich weder die Einwilligung der Betroffenen noch eine spezielle Erlaubnisnorm erforderlich. Die Zulässigkeit der Verarbeitung personenbezogener Daten ergibt sich aus einer Abwägung zwischen dem Grundrecht der Rundfunkfreiheit und den Schutzrechten der Betroffenen (z. B. das allgemeine Persönlichkeitsrecht, die Religions-, Meinungs-, oder Berufsfreiheit,) und ist in § 9c und 57 RStV sowie spezifischen Vorgaben der NDR Staatsvertragsländer ausdrücklich geregelt. In Zweifelsfällen ist die/der Rundfunkdatenschutzbeauftragte zu kontaktieren.

3.4 Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis

3.4.1 Grundsatz

Personenbezogene Daten von Bewerber*innen, Volontär*innen, Hospitant*innen, Praktikant*innen, Auszubildenden, Aushilfen sowie festangestellten und freien Mitarbeiter*innen dürfen nur verarbeitet werden,

- soweit dies erforderlich ist, um das Beschäftigungsverhältnis einzugehen, durchzuführen, zu beenden oder abzuwickeln, oder um technische, organisatorische, personelle oder soziale Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes und zur Aufrechterhaltung der Sicherheit durchzuführen, oder
- soweit eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, soweit diese Daten nicht mehr benötigt werden, es sei denn, dass Rechtsvorschriften entgegenstehen.

3.4.2 Umgang mit Bewerber*innendaten

Sobald feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt, sind die personenbezogenen Daten der Bewerberin/des Bewerbers unverzüglich zu löschen, es sei denn, dass die betroffene Person in die weitere Verarbeitung einwilligt oder überwiegende berechtigte Interessen der Datenverarbeitenden Stelle der Löschung entgegenstehen.

3.4.3 Personalaktendaten

Für alle Beschäftigten wird eine Personalakte geführt. Zweck einer Personalakte ist, möglichst lückenlos über die beschäftigte Person und ihrer dienstlichen Laufbahn Aufschluss zu geben. Eine Personalakte ist daher eine Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse eines Beschäftigten betreffen und in einem inneren Zusammenhang mit dem Beschäftigungsverhältnis stehen. Die Personalakte ist vollständig, richtig und wahrheitsgemäß zu führen. Bestandteile einer Personalakte sind zum Beispiel:

- Bewerbungsunterlagen
- Daten zur Ausbildung, Fortbildung und zum beruflichen Werdegang
- Arbeitsverträge und darauf bezogene Ergänzungen
- Zeugnisse
- Arbeitsrechtliche Maßnahmen

Personalakten können auch in elektronischer Form geführt werden. Sie sind stets vertraulich zu führen und besonders vor einem Zugriff nicht befugter Personen zu schützen. Der Kreis zugriffsberechtigter Personen ist möglichst klein zu halten und durch ein Zugriffs- und Berechtigungskonzept (Lesen, Schreiben, Ändern, Löschen, Drucken) zu definieren.

Die Personalakten werden an der jeweils zuständigen Stelle geführt. Soweit es aus Gründen der Betriebsorganisation erforderlich ist, dass auch an anderer Stelle Unterlagen aus der Personalakte über Beschäftigte aufbewahrt werden, sind die Betroffenen bei der Inanspruchnahme des Einsichtsrechts darauf hinzuweisen. Führungskräfte dürfen Ausdrucke und Kopien von Inhalten der Personalakte nicht dauerhaft aufbewahren. Diese anlassbezogen gefertigten Kopien und Ausdrucke sind unverzüglich nach Zweckerfüllung zu vernichten.

Neben einer Personalakte kann eine Nebenakte geführt werden. Zweck einer Nebenakte ist, bei der zuständigen Stelle rechtlich vorgeschriebene Dokumentationen vorzunehmen und den Kreis der Zugriffsberechtigten einzuschränken. Bestandteile einer Nebenakte können daher z. B.

- arbeitsrechtliche Maßnahmen (Abmahnungen, Ermahnungen und Rügen, die älter als 3 Jahre sind) und
- Dokumentationen aus der Dienstvereinbarung über den Umgang mit Suchtmittelmissbrauch und Maßnahmen zur Vorbeugung sein.

Korrespondenzen zu Personalvorgängen (z. B. Klärung von Planstellenkapazitäten, Berechnungen von Langzeitkonten, Prüfung arbeitsrechtlicher Maßnahmen, Korrespondenzen zur Begleitung gerichtlicher Verfahren) müssen nicht in der Personalakte oder der Nebenakte aufgenommen werden.

Beschäftigte haben einen Anspruch auf Einsicht in ihre vollständige Personalakte und Nebenakte, nicht aber in die Korrespondenzen. Sofern eine Nebenakte geführt wird, sind die Betroffenen bei der Inanspruchnahme des Einsichtsrechts darauf hinzuweisen. Das Einsichtsrecht besteht über die Dauer des Beschäftigungsverhältnisses hinaus.

Vorgesetzte dürfen Einsicht in die Personalakte nehmen, nicht aber in die Nebenakte und die Korrespondenzen.

3.4.4 Private Daten von Beschäftigten

Verarbeitungen von privaten Daten von Beschäftigten (z. B. der Studioküche, Daten aus der privaten Nutzung von IT-Diensten und IT-Endgeräten des NDR) dienen allein Abrechnungszwecken und dürfen nicht mit anderen personenbezogenen Beschäftigtendaten verknüpft werden.

3.4.5 Umgang mit Fremdpersonal

Fremdpersonal muss ebenfalls auf die Einhaltung des Datenschutzes und die Vertraulichkeit verpflichtet werden. Zuständig ist der beauftragende Bereich.

3.5 Gesundheitsdaten

Sozial- und Gesundheitsdaten dürfen nach Maßgabe des Art. 9 DSGVO nur verarbeitet werden, wenn dies eine gesetzliche Vorschrift gestattet. Diese Daten sind aufgrund ihres sensiblen Inhalts besonders zu schützen.

Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz der oder des betroffenen Beschäftigten dient. Die/der Betroffenen ist über die Verarbeitung solcher Daten stets zu informieren.

3.6 Verhaltens- und Leistungskontrolle

Soweit Beschäftigtendaten im Rahmen der Maßnahmen der Datenverarbeitung verarbeitet werden, dürfen sie nicht zu anderen Zwecken, insbesondere nicht zu Zwecken der Verhaltens- oder Leistungskontrolle, genutzt werden.

4 Übermittlung, Weitergabe

Personenbezogene Daten dürfen grundsätzlich nicht an Dritte oder Unbefugte weitergegeben werden. Im Übrigen richtet sich die Zulässigkeit der Datenübermittlung und Datenverarbeitung nach Art. 20 DSGVO, Art. 28 DSGVO. bzw. Art. 44 ff. DSGVO. Im Falle einer Auftragsverarbeitung soll eine Vereinbarung nach Maßgabe des NDR Mustervertrags zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen werden.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten ohne Kenntnis des Mitarbeiters/der Mitarbeiterin nur verarbeitet und an Dritte weitergegeben werden, wenn

- zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Mitarbeiter/die Mitarbeiterin im Beschäftigungsverhältnis eine Straftat begangen hat,
- die Verarbeitung der personenbezogenen Daten zur Aufdeckung erforderlich ist und
- das schutzwürdige Interesse des/der Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt und insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die/der Rundfunkdatenschutzbeauftragte und die zuständige Personalvertretung sind über die geplanten Maßnahmen zu informieren und zu beteiligen.

5 Versand personenbezogener Daten

Die Vertraulichkeit von E-Mails oder anderen elektronischen Kommunikationsformen im Internet ist grundsätzlich nicht gewährleistet. Für vertrauliche Informationen wird der Postweg empfohlen.

Vertrauliche Unterlagen sind, soweit sie nicht persönlich zugestellt werden, im fest verschlossenen Umschlag so zu versenden, dass personenbezogene Daten nur im unvermeidbaren Umfang erkennbar sind.

Bei jeder Art von Versand ist die Richtigkeit der Adressierung unverzüglich zu überprüfen, etwaige Fehler zu korrigieren bzw. die Verbindung unverzüglich abzubrechen.

Im Falle eines elektronischen Versands vertraulicher Daten (z. B. per Telefax oder E-Mail) soll möglichst die/der Empfänger/in über den Zeitpunkt der Übermittlung unterrichtet und – etwa durch Verschlüsslungen – sichergestellt werden, dass Unbefugte keine Einsicht erlangen können. Besonders sensible Daten, insbesondere Sozial-, Steuer- und Gesundheitsdaten sollen nicht elektronisch versandt werden, es sei denn, eine Rechtsvorschrift schreibt dies vor.

Durch die Art der Aufstellung oder geeignete organisatorische Maßnahmen muss sichergestellt werden, dass Unbefugte über IT-Endgeräte (z. B. Multifunktionsgeräte, Drucker, Telefaxgeräte, Monitore, andere vergleichbare Geräte) keine Kenntnisse von personenbezogenen Daten erlangen.

6 Einsatz von IT-Geräten und IT-Diensten

Für dienstliche Zwecke dürfen ausschließlich solche IT-Geräte und IT-Dienste eingesetzt und genutzt werden, die dem vom zuständigen IT-Bereich zuvor geprüft und im Rahmen des hierfür vorgesehenen Verfahrens genehmigt worden sind. Der Einsatz privater IT-Geräte richtet sich nach der Dienstanweisung zur Regelung privater Nutzung von IT-Diensten und IT-Endgeräten des NDR für Kommunikations-, Informationszwecke und Medienproduktion.
Dienstlich genutzte Datenträger dürfen auf externen IT-Systemen nur eingesetzt werden, wenn dies betrieblich zwingend erforderlich und gewährleistet ist, dass hierdurch die Sicherheit der IT-Systeme des NDR, beispielsweise durch die Übertragung von Viren und dergleichen, nicht gefährdet ist. Entsprechendes gilt für die Nutzung externer Datenträger in NDR-eigenen IT-Systemen.

Datenträger sind, soweit möglich, verschlossen zu halten und gesichert zu verwahren. Datenträger sind nach Ende der Nutzungszeit oder bei Defekt gesichert zu löschen bzw. zu entsorgen.

Die Dienstanweisung zur IT-Sicherheit im NDR und das IT-Sicherheitskonzept sind zu beachten.

7 Passwortschutz

Grundsätzlich soll der Zugriff auf automatisierte Anwendungen durch ein Passwort geschützt werden. Die Vergabe von Passwörtern ist nach dem IT-Sicherheitskonzept des NDR vorzunehmen. Es ist nicht zulässig, unter einer fremden Benutzerkennung zu arbeiten.

8 Allgemeine Rechte und Pflichten

8.1 Herausgabeverlangen, Äußerungsrechtliche Erklärungen

Behördliche, gerichtliche oder sonstige Ersuchen auf Herausgabe über die im NDR bzw. in seinem Auftrag verarbeiteten personenbezogenen Daten dürfen nur nach Maßgabe einer Rechtsvorschrift oder mit Einwilligung der/des Betroffenen beantwortet werden. Sowohl für das Herausgabeverlangen wie auch für die Beantwortung gilt das Schriftformerfordernis. In Zweifelsfällen über die Berechtigung und die Angemessenheit der Datenübermittlung ist die/der Dienstvorgesetzte und gegebenenfalls die/der Rundfunkdatenschutzbeauftragte einzuschalten.

Für äußerungsrechtliche Erklärungen (Gegendarstellungen, Unterlassungsbegehren und dergleichen) gelten die spezifischen Vorgaben der NDR Staatsvertragsländer.

8.2 Mitteilungspflicht

Mängel oder Auffälligkeiten in Datenverarbeitungsvorgängen sind unverzüglich der oder dem Vorgesetzten sowie der/dem Rundfunkdatenschutzbeauftragten zu melden.

Die Verletzung des Schutzes personenbezogener Daten ist von der Abteilungsleitung dem Rundfunkdatenschutzbeauftragten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung anzuzeigen. Gleiches gilt für die Maßnahmen zur Behebung der Verletzung.

8.3 Anrufung der/des Rundfunkdatenschutzbeauftragten

Alle Beschäftigten haben das Recht, sich jederzeit unmittelbar an die/den Rundfunkdatenschutzbeauftragte/n zu wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch den NDR oder die in dessen Auftrag tätig werdenden Dritten in ihren oder seinen schutzwürdigen Interessen verletzt worden zu sein. Aus der Wahrnehmung dieses Rechts dürfen der Mitarbeiterin oder dem Mitarbeiter keine Nachteile entstehen.

8.4 Sonstige Rechte

Die sonstigen Rechte der Betroffenen, insbesondere auf Auskunft über Art und Umfang gespeicherter Daten, Berichtigung usw. ergeben sich aus den für den NDR maßgeblichen Vorschriften der Datenschutzgrundverordnung und den spezifischen Vorgaben der NDR Staatsvertragsländer.

Danach kann jede/r Beschäftigte Auskunft über die zu ihrer/seiner Person verarbeiteten personenbezogenen Daten, gegebenenfalls Berichtigung, Löschung und Einschränkung der Verarbeitung verlangen oder Widerspruch einlegen (Betroffenenrechte gem. Art. 15 ff. DSGVO). Unter den Voraussetzungen von Art. 20 DSGVO kann zudem ein Recht auf Datenübertragung in Betracht kommen. Außerdem besteht das Recht, sich bei einer Aufsichtsbehörde zu beschweren, wenn nach Ansicht der/des Beschäftigten ein Verstoß gegen das Datenschutzrecht vorliegt. Zuständige Aufsichtsbehörde für den NDR ist die/der Rundfunkdatenschutzbeauftragte.

Hamburg, 22. Juli 2019

gez. Lutz Marmor

Inhalt drucken