IT-Benutzerrichtlinie & Datensicherheitskonzept für Mitarbeitende der ndF-Gruppe

Stand: 11.09.2023
Klassifikation: INTERN

Eigener: Philip Essinger (externer DSB), Michael Werkmeister (ndF)
Status: freigegeben
Version: 1.0

Änderungsprotokoll

Datum	Version	Erstellt von	Beschreibung der Änderung(en)

Inhaltsverzeichnis

A. Allgemeines

Zweck und Ziel

Diese Richtlinie beschreibt die von der **ndF-Firmengruppe** getroffenen Maßnahmen zum Schutz von personenbezogenen und sonstigen Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeitende und ist darüber hinaus eine grundlegende Information für alle Mitarbeitenden im Hinblick auf den Umgang mit Daten sein.

Diese Richtlinie konkretisiert damit die umfassende **Datenschutzrichtlinie der ndF** (**Anlage 1**) und gibt konkrete Hinweise und Vorgaben zu deren praktischer Umsetzung.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden der neue deutsche Filmgesellschaft mbH sowie ihrer Beteiligungsunternehmen mit Ausnahme der folgenden Unternehmen:

- Securitel Film + Fernsehproduktions- und Verlagsgesellschaft mbH,
- DKF Deutsche Kriminal-Fachredaktion GmbH,
- Spin TV special interest GmbH,
- Schwarm TV Production GmbH & Co. KG und Schwarm TV Production Beteiligungs GmbH,

(im weiteren „ndF“). Dazu gehören alle Festangestellten, Teilzeit- und befristet Angestellte, Auszubildende, Werkstudenten sowie Aushilfskräfte etc..

Auch externe Personen, die regelmäßig in Unternehmen der ndF-Gruppe tätig sind und/oder einen ndF-Account benutzen, wie zum Beispiel Dienstleister auf Werkvertragsbasis, sind verpflichtet, sich an diese Richtlinie zu halten. Die ndF wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat (in der Regel durch Unterschrift der „**Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes**“ – Muster-Dokument der aktualisierten Fassung vom 15.06.2023 als **Anlage 3**).

Verantwortlichkeiten

Für die Einhaltung dieser IT-Richtlinie sind alle Mitarbeitenden der ndF verantwortlich. Bei der Benutzung der IT-Systeme und Applikationen im Unternehmen sind von den Mitarbeitenden die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten Mitarbeitende unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihre*n Vorgesetzte*n zur Klärung zu wenden.

Schulungen

Die ndF trägt Sorge dafür, dass die Mitarbeitenden die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind. Darüber hinaus werden die Mitarbeitenden in regelmäßigen Intervallen zum Umgang mit personenbezogenen Daten in einer Datenschutzschulung unterrichtet.

B. Datenschutzorganisation

(1) Die ndF hat nach Maßgabe des Art. 37 DSGVO, § 38 BDSG einen betrieblichen **Datenschutzbeauftragten** (DSB) bestellt.

Kontaktdaten des Datenschutzbeauftragten: datenschutz@ndf.de

Der DSB nimmt die ihm zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation war. Er berichtet unmittelbar der Geschäftsführung.

(2) Der DSB unterrichtet und berät die Geschäftsführung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeitenden. Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichen beratend bei der Abschätzung des Risikos zur Seite.

(3) Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Geschäftsführung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

(4) Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden liegt die bearbeitende Zuständigkeit bei dem DSB. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen Betroffener.

(5) Zur operativen Umsetzung der zur Einhaltung der Datenschutzvorschriften erforderlich Maßnahmen und Prozesse hat die ndF den Head of IT & Operations als **Datenschutzkoordinator** bestimmt. Die wesentlichen Aufgaben des Datenschutzkoordinators sind:

- Schnittstelle zwischen DSB und Mitarbeitenden sowie Geschäftsführung
- Pflege der laufenden Datenschutz-Dokumentation
- Pflege der DSGVO-relevanten Dokumente und Bereitstellung im ndF Intranet bzw. Übermittlung an die Fachabteilungen
- Beobachtung der DSGVO-relevanten Datenverarbeitungen im Unternehmen; Dokumentation evtl. neuer Verfahren und Hinweis bei evtl. unzulässigen Verfahren
- Ansprechpartner für Auskünfte bei einfachen Datenschutz-Anfragen von Mitarbeitenden und Geschäftsführung und Beratung bei Datenschutz-Fragen

Die Mitarbeitenden werden aufgefordert, sich bei Fragen zum Thema Datenschutz zunächst an den Datenschutzkoordinator zu wenden.

Kontaktdaten des Head of IT & Operations / Datenschutzkoordinator: it@ndf.de.

(6) Jeder Mitarbeitende kann sich mit Hinweisen, Anregungen oder Beschwerden unmittelbar und direkt an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

(7) Der DSB berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Dieser Jahresbericht wird der erweiterten Geschäftsleitung, den Abteilungsleitungen sowie sonstigen leitenden Mitarbeitenden zur Verfügung gestellt.

C. Regelungen und Festlegungen

1. Installation von Software und Zusatzhardware

Die IT-Ausrüstung wird den Mitarbeitenden durch die IT-Abteilung zur Verfügung gestellt. Aktualisierungen erfolgen ausschließlich durch die IT. Es ist nicht gestattet, selbstständige Installation von Hard- oder Software vorzunehmen. Ausnahmen bedürfen einer ausdrücklichen schriftlichen Freigabe durch die IT mit zusätzlicher Genehmigung der Geschäftsführung.

Ausgenommen hiervon sind die von der IT im Microsoft Store auf dem jeweiligen PC / Notebook sowie Apple Store bzw. Google Play Store auf Mobilgeräten freigegebenen Programme/Apps (hier finden sich diverse nützliche Hilfsprogramme) , die von den Mitarbeitenden selbständig über den jeweiligenStore installiert werden können.

2. Einsatz von Firmensoftware auf privaten PCs der Mitarbeitenden

Sowohl der Einsatz von Firmensoftware auf privaten Computern als auch die Weitergabe einer Firmenlizenz an Dritte sind nicht gestattet. Darin eingeschlossen ist die Installation von Microsoft 365-Programmen mit Firmenlizenz, die auf privaten Geräten ebenfalls nicht gestattet ist. Ausnahmen bedürfen einer ausdrücklichen schriftlichen Freigabe durch die IT mit zusätzlicher Genehmigung der Geschäftsführung.

3. Nutzung privater Geräte der Mitarbeitenden in Firmennetzen

Es ist nicht gestattet, private Geräte an das interne Netzwerk der ndF anzuschließen. Hierfür und für Gäste ist das Gast-WLAN ndFm vorgesehen. Vgl. auch Ziff. 11 Abs. 3.

4. Regelung für Bring Your Own Device (BYOD)

Bring Your Own Device (kurz BYOD) sind private mobile Geräte von Mitarbeitenden (Notebooks, Smartphone und andere Geräte), die in das Firmennetzwerk integriert werden, auf denen Unternehmensdaten gespeichert und/oder verarbeitet werden oder mit denen auf Mircrosoft-365-Daten der ndF zugegriffen werden (E-Mail, OneDrive, SharePoint etc.).

BYOD ist wegen der möglichen Vermischung privater und dienstlicher Daten grds. nicht gestattet. Aus datenschutzrechtlicher Perspektive müssen geschäftliche Daten/Kontakte/Adressdaten und E-Mails von den persönlichen Daten, Kontakten und E-Mails getrennt werden.

Die ndF duldet derzeit aufgrund der besonderen Arbeitsweise bei der Film- und TV-Praxis die Verwendung privater Endgeräte zur Verarbeitung von Unternehmensdaten unter den hier beschriebenen Voraussetzungen. Die Verarbeitung von Unternehmensdaten auf privaten Endgeräten (PC, Laptop, Tablet, Smartphone etc.) bedarf in jedem Fall der Freigabe durch die IT mit zusätzlicher Genehmigung der Geschäftsführung. Antrag und Freigabe erfolgen elektronisch im **ndF: Intranet**.

Bei der Verwendung privater Endgeräte zur Verarbeitung von Unternehmensdaten müssen auf dem privaten Endgerät regelmäßig Sicherheitsupdates durchgeführt werden.

Die Mitarbeitenden sind durch die „Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes“ (vgl. **Anlage 3**) bei der Verwendung privater Endgeräte zur Verarbeitung von Unternehmensdaten zur gleichen Sorgfalt verpflichtet und unterliegen den gleichen Vorgaben wie bei der Verwendung von Firmengeräten.

Zum Umgang mit etwaigen auf privaten Geräten verbliebene Unternehmensdaten bei Beendigung des Arbeitsverhältnisses siehe Ziff. 16.

5. Regelungen für Homeoffice, Mobiles Arbeiten und Produktionsbüros

Die Arbeit im Homeoffice innerhalb der ndF-Gruppe ist in den jeweiligen Arbeitsverträgen und/oder zusätzlichen Vereinbarungen geregelt.

Zur Einhaltung der datenschutzrechtlichen Vorgaben und der IT-Sicherheit hat die ndF eine ergänzende „IT-Benutzer- und Datenschutzrichtlinie für Homeoffice, Mobiles Arbeiten und Produktionsbüros“ festgelegt

(**Anlage 2**), die sich an den „Best-Practice-Prüfkriterien“ des Bayerischen Landesamt für Datenschutzaufsicht orientiert.

Wichtig: Diese Vorgaben gelten für die **Produktionsbüros** der ndF entsprechend!

Die wichtigsten Grundprinzipien dieser Richtlinie sind:

- Sicherer Umgang mit Zugangsdaten und Befolgen der Passwort-Policy (Passwortrichtlinie)
- Nutzung von VPN (sofern zutreffend)
- Sprachassistenten wie Siri, Alexa und Co. deaktivieren
- Externe Datenträger nur in Ausnahmefällen verwenden und nur, wenn sie verschlüsselt sind (Bitlocker): Wann immer möglich Daten auf Fileserver (VPN), OneDrive oder SharePoint speichern
- Nur Software benutzen, die von der IT-Abteilung / Geschäftsführung freigegeben sind (gilt insbesondere für Videokonferenzsysteme)
- Ausschließlich Nutzung von firmeneigenen Cloud-Diensten (Microsoft 365 SharePoint, OneDrive)
- Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt oder Dritten überlassen (inklusive Kinder)

6. Sicherheitsverpflichtungen und der richtige Passwortgebrauch

Die ndF hat eine hohe Verantwortung gegenüber Auftraggebern und Mitarbeitenden, deren im IT-System vorhandene Daten vor unbefugtem Zugriff und unberechtigter Nutzung zu schützen.

Zugang zum System, Anwendungen und Daten dürfen daher nur solche Personen erhalten, welche Berechtigte im Sinne der Datenschutzgesetze sowie der mit Mitarbeitenden, Kunden und Dritten getroffenen Vereinbarungen sind. Um dies sicherzustellen ist es wichtig, diese Richtlinie und die Passwort-Policy zu befolgen.

Der Zugang zu IT-Systemen und zu Daten ist i.d.R. durch Passwörter geschützt. Grundsätzlich gibt es derzeit folgende Kategorien von Passwörtern:

- Das Zugangspasswort zum ndF-Account (Arbeitsstation, lokales Netzwerk, Microsoft 365 etc.)
- Passwörter für einzelne Anwendungen

Die IT verfolgt das Ziel, baldmöglichst und soweit mit vertretbarem Aufwand möglich, alle noch verbleibenden Accounts mit separaten Login-Daten/Passwörtern zur Steigerung der Sicherheit und zur Verbesserung der Benutzerfreundlichkeit auf Single Sign On (SSO) mit dem ndF-Account umzustellen.

Passwörter, die den Zugang zum Netzwerk, zu einzelnen Rechnern und zu Anwendungen gewähren, werden initial von der IT-Administration vergeben und dem einzelnen Benutzer bei Eintritt in ein Unternehmen der ndF-Gruppe mitgeteilt. Das jeweilige Passwort ist geheim zu halten, darf nicht niedergeschrieben und darf unter keinen Umständen an irgend eine andere Person (fern-)mündlich mitgeteilt werden, auch nicht gegenüber der IT oder deren Dienstleistern (oder Personen, die sich als solche ausgeben). Sollte das Passwort vergessen werden, so kann die IT ein neues Passwort vergeben.

Wenn ein Passwort verloren geht – also Dritten bekannt wird – muss dieses umgehend geändert werden sowie die IT-Abteilung davon in Kenntnis gesetzt werden.

7. Schutz vor Malware und Computerviren

Durch Computerviren, Würmer, Trojaner oder Ransomware (sogenannte Malware) sind die Daten der einzelnen Computer, aber auch des Firmennetzwerkes zunehmend großen Gefahren ausgesetzt. Dieses ist einerseits durch eine zunehmende Vernetzung von Computern bedingt, andererseits durch die elektronische Weitergabe von Daten (z.B. E-Mail) und/oder Datenträgern (z.B. USB-Sticks).

Aus diesem Grund sind sämtliche Computersysteme, an denen Benutzer arbeiten, mit einer Virenschutzlösung gesichert. Diese sorgt in der Regel dafür, dass Malware gezielt unschädlich gemacht wird. Zugleich wird bei einem solchen Vorfall der Benutzer am Bildschirm darüber informiert und der Vorfall wird zentral gespeichert.

Sollte trotz aller Vorsichtsmaßnahmen eine Vireninfektion aufgetreten sein, ist ohne Verzögerung die IT-Abteilung zu unterrichten. Alle betroffenen Geräte sind unverzüglich der IT zu übergeben, um das Risiko eines

Datenverlustes und die Verbreitung dieses Virus zu minimieren. Sämtliche Datenträger, die auf dem betroffenen Computer benutzt wurden, sind der IT für eine Untersuchung zu übergeben. Sollte ein einzelnes Gerät in einer Arbeitsgruppe betroffen sein, ist zusätzlich zu den oben beschriebenen Maßnahmen eine Mitteilung an alle Mitglieder dieser Arbeitsgruppe zu geben. Alle Geräte dieser Arbeitsgruppe sind zu überprüfen. Die Weitergabe von Daten oder der Datenträger ist bis zur Klärung des Vorfalles zu unterlassen.

8. Datenspeicherung und Löschung

(1) Die Speicherung von Daten erfolgt grundsätzlich ausschließlich auf den hierzu zur Verfügung gestellten Netzlaufwerken oder alternativ auf Microsoft 365 (persönliches OneDrive oder SharePoint, üblicherweise durch Zugriff im Datei Explorer/Finder und Synchronisation über den OneDrive Client). Die Datenablage auf lokalen oder mobilen Datenträgern ist explizit nicht gestattet (mit Ausnahme der mit Microsoft 365 synchronisierten Dateiordner).

(2) Eine manuelle Sicherung (das Kopieren/Herunterladen) der zentral abgelegten Daten durch den Benutzer ist nicht gestattet.

(3) Eine ausnahmsweise Speicherung auf mobilen Datenträgern oder anderen nicht von ndF bereitgestellten Cloudspeichern bedarf der schriftlichen Freigabe durch die IT mit zusätzlicher Genehmigung der Geschäftsführung.

(4) Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren. Hierzu sind die aus dem **Löschkonzept** (**Anlage 4**) bekannten Löschfristen auf die zuständigen Systeme und Datensätze anzuwenden.

(5) Private Daten dürfen weder auf Firmengeräten, noch auf einem Netzlaufwerk oder einem Cloudspeicher (Office 365, SharePoint, OneDrive) der ndF abgelegt werden.

9. Datensicherung und Datenarchivierung

Die zur Verfügung gestellten Netzwerke speichern alle Benutzerdaten zentral. Alle zentral auf Netzlaufwerken oder in Microsoft 365 gespeicherten Daten werden täglich vollautomatisch komplett gesichert.

10. Grundsätze bei der Erhebung/Verarbeitung von personenbezogenen Daten

(1) Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Die Erhebung oder Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der Datenschutzgrundverordnung (DSGVO) bzw. Bundesdatenschutzgesetz (BDSG) grundsätzlich erhoben und verarbeitet werden:

- Im Zuge der Vertragsanbahnung oder -abwicklung mit dem Betroffenen.
  Beispiel: Kunde K fordert Informationen zu Produkt X an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung des Rechtsgeschäfts erhoben und verarbeitet werden.
- Wenn und soweit der Betroffene informiert eingewilligt hat.
  Beispiel: Der Betroffene meldet sich zum Erhalt eines Newsletters an.
- Wenn eine spezielle Rechtsvorschrift außerhalb der DSGVO die Verarbeitung erfordert.
  Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).
- Wenn weitere Erlaubnistatbestände der DSGVO / BDSG vorliegen.
  Beispiel: Berechtigtes Interesse eine Überwachungskamera im Eingangsbereich zu installieren (mit Hinweis-Schild), weil mehrfach Einbrüche und Diebstähle vorgefallen sind.

(2) Personenbezogene Daten dürfen nur für einen zuvor festgelegten Zweck erhoben und verarbeitet werden. Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist nur mit einer gesetzlichen Erlaubnisnorm oder der Einwilligung des Betroffenen zulässig.

(3) Bei der Erhebung und Verarbeitung von besonderen Kategorien (z.B. rassische und ethnische Herkunft, Gesundheitsdaten, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit) personenbezogener Daten müssen die besonderen Voraussetzungen, die an deren Verarbeitung geknüpft

sind, beachtet werden. Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit ausdrücklicher Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben und verarbeitet werden. Ferner sind die zusätzlichen technischen und organisatorischen Maßnahmen, welche im Einzelfall für die Verarbeitung der Daten in Absprache mit dem DSB getroffen wurden, vom Mitarbeitenden einzuhalten. (z. B. Verschlüsselung beim Transport).

11. Internetnutzung

(1) Der Zugang zum Internet wird allen Mitarbeitenden, sofern diese für ihre Tätigkeit einen Computer benötigen, zur Verfügung gestellt. Der Internet-Zugang darf während der Arbeitszeiten nur zu dienstlichen Zwecken genutzt werden. Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch zu Lasten der ndF ist unzulässig.

(2) Die private Internetnutzung auf Firmengeräten im geringfügigen Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.

(3) Die Nutzung des Gast-WLAN „ndFm“ an den verschiedenen Standorten mit privaten Mobilgeräten ist gestattet. Absatz 2 gilt entsprechend.

(4) Der dienstliche E-Mail-Account darf nur für berufliche Kommunikation verwendet werden. Eine private Nutzung ist nicht gestattet. Privater E- Mail-Verkehr darf nur über persönliche Webmail-Dienste und im Rahmen der in Absatz 2 geregelten privaten Internetnutzung abgewickelt werden.

(5) ndF ist jederzeit berechtigt, Firewalls und andere Zugangs- und Filtersysteme einzuführen und diese soweit zu modifizieren, dass Internet-Adressen vom Zugriff der Benutzer ausgeschlossen werden können. ndF ist ferner berechtigt, Daten zu filtern und zu unterdrücken, welche nach dem jeweiligen Kenntnisstand potentiell eine Gefahr für die IT-Systeme der ndF bedeuten können (z.B. Virenbefall, Spam).

(6) ndF ist berechtigt, die Nutzung des Internets durch die Benutzer zu protokollieren und zu dokumentieren. ndF wird hierbei die Bestimmungen des DSGVO/BDSG und des TDSG beachten und sicherstellen, dass personenbezogene Daten der Nutzer nicht unzulässig erhoben oder verarbeitet werden.

(7) Der Benutzer ist darüber informiert, dass der Systembetreuer bei technischer Notwendigkeit eine arbeitsplatzbezogene Auswertung durchführen kann, welche Seiten von diesem aufgerufen wurden. Eine arbeitsplatzbezogene Auswertung bei Missbrauchsverdacht darf nur auf Anordnung der Geschäftsführung erfolgen. Im Falle des Missbrauchsverdachts wird der Benutzer auf diesen Verdacht hingewiesen und zu einer schriftlichen Erklärung aufgefordert. Hierbei wird ihm Gelegenheit gegeben, Einblick in die ihn betreffenden Protokolldateien zu nehmen.

(8) Das Herunterladen und Installieren von Software und Ähnlichem, sowie die Nutzung von Spielen und das Aufsuchen von Seiten mit Angeboten zum Herunterladen von Spielen sind nicht gestattet.

(9) Es ist ferner ausdrücklich verboten, Seiten mit pornographischen, Gewalt verherrlichenden oder rassistischen Inhalten sowie Seiten, die einen kriminellen Charakter haben, aufzurufen.

12. E-Mail-Nutzung

(1) E-Mail wird allgemein zur internen und externen Kommunikation zur betrieblichen Nutzung sowohl über Outlook, per Webbrowser (Outlook Web Access) und zum Abruf auf Mobilgeräten zur Verfügung gestellt.

ndF ist hierbei berechtigt, über Firewalls solche Anhänge zu filtern und zu unterdrücken, welche nach dem jeweiligen Kenntnisstand potentiell eine Gefahr für die IT-Systeme der ndF bedeuten können (z.B. Virenbefall, Spam). Der Benutzer hat daher keinen Anspruch darauf, dass Anhänge, welche zu E-Mails angehängt wurden, durch ndF am Arbeitsplatz des Benutzers zur Verfügung gestellt werden. Soweit technisch möglich, wird die IT in diesen Fällen den Benutzer über diese Mail und die Tatsache der Unterdrückung von Anhängen informieren.

(2) Jeder Inhaber eines E-Mail-Accounts hat im Falle einer geplanten Abwesenheit dafür Sorge zu tragen, dass während der Dauer der Abwesenheit der Absender eine Meldung über die Abwesenheit erhält (Abwesenheitsassistent). Bei längerer ungeplanter Abwesenheit wird die IT nach Absprache mit der betreffenden Abteilung einen Abwesenheitsassistent und eine Weiterleitung veranlassen.

(3) Es ist nicht gestattet, über E-Mail private Nachrichten zu versenden. Sämtliche E-Mail-Korrespondenz über den jeweiligen ndF-Account wird daher als dienstlich betrachtet und kann im Rahmen des Dienstverhältnisses vom Arbeitgeber oder auch einem Vertreter des Mitarbeitenden eingesehen werden. ndF weist darauf hin, dass auch die Nutzung des E-Mail-Verkehrs als Teil der Internetnutzung der elektronischen Protokollierung unterliegt.

(4) Es dürfen ohne vorherige ausdrückliche schriftliche Zustimmung des Empfängers keine vertraulichen Daten unverschlüsselt über das Internet versandt werden (E-Mail Versand erfolgt grundsätzlich unverschlüsselt). Beispiel: Adresslisten, Gesundheitszeugnis, ärztliches Attest, Bewerbungsunterlagen. Vertrauliche Daten können stattdessen sicher per OneDrive- oder SharePoint-Link versendet werden, vgl. unten. Eine Anleitung zur geeigneten Erstellung und zum Versand von OneDrive- oder SharePoint-Links (je nach Anwendungsfall) findet sich im **ndF Intranet**.

(5) Datenmengen, die aufgrund ihrer Größe die Kapazität eines E-Mail-Anhangs überschreiten (derzeit 20 MB), dürfen ausschließlich per Link über das firmeneigene Microsoft 365 OneDrive bzw. SharePoint verschickt werden. Die Nutzung anderer vergleichbarer Dienste, wie zum Beispiel Dropbox oder mit weTransfer ist ausdrücklich nicht gestattet.
Diese Versandmethode eignet sich grundsätzlich auch für kleinere Dateien vertraulichen Inhalts, da hierüber eine verschlüsselte Übertragung sichergestellt werden kann (vgl. vorhergehender Absatz).

(6) Bei E-Mails mit mindestens einem externen Empfänger ist grundsätzlich die zentral vorgegebene anzufügen. Die Signatur enthält die gesetzlich vorgeschriebenen Pflichtangaben gem. § 35 a GmbHG (elektronischer Geschäftsbrief). Es wird empfohlen, die Signatur grundsätzlich immer, d.h. auch an interne Mails bei anzufügen (im Outlook-Desktop-Programm kann die Signatur entfernt oder bei einzelnen Mitarbeitenden durch eine andere Signatur ersetzt werden, bei Mobilgeräten wird immer die Standardsignatur angefügt).

(7) Es ist grundsätzlich untersagt, sich mit der Firmen-E-Mail-Adresse in privaten Internet-Mailing-Listen, News-Groups oder Websites einzutragen. Begründete Ausnahmen hierzu bedürfen der vorherigen Freigabe durch die IT mit zusätzlicher Genehmigung der Geschäftsführung.

13. Externe Dienstleister und Auftragsverarbeitung

(1) Sofern externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten beauftragt werden (z.B. Erhebung, Löschung, Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur), bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, ist der DSB vor der Beauftragung unter Vorlage der Kriterien der erfolgten Auftragskontrolle zu informieren.

(2) Das erstmalige Tätigwerden des beauftragten Dienstleisters ist erst mit Vorliegen eines unterzeichneten Vertrags, welcher den Anforderungen des Art. 28 DSGVO genügt, gestattet. Der Vertragsentwurf ist vor Unterzeichnung dem DSB zur Überprüfung zu übermitteln.

14. Unrechtmäßige Kenntniserlangung von Daten („Datenpanne“ / Data Breach)

(1) Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, auf Spionage etc. ist die IT-Abteilung und der DSB unverzüglich zu informieren.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen. Näheres hierzu ist im **Meldeblatt zu Datenpannen** enthalten (**Anlage 5**).

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber Betroffenen oder Aufsichtsbehörden erfolgt ausschließlich durch die Geschäftsführung bzw. in deren Auftrag durch den DSB.

15. Verhalten bei Sicherheitsvorfällen

Sollte der Mitarbeitende bemerken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an die IT-Abteilung und an seinen/ihren Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

16. Austritt von Mitarbeitenden

Mit dem Austritt eines Mitarbeitenden aus einem Unternehmen der ndF (Beendigung des Arbeitsverhältnisses) bestätigt diese*r mit ihrer/seiner Unterschrift, dass alle von ihr/ihm erzeugten und gespeicherten Daten unwiderruflich gelöscht werden können.

Die/der Mitarbeitende hat vor seinem Austrittt sicherzustellen, dass Daten auf persönlichen Speicherorten, die für das Unternehmen und/oder für andere Mitarbeitende des Unternehmens von Bedeutung sein könnten, entsprechend übergeben werden.

Nach Beendigung des Arbeitsverhältnisses löscht der/die Mitarbeitende nach Wahl des Arbeitgebers alle im Auftrag des Arbeitgebers verarbeiteten personenbezogenen Daten und bescheinigt dem Arbeitgeber, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Arbeitgeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten geht die Verantwortung gem. Art. 4 DSGVO auf den/die Mitarbeitende*n über.

Die Personalabteilung informiert die IT-Abteilung rechtzeitig über anstehende Austritte, in der Regel mindestens zwei Werktage vorab, bei nicht geplanten Austritten unverzüglich. Im Bereich der Produktionen zu informiert die jeweilige Produktionsleitung entsprechend die IT.

IT-Equipment, welches die/der Mitarbeitende von ndF erhalten hat, ist mit einem Übergabeprotokoll zurückzugeben.

17. Weisungen

Die Mitarbeitenden sind verpflichtet, den Weisungen der IT-Abteilung und des DSB Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen der IT-Abteilung oder des DSB bestehen, muss die Geschäftsführung hinzugezogen werden.

D. Grundlagen der DSGVO nach Art. 5

1. Datensparsamkeit und Datenvermeidung

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by design").

2. Rechte von Betroffenen

(1) Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den DSB bzw. durch die Fachabteilungen, wenn eine explizite Anweisung durch die Geschäftsführung vorliegt. Auskunfts- und Einsichtsrechte von Mitarbeitenden werden durch die Personalverantwortlichen erfüllt.

(2) Sollte eine andere Stelle Informationen über Betroffene anfordern, wie bspw. Kunden oder Beschäftigte, ist eine Weitergabe von Informationen ohne dessen Einwilligung nur zulässig, wenn legitimes Interesse der ndF besteht, welche die Weitergabe rechtfertigt oder eine gesetzliche Verpflichtung besteht und die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.
Bei Zweifel über eine legitime Rechtsgrundlage ist der DSB zu kontaktieren.

3. Transparenz der Datenverarbeitung

(1) Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der DSB ein Verzeichnis von Verarbeitungen gem. Art. 30 DSGVO. Der für eine neue Verarbeitung Verantwortliche bzw. der Datenschutzkoordinator meldet dieses zeitnah an den DSB gemäß den vom DSB definierten Vorgaben. Gleiches gilt für Veränderungen.

(2) Unabhängig von dieser Meldung ist der der Datenschutzkoordinator und/oder DSB bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren.

(3) Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilt er dies umgehend mit. Das Verfahren darf in diesem Fall erst nach Zustimmung des DSB durchgeführt werden. Im Zweifel entscheidet die Geschäftsführung.

E. ANLAGEN / referenzierte Dokumente

1. **Datenschutzrichtlinie der ndF**

   Download: https://www.ndf.de/fileadmin/media/documents/Datenschutzrichtlinie.pdf

2. **IT-Benutzer- und Datenschutzrichtlinie für Homeoffice, Mobiles Arbeiten und Produktionsbüros**

3. **Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes inkl. Merkblatt zu den Rechtsgrundlagen**

4. **Löschkonzept**

5. **Meldeblatt zu Datenpannen**

Anlage 2: IT-Benutzer- und Datenschutz-richtlinie für Homeoffice, Mobiles Arbeiten und Produktionsbüros

Anlage zur IT-Benutzerrichtlinie & Datensicherheitskonzept für Mitarbeitende der ndF-Gruppe

Stand: 11.09.2023
Klassifikation: INTERN

Eigener: Philip Essinger (externer DSB), Michael Werkmeister (ndF)
Status: freigegeben
Version: 1.0

Änderungsprotokoll

Datum	Version	Erstellt von	Beschreibung der Änderung(en)

IT-Benutzer- und Datenschutzrichtlinie für Homeoffice, Mobiles Arbeiten und Produktionsbüros

Anlage zur IT-Benutzerrichtlinie & Datensicherheitskonzept für Mitarbeitende der ndF-Gruppe

Die Arbeit im Homeoffice innerhalb der ndF-Gruppe ist in den jeweiligen Arbeitsverträgen und/oder zusätzlichen Vereinbarungen geregelt.

Zur Einhaltung der datenschutzrechtlichen Vorgaben und der IT-Sicherheit hat die ndF als Ergänzung zur Anlage zur „IT-Benutzerrichtlinie & Datensicherheitskonzept für Mitarbeitende der ndF-Gruppe“ eine ergänzende „IT-Benutzer- und Datenschutzrichtlinie für Homeoffice, Mobiles Arbeiten und Produktionsbüros“ festgelegt, die sich an den „Best-Practice-Prüfkriterien“ des Bayerischen Landesamt für Datenschutzaufsicht orientiert.

Wichtig: Diese Vorgaben gelten für die **Produktionsbüros** der ndF entsprechend!

1. Arbeitsumgebung

Bei der Arbeit zu Hause soll die Umgebung so ausgestaltet sein, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

- Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook oder in die Papierunterlagen werfen können.
- Arbeitsunterlagen werden am Ende des Tages so in einem Schrank o.ä. verschlossen, dass diese für Dritte (inkl. Familienmitglieder und Mitbewohner) nicht ohne Weiteres zugänglich sind. Die ndF stellt Mitarbeitern auf Anfrage geeignete verschließbare Mappen, Rollcontainer o.ä. zur Verfügung oder übernimmt die Kosten für die Anschaffung.
- Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
- Sperrung des Notebooks bei Verlassen des Arbeitsplatzes falls ein anderer Zugriff (z. B. Kinder, Katze) nicht ausgeschlossen ist (Windows: Windows-Taste ⊞ + L / Mac: control + command + Q)
- Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz, …)
- Sprachassistenten wie Siri, Alexa und Co. werden deaktiviert!

2. Genutzte Hardware

- Es werden nur von der ndF gestellte Notebooks und Smartphones verwendet.
- Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt.
- Die dienstlichen Geräte werden nicht an Dritte zur Nutzung weitergegen, dies schließt Familienmitglieder inkl. Kinder mit ein.

3. Umgang mit Papierdokumenten

Noch nicht alle Arbeitsabläufe sind komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen Risiken, die in den Räumlichkeiten des Büros so nicht auftreten.

- Papierunterlagen werden in geeigneten Mappen (mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen.
- Papierunterlagen werden beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant, …) ausgesetzt.
- Entsorgung von Papierunterlagen erfolgt nicht über den Hausmüll, sondern entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 (nach DIN 66399).
- Es wird über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen oder Haustiere zerreißen ein Originaldokument) sensibilisiert und es wird bei solchen Dokumenten mit Kopien gearbeitet, sofern möglich.

4. Nutzung von Videokonferenzsystemen

Bei der Auswahl von Videokonferenzlösungen, mit denen Präsenzbesprechungen ersetzt werden sollen, müssen bestimmte Anforderungen beachtet werden:

- Es wird ausschließlich Microsoft Teams im Rahmen des ndF Microsoft 365 Accounts verwendet.

5. Sicherheit

Das eigene Homeoffice gilt als virtuelles Büro. Durch die Anbindung an das Internet erhöhen sich dabei die Sicherheitsrisiken enorm. Technische Lösungen helfen, diese Risiken zu minimieren.

- Anbindung an das Firmennetz mit verschlüsselten VPN- Verbindungen nach Stand der Technik
- Nutzung vom heimischen WLAN mit starken Passwörtern
- Nutzung öffentlicher WLAN-Hotspots nur bei durchgängig aktivierter VPN- Anbindung
- Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen oder auf Microsoft 365 (OneDrive/SharePoint)
- Keine Verwendung von externen Datenträgern (Festplatten / USB-Sticks)

6. Nutzung von Cloud-Diensten

Im Homeoffice setzt die Zusammenarbeit im Team häufig geeignete Softwarewerkzeuge, sog. Collaboration Tools, voraus. Diese können unter bestimmten Voraussetzungen eingesetzt werden.

- Es wird ausschließlich Microsoft 365 im Rahmen des ndF-Accounts verwendet.

7. Nutzung von Messenger-Diensten

Neben E-Mails werden zunehmend auch Messenger- Systeme für die interne Kommunikation eingesetzt. Die verwendeten Dienste müssen für einen aus Datenschutzsicht beanstandungsfreien Einsatz bestimmte Anforderungen erfüllen.

- Es wird ausschließlich Microsoft Teams im Rahmen des ndF Microsoft 365 Accounts verwendet.
  Die Verwendung bspw. von WhatsApp ist nicht zulässig!

Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Herr/Frau .....

nachfolgend als „**Verpflichteter**“ bezeichnet

wird hiermit seitens

neue deutsche Filmgesellschaft mbH, Kanalstraße 7, 85774 Unterföhring

nachfolgend als „**Unternehmen**“ bezeichnet

- über die einschlägigen Vorschriften der Datenschutzgrundverordnung (nachfolgend „**DS-GVO**“) und des **Bundesdatenschutzgesetzes-neu** (nachfolgend **„BDSG-neu“**) in Kenntnis gesetzt,
- über die sich daraus ergebenden besonderen Anforderungen an die Datensicherheit und den Datenschutz bei der Ausübung der jeweiligen Tätigkeit vertraut gemacht (insbesondere der **Sorgfalt- und Geheimhaltungspflichten**) und
- schriftlich auf die Wahrung der Vertraulichkeit und des Datenschutzes verpflichtet.

Etwaige darüber hinaus bestehende Geheimhaltungspflichten nach anderen Vorschriften werden durch diese Verpflichtung nicht berührt.

1. Begriffsdefinition

Die Begriffe „personenbezogene Daten und „Verarbeitung“ bzw. „verarbeiten“ verwenden wir im Sinne der gesetzlichen Definitionen. In Art. 4 DS-GVO definiert der Gesetzgeber die Begriffe wie folgt:

- Unter einer „**Verarbeitung**“ versteht die DS-GVO jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, egal ob er mit oder ohne die Hilfe automatischer Verfahren ausgeführt wird. Darunter fallen zum Beispiel 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**, der **Abgleich** oder die **Verknüpfung**, die **Einschränkung**, das **Löschen** oder die **Vernichtung von personenbezogenen Daten**.

- „**Personenbezogene Daten**“ im Sinne der DS-GVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
  Eine natürliche Person wird als identifizierbar angesehen, wenn sie direkt oder indirekt, insbesondere durch Zuordnung zu einem Namen, zu einer Kennnummer, zu Standortdaten, oder zu einer Online-Kennung identifiziert werden kann. Das gilt auch, wenn sie durch die Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person identifiziert werden kann.

2. Zulässigkeit der Datenverarbeitung

Dem Verpflichteten ist es untersagt, personenbezogene Daten zu einem anderen Zweck als **zur Erfüllung der ihm vom Unternehmen übertragenen Aufgaben** zu verarbeiten.
Im Rahmen einer zulässigen Datenverarbeitung müssen insbesondere folgende Kriterien erfüllt sein:

- Es dürfen nur die für die konkrete Aufgabenerfüllung unbedingt notwendigen Daten verarbeitet werden.
- Die Datenverarbeitung muss den Vorgaben der Datenschutzrichtlinie des Unternehmens (https://www.ndf.de/fileadmin/media/documents/Datenschutzrichtlinie.pdf), der „IT-Benutzerrichtlinie & Datensicherheitskonzept für Mitarbeitende der ndF-Gruppe“ (https://www.ndf.de/intern/it-benutzerrichtlinie, Passwort: Datenschutz) sowie den ergänzend geltenden Bestimmungen der DS-GVO und des BDSG-neu entsprechen. Die vorgenannten Richtlinien können vom Verpflichteten unter den vorgenannten URLs oder in der Personalabteilung des Unternehmens eingesehen werden. Mit der Unterschrift bestätigt der Verpflichtete, über diese Möglichkeit der Einsichtnahme unterrichtet worden zu sein.
- Alle personenbezogenen Daten dürfen nur auf die Weise verarbeitet werden, die von der Geschäftsführung des Unternehmens angeordnet wurde. Bei (vermeintlich) widersprüchlichen Weisungen und in Zweifelsfällen ist die Geschäftsführung vor der Verarbeitung zu kontaktieren.
- Eine Weitergabe personenbezogener Daten an natürliche oder juristische Personen außerhalb des Unternehmens ist nur zulässig, wenn der Verpflichtete zur Weitergabe an den jeweiligen Empfänger seitens der Geschäftsführung des Unternehmens ermächtigt wurde und für den Verpflichteten keine Umstände erkennbar sind, die Zweifel daran begründen, dass dem Empfänger ein Recht auf Kenntnisnahme zusteht.
- Durch eine Veränderung von personenbezogenen Daten (insbesondere durch Hinzuspeichern von weiteren Daten, Verknüpfung mit weiteren Daten, Weglassen von Daten) dürfen keine unrichtigen personenbezogenen Daten entstehen.

3. Sorgfalts- und Geheimhaltungsmaßnahmen

Für eine zulässige Datenverarbeitung müssen folgende Sorgfalts- und Geheimhaltungsmaßnahmen eingehalten sein:

- Daten, Programme und andere Informationen dürfen nicht zu einem anderen als dem geschäftlichen Zweck ausgelesen, abgefragt, vervielfältigt oder in sonstiger Weise genutzt werden.
- Es ist untersagt, Daten oder Programme und andere Informationen zu verfälschen, unechte Daten oder Programme herzustellen sowie vorsätzlich unechte oder verfälschte Daten und Programme zu gebrauchen.
- Ein Auslesen und/oder eine Weitergabe von Daten und/oder Programmen an Dritte ist nur mit ausdrücklicher Zustimmung der jeweils entscheidungsberechtigten Stelle zulässig.
- Die vom Unternehmen vorgegebenen technischen und organisatorischen Maßnahmen sind zu beachten. Über Aktualisierungen, auf die das Unternehmen den Verpflichteten hinweist, wird sich dieser informieren.
- Die vom Unternehmen vorgegebenen Grundsätze zur Passwortgestaltung und -verwaltung sind zu beachten.
- Datenträger sind sicher zu verwahren und vor dem Zugriff Unberechtigter zu schützen. Nicht mehr benötigte personenbezogene Datenträger müssen umgehend datenschutzgerecht vernichtet werden, damit eine missbräuchliche Weiterverwendung nicht möglich ist.
- Sonstige Unterlagen mit personenbezogenen Daten sind unter Einhaltung der vom Unternehmen vorgegebenen Sicherungsmaßnahmen vor dem Zugriff Dritter aufzubewahren.
- Zur Löschung oder zur Vernichtung vorgesehene Datenträger oder Ausdrucke sind unter Einhaltung der vom Unternehmen vorgegebenen Vorschriften zu löschen oder zu vernichten.
- Für den Fall, dass Unterlagen, Ausdrucke und Datenträger etc. mit personenbezogenen Daten aus den Geschäftsräumen des Unternehmens entfernt werden, sind geeignete Vorkehrungen zu treffen, um einen Zugriff Dritter auf die darin enthalten Informationen zu vermeiden.
- Die Verarbeitung von Unternehmensdaten auf privaten Endgeräten (PC, Laptop, Tablet, Smartphone, Datenträger) bedarf der ausdrücklichen Zustimmung des Unternehmens.
- Für den Fall von Datenpannen, die ein Risiko für die Verletzung des Schutzes personenbezogener Daten bergen, wurde im Unternehmen ein Meldeverfahren implementiert, das dem Verpflichteten bekannt zu sein hat. Darin geregelte zeitliche sowie inhaltliche Vorgaben sind unter allen Umständen einzuhalten.

4. Zeitliche Geltung der Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Die Verpflichtung zur Beachtung des Datenschutzes und zur Wahrung der Vertraulichkeit besteht ohne zeitliche Begrenzung und auch nach Beendigung der Tätigkeit fort.

5. Folgen von Verstößen gegen die Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Unter Geltung der DS-GVO können Verstöße gegen Datenschutzbestimmungen nach § 42 BDSG-neu sowie nach anderen Strafvorschriften mit **Freiheits- oder Geldstrafe** geahndet werden. Datenschutzverstöße können zugleich eine **Verletzung arbeits- oder dienstrechtlicher Pflichten** bedeuten und entsprechende Konsequenzen haben.

Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu **Ersatzansprüchen** der Betroffenen gegenüber dem Verpflichteten führen können.

Die einschlägigen Rechtsvorschriften aus der DS-GVO und dem BDSG-neu sowie in sonstigen Gesetzen enthaltener Regelungen zur Wahrung der Vertraulichkeit sind in dem **beigefügten Merkblatt** aufgelistet.

Der Empfang und die Kenntnisnahme dieser Verpflichtungserklärung samt Merkblatt wird durch Rücksendung eines unterschriebenen Exemplars bestätigt. Das unterschriebene Exemplar wird der Personalakte beigelegt.

6. Löschung und/oder Rückgabe von Daten nach Beendigung der Tätigkeit

Nach Beendigung des Vertrags löscht der Verpflichtete nach Wahl des Unternehmens alle im Auftrag des Unternehmens verarbeiteten personenbezogenen Daten und bescheinigt dem Unternehmen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an das Unternehmen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten geht die Verantwortung gem. Art. 4 DSGVO auf den/die Verpflichteten über.

_____

Merkblatt: Rechtsgrundlagen für die Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

1. Auszüge aus der Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG-neu)

Art. 5 DSGVO - Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen
   a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
   b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
   e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
   f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 6 Abs. 1 DS-GVO – Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
   a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
   b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
   c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
   d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
   e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
   f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

(2) (…)

§ 42 des BDSG-neu sieht folgende Strafvorschriften vor:

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
   1. einem Dritten übermittelt oder
   2. auf andere Art und Weise zugänglich macht

   und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
   1. ohne hierzu berechtigt zu sein, verarbeitet oder
   2. durch unrichtige Angaben erschleicht

   und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

2. Gesetz gegen unlauteren Wettbewerb (UWG)

§ 17 UWG Verrat von Geschäfts- und Betriebsgeheimnissen

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen,
   1. sich ein Geschäfts- oder Betriebsgeheimnis durch
      a) Anwendung technischer Mittel,
      b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
      c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,
      unbefugt verschafft oder sichert oder
   2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mittellungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
   1. gewerbsmäßig handelt,
   2. bei der Mitteilung weiß, dass das. Geheimnis im Ausland verwertet werden soll, oder
   3. eine Verwertung nach Absatz 2 Nummer 2 im Ausland selbst vornimmt.

(5) Die Tat wird nur auf Antrag verfolgt. es sei denn. dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(6) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.

3. Strafgesetzbuch (StGB)

§ 5 StGB Auslandstaten gegen inländische Rechtsgüter

Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden:

(…)

7. Verletzung von Betriebs- oder Geschäftsgeheimnissen eines im räumlichen Geltungsbereich dieses Gesetzes liegenden Betriebs, eines Unternehmens, das dort seinen Sitz hat, oder eines Unternehmens mit Sitz im Ausland, das von einem Unternehmen mit Sitz im räumlichen Geltungsbereich dieses Gesetzes abhängig ist und mit diesem einen Konzern bildet;

§ 202 a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.,

(2) Daten im Sinne des Abschnittes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202 b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202 a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht Ist.

§ 202 c StGB Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202 a oder§ 202 b vorbereitet, indem er
   1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs. 2) ermöglichen, oder
   2. Computerproramme, deren Zweck die Begehung einer solchen Tat ist,
      herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 263 a StGB Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 303 a StGB Datenveränderung

(1) Wer rechtswidrig Daten (§ 202 a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202 c entsprechend.

§ 303 b StGB Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
   1. eine Tat nach§ 303 a Abs. 1 begeht,
   2. Daten (§ 202 a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
   3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

   wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.
(3) Der Versuch ist strafbar.
(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
   1. einen Vermögensverlust großen Ausmaßes herbeiführt,
   2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
   3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202 c entsprechend.

3. Urheberrechtsgesetz

§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

Stand: 26.05.2018

Löschkonzept für Mitarbeitende der ndF-Gruppe

Stand: 11.09.2023
Klassifikation: INTERN

Eigener: Philip Essinger (externer DSB), Michael Werkmeister (ndF)
Status: freigegeben
Version: 1.0

Änderungsprotokoll

Datum	Version	Erstellt von	Beschreibung der Änderung(en)

Inhalt

1. Grundsätzliches

1.1 Aufbewahrung von Daten im Unternehmen

Die in einem Unternehmen verarbeiteten personenbezogenen Daten betreffen regelmäßig die eigenen Beschäftigten sowie Beschäftigte bei Geschäftskunden und Lieferanten; bietet ein Unternehmen seine Leistungen und/oder Produkte an Endkunden an, werden auch die personenbezogenen Daten dieser Kunden verarbeitet. Darüber hinaus können Daten von Menschen in unterschiedlichen Rollen verarbeitet werden, z.B. Angehörige, Gäste, Partner, Freelancer, Webseitenbesucher, etc.

Neben allgemeinen Informationen zu Personen, wie Namens-, Adress- und Kontaktdaten, fällt je nach Gruppe der Personen möglicherweise eine Vielzahl weiterer Daten an, z.B. Bank- und Zahlungsdaten, Anmeldedaten, Daten zur Qualifikation, Nutzungsdaten, Kaufhistorie.

Daten werden regelmäßig verarbeitet, um Verträge mit der Person zu erfüllen, Leistungen zu erbringen und abzurechnen, notwendige Dokumente zu erstellen, und gesetzliche Pflichten, insbesondere Aufbewahrungspflichten, zu erfüllen. Daneben bestehen eine Reihe von legitimen eigenen Zwecken des Unternehmens, z.B. Kontrolle und Verbesserung der Qualität, wirtschaftlicher Betrieb, Statistiken, Informationssicherheitsanforderungen.

In Fällen der Produkthaftung oder Gewährleistung kann Dokumentation ein wichtiges Beweismittel darstellen. Ihr Fehlen kann zu nachteiligen Konsequenzen bei einer gerichtlichen Beweiserhebung führen. Bei der Festlegung von Aufbewahrungsfristen und Interessensabwägung ist diesem Umstand Rechnung zu tragen.

1.2 Datenschutz-Grundsätze

Datenminimierung und **Speicherbegrenzung** sind Grundsätze für die Verarbeitung personenbezogener Daten und in der Datenschutzgrundverordnung (DSGVO) als gesetzliche Grundlage formuliert:

„Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen.“ (DSGVO, Erwägungsgrund 39)

Personenbezogene Daten dürfen demnach nicht zu lange aufbewahrt werden. Die genaue Dauer der Aufbewahrung richtet sich zum einen nach dem Zweck, zu dem die Daten verarbeitet werden, zum anderen nach gesetzlichen Vorschriften zur Mindestaufbewahrungsdauer, beispielsweise aus dem Handelsrecht (BGB, HGB, AO), den Sozialgesetzen (SGB) oder speziellen Rechtsvorschriften (ArbGG). In den meisten Fällen liegt die gesetzliche Aufbewahrungsfrist bei 10 Jahren. Personenbezogene Daten müssen nach Ablauf dieser Frist gelöscht werden oder anonymisiert werden.

Ausnahmen können für wissenschaftliche Forschung oder statistische Zwecke bestehen; diese müssen begründet sein und unterliegen dem Vorbehalt wirksamer Schutzmaßnahmen.

1.3 Löschpflichten im Datenschutz

Personenbezogene Daten sind zu löschen, wenn

- die Daten objektiv unrichtig sind (Daten korrigieren und ggf. falsche Daten löschen)
- die betroffene Person die Löschung verlangt und keine rechtlichen Gründe oder eindeutig überwiegende Interessen die weitere Verarbeitung bzw. Speicherung erlauben
- die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind und keine rechtlichen Gründe die weitere Aufbewahrung vorschreiben
- die betroffene Person ihre Einwilligung zur Verarbeitung widerruft und eine anderweitige Rechtsgrundlage wie z. B. gesetzliche Aufbewahrungspflichten fehlt
- die betroffene Person gemäß Art. 21 Abs. 1 Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen
- die Daten zur Direktwerbung dienen und die betroffene Person dagegen Widerspruch einlegt
- die Daten unrechtmäßig verarbeitet wurden. Unzulässig erhobene personenbezogene Daten müssen umgehend gelöscht werden, sofern keine gesetzlichen Erfordernisse eine Löschung verbieten.
- die Löschung zur Erfüllung einer gesetzlichen Verpflichtung der Verantwortlichen erforderlich ist, z.B. nationales Recht, Gerichtsurteile, oder Anordnungen einer Datenschutzaufsichtsbehörde.

1.4 Geltungsbereich

Dieses Löschkonzept gilt für die neue deutsche Filmgesellschaft mbH (ndF) sowie ihrer Beteiligungsunternehmen mit Ausnahme der Securitel Film + Fernsehproduktions- und Verlagsgesellschaft mbH, DKF Deutsche Kriminal-Fachredaktion GmbH, Spin TV special interest GmbH sowie Schwarm TV Production GmbH & Co. KG und Schwarm TV Production Beteiligungs GmbH (im weiteren „ndF") und enthält die grundlegenden, für alle Organisationsteile und Anwendungen gleichermaßen geltenden Regelungen.

Das vorliegende Löschkonzept dient als Grundlage und Nachweis der Umsetzung der Löschpflichten.

1.5 Übliche Datenkategorien

a) Beschäftigte

- Stammdaten (Anrede, Titel, Name, Geburtsdatum, Geburtsort, Familienstand, SV-Nummer, Bankverbindung)
- Adressdaten (Straße, Hausnummer, PLZ, Ort, Land)
- Kontaktdaten (private und geschäftliche Mailadressen, private und geschäftliche Telefonnummern, ggf. Soziale Medien, Messenger)
- Qualifikationsdaten (Zeugnisse, Weiterbildungen)
- Gehaltsdaten, Abrechnungsrelevante Daten zur Arbeitszeit und Arbeitsleistung
- Daten zur Beurteilung der Arbeitsleistung
- Organisatorische Daten (Funktion im Unternehmen, Kostenstellenverantwortung, etc.)
- Anmeldedaten zu IT-Systemen, Protokolldaten zur Systemnutzung
- Schriftverkehr von und an den geschäftlichen Mailaccount, Chatprotokolle

b) Beschäftigte bei Geschäftspartnern, Lieferanten

- Stammdaten (Anrede, Titel, Name)
- Kontaktdaten (Mailadressen, geschäftliche Telefonnummern, ggf. Soziale Medien, Messenger)
- Schriftverkehr von und an den geschäftlichen Mailaccount, Chatprotokolle
- Funktion im Unternehmen
- Ggf. Anmeldedaten zu IT-Systemen, Protokolldaten zur Systemnutzung

c) Kunden

- Stammdaten (Anrede, Titel, Name, ggf. Geburtsdatum)
- Bankdaten, ggf. Zahlungsdaten, ggf. Bonität
- Ggf. Anmeldedaten zu IT-Systemen, Protokolldaten zur Systemnutzung
- Schriftverkehr von und an Privatadresse/ Mailaccount, ggf. Gesprächsprotokolle (Chat, Aufzeichnung)

1.6 Abwägung hinsichtlich Aufbewahrungsfristen

Personenbezogene Daten im Rahmen des Geschäftsbetriebs und der Verwaltung werden grundsätzlich 10 Jahre aufbewahrt. Hier sind spezialgesetzliche Regelungen zur Aufbewahrung zu beachten (s. Anhang: Aufbewahrungsfristen).

Eine verlängerte Aufbewahrung aus legitimem Interesse der Klärung und Abwehr von etwaigen Schadenersatzansprüchen kann auf 30 Jahre (§ 197 I 1 BGB) verlängert werden, wenn die Betrachtung der letzten 10 Jahren eine erhöhte Wahrscheinlichkeit rechtlicher Auseinandersetzungen anzeigt.

Als erhöht gilt die Wahrscheinlichkeit, wenn

- in mehr als 5 Prozent der Fälle eine Schadenersatzforderung, Beschwerde oder Klage folgte, oder
- das durchschnittliche Schadenersatzvolumen mehr als 3 Prozent des Jahresumsatzes betrug, oder
- die Anzahl der eingereichten Klagen oder Beschwerden durchschnittlich um mehr als 5% pro Jahr stieg.

Sofern bestimmte Produkte oder Leistungen überwiegend von Klagen und Forderungen betroffen sind, ist die Geltung der verlängerten Aufbewahrungsfrist auf diese einzuschränken.

Die Organisation führt dazu im Rahmen ihrer Risikobetrachtung eine Übersicht der rechtlichen Auseinandersetzungen. Die Festlegung der Aufbewahrungsfristen sowie deren regelmäßige Überprüfung erfolgt durch die Geschäftsleitung.

2. Prozessbeschreibung

2.1 Verantwortlichkeiten

Die **Geschäftsführung** ist für die Festlegung von Aufbewahrungsfristen sowie für die Bewertung von Risiken im Zusammenhang mit der Aufbewahrung von Informationen und personenbezogenen Daten verantwortlich. Sie trifft Entscheidungen mit Wirkung für die Organisation, stellt erforderliche Ressourcen bereit und weist die Umsetzung an.

Die Festlegung der Aufbewahrungsfristen unter Berücksichtigung gesetzlicher Regelungen und berechtigter Interessen ist Aufgabe der **Fachabteilungen** bzw. der jeweiligen Leitung (Betrieb, Bereich).

Für die technische Umsetzung von Löschungen ist die **IT-Leitung** zuständig. Dies umfasst die Abstimmung mit den Fachbereichen, die Auswahl von Lösungen und Dienstleistern sowie die Umsetzung und Kontrolle der Löschpflichten.

Der **Datenschutzbeauftragte** prüft die Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen von Audits und berichtet über die Ergebnisse an die Geschäftsführung.

Alle **Beschäftigten** sind für den ordnungsgemäßen Umgang mit Informationen und personenbezogenen Daten verantwortlich. Insbesondere sind sie zur Einhaltung der Richtlinien zum Umgang mit Daten und die Meldung von Auffälligkeiten verpflichtet.

2.2 Umgang mit Löschanträgen betroffener Personen

Stellt eine betroffene Person einen Antrag auf Löschung der auf sie bezogenen Daten, wird gemäß dem festgelegten Prozess vorgegangen. Dabei wird u.a. festgestellt, ob gewichtige Gründe einer Löschung entgegenstehen, z.B.:

- Die Verarbeitung ist erforderlich zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen
- Die Verarbeitung ist aus überwiegenden berechtigten Interessen des Unternehmens weiterhin erforderlich (z.B. bei einer anstehenden oder laufenden gerichtlichen Auseinandersetzung)
- Die Verarbeitung erfolgt für wissenschaftliche Forschungszwecke oder statistische Zwecke und eine Löschung würde eine Verwirklichung dieser Zwecke nachweislich unmöglich machen.
- Die Verarbeitung (z.B. Aufbewahrung) ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich (s. oben)´

Löschanliegen betroffener Personen werden durch den Verantwortlichen unverzüglich geprüft. Das Ergebnis der Prüfung und ggf. die Löschung sollen im Regelfall innerhalb von 30 Tagen vorliegen bzw. umgesetzt sein. In begründeten Ausnahmefällen kann diese Frist auf 90 Tage verlängert werden.

3. Standards zur Löschung

3.1 Prinzipielle Löschverfahren

Die gesetzlichen Vorgaben zur Löschung sind technikneutral. Die konkrete Umsetzung der Löschung wird je Anwendung festgelegt. Folgende Möglichkeiten sind grundsätzlich gegeben und nach Eignung anzuwenden:

Anonymisieren: Entfernen von Bezügen zu einer natürlichen Person (z.B. Namen, ID-Nummern, etc.). Dabei muss sichergestellt sein, dass der Personenbezug von keiner Seite ohne unverhältnismäßig hohen Aufwand wiederhergestellt werden kann.

Überschreiben: Ein Überschreiben von Daten kann als Löschen gelten, wenn das ursprüngliche Datum auch mit technischen Mitteln nicht wiederhergestellt werden kann. Dagegen ist das Löschen einer Verknüpfung, eines Verweises, einer Zuordnungseinheit oder einer Sicht auf eine Datei keine tatsächliche Löschung. Solche Daten sind nicht gelöscht, sondern noch vorhanden und lediglich schwieriger zu finden. Sichere Löschung erfordert mehrfaches und vollständiges Überschreiben mit Nullen oder Zufallszahlen.

Verschlüsseln: Das Verschlüsseln von Daten mittels aktuell starker Verschlüsselung und das Löschen des Schlüssels führt zu einem Zustand, der als Löschung bezeichnet werden kann. Allerdings ist hierbei zu beachten, dass mit zunehmendem technischen Fortschritt Verschlüsselungsalgorithmen unsicher werden und somit keine nachhaltige Sicherheit für das Löschen von Daten darstellen.

Vernichten: Das physische Zerstören von Datenträgern, z.B. durch Shredder, oder die dauerhafte Unleserlichkeit, z.B. durch Entmagnetisierung, stellt eine Form der Löschung dar. Zu beachten ist, dass das Ergebnis der Zerstörung (z.B. Papierschnipsel, durchbohrte Festplatte) eine Wiederherstellung zuverlässig verhindern sollte. Zu große Papierschnipsel (Streifen-Shredder, einfacher Cross-Cut) oder Durchbohren bei Solid State Disks wären beispielsweise nicht geeignet; hier ist jeder Chip zu zerstören. Anhaltspunkte liefert das BSI oder die DIN 66399-1. Wo immer sinnvoll und machbar, sollte ein nach DIN 666399 zertifizierter Anbieter zur Zerstörung eingesetzt. Die Zerstörung sollte vorzugsweise auf Betriebsgelände erfolgen, oder mittels Transports in sicheren Behältern.

3.2 Zeiten und Protokollierung der Löschung

- Die Löschung von Informationen und personenbezogenen Daten erfolgt vornehmlich stichtagsbezogen.
- Mit Ablauf festgelegter Daten werden Daten, ob in Papierform oder elektronisch, sicher und datenschutzkonform gelöscht bzw. die Datenträger zerstört.
- Wo immer möglich, wird ein automatisierter Prozess verwendet.
- Protokolle der Löschvorgänge sind wo immer möglich zu erstellen und aufzubewahren.
- Sofern eine Löschung technisch bedingt nicht durchgeführt werden kann, hat eine Sperrung der Daten zu erfolgen, so dass die gespeicherten Daten nicht mehr verändert werden können. Dies betrifft insbesondere die in zentralen Anwendungen (ERP, CRM) vorgehaltenen Daten.
- Sicherungskopien und Archive sind entsprechend ebenfalls nach Ablauf der Aufbewahrungsfrist zu löschen. Sofern Sicherungen und Archive technisch bedingt noch Daten enthalten, die in den Produktivsystemen gelöscht wurden, sind diese im Rahmen des Datensicherung bzw.
- Archivierung zum nächstmöglichen Regelzeitpunkt gemäß dem festgelegten Verfahren zu behandeln (überschreiben, verschlüsseln, etc.).

3.3 Überprüfung des Löschkonzepts

Das Löschkonzept wird in regelmäßigen Zeitabständen (min. alle 2 Jahre) und darüber hinaus anlassbezogen durch die Geschäftsführung hinsichtlich seiner Angemessenheit überprüft. Bei Bedarf werden Änderungen beschlossen und angewiesen.

3.4 Löschkonzept der Anwendungen

Die spezifischen Festlegungen für die identifizierten Verfahren (Anwendungen/Systeme) sind in der Datei: **ndF-Löschkonzept-v0.2.xlsx** (Excel-Tabelle) im Detail dokumentiert.

Hierbei werden Löschverfahren, Zeitpunkte und rechtlichen Grundlagen zur Aufbewahrung/Löschung beschrieben.

Anhang

Häufig gestellte Fragen (FAQ)

Sind auch Daten in Datensicherungen zu löschen?

Ja, grundsätzlich sind alle Daten zu löschen. Sofern eine Datensicherung regelmäßig (z.B. nach 3 Monaten) komplett überschrieben ist, kann akzeptiert werden, die Daten in den Anwendungen zu löschen und die Löschung im Backup im Zuge des Überschreibe-Zyklus vorzunehmen.

Wir haben in unserer zentralen Anwendung (ERP) personenbezogene Daten, die weit über 10 Jahre zurückliegen. Ist das rechtskonform?

Möglicherweise nicht. Sofern eine Leistungsbeziehung (Vertrag) weiterhin besteht, ist dies ggf. noch vertretbar. Der Datensatz eines Kunden, der zuletzt 2007 bestellt hat, sollte im Normalfall jedoch im ERP gelöscht sein. Sofern Daten an ein Archivsystem ausgelagert wurden, sind sie dort nach Ablauf der Mindestaufbewahrungszeit zu löschen.
Für die ndF-Gruppe gilt der branchenspezifische Sonderfall, dass alle potenziellen urheberrechtlich relevanten Daten grundsätzlich bis zu 70 Jahre nach Tod des Urhebers gespeichert werden dürfen bzw. sogar müssen.

In unserem revisionssicheren Archivsystem stehen personenbezogene Daten von ehemaligen Kunden und Interessenten in unveränderbarer Form. Wir haben eine Aufbewahrungszeit von 10 Jahren festgelegt. Im ersten 11. Jahr wird innerhalb von 6 Monaten das entsprechende Jahres-Band durch Entmagnetisierung gelöscht. Ist dies vertretbar?

Ja. Beispielsweise müssen Daten aus dem Kalenderjahr 2019 bis zum 31.12.2019 aufbewahrt werden. Es ist zulässig, einen angemessenen Zeitraum zu definieren, innerhalb dessen die Löschung erfolgen muss. Allerdings gilt dies nur für Daten in Belegen mit steuerlicher Relevanz. Das Aufbewahren von Unterlagen von Personen, mit denen keine Vertragsbeziehung bestand, oder von Unterlagen ohne steuerliche Relevanz wurde von den Aufsichtsbehörden als unzulässig bewertet und mit hohen Geldbußen belegt.

Wir haben vom Finanzamt einen vorläufigen Steuerbescheid erhalten; die 10-Jahres-Frist läuft aber aus. Müssen Belege mit personenbezogenen Daten nun gelöscht werden?

Die Daten sind in jedem Fall 10 Jahre aufzubewahren. Wenn die Steuer für ein Geschäftsjahr nur vorläufig durch das Finanzamt festgesetzt wurde, dann müssen die Belege mindestens so lange aufbewahrt werden, bis der endgültige Steuerbescheid erteilt ist. Aufschiebende Wirkung können auch schwebende Verfahren, Ermittlungen oder Rechtsstreitigkeiten haben. Es empfiehlt sich daher, vor einer Löschung eine Prüfung auf mögliche Ablaufhemmnisse vorzunehmen.

Ein ehemaliger Mitarbeiter hat uns nach seiner Personalakte gefragt, da er diese im Zuge eines Rechtsstreits benötigt. Allerdings ist die Aufbewahrungsfrist vor zwei Monaten abgelaufen und die Akte ist zur Vernichtung freigegeben worden. Wie sollen wir uns verhalten?

Die Datenschutzgesetze sehen vor, dass eine betroffene Person verlangen kann, dass ihre Daten nicht gelöscht, sondern lediglich eingeschränkt („gesperrt“) werden, sofern sie diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Sofern die Akte also noch nicht vernichtet wurde, sollten Sie die betroffene Person kontaktieren und ihre Entscheidung abwarten, ob die Akte gelöscht werden kann oder nur gesperrt werden soll.

In unserem Betrieb bewahren wir Kundenakten vollständig über 30 Jahre auf, da in diesem Zeitraum noch Rechtsansprüche gestellt werden können. Ist das zulässig?

Sie können Akten über einen längeren Zeitraum als 10 Jahre aufbewahren, wenn Sie als berechtigtes Interesse ihre Verteidigung gegenüber Schadenersatzansprüchen (§ 197 BGB) geltend machen. Allerdings reicht die bloße Möglichkeit einer Schadenersatzklage nicht aus. Vielmehr muss eine entsprechende Klage auch hinreichend wahrscheinlich sein. Sollten Sie über Nachweise verfügen, dass nach Ablauf der 10 Jahre Regelaufbewahrungsfrist in einer nicht vernachlässigbaren Zahl von Fällen (z.B. mehr als 5 Prozent) Rechtstreitigkeiten folgten, ließe sich ihr berechtigtes Interesse belegen. Wenn es dagegen in den letzten 20 Jahren zu keiner Situation gekommen sein, die eine Aufbewahrung der Unterlagen erforderte, spricht die Interessensabwägung gegen die Aufbewahrung.

Glossar

Anonymisierung	Prozess, durch den personenbezogene Daten irreversibel verändert werden. Anonym ist, wer in einer Gruppe nicht identifiziert werden kann.
Aufbewahrungsfrist	Zeitraum, innerhalb dessen Datenobjekte nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein müssen
Datenlöschung	Arbeitsgang, der zur dauerhaften Entfernung von Informationen aus dem betreffenden Speicher oder Speichermedium führt.
Datenobjekte	Elemente, die Daten enthalten, wie z. B. Dateien, Dokumente, Datensätze oder Attribute
Elektronisches Archiv	Sammlung von Dokumenten in einem Speicher für historische Zwecke oder als Sicherungsmaßnahme.
Identifikation	Erkennung einer Person in einem bestimmten Bereich mithilfe einer Reihe ihrer Attribute.
Identifizierbare Person	Person, die direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren spezifischen Kennzeichen ihrer körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität.
Löschung	Prozess, durch den personenbezogene Daten so verändert werden, dass diese nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können
Löschfrist	Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden soll
Löschkonzept	Festlegungen, mit denen ein Verantwortlicher sicherstellt, dass seine Bestände an personenbezogenen Daten rechtskonform gelöscht werden.
Löschregel	Kombination aus Löschfrist und konkreter Bedingung für den Startzeitpunkt des Fristlaufs
Shreddern	Mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe
Vernichtung	Vorgang, durch den Datenträger durch mechanische Zerstörung unlesbar, unleserlich und nicht rekonstruierbar gemacht werden

Wesentliche gesetzliche Aufbewahrungsfristen

Allgemeine Aufbewahrungsfristen (Beispiele)

Art der Unterlagen	**Aufbewahrungsdauer**	**Rechtsgrundlage**
Arbeitnehmerüberlassung – Geschäftsunterlagen des Verleihers	3 Jahre	§ 7 Abs. 2 AÜG
Aufzeichnungen über Ergebnisse der Arbeitsmittelprüfung	bis zur nächsten Prüfung	§ 11 BetrSichV
Arbeitszeitnachweise (allgemein)	2 Jahre	§ 16 Abs. 2 ArbZG
Bewerbungsunterlagen	6 Monate (bis Ablauf der variablen Klagefristen)	§ 15 Abs. 4 AGG, § 61 Abs. 1 ArbGG
DEÜV-Bescheinigung über Datenübermittlungen	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres	§ 25 DEÜV
Doppelbesteuerungsbescheinigung	6 Jahre	§ 39b Abs. 6, § 41 Abs. 1 EstG
Fahrtenschreiber-Schaublätter	1 Jahr	§ 57a Abs. 2 StvZO
Fahrtkostenerstattung	6 Jahre	§ 41 Abs. 1 EStG i.V.m. R 38 der Lohnsteuerrichtlinien
Heimarbeit-Entgeltbelege	3 Jahre	§ 13 HAGDV 1
Heimarbeit-Personenlisten	bis zum Ablauf des Kalenderjahres, das auf das Jahr der Anlegung folgt	§ 9 Abs. 3 HAGDV 1
Infektionsschutzgesetz – Gesundheitszeugnis und letzte Dokumentation der Belehrung	bis zum Ausscheiden des Arbeitnehmers	§ 43 Abs. 5 IfSG
Jugendarbeitsschutz-Unterlagen	2 Jahre	§ 50 Abs. 2 JArbSchG
Ladenschlussgesetz-Verzeichnisse und Unterlagen	1 Jahr	§ 22 Abs. 3 Nr. 2 LadSchlG
Lohnkonto (Steuer)	6 Jahre	§ 41 Abs. 1 EStG
Lohnsteuerpauschalierung	6 Jahre	§ 4 Abs. 2 Nr. 8 LStDV i.V.m. § 41 Abs. 1 EstG
Lohnunterlagen (Sozialversicherung)	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres	§ 28f Abs. 1 S. 1 SGB IV
Mutterschutz-Unterlagen	2 Jahre	§ 19 Abs. 2 MuSchG

Weitere typische gesetzl. Aufbewahrungsfristen

Abmahnungen von Arbeitnehmern	Spätestens nach Ausscheiden
Abtretungsunterlagen (Zessionen)	6 Jahre
An-, Ab- und Ummeldungen der AOK und Ersatzkassen	6 Jahre
Anträge auf Arbeitnehmersparzulage	6 Jahre
Anwesenheitsliste (z.B. Stempelkarten), soweit für Lohnbuchhaltung erforderlich	10 Jahre
Arbeitsunfähigkeitsbescheinigungen (bei Auswirkung auf Lohn)	10 Jahre
Arbeitsunfähigkeitsbescheinigungen (ohne Auswirkung auf Lohn)	3 Jahre
Bankauszüge, Bankbelege	10 Jahre
Beitragsabrechnungen zur Sozialversicherung	10 Jahre
Belege, Sammelbelege, Beleglisten soweit Buchungsunterlagen	10 Jahre
Bewerbungen	6 Monate
Bewirtungsunterlagen	10 Jahre
Bürgschaftsinformationen (nach Vertragsende)	6 Jahre
Darlehensunterlagen	10 Jahre
Dauerauftragsunterlagen	6 Jahre
Debitorenbuchhaltung	10 Jahre
E-Mail mit steuerrelevantem Inhalt	10 Jahre
Essenmarkenabrechnungen	10 Jahre
Fahrtkostenerstattungsunterlagen	10 Jahre
Gehaltslisten	10 Jahre
Geschäftsbriefe	6 Jahre
Geschenknachweise	10 Jahre
Inkassobücher, -karteien, -quittungen	10 Jahre
Jahreslohnnachweise für Berufsgenossenschaften	10 Jahre
Kontoauszüge	10 Jahre
Kreditorenbuchhaltung	10 Jahre
Lastschriftanzeigen	10 Jahre

Lohnkontenarten	10 Jahre
Lohnlisten	10 Jahre
Lohnsteuer-Jahresausgleichsunterlagen	10 Jahre
Mahnvorgänge	6 Jahre
Mietverträge (nach Vertragsende)	6 Jahre
Offenbarungseidanträge	6 Jahre
Pachtverträge (nach Vertragsende)	6 Jahre
Pensionskassenunterlagen	10 Jahre
Personalunterlagen	6 Jahre
Pfändungsunterlagen	10 Jahre
Prämienunterlagen (z.B. Versicherung), soweit Buchungsunterlagen	10 Jahre
Provisionsabrechnungen mit Unterlagen	10 Jahre
Quittungen, wenn Buchungsunterlagen	10 Jahre
Rechnungen und -unterlagen	10 Jahre
Rechtsstreitfälle mit allen Unterlagen, Klageakten (nach Verfahrensabschluss)	6 Jahre
Reisekostenabrechnungen	10 Jahre
Schriftwechsel (auch innerbetrieblich)	6 Jahre
Sozialversicherungsunterlagen	6 Jahre
Spendenbescheinigungen	10 Jahre
Telefonkostennachweise	10 Jahre
Überstundenlisten (nicht buchhaltungsrelevant)	2 Jahre
Überstundenlisten (buchhaltungsrelevant)	10 Jahre
Urlaubsanträge (sofort löschen nach Abschluss des Vorgangs)	0 Jahre
Urlaubsgenehmigung (soweit buchungsrelevant z.B. wg. Urlaubsgeld)	10 Jahre
Verträge (nach Vertragsende)	6 Jahre

Verfahren zur Meldung von Datenpannen nach § 42a BDSG / Art. 33 und 34 DSGVO

Inhaltsverzeichnis

Richtlinie / Verfahren nach § 42a BDSG, Art. 33 und 34 DS-GVO

1. Informationspflichten unter dem Bundesdatenschutzgesetz

Kommt es nach jetziger Rechtslage unter dem BDSG zu einer Datenpanne, d.h. einer Verletzung von Datenschutzvorschriften, etwa weil personenbezogene Daten einem unbefugten Dritten zur Kenntnis gelangt sind oder gelangen konnten (etwa durch Hacker-Angriff, Verlust eines Datenträgers oder mobilen Endgeräts), so können Informationspflichten nach § 42a BDSG bestehen.

Nach § 42a BDSG muss zum einen unverzüglich die zuständige Datenschutzaufsichtsbehörde informiert werden. Zum anderen müssen auch die von der Datenpanne betroffenen Personen informiert und es müssen diesen geeignete Maßnahmen zur „Minderung möglicher nachteiliger Folgen“ vorgeschlagen werden. Wenn der Kreis der Betroffenen so groß ist, dass dies einen „unverhältnismäßigen Aufwand erfordern würde“, ist die „Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme“ über die Datenpanne zu unterrichten.

Die Meldepflicht des § 42a BDSG greift aber nicht bei jedem beliebigen Datenschutzverstoß, sondern nur wenn, wenn besonders „sensible“ Daten von dem Verstoß betroffen sind. So muss es sich gem. § 42a BDSG um besondere Arten personenbezogener Daten gem. § 3 Absatz 9 BDSG (z.B. Gesundheitsdaten), einem Berufsgeheimnis unterliegende personenbezogene Daten, sich auf strafbare Handlungen, Ordnungswidrigkeiten oder auf den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehende personenbezogene Daten oder personenbezogene Daten zu Bank- oder Kreditkartenkonten handeln.
Außerdem müssen durch die Datenpanne „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ drohen, was aufgrund der aufgeführten besonders sensiblen Datenbereiche allerdings der Regelfall ist.

2. Informationspflichten unter der Datenschutzgrundverordnung

Unter der Datenschutzgrundverordnung (DSGVO), welche ab Mai 2018 Geltung haben wird, werden die Meldepflichten bei Datenpannen nunmehr in zwei Vorschriften geregelt: Art. 33 DSGVO regelt die Informationspflicht gegenüber den Datenschutzaufsichtsbehörden während Art. 34 DSGVO die Anzeigepflicht gegenüber dem Betroffenen regelt.

3. Anzeige der Datenpanne bei der Datenschutzaufsichtsbehörde

Die zuständige Aufsichtsbehörde ist gem. Art. 33 DSGVO bei einer Verletzung des Schutzes personenbezogener Daten zu informieren. Eine solche Datenschutzverletzung liegt nach Art. 4 Nr. 12 DSGVO stets vor bei einer „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“

4. Verschärfte Anforderungen unter der DSGVO

Im Unterschied zu § 42a BDSG gilt die Meldepflicht unter der Datenschutzgrundverordnung nach Art. 33 DSGVO nicht nur bei Datenpannen bzgl. bestimmter „sensibler“ personenbezogener Daten (wie etwa Gesundheits- oder Bankdaten), sondern bei jeglicher Verletzung personenbezogener Daten. Einzige Einschränkung ist, dass eine Meldung an die Aufsichtsbehörde nicht erfolgen müsse, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“ Welche Erwägungen hier anzustellen sind, definiert Erwägungsgrund 75 der DSGVO.
Ein weiterer großer Unterschied zur bestehenden Rechtslage ist der Umstand, dass nach der Definition des Art. 4 Nr. 12 DSGVO für eine Meldepflicht bereits eine Datenschutzverletzung an sich ausreicht (z.B. ein reiner Datenverlust) und im Gegensatz zu § 42a BDSG ein „unrechtmäßiges Übermitteln“ oder eine „unrechtmäßige Kenntnisnahme“ von Dritten nicht erforderlich ist.
Dies stellt eine deutliche Verschärfung der Informationspflicht nach der Datenschutzgrundverordnung im Vergleich zur Rechtslage unter dem BDSG dar.
Art. 33 DSGVO sieht vor, dass die Meldung an die Datenschutzaufsichtsbehörde unverzüglich und „möglichst binnen 72 Stunden“ nach Bekanntwerden der Datenpanne erfolgen muss. Mit der Meldepflicht einher kommt eine umfassende Dokumentationspflicht gem. Art. 33 Abs. 5 DSGVO (und zwar der Datenschutzverletzung, deren Auswirkungen und den ergriffenen Abhilfemaßnahmen).

5. Bekanntgabe der Daten an die Betroffenen nach DSGVO

Bedeutet die Datenpanne „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ des Betroffenen, so ist der Betroffene unverzüglich gem. Art. 34 DSGVO von der Datenschutzverletzung „in klarer und einfacher Sprache“ zu unterrichten. Auch unter Art. 34 DSGVO kann bei „unverhältnismäßigen Aufwand“ der individuellen Benachrichtigung eine öffentliche Bekanntmachung angezeigt sein, allerdings ohne hier wie § 42a BDSG weitere Details festzulegen.

6. Ausnahmen von der Benachrichtigungspflicht

Eine Benachrichtigung des Betroffenen oder eine öffentliche Bekanntmachung kann nach Art. 34 Abs. 3 a oder b DSGVO allerdings unterbleiben, wenn insbesondere durch bereits vor der Datenpanne ergriffene technische und organisatorische Maßnahmen eine unbefugte Kenntnisnahme der Daten durch Dritte ausgeschlossen werden kann. Ein Anwendungsfall hierfür könnte etwa sein, dass etwa ein Datenträger mit hierauf gespeicherten personenbezogenen Daten verlustig gegangen ist, die personenbezogenen Daten aber ausreichend verschlüsselt sind, sodass ein Finder diese Daten nicht auslesen kann.
Eine Benachrichtigung des Betroffenen ist auch dann nicht erforderlich, wenn durch nach der Datenpanne ergriffene Maßnahmen das „hohe Risiko für die Rechte und Freiheiten der betroffenen Personen“ nicht mehr besteht. Zu beachten ist allerdings, dass auch wenn der Betroffene aus diesen Gründen (Art. 34 Abs. 3 a oder b DSGVO) nicht zu benachrichtigen ist, eine Meldepflicht gegenüber der Datenschutzaufsichtsbehörde nach Art. 33 DSGVO nach wie vor besteht.

7. Mitteilungspflicht bei Auftragsverarbeitungen

Sofern eine Datenpanne im Rahmen einer Auftragsdatenverarbeitung (oder künftig: Auftragsverarbeitung) geschieht, ist nach den Festlegungen in den notwendigen Vereinbarungen zur Auftrags(daten)verarbeitung der jeweilige Vertragspartner in der Regel zu informieren, zumindest sofern dessen Daten von der Datenpanne betroffen sind.

8. Checkliste des Data-Breach-Notification-Verantwortlichen

1. Bei Meldung der Datenpanne sind zunächst mittels des Meldeblatts nähere Informationen über den Vorfall von der meldenden Person einzuholen (***Anlage: Meldeblatt zu Datenverlust im Unternehmen***)
2. Einleitung von erforderlichen Maßnahmen mit den Fachbereichen zur Sicherung der personenbezogenen Daten bzw. um Missbrauch der personenbezogenen Daten zu verhindern oder dessen Folgen einzudämmen
3. Untersuchung des Datenverlustes mit dem Datenschutzbeauftragten, ob eine Meldeverpflichtung vorliegt. Folgende Fragen sind hierbei zu beantworten:
   - 3.1. Nach §42a BDSG
     - 3.1.1. Sind Daten im Sinne des § 42a S.1 Nr. 1-4 BDSG betroffen?
     - 3.1.2. Haben Dritte unrechtmäßig Kenntnis von den Daten erhalten?
     - 3.1.3. Drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen?
   - 3.2. Nach Art. 33 und 34 DS-GVO
     - 3.2.1. Führt die Datenpanne voraussichtlich zu einem Risiko für den Betroffenen?
     - 3.2.2. Ist das Risiko für die Rechte und Freiheiten der betroffenen Person als hoch einzustufen?
     - 3.2.3. Wurden geeignete technische und organisatorische Sicherheitsvorkehrungen im Vorfeld getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt?
     - 3.2.4. Ist das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach mit der Durchführung von nachfolgenden Maßnahmen zur Datenpanne weiter vorhanden?
     - 3.2.5. Ist die Benachrichtigung der einzelnen Betroffenen mit einem unverhältnismäßigen Aufwand verbunden?
4. Soweit es sich um einen meldepflichtigen Datenverlust handelt:
   - 4.1. Information an die zuständige Aufsichtsbehörde
   - 4.2. Abstimmung des weiteren Vorgehens mit der Aufsicht
   - 4.3. Abklärung, ob Strafanzeige zu erstatten/Strafantrag zu stellen ist
   - 4.4. Ggf. Information der Betroffenen

Anlage: Meldeblatt zu Datenverlust im Unternehmen

1. Art der Verletzung

☐ Vernichtung ☐ Verlust

☐ Veränderung ☐ unbefugte Offenlegung bzw. unbefugter Zugang

2. Wann ist die Datenpanne aufgetreten (Datum, Uhrzeit)?

3. Wann wurde das Vorhandensein einer Datenpanne festgestellt?

4. Beschreibung des Vorfalls

5. Wie viele Personen sind [ungefähr] betroffen?

6. Welche Kategorien von Personen sind betroffen?

☐ Kunden ☐ Geschäftspartner

☐ Beschäftigte ☐ Interessenten

☐ Lieferanten ☐ Berater/Handelsvertreter

☐ Ansprechpartner ☐ sonstige: _____

7. Welche Kategorien von Daten sind betroffen?

☐ Gesundheit ☐ Berufsgeheimnis

☐ Bank- oder Kreditbereich ☐ Fotos/Videos

☐ Religion ☐ Standort

☐ Sexualität ☐ Biometrie

☐ Politik ☐ Adressen

☐ E-Mail-Adressen ☐ Sonstige: _____

☐ Passwörter

8. Wie viele Datensätze sind [ungefähr] betroffen?

9. Sind Maßnahmen zur Sicherung der Daten ergriffen worden?

☐ Ja Wenn ja, welche?

☐ Nein

10. Sonstige Mitteilungen:

_____

Datum, Unterschrift des Aufnehmenden