Leitfaden für Behörden:

Das NDIG und andere Gesetze zur digitalen Verwaltung

30.06.2020

Niedersächsisches Ministerium für Inneres und Sport

Inhaltsverzeichnis

1 Einleitung

Am 24.10.2019 hat der Niedersächsische Landtag das „Gesetz zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes“ beschlossen. Das Gesetz wurde am 1.11.2019 verkündet[1]. Damit ist für Niedersachsen der rechtliche Rahmen dafür geschaffen worden, dass Bürgerinnen, Bürger, Unternehmen und Verbände zukünftig ihre Verwaltungsdienstleistungen umfassend online abwickeln können. Außerdem trifft das Gesetz Regelungen zur Informationssicherheit in der Verwaltung, um diese auch in Zukunft gegen Angriffe zu schützen. Das Gesetz enthält in Artikel 1 das „Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)“. Mit diesem Gesetz regelt Niedersachsen - wie der Bund und die anderen Länder - wichtige Rahmenbedingungen der digitalen Verwaltung. Dieser Leitfaden erläutert insbesondere für niedersächsische Behörden, welche Konsequenzen sich aus dem NDIG ergeben. Wo nötig werden auch fachliche und technische Hintergründe sowie Beweggründe für Regelungen aufgeführt.

Das Gesetz verpflichtet Behörden, z.B. zur Bereitstellung von Online-Diensten, es ermächtigt sie aber auch, bestimmte technische Verfahren einzuführen. Der Leitfaden erläutert daher insbesondere, mit welchen Maßnahmen die Behörden ihre Verpflichtungen kostengünstig und zugleich erfolgreich erfüllen können, und informiert, wo weitere Informationen zu den einzelnen Regelungen und Themen und zu deren Umsetzung zu finden sind.

Der Leitfaden soll bei der Umsetzung des NDIG helfen, er ersetzt aber natürlich nicht die gesetzliche Regelung. Es ist also weiterhin wichtig, den konkreten Wortlaut des Gesetzes zu kennen, der auch maßgeblich ist bei Fragen der Rechtsauslegung.

Neben dem NDIG gibt es weitere wichtige rechtliche Regelungen zur digitalen Verwaltung. Die wichtigsten werden in diesem Leitfaden auch berücksichtigt, insbesondere

- die Niedersächsische Verordnung über den elektronischen Rechnungsverkehr (NERechVO)[2], die auf Grundlage von § 6 Abs. 4 NDIG die Regelungen zur elektronischen Rechnungsstellung konkretisiert,
- das E-Government-Gesetz des Bundes (EGovG), auf das sich das NDIG an vielen Stellen bezieht,
- das Onlinezugangsgesetz (OZG), das Bund und Länder ab dem 1.01.2023 u.a.
    - zur elektronischen Bereitstellung aller Verwaltungsleistungen und
    - zur Bereitstellung von Nutzerkonten zur einheitlichen Identifizierung

  verpflichtet,
- die SDG[3]-Verordnung (Verordnung über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012), die u.a.
    - ab 12.12.2020 zur Bereitstellung von Informationen u.a. über Rechte, Pflichten und Vorschriften zu bestimmten Verwaltungsleistungen (SDG-Leistungen im Bereich Reisen, Arbeit, Fahrzeug, Wohnsitz, Bildung u.a.) verpflichtet (Art. 4 SDG-Verordnung),
    - ab 12.12.2020 zum elektronischen Zugang zu bestimmten Hilfs- und Problemlösungsdiensten verpflichtet,

[1] Nds. GVBl. Nr. 18/2019, ausgegeben am 1.11.2019
[2] Nds. GVBl. Nr. 9/2020, ausgegeben am 9.04.2020, sowie Nds. GVBl. Nr. 12/2020, ausgegeben am 5.05.2020
[3] SDG: Single Digital Gateway, ABl. L 295/1 vom 21.11.2018

  - ab 12.12.2023 zur Bereitstellung von Online-Diensten auch über das SDG verpflichtet (Art. 6 SDG-Verordnung),
  - ab dem 12.12.2023 zu Maßnahmen in Hinblick auf das Once-Only-Prinzip verpflichtet.

- das Niedersächsische Verwaltungsverfahrensgesetz (NVwVfG[4]) in Verbindung mit dem Verwaltungsverfahrensgesetz (VwVfG[5]), auf welches das NVwVfG dynamisch verweist und welches in § 3a VwVfG die elektronische Kommunikation in Verwaltungsverfahren regelt.

Am Ende der Kapitel sind meist Hinweise zu weiteren Informationen und Kontakten aufgeführt. Viele Projekte zur Umsetzung des OZG und des NDIG wurden und werden im Programm „Digitale Verwaltung in Niedersachsen“ (DVN) gebündelt. Auf diese Projekte wird hingewiesen, wenn sie für die Umsetzung des NDIG von besonderer Bedeutung sind. Der Leitfaden bietet aber keine vollständige Übersicht über die einzelnen Projekte des Programms DVN. Auch sei darauf hingewiesen, dass der Leitfaden die aktuelle Situation darstellt und sich insbesondere bei der Projektarbeit und den Kontaktpersonen häufig Änderungen ergeben. Das Ministerium für Inneres und Sport (MI) strebt daher an, diesen Leitfaden zu gegebener Zeit zu aktualisieren.

Bei allgemeinen Fragen zum NDIG und zum Programm digitale Verwaltung in Niedersachsen (DVN) wenden Sie sich bitte an:

eMail: digitaleverwaltung@mi.niedersachsen.de

Michael Zickler (NDIG): 0511 120 4778

Dr. Martin Hube (NDIG): 0511 120 4749

Burkhard Gärtner (Programm DVN): 0511 120 4662

Für den kommunalen Bereich ist im Programm DVN ein kommunales Kompetenzteam (KKT) eingerichtet worden. Mehr Informationen hierzu finden Sie hier im Landesintranet:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=506273&_psmand=153

Das KKT bietet auch einen geschützten Informationsbereich im Internet unter www.dvn-kommunal.de.

Das kommunale Kompetenzteam ist erreichbar unter:

eMail: kkt-digitaleverwaltung@it.niedersachsen.de

[4] Nds. GVBl. 2019, 316

[5] Neugefasst durch Bek. v. 23.1.2003 I 102; zuletzt geändert durch Art. 5 Abs. 25 G v. 21.6.2019 I 846

2 Digitale Verwaltung

Die rechtlichen Regelungen zur digitalen Verwaltung im NDIG und anderen Gesetzen beruhen auf Vorstellungen, wie die Prozesse in der digitalen Verwaltung ablaufen sollen. Sie berücksichtigen bisherige Geschäftsprozesse, versuchen aber auch, die Vorteile der elektronischen Unterstützung für die Prozessoptimierung zu nutzen. Ein hieraus resultierendes Schema eines Referenzprozesses ist in Abb. 1 dargestellt.

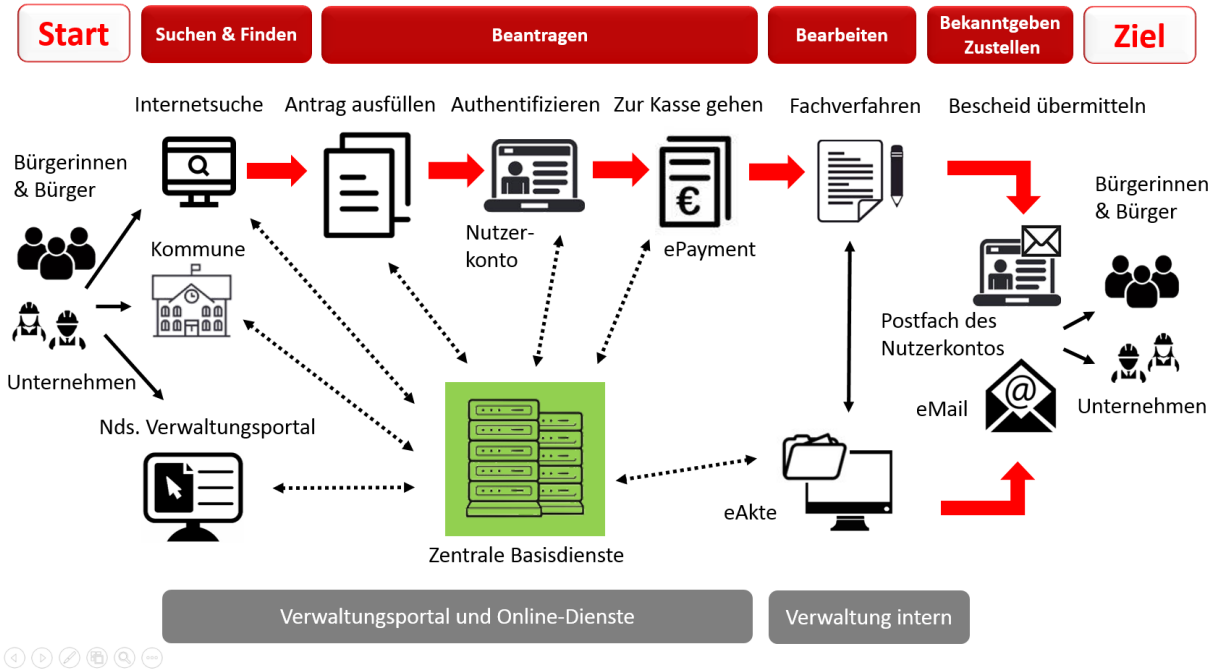


Abbildung 1 Schema für einen Referenzprozess der Verwaltung

In der Regel wenden sich Bürgerinnen, Bürger und Unternehmen an die Verwaltung mit einem Anliegen. In der digitalen Verwaltung ist es Ziel, dass hierfür, bis auf wenige Ausnahmen, kein physischer Behördengang mehr erforderlich ist. Vielmehr sollen sie ihr Anliegen von überall und jederzeit virtuell über das Internet erledigen können.

Hierfür benötigen sie zunächst Informationen zu ihrem Anliegen, die sie über eine Internetsuche finden. Daher gibt es Verpflichtungen zur Bereitstellung von Informationen zu allen Verwaltungsleistungen im Internet. Von diesem Informationsportal erfolgt die zielgerichtete Weiterleitung zu einem Online-Antragsverfahren der zuständigen Behörde. In diesem werden die erforderlichen Daten erhoben und bei Bedarf elektronische Nachweise beigefügt. In der Regel ist eine elektronische Authentifizierung erforderlich, die möglichst immer mit dem gleichen Verfahren erfolgen soll. Über ein gesondertes System erfolgt die elektronische Bezahlung. Danach werden die Antragsunterlagen elektronisch an die zuständige Behörde übermittelt, die den Antrag in einem Fachverfahren bearbeitet und die Unterlagen in einer elektronischen Akte ablegt. Die Antwort der Behörde, z.B. der Bewilligungsbescheid wird elektronisch an den Antragsteller oder die Antragstellerin übermittelt.

Um die Aufwände für die IT-Unterstützung zu minimieren, sind für nahezu alle Schritte zentrale Basisdienste sinnvoll. Das NDIG sieht daher Verpflichtungen zur Bereitstellung und Nutzung von Basisdiensten vor. Informationen und Online-Dienste sollen sowohl auf den Internetseiten der zuständigen Behörde als auch in einem niedersächsischen Verwaltungsportal zur Verfügung stehen sowie über den

bundesweiten Portalverbund und ein zentrales europaweites Portal (Single Digital Gateway) erreichbar sein, um die Auffindbarkeit zu erhöhen. Dabei wird aber immer auf das gleiche Informationssystem und die gleichen Online-Antragsverfahren zugegriffen.

Aus diesem Referenzprozess ergeben sich Regelungsbedarfe, die im NDIG und den anderen Gesetzen zur digitalen Verwaltung umgesetzt wurden.

3 Für wen gilt das NDIG?

Das NDIG verwendet für den Geltungsbereich des zweiten Teils des Gesetzes den umfassenden Behördenbegriff des VwVfG (Behörden sind alle Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen), schränkt diesen aber durch Ausnahmen vom Geltungsbereich wieder ein. Diese Ausnahmen unterscheiden sich deutlich zwischen dem Teil digitale Verwaltung (zweiter Teil des NDIG) und dem Teil Informationssicherheit (dritter Teil des NDIG).

3.1 Geltungsbereich im Teil digitale Verwaltung (zweiter Teil NDIG)

§ 3 NDIG listet die Verwaltungsbereiche auf, die von den Regelungen zur digitalen Verwaltung (§§ 4 bis 12 NDIG) ausgenommen sind. So sind öffentliche Stellen ausgenommen, deren Tätigkeiten im Schwerpunkt deutlich von dem in Kap. 2 skizzierten Referenzprozess abweichen (z.B. Hochschulen, Kirchen, Kreditinstitute, Schulen). Außerdem sind Bereiche ausgenommen, in denen bereits weitgehende spezifische Regelungen zur digitalen Verwaltung in Kraft sind (z.B. Justizverwaltung, Strafverfolgung, Finanzbehörden).

Der Schwerpunkt des Geltungsbereichs des NDIG liegt daher bei der allgemeinen Landesverwaltung (Ministerien, Landesämter, Landesbetriebe) sowie den Kommunen. Die Regelungen für die Behörden des Landes sind dabei deutlich weitgehender als für die übrigen Behörden. Natürlich sind vom NDIG immer nur die niedersächsischen Behörden betroffen

Besondere Verpflichtungen werden dem für die zentrale IT-Steuerung zuständigen Ministerium auferlegt (siehe z.B. § 12 NDIG). Dies ist zurzeit das MI. Beim MI ist zurzeit auch der oder die IT-Bevollmächtige des Landes (CIO, siehe § 2 NDIG) und die Zentralstelle für Informationssicherheit (N-CERT, siehe § 14 Abs. 1 NDIG) angesiedelt.

Für die Regelungen zum Empfang und zur Verarbeitung von elektronischen Rechnungen (§ 6 Abs. 3 und 4 NDIG) ist der Geltungsbereich wesentlich größer. Diese Regelungen gelten für praktisch alle öffentlichen Auftraggeber in Niedersachsen (siehe § 3 Abs. 6 NDIG).

Für Behörden, die aufgrund der beschriebenen Ausnahmen nicht zur Einführung der digitalen Verwaltung verpflichtet sind, ist es natürlich geboten, ebenfalls den Weg zur Digitalisierung zu finden. Soweit dies nicht ohnehin durch spezialgesetzliche Regelungen vorgegeben ist, sollten sich diese Behörden an den Regelungen des NDIG orientieren, damit Bürgerinnen, Bürger und Unternehmen einen umfassenden, aufeinander abgestimmten digitalen Service nutzen können.

Das OZG und die SDG-Verordnung sehen keine dem § 3 NDIG entsprechende Ausnahmen aus ihrem jeweiligen Geltungsbereich vor.

3.2 Geltungsbereich im Teil Informationssicherheit (dritter Teil NDIG)

Die Geltungsbereiche der Regelungen zur Informationssicherheit (§ 13 bis 30 NDIG) sind in den einzelnen Bereichen unterschiedlich festgelegt. So gelten die Verpflichtungen zur Einhaltung von Sicherheitsmaßnahmen in § 13 NDIG für alle Behörden und Gerichte des Landes, die am Landesdatennetz angeschlossen sind. Der Einsatz von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit (§§ 17 bis 30 NDIG) gilt für alle Behörden außer den Hochschulen und Forschungseinrichtungen und enthält Sonderregelungen für den Geschäftsbereich des Justizministeriums, den Landesrechnungshof, die von der oder dem Landesbeauftragten für Datenschutz geleiteten Behörde und die Landtagsverwaltung.

4 Elektronische Zugänge (§ 4 NDIG)

4.1 Warum verpflichtet das NDIG zur elektronischen Zugangseröffnung?

In der herkömmlichen Verwaltung erreicht man Behörden durch den Besuch im Amt oder per Post. In der digitalen Verwaltung werden elektronische Kommunikationsverfahren benötigt. Alle Behörden müssen über diese erreichbar sein. Bürgerinnen, Bürger und Unternehmen müssen erkennen können, welche elektronischen Kommunikationsverfahren eine Behörde anbietet. Sie müssen sich darauf verlassen können, dass die Behörden elektronische Nachrichten entgegennehmen, als rechtswirksame Anträge oder Nachweise anerkennen und bearbeiten, z.B. damit gesetzliche Fristen eingehalten werden können, und dass der Eingang von Nachrichten in den Behörden regelmäßig geprüft wird. Damit dies sichergestellt ist, verpflichtet das NDIG zur elektronischen Zugangseröffnung.

Da Bürgerinnen, Bürger und Unternehmen grundsätzlich nicht zur elektronischen Kommunikation verpflichtet werden sollen, müssen die elektronischen Kommunikationsangebote so attraktiv sein, dass sie freiwillig genutzt werden. Dies erfordert, dass die elektronischen Kommunikationsverfahren bestimmte Anforderungen erfüllen. Für eine hohe Attraktivität ist es zudem wichtig, dass die Kommunikationsangebote verschiedener Behörden so weit wie möglich einheitlich sind. Bürgerinnen, Bürger und Unternehmen sollen gleiche Kommunikationsverfahren bei verschiedenen Behörden nutzen können. Daher verpflichtet das NDIG die Behörden - mit bestimmten Ausnahmen - die gleichen Kommunikationsverfahren bereitzustellen und dort eingehende Anträge und Nachweise anzuerkennen und zu bearbeiten.

4.2 Warum mehrere elektronische Zugangsverfahren?

Damit die von den Behörden angebotenen elektronischen Kommunikationsverfahren ihren Zweck erfüllen, müssen sie je nach Situation eine oder mehrere der folgenden Anforderungen erfüllen:

- Die Kommunikation mit der Behörde muss so einfach wie möglich sein.
- Die Kommunikation muss vertraulich sein.
- Die Kommunikation muss authentisch sein. D.h. es muss feststellbar sein, wer Sender der Nachricht ist und dass die Nachricht bzw. die übersandten Dokumente nach der Versendung nicht verändert wurden.
- Die Nachricht oder die übersandten Unterlagen müssen der Schriftform genügen, d.h. sie müssen mit einem schriftformersetzenden elektronischen Verfahren übersandt werden.

Leider lassen sich diese Anforderungen nicht mit einem einzigen Kommunikationsverfahren erfüllen. Daher legt das NDIG die Zugangseröffnung für vier verschiedene Verfahren fest, die in verschiedenen Situationen jeweils eine gute Lösung darstellen. Mit Ihnen soll erreicht werden:

1. Eine sehr einfache Kommunikation (einfacher Zugang, § 4 Abs. 1 NDIG),
2. ein Universalverfahren, dass möglichst viele Kommunikationsanforderungen erfüllt (Nutzerkonto, § 4 Abs. 2 NDIG),
3. ein schriftformersetzendes Verfahren (z.B. De-Mail, § 4 Abs. 3 NDIG),
4. ein sicheres Identifizierungsverfahren (eID-Funktion des Personalausweises, § 4 Abs. 4 NDIG).

Die vier Regelungen sind in den folgenden Kapiteln erläutert.

Es gibt weitere Gesetze, die die elektronische Kommunikation mit Behörden regeln. Die Regelungen im NDIG sind so gestaltet, dass sie mit den weiteren gesetzlichen Regelungen harmonieren. Von besonderer Bedeutung sind dabei

- das E-Government-Gesetz des Bundes, das in § 2 EGovG den elektronischen Zugang regelt,
- das Onlinezugangsgesetz, das in § 3 OZG die Nutzerkonten regelt,
- das Verwaltungsverfahrensgesetz (VwVfG), das in § 3a die schriftformersetzende Kommunikation regelt (das Niedersächsische Verwaltungsgesetz enthält eine dynamische Verweisung auf das VwVfG),
- die eIDAS-Verordnung[6], die einheitliche Regelungen für Signaturen und die Bereitstellung von Vertrauensdiensten im EU-Binnenmarkt schafft, sowie das Vertrauensdienstegesetz (VDG), das die wirksame Durchführung der eIDAS-Verordnung regelt.

4.3 Einfacher Zugang (§ 4 Abs. 1 NDIG)

Ab sofort müssen alle Behörden einen einfachen Zugang zur Übermittlung elektronischer Dokumente eröffnen.

Die Verpflichtung ist erfüllt, wenn eine Möglichkeit angeboten wird eMails zuzusenden und die eMail-Adresse auf der Homepage bzw. im Bürger- und Unternehmensservice (BUS, siehe Kap. 5) veröffentlicht ist. Neben einer allgemeinen Kontakt-eMail-Funktion sind in der Regel spezifische eMail-Adressen für die einzelnen Verwaltungsleistungen sinnvoll. Die eMail-Postfächer müssen von den Behörden regelmäßig eingesehen und die dortigen eMails bearbeitet werden. eMails oder Anlagen mit qualifizierter elektronischer Signatur (QES) müssen akzeptiert und als Schriftformersatz anerkannt werden. Es darf keinen Hinweis auf die Annahmeverweigerung von Dokumenten mit QES geben.

Das MI hat nach § 12 Abs. 1 Nr. 1 NDIG einen Basisdienst für den einfachen Zugang bereitzustellen. Der zentrale E-Mail-Service für Behörden des Landes wird von IT.Niedersachsen (IT.N) wahrgenommen. Auch sonstige Behörden können diesen Dienst gegen Entgelt nutzen. Da die Behörden bereits heute entweder selbst einen eMail-Service betreiben oder einen Provider beauftragt haben, besteht in der Regel kein Handlungsbedarf.

[6] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. ABl. L 257/73 vom 28.08.2014. eIDAS steht für „electronic IDentification, Authentication and trust Services“.

IT.N kann auch unterstützen, wenn Dokumente mit QES auf ihre Authentizität zu prüfen sind. Zurzeit werden allerdings noch sehr selten Dokumente mit QES übermittelt.

Weitere Informationen zu IT.Niedersachsen sowie Kontaktdaten finden Sie hier:

https://www.it.niedersachsen.de

4.4 Nutzerkonto (§ 4 Abs. 2 NDIG)

Ab dem 1.07.2021 müssen alle Behörden einen Zugang zur Übermittlung elektronischer Dokumente über Nutzerkonten eröffnen.

Analog zum OZG definiert auch das NDIG das Nutzerkonto als eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung der Nutzerinnen und Nutzer zu Zwecken der Inanspruchnahme von Leistungen der öffentlichen Verwaltung (§ 1 Abs. 1 Nr. 9 NDIG).

Nutzerkonto-Verfahren sind heute in der Wirtschaft die mit großem Abstand häufigsten Identifizierungsverfahren, um Geschäftsprozesse im Internet mit Kunden abzuwickeln. Fast in jedem Online-Verfahren von Unternehmen gibt es für Kunden die Möglichkeit, sich zu registrieren und mindestens durch Angabe von persönlichen Daten, die per eMail zu bestätigen sind, zu identifizieren („Online-Registrierung“). Das so entstandene Nutzerkonto kann dauerhaft bei der Nutzung von unterschiedlichen Online-Diensten verwendet werden. Die eigentliche Kommunikation erfolgt dabei in der Regel durch Dateneingabe des Kunden oder über den Upload von Daten im Online-Dienst (wenn z.B. Nachweise beigefügt werden). Diese Daten werden in einer Datenbank des Anbieters gespeichert und möglichst über standardisierte Schnittstellen an interne Fachverfahren weitergeleitet. Durch die Verwendung des Nutzerkontos können die gespeicherten Daten jederzeit einer Person zugeordnet werden.

Nutzerkonten bieten auch für die öffentliche Verwaltung die Möglichkeit, Verwaltungsverfahren mit ihren „Kunden“ abzuwickeln. Sie ermöglichen eine hohe Akzeptanz, weil das Verfahren aus der Wirtschaft bekannt und meist einfach einzurichten ist. Darüber hinaus bieten sie auch die Möglichkeit eines „Rückkanals“, also der Übermittlung von Daten der Verwaltung an die Nutzerkonto-Personen, wenn das Nutzerkonto über eine Postfachfunktion verfügt.

Ein Nutzerkonto-Basisdienst erfordert zunächst eine einmalige Registrierung und Identifizierung. Die Identifizierungsmethode hängt vom Sicherheitsniveau[7] bzw. vom Vertrauensniveau[8] ab, für das das Nutzerkonto genutzt werden soll, und kann von einer einfachen Bestätigung der Registrierung per eMail bis zu einer Identifizierung per Personalausweis reichen (durch Vorlage in der Behörde oder elektronisch mit der eID-Funktion des Personalausweises). Es besteht auch die Möglichkeit, z. B. zunächst nur eine einfache Identifizierungsmethode anzubieten und später weitere Methoden hinzuzufügen.

[7] Die eIDAS-Verordnung beschreibt in Artikel 8 die Sicherheitsniveaus niedrig, substanziell und hoch.
[8] In den technischen Richtlinien des BSI, insbesondere TR-03107-1 und TR-03147, sowie in Unterlagen des IT-Planungsrats Bund/Länder wird der Begriff Vertrauensniveau verwendet und die Niveaus "normal", "substantiell" und "hoch" definiert. Die Vertrauensniveaus der technischen Richtlinien entsprechen den Sicherheitsniveaus der eIDAS-Verordnung.

Abbildung 2 Mögliche Nutzerregistrierungsoptionen

Nach der Registrierung kann das Nutzerkonto im Rahmen von Online-Antragsverfahren genutzt werden. In der Regel erfolgt die Übermittlung des Antrags an die Behörde, nachdem sich der Antragsteller am Nutzerkonto angemeldet hat. Somit erfolgt eine Authentifizierung des Antrags mithilfe des Nutzerkontos. Die Anmeldung erfolgt dabei z. B. durch Eingabe von Kennung und Passwort, gegebenenfalls auch durch weitere bzw. andere Identifizierungsmechanismen.

Mithilfe des Nutzerkontos muss die Übermittlung von Daten über eine Postfachfunktion möglich sein (§ 4 Abs. 2 Satz 2 NDIG). Dies gilt allgemein, ist also nicht auf die Datenübermittlung in ausgewählten Online-Diensten beschränkt. Diese Verpflichtung lässt sich erfüllen, wenn jede Behörde einen Online-Dienst mit einem formfreien Mitteilungsformular bereitstellt und auch das Anhängen von Dokumenten in festgelegten Formaten ermöglicht. Die Verwendung des formfreien Mitteilungsformulars muss aber die Ausnahme sein. In der Regel erfolgt die Kommunikation über die pro Verwaltungsleistung online bereitgestellten Antragsverfahren oder Formulare, die mithilfe des Nutzerkontos authentifiziert werden.

Über die Postfachfunktion muss auch der „Rückkanal“ möglich sein. Z.B. müssen Behörden den Nutzerinnen und Nutzern Bescheide aus einem Fachverfahren der Behörde im Postfach des Nutzerkontos bereitstellen können.

Nach § 12 Abs. 1 Satz 1 Nr. 1 NDIG ist das Land verpflichtet, Nutzerkonten als Basisdienst bereitzustellen. Die Behörden sind verpflichtet, diesen Basisdienst zu nutzen.

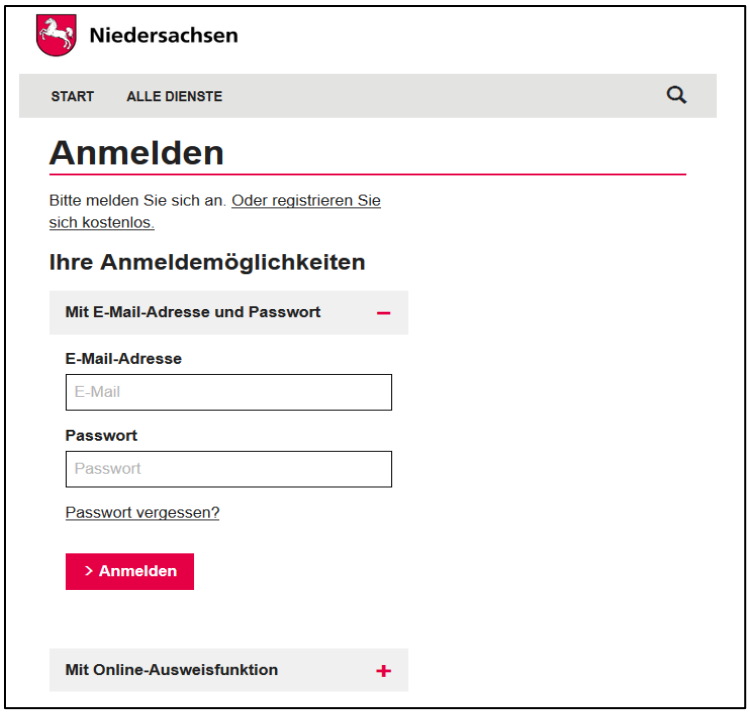


Abbildung 3 Anmeldung zum niedersächsischen Nutzerkonto (Prototyp)

Der Auf- und Ausbau des Nutzerkonto-Basisdienstes erfolgt im Rahmen des Programms DVN im Projekt P 4 „Einführung des Servicekontos“. Servicekonto ist ein anderer Begriff für das Nutzerkonto. Im Rahmen des Projekts soll ein Basisdienst für Bürgerinnen und Bürger („Bürgerkonto“) und später auch für Organisationen („Organisationskonto“) bereitgestellt werden. Organisationen sind in diesem Zusammenhang Unternehmen, Behörden und sonstige Organisationen. Im Rahmen eines Organisationskontos soll es möglich sein, die Zugehörigkeit von Personen zur Organisation zu bestätigen (vergleichbar mit einem Firmenstempel oder -siegel). Auch soll es eine Administratorfunktion im Organisationskonto geben, mit dem das Einrichten von Rollen und Rechten für einzelne Personen der Organisation möglich ist.

Die Bereitstellung des Nutzerkonto-Basisdienstes erfolgt in enger Abstimmung mit dem Bund und den anderen Ländern, u.a. weil § 3 Abs. 2 OZG die einheitliche Identifizierung für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen fordert. Ziel ist es, gemeinsame oder zumindest interoperable Nutzerkonten in Deutschland bereitzustellen. Das Unternehmenskonto soll auf jeden Fall bundesweit einheitlich sein. Das niedersächsische Servicekonto wird durch IT.N bereitgestellt. IT.N kooperiert bei der Bereitstellung des Nutzerkonto-Basisdienstes mit der Dataport AöR, die auch für mehrere andere norddeutsche Länder den Basisdienst bereitstellt.

Bei der Bereitstellung von Zugangsverfahren müssen gemäß Artikel 6 eIDAS-Verordnung auch notifizierte Identifizierungsverfahren anderer EU-Staaten angebunden werden. Bei Online-Diensten der Behörden muss es also möglich sein, sich mit dem niedersächsischen Nutzerkonto, mit anderen deutschen Nutzerkonten und auch mit den notifizierten Verfahren anderer EU-Staaten anzumelden. Dies sollte immer über die Verknüpfung des niedersächsischen Nutzerkontos im Portalverbund erfolgen. Eine direkte Anbindung von notifizierten Identifizierungsverfahren an einzelne Online-Dienste ist nicht sinnvoll.

Der Nutzerkonto-Basisdienst ist ein zentraler Identifizierungsdienst, der bei der Kommunikation in Verwaltungsverfahren genutzt werden soll. Alle Behörden sollen ihre Online-Dienste so erstellen und umgestalten, dass die Authentifizierung mit dem Nutzerkonto möglich ist. Ausgenommen sind nur die Online-Dienste, für die keine Authentifizierung erforderlich ist. Für die Anbindung des Nutzerkontos wird eine Schnittstelle bereitgestellt. Die Online-Dienste müssen diese Schnittstelle einbinden. In der weiteren Bearbeitung sollten die Verfahren so gestaltet werden, dass die Identifizierung des Nutzers mit dem Nutzerkonto jederzeit nachgewiesen werden kann.

Weitere Informationen zum Nutzerkonto im Internet finden Sie hier:

https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/03_Nutzerkonto_BuU/Nutzerkonto_node.html

Weitere Informationen zum Nutzerkonto im Landesintranet finden Sie hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505473&_psmand=153

Kontakt zum Thema Nutzerkonto:

eMail: P4-DigitaleVerwaltung@it.niedersachsen.de

4.5 Welches Vertrauensniveau für welchen Online-Dienst?

Im Rahmen von Online-Verwaltungsleistungen prüft die Verwaltung die Herkunft, Echtheit und Gültigkeit elektronisch übermittelter Identitäten und Unterlagen. Dabei bestimmt die Verwaltungsleistung die Anforderung an die Vertrauenswürdigkeit der übermittelten Daten. Soll eine gesetzlich vorgeschriebene Schriftform im Rahmen einer Verwaltungsleistung durch die elektronische Form ersetzt werden, sind gemäß § 3a VwVfG nur bestimmte Authentisierungsmittel mit besonders hohen Anforderungen an die Vertrauenswürdigkeit zugelassen (zurzeit qualifizierte elektronische Signatur, eID-Funktion des Personalausweises oder absenderbestätigte De-Mail).

Ist keine Schriftform vorgeschrieben, muss ein Authentisierungsmittel bestimmt werden, das dem erforderlichen Vertrauensniveau für die Verwaltungsleistung entspricht. Dazu wird die Verwaltungsleistung zunächst einem der drei eingeführten Vertrauensniveaus zugeordnet. Hierfür kann die folgende vereinfachte Zuordnung verwendet werden.

Vertrauensniveau	Gefährdung durch Rechtsverstöße	Gefährdung durch finanzielle Auswirkungen
normal/ niedrig[9]	geringfügige Konsequenzen (Beispiel: Verstoß führt zu OWI-Verfahren mit Bußgeldern bis ca. 100.-)	Schaden tolerabel (Beispiel: Finanzieller Schaden in der Regel unter ca. 100.-)
substantiell	substantielle Konsequenzen (Beispiel: Verstoß führt zu OWI-Verfahren mit Bußgeldern über ca. 100.-)	substantieller Schaden möglich (Beispiel: Finanzieller Schaden in der Regel zwischen ca. 100.- und 1.000.-)
hoch	erhebliche Konsequenzen (Beispiel: Verstoß führt zu Strafverfahren)	beachtliche finanzielle Verluste (Beispiel: Finanzieller Schaden in der Regel über ca. 1000.-)

[9] Das BSI verwendet für dieses Vertrauensniveau auch den Begriff „normal“, die eIDAS-Verordnung den Begriff „niedrig“.

Die in der Tabelle aufgeführten Beispiele beziehen sich jeweils auf ein einzelnes Verfahren (z.B. den Antrag einer Person). Für die Einstufung in ein Vertrauensniveau reicht es, dass eine der zwei Gefährdungen besteht (Gefährdung durch Rechtsverstöße oder Gefährdung durch finanzielle Auswirkungen). Dabei ist zusätzlich die Eintrittswahrscheinlichkeit zu beachten, die die Einstufung um eine Stufe nach oben oder unten verändern kann. Die Beispiele sind als Anhaltspunkte zu verstehen. Die tatsächliche Bewertung ist von der jeweils zuständigen Behörde selbst vorzunehmen.

Beim Nutzerkonto gibt es zurzeit folgende Zuordnung zu den Vertrauensniveaus:

Vertrauensniveau	Beschreibung	Registrierung	Anmeldung
normal/niedrig	Die Nutzerkontodaten sind plausibel, die Authentisierung erfolgt einfach	Online-Registrierung mit Bestätigung per eMail	Kennung und Passwort
substanziell	Die Nutzerkontodaten sind geprüft, Zwei-Faktor-Authentisierung	Online-Registrierung mit verlässlicher Identifizierung	Kennung und Passwort, Bestätigung mit Software-Zertifikat oder PushTAN
hoch	Die Nutzerkontodaten sind geprüft, Zwei-Faktor-Authentisierung. Für den Ersatz der Schriftform geeignet.	Online-Registrierung mit eID-Funktion des Personalausweises oder Aufenthaltstitels	eID-Funktion des Personalausweises oder Aufenthaltstitels

Eine verlässliche Registrierung kann z.B. auf folgende Weise geschehen:

1. Registrierung mit der eID-Funktion des Personalausweises
2. Registrierung mit einem Servicekonto im Bund oder in einem anderen Land im Vertrauensniveau substanziell oder hoch
3. Registrierung mit der ELSTER-Kennung (in Planung)
4. Registrierung durch Vorlage des Ausweises im Bürgerbüro oder einer anderen geeigneten Prüfstelle (in Prüfung)

Weitere Informationen zu den Vertrauensniveaus beim Bundesamt für Informationssicherheit (BSI):

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03147/tr03147_node.html

Weitere Informationen zu den Vertrauensniveaus beim IT-Planungsrat Bund/Länder:

https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/eID/Handreichung_Vertrauensniveaus.html;jsessionid=7105F587B41CF9055F5AA592414AE3B4.1_cid332?nn=6848472

4.6 De-Mail (§ 4 Abs. 3 NDIG)

§ 4 Abs. 3 NDIG verpflichtet die Behörden, ab dem 1.07.2021 einen Zugang per De-Mail oder einen anderen schriftformersetzenden Dienst zu eröffnen.

Über De-Mail können Bürgerinnen, Bürger und Unternehmen authentisch und vertraulich mit der Verwaltung elektronisch kommunizieren. Die Vorgaben für De-Mail sind im De-Mail-Gesetz vom 28.04.2011[10] festgelegt. De-Mail-Verfahren werden von akkreditierten De-Mail-Providern bereitgestellt, die alle gesetzlichen Voraussetzungen zu erfüllen haben.

Bei Anträgen oder Anzeigen an eine Behörde ersetzt eine De-Mail mit Absenderbestätigung gemäß § 3 a Abs. 2 Satz 4 Nr. 2 VwVfG die Schriftform. Durch Einrichtung eines De-Mail-Postfachs bietet eine Behörde somit ein schriftformersetzendes Kommunikationsverfahren an. Durch die Zugangseröffnung per eMail nach § 4 Abs. 1 NDIG und der Bereitschaft, qualifiziert elektronische signierte Dokumente entgegenzunehmen, haben Behörden allerdings auch schon einen Zugang für schriftformersetzende Dokumente geschaffen. Wenn Behörden für die Übermittlung von Dokumenten auch die Identifizierung mit der eID-Funktion des Personalausweises anbieten, z.B. im Zusammenhang mit dem Nutzerkonto-Basisdienst, eröffnen sie ebenfalls einen Zugang für die Übermittlung von Dokumenten, die die Schriftform ersetzen. Daher kann die Verpflichtung aus § 4 Abs. 3 NDIG auch auf andere Weise erfüllt werden, ein De-Mail-Zugang ist hierfür nicht zwingend erforderlich. Es wird dennoch empfohlen, einen De-Mail-Zugang anzubieten, weil hierdurch Bürgerinnen, Bürgern und Unternehmen ein schriftformersetzender Dienst angeboten wird, der keine zusätzliche Hardware erfordert. De-Mail eignet sich auch als Rückkanal, also etwa für die Übermittlung von Bescheiden an antragstellende Bürgerinnen und Bürger nach § 3 a Abs. 2 Nr. 3 VwVfG. Zudem eignet sich De-Mail auch für die authentische Kommunikation zwischen beliebigen Partnern außerhalb der Verwaltung, z.B. beim verlässlichen Austausch von Vertragsdokumenten.

Wie funktioniert De-Mail?

Aus Nutzersicht ist De-Mail ein webbasiertes Kommunikationsverfahren, sehr ähnlich wie ein eMail-Dienst. De-Mail verwendet auch eMail-ähnliche Adressen, die aber immer mit De-Mail.de enden. De-Mail wird von Providern bereitgestellt. Nach Anmeldung im Internet am De-Mail-Dienst des Providers lassen sich Nachrichten wie eMails versenden, allerdings nur an Empfänger, die auch über eine De-Mail-Adresse verfügen. Bei der Einrichtung eines De-Mail-Kontos ist eine Identifizierung mit dem Personalausweis oder dem elektronischen Aufenthaltstitel erforderlich (vor Ort oder per eID-Funktion). Die sichere Kommunikation basiert hauptsächlich auf TLS-gesicherten Kommunikationskanälen (Transportverschlüsselung). Die Ende-zu-Ende-Verschlüsselung stellt gemäß der Technischen Richtlinie eine zusätzliche Option dar, die der Diensteanbieter zu unterstützen hat. Für private Nutzer fallen in der Regel Kosten für den Versand von De-Mails an, die aber geringer sind als Briefportokosten. Für Behörden fallen zusätzlich geringfügige monatliche Kontoführungskosten an. Nutzerinnen und Nutzer benötigen lediglich einen Internet-Zugang (z.B. Notebook) und ggf. ein Smartphone zur Bestätigung von Push-TANs. Eine Chipkarte, ein Lesegerät oder andere Zusatzgeräte sind nicht erforderlich.

[10] BGBl I 2011, 666

Mindestens die Kommunen sind gemäß § 110 c des Gesetzes über Ordnungswidrigkeiten in Verbindung mit § 32 a Abs. 1, 3 und 4 der Strafprozessordnung (StPO) verpflichtet, einen De-Mail-Zugang vorzuhalten, da ihnen die Zuständigkeiten für mehrere Ordnungswidrigkeiten obliegen.

Die Bearbeitung von De-Mails für Behörden lässt sich erleichtern, wenn der De-Mail-Dienst behördenintern mit dem eMail-Dienst, einem Fachverfahren oder einem eAkte-System verbunden wird. Hierfür sind ein De-Mail-Gateway und ein Multimessenger-Dienst erforderlich, der De-Mails an das interne System weiterleitet und von diesem entgegennimmt. Das Land prüft derzeit, ob diese Infrastruktur aufgebaut werden soll.

Gemäß § 12 Abs. 1 Nr. 1 NDIG ist das Land verpflichtet, einen Basisdienst nach § 4 Abs. 3 NDIG bereitzustellen. Auch hier gilt, dass dies u.a. durch den eMail-Dienst nach § 4 Abs. 1 NDIG bereits erfüllt ist. IT.N wird dennoch Behörden, die einen De-Mail-Zugang eröffnen wollen, durch Einrichtung einer Adresse mit der Endung niedersachsen.De-Mail.de und die Vermittlung eines Providers unterstützen.

Weitere Informationen zu De-Mail: https://www.De-Mail.info

Weitere Informationen zu IT.Niedersachsen sowie Kontaktdaten finden Sie hier:

https://www.it.niedersachsen.de

4.7 eID-Funktion von Personalausweis und Aufenthaltstitel (§ 4 Abs. 4 NDIG)

§ 4 Abs. 4 NDIG verpflichtet die Behörden des Landes, ab dem 1.07.2021 eine elektronische Identifizierung mit den Personalausweis oder dem elektronischen Aufenthaltstitel anzubieten, wenn die Identifizierung in elektronischen Verwaltungsverfahren erforderlich ist. Personalausweise verfügen seit November 2010 über einen Computerchip, mit dem u.a. eine elektronische Identifizierung möglich ist. Diese Funktion wird eID-Funktion genannt (eID = electronic Identity).

Wie funktioniert die eID-Funktion des Personalausweises?

Der aktuelle Personalausweis enthält mit seinem Computerchip eine Online-Ausweisfunktion (eID-Funktion), die eine sichere elektronische Identifizierung ermöglicht. Gleiches gilt für den elektronischen Aufenthaltstitel. Auch für EU-Bürger steht voraussichtlich zum 1.11.2020 eine entsprechende ID-Karte zur Verfügung.

Nutzung der eID-Funktion:

- Der Ausweisinhaber oder die -inhaberin installiert auf einem Rechner oder Smartphone die kostenlose AusweisApp2.
- Er oder sie muss außerdem einen geeigneten Kartenleser oder ein geeignetes Handy mit NFC-Funktion besitzen.
- Der Ausweisinhaber oder die –inhaberin aktiviert die eID-Funktion mithilfe der AusweisApp2. Er oder sie nutzt hierfür eine PUK, die nach Ausgabe des Personalausweises oder auf Antrag zugesandt wird. Er oder sie erhält zusätzlich eine PIN für die Identifizierungsverfahren zugesandt.

- Wenn in einem Online-Verwaltungsverfahren die Identifizierung oder eine elektronische Signatur erforderlich ist, sendet das Antragsverfahren eine Identifizierungsanfrage. Zur Identifizierung legt der Ausweisinhaber oder die –inhaberin den Ausweis auf das Lesegerät und gibt die PIN ein. Daraufhin werden die angeforderten Daten aus dem Ausweis ausgelesen und zur Identifizierung an die anfordernde Stelle gesandt.

Das Auslesen des Personalausweises wird ausschließlich durch einen besonders geschützten eID-Server durchgeführt, an den die Online-Dienste ihre Anfrage senden. Behörden, die Anfragen an den eID-Server senden wollen, benötigen hierfür ein Zertifikat vom Bundesverwaltungsamt, das auch konkret festlegt, welche Datenfelder des Personalausweises ausgelesen werden dürfen. Hierdurch wird sichergestellt, dass nur die Daten aus dem Personalausweis ausgelesen werden können, die im Rahmen der gesetzlichen Aufgaben benötigt werden.

§ 4 Abs. 4 NDIG verpflichtet zwar nur die Behörden des Landes, alle Behörden sollten aber in Online-Angeboten immer dann die Identifizierung mit der eID-Funktion des Personalausweises oder dem Aufenthaltstitel anbieten, wenn eine sichere Identitätsfeststellung benötigt wird, weil dieses Verfahren besonders datenschutzfreundlich und verlässlich ist. Je nach Anforderung sollten aber auch andere, für die Nutzer ggf. weniger aufwändigere Verfahren zur Identitätsfeststellung eingesetzt werden (z.B. Nutzerkonto, Video-Ident-Verfahren, Scan des Personalausweises[11]).

Die eID-Funktion des Personalausweises kann nicht nur zur reinen Identitätsfeststellung verwendet werden. Nach § 3a Abs. 2 Satz 4 Nr. 1 VwVfG dürfen auch elektronische Formulare online unterschrieben werden, wenn in diesem Zusammenhang die eID-Funktion des Personalausweises genutzt wird. Die eID-Funktion des Personalausweises kann damit als Schriftformersatz verwendet werden.

Die eID-Funktion des Personalausweises wird auch genutzt, um eine Nutzerkonto-Registrierung mit dem Vertrauensniveau hoch zu realisieren.

Ausweise mit eID-Funktion

Damit grundsätzlich alle Bürgerinnen und Bürger der Europäischen Union die Online-Dienste der deutschen Verwaltungen nutzen können, wurden drei verschiedene Karten mit eID-Funktion eingeführt:

- der Personalausweis (siehe § 18 Personalausweisgesetz) für Bürgerinnen und Bürger mit deutscher Staatsangehörigkeit
- der elektronische Aufenthaltstitel (§ 78 Abs. 5 Aufenthaltsgesetz, AufenthG) für Ausländer mit Aufenthaltserlaubnis in Deutschland
- die eID-Karte (§ 12 eID-Karte-Gesetz) für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums. Die Einführung der eID-Karte erfolgt ab November 2020. Sie ist im NDIG noch nicht aufgeführt, aber bei der elektronischen Identifizierung mit zu berücksichtigen.

[11] In diesem Fall muss die Ablichtung eindeutig und dauerhaft als Kopie erkennbar sein.

Das Land ist gemäß § 12 Abs. 1 Nr. 2 NDIG verpflichtet, einen Basisdienst für den elektronischen Identitätsnachweis nach § 4 Abs. 4 NDIG bereitzustellen. IT.N bietet hierfür einen zentralen eID-Server an. Behörden des Landes müssen diesen Basisdienst nutzen, die übrigen Behörden können ihn nutzen.

Das Auslesen des Personalausweises über die eID-Funktion erfolgt über den eID-Server und ist nur möglich, wenn ein Berechtigungszertifikat vorliegt. Nähere Informationen hierzu erteilt IT.N.

Weitere Informationen finden Sie hier: https://www.personalausweisportal.de

Weitere Informationen im Landesintranet:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505473&_psmand=153

Kontakt zum Thema eID-Funktion:

eMail: P4-DigitaleVerwaltung@it.niedersachsen.de

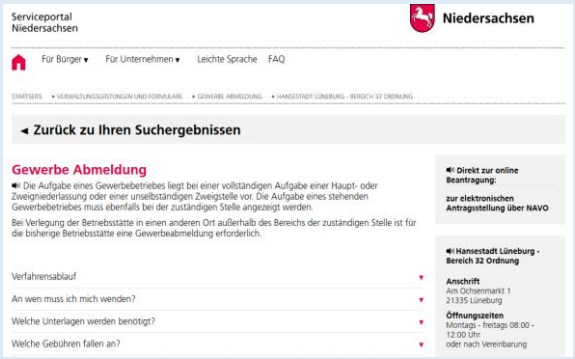
5 Elektronische Informationen (§ 5 NDIG)

Bürgerinnen, Bürger und Unternehmen werden Angebote der digitalen Verwaltung nur nutzen, wenn Ihnen leicht auffindbare, verständliche und korrekte Informationen über diese Angebote zur Verfügung stehen. § 5 NDIG verpflichtet daher die Behörden umfassend zur Bereitstellung von Informationen im Internet. Diese Verpflichtungen werden in den folgenden Kapiteln näher erläutert. Ab dem 1.07.2021 ist das MI verpflichtet, einen Basisdienst für die Bereitstellung dieser Informationen zur Verfügung zu stellen[12]. Alle Behörden im Geltungsbereich des NDIG sind dann verpflichtet, diesen Basisdienst zu nutzen. Damit entsteht in Niedersachsen ein umfassendes Informationssystem mit Beschreibungen der Verwaltungsleistungen.

Mit dem Bürger- und Unternehmensservice (BUS) betreibt das Land bereits seit vielen Jahren einen entsprechenden Basisdienst, der im Rahmen der Umsetzung des OZG und des NDIG weiter ausgebaut wird. Der BUS ist für die Umsetzung von § 5 Abs. 1 und 2 NDIG zu nutzen. Die gemeinsame Nutzung des BUS soll nicht nur einen umfassenden, aussagekräftigen Informationspool für die Nutzer schaffen, sondern auch die Bereitstellungsaufwände der zuständigen Behörden deutlich verringern.

Der Bürger- und Unternehmensservice Niedersachsen (BUS)

Der Bürger- und Unternehmensservice Niedersachsen (BUS) enthält über 1.400 Beschreibungen zu Verwaltungsleistungen der niedersächsischen Behörden sowie zu länderübergreifenden Leistungen der öffentlichen Verwaltung von A wie Abbruchanzeige bis Z wie Zweitwohnungssteuer.



[12] § 12 Abs. 1 Satz 1 Nr. 3 NDIG

Die Inhalte des BUS werden von einer Landesredaktion im Auftrag des MI betreut, die Texte über den Leistungskatalog des Bundes und der Länder (LeiKa) erhält oder Inhalte basierend auf landesrechtlichen Vorgaben und nach Bedarf der Behörden in Kooperation mit Ressorts und Kommunen erstellt. Der Informationsaufbau unterstützt dabei den XÖV-Standard XZUFI.

Im BUS ist es möglich, eine vollständige vertikale Abbildung von Zuständigkeiten über alle Verwaltungsebenen hinweg zu erfassen und darzustellen. Bei der Erfassung und Pflege der Daten werden alle Ebenen der Verwaltung einbezogen: Die Fachressorts in den Landesministerien erstellen rechtssichere Leistungsbeschreibungen, beruhend auf Landesrecht oder in Erweiterung von Bundesrecht, die in der Ebene der Kommunalverwaltung um regionale und kommunale Besonderheiten zum Vollzug ergänzt und mit den tatsächlich zuständigen Stellen versehen werden. So ist bspw. die Abbildung kommunaler Satzungen und Formulare möglich. Die Erfassung der zuständigen Stellen direkt durch die Verwaltungen vor Ort sichert gerade in der Aufgabenteilung zwischen Gemeinde und Landkreis sachlich richtige Aussagen zur Zuständigkeit.

Im BUS eingestellte Inhalte können über Schnittstellen bezogen und für eigene behördliche Internetportale verwendet werden. Sie werden auch für die Auskunft der Behördennummer 115 bereitgestellt.

Einbindungsvarianten für niedersächsische Behörden

Der BUS wird durch IT.N bereitgestellt und basiert auf der Software Infodienste der Fa. Teleport. Er wird als Hauptbestandteil des Niedersächsischen Verwaltungsportals unter https://service.niedersachsen.de bereitgestellt.

Der BUS bietet zudem unterschiedliche Möglichkeiten, Bürger- und Unternehmensinformationen in die eigene Webpräsenz einer Behörde einzubinden. Somit steht Kommunen und anderen Behörden der gesamte Datenbestand jederzeit und gepflegt zur Verfügung, eine homogene Darstellung der Daten auf den einzelnen Verwaltungsebenen wird so sichergestellt. Die Bereitstellung der Daten erfolgt layoutneutral.

Grundsätzlich existieren drei Einbindungsvarianten:

1. Einbindungsassistent (Include-Wizard)

   Mit dem Include-Wizard können Kommunen einen eigenen Mandanten im BUS einrichten lassen, mit einem Redaktionsteam Daten einpflegen und diese im eigenen Layout in den Internetauftritt der Kommune einbinden.

2. Webservice mit lesender und/oder schreibender SOAP-Schnittstelle

   Kommunen können ihr eigenes Informationssystem betreiben und dieses über eine SOAP-Schnittstelle mit dem BUS synchronisieren.

3. REST-Webservices zur Abdeckung häufiger Einsatzszenarien.

   Kommunen können ihr eigenes Informationssystem betreiben und dieses über eine REST-Schnittstelle mit dem BUS synchronisieren. Diese Schnittstelle ist die aktuellere Variante.

Neben Niedersachsen verwenden sieben weitere Länder die Software Infodienste für ihr zentrales Verwaltungsportal. Die Länder bilden gemeinsam eine Entwicklungsgemeinschaft.

Der BUS wird im niedersächsischen Verwaltungsportal unter https://service.niedersachsen.de bereitgestellt. Er ist aber auch als Informationssystem in vielen kommunalen Auftritten verfügbar. Außerdem werden die Daten des BUS dem Bund und den anderen Ländern im Rahmen des Portalverbunds über ein Online-Gateway zur Verfügung gestellt. Ebenso dient der BUS als Datenbasis für die Behördennummer 115. Schließlich werden die Daten des BUS über den Portalverbund an das Single Digital Gateway der EU-Kommission weitergeleitet (siehe auch Kap. 5.4). Eine Übersicht über diese Verknüpfungen ist in Abb. 4 dargestellt.

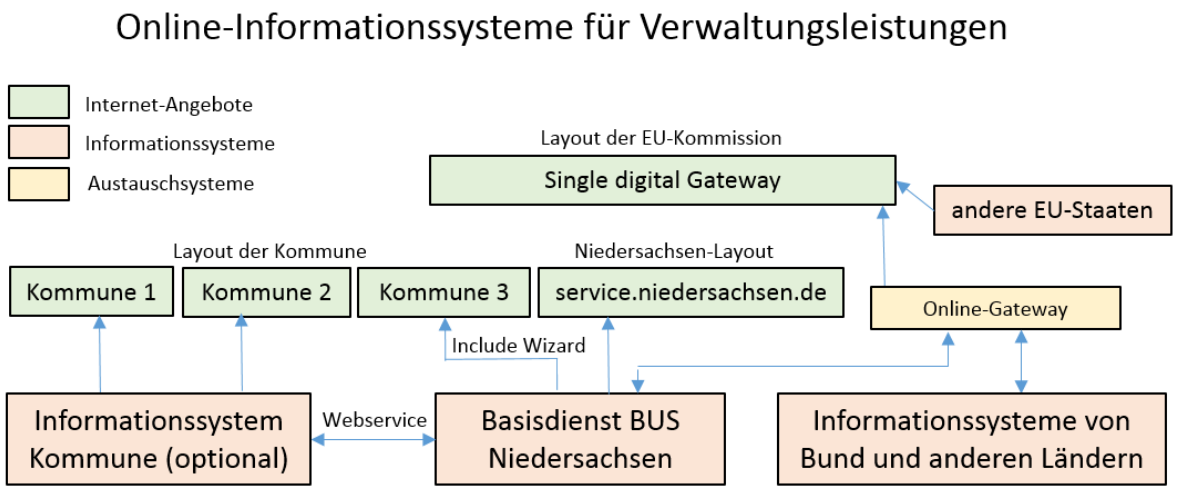


Abbildung 4 Einbindung des BUS in die Online-Informationssysteme für Verwaltungsleistungen

Der BUS wird den niedersächsischen Behörden kostenfrei zur Verfügung gestellt. Betreiber ist IT.N im Auftrag des MI. Das MI erfüllt damit seine Verpflichtung nach § 12 Absatz 1 Nr. 3 NDIG (Basisdienst für die Informationsbereitstellung).

Als Unterstützungsleistung des Landes erfolgt eine Beratung und Schulung von Redaktionen, die den Include-Wizard verwenden, sowie ein Zertifizierungsworkshop für spätere Webservicenutzer.

Weitere Informationen finden Sie hier: https://service.niedersachsen.de

Kontakt für die Aufnahme von Behörden in den BUS: buergerservice@mi.niedersachsen.de

Kontakt zur BUS-Redaktion:

eMail: landesredaktion@niedersachsen.de

Tel.: 0511 120 27125

Kontakt zum technischen Support des BUS:

eMail: ServiceDesk@it.niedersachsen.de

Tel.: 0511 120 3999

5.1 Allgemeine Informationen (§ 5 Abs. 1 NDIG)

§ 5 Abs. 1 NDIG verpflichtet alle Behörden, ab sofort allgemeine Informationen über die Behörde im Internet bereitzustellen.

Dies betrifft folgende Informationen:

- Aufgaben
- Anschrift
- Geschäftszeiten
- Erreichbarkeit (postalisch, telefonisch, elektronisch)

Diese Informationen müssen im Basisdienst[13], also im BUS, eingetragen und hierüber im Internet verfügbar sein. Auf diese Weise erfolgt auch eine Zugangseröffnung für die elektronischen Zugänge nach § 4 NDIG.

5.2 Informationen für einzelne Verwaltungsleistungen (§ 5 Abs. 2 und 3 NDIG)

§ 5 Abs. 2 NDIG verpflichtet die Behörden, ab dem 1.07.2021 konkrete Informationen zu den einzelnen Verwaltungsleistungen im Internet bereitzustellen.

Dies betrifft die folgenden Informationen:

- Nach außen wirkende öffentliche Tätigkeit (Verwaltungsleistungen)
- damit verbundene Gebühren
- beizubringende Unterlagen
- zuständige Ansprechstelle und ihre Erreichbarkeit

Außerdem sind die jeweils erforderlichen elektronischen Formulare bereitzustellen.

Auch diese Informationen müssen im Basisdienst, also im BUS, bereitgestellt werden.

Die Informationen sollen in allgemein verständlicher Sprache verfasst werden. Ziel sind also klare und adressatengerechte Formulierungen, um den Bürgerinnen und Bürgern, Unternehmen und Verbänden Informationen an die Hand zu geben, die nicht durch fachterminologische Begrifflichkeiten verwirren. Hiermit ist nicht die im Behindertengleichstellungsgesetz geregelte „leichte Sprache“ gemeint.

Um diese Vorschrift umzusetzen und die damit verbundenen Lasten möglichst themengerecht zu verteilen, haben sich Bund und Länder auf den Aufbau und die Pflege eines Leistungskatalogs der öffentlichen Verwaltung (LeiKa) verständigt, der auch im Portalverbund verwendet werden soll (siehe Informationskasten).

Dieser Katalog unterstützt als Teil des föderalen Informationsmanagements die Anbieter von Informationen zu Verfahren auf allen föderalen Ebenen. Bundesbehörden oder oberste Landesbehörden stellen für den LeiKa sogenannte Stammtexte zu den Verfahren bereit, deren Ausführung den Ländern übertragen wurde. Das Land ergänzt diese Stammtexte anhand von Ausführungsvorschriften und stellt sie ebenso wie die entsprechend strukturierten Informationen zu landesgesetzlich geregelten Verfahren über den BUS den vollziehenden Behörden auf Landes- oder kommunaler Ebene zur Verfügung

[13] Die Eintragung in den BUS ist erst ab dem 1.07.2021 gesetzlich vorgeschrieben, sollte aber sofort erfolgen, weil der BUS bereits jetzt zur Verfügung steht.

(siehe Kap. 5.3). Soweit die von den Bundesbehörden bereitzustellenden Stammtexte für bundesrechtlich geregelte Verfahren noch nicht vorliegen, stellen die fachlich federführenden obersten Behörden des Landes diese Texte bereit. Die obersten Behörden des Landes werden durch eine vom MI koordinierte Portalredaktion so weit wie möglich unterstützt.

Die Verpflichtungen nach § 5 Abs. 2 NDIG erfordern, dass die zuständigen Stellen die im BUS bereitgestellten LeiKa-Informationen einschließlich der Stammtexte für ihre Aufgaben prüfen, übernehmen, ggf. anpassen und mit den gemäß § 5 Abs. 2 NDIG erforderlichen behördenspezifischen Zusatzinformationen ergänzen. Dies sind z.B. Ansprechpartner, Erreichbarkeit und Öffnungszeiten (für diejenigen, die den Online-Dienst nicht nutzen). Die Kommunen können die von den obersten Landesbehörden zu Verfügung gestellten Informationen auch anpassen oder ergänzen. Sie sind also nicht verpflichtet, die Informationen unverändert zu übernehmen.

Föderales Informationsmanagement (FIM): Der Standard für Verwaltungsleistungen

Das Föderale Informationsmanagement (FIM) dient dazu, leicht verständliche Bürgerinformationen, einheitliche Datenfelder für Formularsysteme und standardisierte Prozessvorgaben für den Verwaltungsvollzug bereitzustellen. Ziel ist es, den Übersetzungs- und Implementierungsaufwand rechtlicher Vorgaben zu senken. Länder und Kommunen sollen - bezogen auf die redaktionelle und organisatorische Umsetzung eines Verwaltungsverfahrens - nicht mehr für sich alleine agieren müssen. Stattdessen können sie auf qualitätsgesicherte Vorarbeiten der nächsthöheren Verwaltungsebene zurückgreifen**.**

Weitere Informationen sind hier zu finden: https://fimportal.de/

LeiKa

Mit dem **LeiKa** (Leistungskatalog der öffentlichen Verwaltung) wird in Deutschland ein einheitliches, vollständiges und umfassendes Verzeichnis der Verwaltungsleistungen über alle Verwaltungsebenen hinweg bereitgestellt. Der LeiKa einhält zurzeit ca. 6.000 Leistungen und wird ständig fortgeschrieben.

Leistungen im LeiKa werden modular beschrieben. Ein sogenannter Stammtext setzt sich aus 23 Modulen zusammen und teilt sich in LeiKa-Schlüssel, Leistungsbeschreibung und Zuständigkeit auf. Im Stammtext werden nur die Teile einer Leistung beschrieben, die bundesweit einheitlich geregelt sind. Jedes einzelne Modul kann durch Nachnutzer (vor allem Länder und Kommunen) durch eigene Informationen ergänzt oder ersetzt werden.

Der LeiKa folgt der Logik, dass eine Verwaltungsleistung aus einem Leistungsobjekt (z. B. Personalausweis, Führerschein) und der hieran ausgeführten Verrichtung (z.B. Ausstellung, Änderung; Ersatz) besteht. Die Verrichtung entspricht hierbei der Leistung, die die Behörde gegenüber dem Bürger erbringt. Ergänzt wird diese Definition in einigen Fällen um Verrichtungsdetails, die die Verrichtung insbesondere in Bezug auf verschiedene Verfahrensabläufe, Zielgruppen oder Ausnahmen innerhalb einer Leistung spezifizieren.

Das Leistungsobjekt beantwortet die Frage "Worum geht es?" (Führerschein), während die Verrichtung die Frage "Was tut die Verwaltung" (Änderung).

Der Betrieb des LeiKa ist integriert in die Anwendung „Föderales Informationsmanagement - FIM“ des IT-Planungsrats des Bundes und der Länder und ist dort Teil des FIM-Bausteins „Leistungen“.

Der LeiKa ist hier zu finden: https://fimportal.de

Die Behörden haben die Informationen im BUS aktuell zu halten. Bei Änderungen der Rechtsgrundlage, aber auch bei Ansprechpartnerwechsel oder anderen Umorganisationen sind die Eintragungen im BUS unverzüglich zu aktualisieren

Weitere Informationen finden Sie hier: https://service.niedersachsen.de

Und im Landesintranet hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505402&_psmand=153

Kontakt zur BUS-Redaktion:

eMail: landesredaktion@niedersachsen.de

Grundsatzfragen zum BUS und zum föderalen Informationsmanagement (FIM):

eMail: digitaleverwaltung@mi.niedersachsen.de

5.3 Informationsbereitstellung durch oberste Landesbehörden (§ 5 Abs. 4 NDIG)

Ein besonders großer Vorteil des BUS ist es, dass nicht jede Kommune die Informationen für ihre Verwaltungsleistungen selbst formulieren muss. § 5 Abs. 4 NDIG verpflichtet vielmehr die obersten Landesbehörden, dafür Sorge zu tragen, dass die Informationen bei Vollzug von Bundes- oder Landesrecht durch die Kommunen über das Internet verfügbar sind. Die obersten Landesbehörden müssen also die über das föderale Stammtext-Management gelieferten Daten sichten und gegebenenfalls anpassen und ergänzen, bevor sie im BUS eingestellt werden. Wenn Landesrecht ausgeführt wird oder über das föderale Management keine Daten geliefert werden, müssen sie selbst die Stammtexte liefern.

Kontakt zu Fragen der Informationsbereitstellung von obersten Landesbehörden:

eMail: landesredaktion@it.niedersachsen.de

oder

eMail: digitaleverwaltung@mi.niedersachsen.de

5.4 Informationsbereitstellung nach der SDG-Verordnung (Artikel 2 ff. SDG-Verordnung)

Die SDG-Verordnung sieht besondere Informationspflichten für bestimmte Bereiche der Verwaltung vor. Die Verordnung unterscheidet dabei

- Rechte, Pflichten und Vorschriften in 17 Bereichen der Verwaltung (z.B. Reisen, Fahrzeuge, Wohnsitz, Steuern), siehe Anhang I der SDG-Verordnung,

- 21 konkrete Verwaltungsleistungen (z.B. Nachweis Geburtsregistereintrag, Wohnsitznachweis, Antrag Studienfinanzierung), siehe Anhang II der SDG-Verordnung,
- 7 Hilfs- und Problemlösungsdienste (z.B. einheitlicher Ansprechpartner), siehe Anhang III der SDG-Verordnung.

Hinzu kommen Verwaltungsbereiche, die in bestimmten EU-Richtlinien geregelt werden (insbesondere die EU-Dienstleistungsrichtlinie).

Die Informationen über diese Bereiche müssen ab dem 12.12.2020 im Internet veröffentlicht sein (Artikel 4 SDG-Verordnung) und bestimmten Qualitätsanforderungen entsprechen (Artikel 9 SDG-Verordnung). Die Informationen sollen möglichst auch in Englisch verfügbar sein (siehe Artikel 12 SDG-Verordnung). Den Kommunen wird in Artikel 39 SDG-Verordnung eine längere Frist zugestanden (bis 12.12.2022), die zum Teil durch die Frist zur Informationsbereitstellung des NDIG (1.07.2021) wieder verkürzt wird.

Die Europäische Kommission hat unter https://europa.eu/youreurope ein einheitliches digitales Zugangstor (Single Digital Gateway) eingerichtet, in dem alle oben aufgeführten Informationen zugänglich sein werden. Dies erfolgt über eine Nutzerschnittstelle (Artikel 18 SDG-Verordnung).

Im Rahmen des IT-Planungsrats Bund/Länder wurde vereinbart, dass diese Informationspflichten in Deutschland über den nach OZG vorgegebenen Portalverbund erfüllt werden sollen. Für Niedersachsen bedeutet dies, dass die Behörden ihre Informationen im BUS zur Verfügung stellen müssen. Über das Portalverbund-Gateway sind diese Daten dann im Portalverbund verfügbar. Der Portalverbund wiederum wird über die SDG-Nutzerschnittstelle mit dem SDG verbunden (siehe auch oben Abb. 5).

Weitere Informationen zur SDG-Verordnung finden Sie hier:

https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/04_SDG/SDG_node.html

5.5 Das niedersächsische Verwaltungsportal (§ 5 Abs. 5 NDIG)

Ab dem 1.01.2023 muss das IT-Ministerium ein niedersächsisches Verwaltungsportal bereitstellen und mit dem Portalverbund von Bund und Ländern verknüpfen. Die Behörden müssen ihre Verwaltungsleistungen auch über das Verwaltungsportal bereitstellen.

Das niedersächsische Verwaltungsportal wird bereits heute von IT.N im Auftrag des MI als Serviceportal Niedersachsen unter der Adresse

https://service.niedersachsen.de/

bereitgestellt. Hauptbestandteil des Verwaltungsportals ist der BUS. Das Portal soll auch die erforderlichen Formulare, den Link zu Online-Diensten sowie die Anmeldung zum Nutzerkonto enthalten. Das Portal ist so zu gestalten, dass bei der Suche nach Verwaltungsleistungen nicht nur die niedersächsischen, sondern auch die des Bundes und die der anderen Länder gefunden werden. Der Austausch im Portalverbund wird wiederum so gestaltet, dass die relevanten Leistungen im europaweiten Single Digital Gateway erreichbar sind.

Durch die Nutzung des BUS im eigenen Portal oder die Verknüpfung des BUS mit dem eigenen Portal können Behörden, insbesondere Kommunen, viele Funktionen des niedersächsischen Verwaltungsportals auf dem eigenen Portal im eigenen Look & Feel bereitstellen. Sie können so ihren „Kunden“ ein behördeneigenes Verwaltungsportal anbieten und zugleich das NDIG, das OZG und die SDG-Verordnung erfüllen.

Die Verpflichtung der Behörden, ihre Verwaltungsleistungen auch über das Verwaltungsportal bereitzustellen, macht deutlich, dass sie alle Verwaltungsleistungen elektronisch verfügbar machen müssen, so wie es das OZG vorsieht. Dies wird bereits erreicht, wenn Nutzer die Möglichkeit haben, nach § 5 Abs. 2 bereitzustellende elektronische Formulare auch elektronisch über einen der eröffneten Zugänge zu übermitteln. Besser ist es jedoch, wenn Behörden nutzerfreundliche Antragsverfahren bereitstellen, die in einem interaktiven Prozess die einzelnen Schritte der Antragsstellung durchlaufen. Hierfür hat das MI nach § 12 Abs. 1 Satz 1 Nr. 4 ein Antragsverwaltungssystem als Basisdienst bereitzustellen. Das MI erfüllt diese Verpflichtung durch Bereitstellung des Antragsverwaltungssystems NAVO.

OZG und NDIG treffen keine Festlegungen, wie elektronische Antragsverfahren zu gestalten sind oder wie über das Verwaltungsportal eingehende Anträge in den Behörden weiterverarbeitet werden sollen. Es liegt aber nahe, hierfür möglichst bundesweit Standards zu vereinbaren.

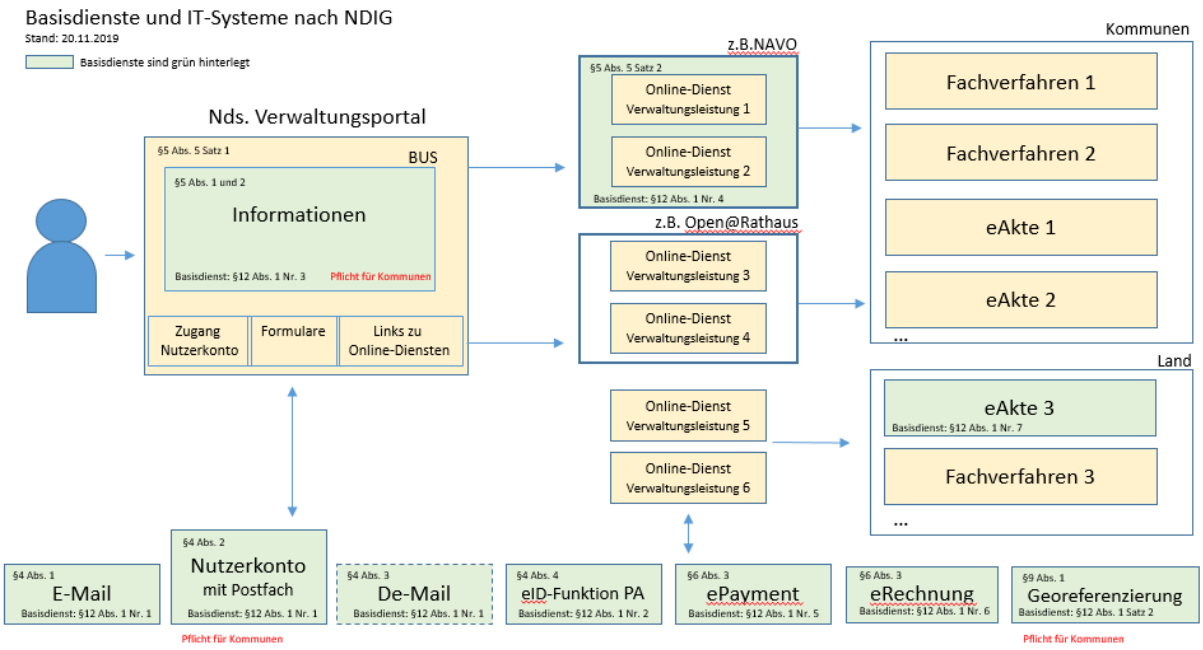


Abbildung 5 Verknüpfung des nds. Verwaltungsportals mit den übrigen Basisdiensten und IT-Systemen

5.6 Online-Bereitstellung von Verfahren nach der SDG-Verordnung

Ab dem 12.12.2023 sind gemäß Artikel 6 der SDG-Verordnung 21 konkrete Verwaltungsleistungen (z.B. Nachweis Geburtsregistereintrag, Wohnsitznachweis, Antrag Studienfinanzierung; siehe Anhang II der SDG-Verordnung) online bereitzustellen. Dabei sind bestimmte Qualitätskriterien einzuhalten. U.a. müssen die Anweisungen zur Abwicklung der Verfahren auch in Englisch zur Verfügung stehen. Die Verfahren müssen über das SDG erreichbar sein.

Diese Verpflichtungen werden erfüllt, wenn die Online-Verfahren über das niedersächsische Verwaltungsportal bereitgestellt und die Qualitätskriterien beachtet werden, weil das nds. Verwaltungsportal über den Portalverbund mit dem SDG verbunden wird.

Weitere Informationen im Landesintranet finden Sie hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505284&_psmand=153

Kontakt zum Thema Online-Dienste in Niedersachsen finden Sie hier:

eMail: P3-DigitaleVerwaltung@IT.Niedersachsen.de

6 Elektronische Bezahlmöglichkeiten (§ 6 Abs. 1 und 2 NDIG)

§ 6 Abs. 1 und 2 NDIG verpflichtet die Behörden, ab dem 1.07.2021 elektronische Bezahlmöglichkeiten zu schaffen, wenn in einem elektronisch durchgeführten Verwaltungsverfahren Gebühren oder sonstige Forderungen anfallen.

§ 6 Abs. 2 NDIG verlangt, dass nach dem Bezahlen die Gutschrift (das sogenannte Zahlungsversprechen) bei der empfangenden Behörde sofort erkennbar ist. Dies gilt für den Fall, dass die Höhe der Gebühren oder der sonstigen Forderungen bereits bei der Antragstellung feststeht und die Verwaltungsleistung erst nach deren Zahlung erbracht wird („Erst zahlen, dann leisten“). Die empfangende Behörde kann dann unmittelbar tätig werden und muss nicht auf den Zahlungseingang bei der Bank warten. Diese Verpflichtung wird mit einem im Internet üblichen ePayment-Verfahren erfüllt, wenn der Bezahlvorgang wie im folgenden vereinfachten Beispiel beschrieben online abgewickelt wird:

1. Im Online-Antragsverfahren der Behörde kann aufgrund der Angaben die Höhe der Zahlungsverpflichtung bereits vor der Leistungserbringung festgesetzt und mitgeteilt werden.
2. Der Antragsteller oder die Antragstellerin betätigt den „Bezahl-Button“.
3. Das Antragsverfahren übermittelt die Daten der Zahlungsverpflichtung an das ePayment-Verfahren unter Angabe eines Urbelegschlüssels bzw. Kassenzeichens.
4. Im ePayment-Verfahren wählt der Antragsteller oder die Antragstellerin die Zahlungsart aus und führt die Zahlung durch.
5. Das ePayment-Verfahren informiert das Antragsverfahren über die erfolgreiche Zahlung.
6. Die zuständige Behörde erhält den Antrag sowie das Zahlungsversprechen mit Angabe des Urbelegschlüssels bzw. Kassenzeichens und kann unmittelbar mit der Bearbeitung der Verwaltungsleistung beginnen. Bei vollautomatisierten Leistungen (z. B. Bereitstellung von kostenpflichtigen elektronischen Informationen) kann die Leistung sofort geliefert werden.

Die Bezahlung mithilfe einer Überweisung im normalen Online-Banking erfüllt dagegen nicht § 6 Abs. 2 NDIG, weil hierbei die empfangende Behörde erst zu einem späteren Zeitpunkt Nachricht über den Eingang der Zahlung erhält. Wenn Kreditinstitute entsprechende Verfahren anbieten (z.B. paydirekt), können aber durchaus Zahlverfahren im Rahmen des ePayment-Verfahrens angeboten werden, bei

denen unmittelbar eine Überweisung durchgeführt wird; in diesem Falle geht der zuständigen Behörde ebenfalls das Zahlungsversprechen umgehend zu.

Für den Fall, dass die Höhe der Gebühr erst zu einem späteren Zeitpunkt ermittelt werden kann (z. B. bei „Erst leisten, dann zahlen“), kann der Antragsteller oder die Antragstellerin nicht sofort bezahlen. Nachdem die zu erbringende Leistung bewertet und deren Entgelt festgesetzt wurde, ist dennoch ein geeignetes ePayment-Verfahren anzubieten.

Nach § 12 Abs. 1 Nr. 5 NDIG muss das MI ein ePayment-Verfahren als Basisdienst bereitstellen. Das MI hat als Basisdienst pmPayment von der Fa. GovConnect GmbH festgelegt. Für Behörden des Landes im Geltungsbereich des NDIG ist die Nutzung vom pmPayment als Bezahlverfahren im Internet obligatorisch (§ 12 Abs. 2 Nr. 5 NDIG). Den übrigen Behörden wird dieser Basisdienst ebenfalls zur Verfügung gestellt.

Weitere Informationen und Kontakt zum ePayment des Landes im Landesintranet finden Sie hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505769&_psmand=153

eMail: P5-DigitaleVerwaltung@it.niedersachsen.de

Weitere Informationen zu pmPayment finden Sie hier:

https://www.govconnect.de/Produkte/E-Government/pmPayment

7 Elektronische Rechnungen (§ 6 Abs. 3 und 4 NDIG)

Öffentliche Auftraggeber in Niedersachsen sind gemäß § 6 Abs. 3 und 4 NDIG ab dem 18.04.2020 verpflichtet, elektronische Rechnungen im Format XRechnung zu empfangen und zu verarbeiten. Auch sonstige elektronische Rechnungen, die dem europäischen Standard EN 16931-1 entsprechen, müssen entgegengenommen werden.

Geltungsbereich und Fristen dieser Regelung folgen aus der Richtlinie 2014/55/EU und sind deshalb abweichend von den sonstigen Regelungen des NDIG. Der Geltungsbereich bezieht sich auf alle öffentlichen Auftraggeber (siehe § 3 Abs. 6 NDIG).

Näheres wird in der Niedersächsischen Verordnung über den elektronischen Rechnungsverkehr (NERechVO[14]) geregelt. Dort ist auch festgelegt, welche Standards für elektronische Rechnungen zulässig sind. Nach § 4 Abs. 3 NERechVO kann das MI zeitlich befristet den Empfang und die Verarbeitung von nicht standardkonformen elektronischen Rechnungen einzelner Rechnungsteller zulassen.

Rechnungsempfänger müssen gemäß § 3 NERechVO die Übermittlung von elektronischen Rechnungen mindestens per eMail oder Webupload ermöglichen. Gemäß § 12 Abs. 1 Nr. 6 NDIG muss das MI einen Basisdienst für den Empfang von eRechnungen bereitstellen. Die Behörden des Landes müssen diesen Dienst nutzen. Die übrigen Behörden können ihn nutzen. Der Basisdienst muss folgende Übermittlungswege bereitstellen:

1. die Weberfassung (manuelle Erstellung einer XRechnung im Internet),

2. den Webupload,

[14] Nds. GVBl. Nr. 9/2020, ausgegeben am 9.04.2020.

3. die Übersendung per eMail (mit der XRechnung im Anhang) und

4. einen Webservice über die Infrastruktur von Pan-European Procurement OnLine (PEPPOL)[15]

Nicht standardkonforme eRechnungen müssen zurückgewiesen werden.

Der Basisdienst wird von IT.N in Form einer ePoststelle für eRechnungen bereitgestellt (siehe https://rechnung.niedersachsen.de). Die ePoststelle nimmt die eRechnungen entgegen, prüft sie auf Schadsoftware und Standardkonformität und stellt sie dem Rechnungsempfänger zur Verarbeitung bereit. Dies erfolgt im XML-Format sowie visualisiert im PDF-Format. Außerdem speichert die ePoststelle die eingehenden eRechnungen nachweissicher ab. Ein eRechnung-Verarbeitungssystem wird von der ePoststelle nicht zur Verfügung gestellt.

Damit die ePoststelle die eRechnung der zuständigen Behörde zuordnen kann, muss diese eine Leitweg-ID enthalten. Jeder Rechnungsempfänger kann bei IT.N eine oder mehrere Leitweg-IDs beantragen.

Weitere Informationen zur ePoststelle des Landes im Landesintranet finden Sie hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505314&_psmand=153

Rechnungssteller und Rechnungsempfänger finden hier weitere Informationen:

https://rechnung.niedersachsen.de

Kontakt für die Nutzung der ePoststelle:

service-erechnung@niedersachsen.de

8 Elektronische Nachweise und Once-Only-Prinzip (§ 7 NDIG)

8.1 Elektronische Nachweise (§ 7 NDIG)

Bürgerinnen, Bürger und Unternehmen sollen Verwaltungsleistungen möglichst einfach nutzen können. § 7 NDIG ermöglicht es daher, dass Nachweise in der Regel auch elektronisch eingereicht werden können. Z.B. soll es möglich sein, dass ein Antragsteller einen Nachweis einscannt oder fotografiert und diesen dann per Upload im Antragsverfahren oder mit dem Postfach des Nutzerkontos der zuständigen Behörde zur Verfügung stellt.

Wenn ein Nachweis von einer anderen Behörde eingeholt werden muss, soll dies mit Einwilligung der betroffenen Person direkt elektronisch bei der ausstellenden Behörde erfolgen. In der Praxis kann dies per Einzelanfrage oder durch den Online-Zugriff auf ein Register erfolgen.

Die niedersächsischen Behörden sollten die Abwicklung ihrer Verwaltungsleistungen entsprechend umgestalten. Das NDIG verpflichtet hierzu zwar nicht, wohl aber die SDG-Verordnung (siehe Folgekapitel).

[15] Gemäß § 7 Satz 2 Nr. 2 NERechVO ab dem 18.04.2022.

8.2 Once-Only-Prinzip nach Artikel 14 SDG-Verordnung

Ab dem 12.12.2023 hat die EU-Kommission eine Plattform einzurichten, über die der Austausch von Nachweisen möglich ist. Für

- 21 konkrete Verwaltungsleistungen (z.B. Nachweis Geburtsregistereintrag, Wohnsitznachweis, Antrag Studienfinanzierung), siehe Anhang 2 der SDG-Verordnung,
- Berufsanerkennungsverfahren,
- Verwaltungsleistungen für Dienstleistungsunternehmen (EU-Dienstleistungsrichtlinie 2006/123/EG) und
- öffentliche Auftragsverfahren

müssen dann Nachweise über die Austauschplattform möglich sein, wenn Nutzerinnen oder Nutzer dies wünschen. Wenn also Behörden Nachweise, die für oben genannten Verfahren von Belang sind, in einem elektronischen Austauschformat ausstellen, müssen sie diese Nachweise auch anfordernden zuständigen Behörden aus anderen Mitgliedstaaten in einem elektronischen Format zur Verfügung stellen.

Die Kommission hat bis zum 12.06.2021 die technischen und operativen Spezifikationen der Austauschplattform festzulegen.

9 Georeferenzierung (§ 9 NDIG)

Mit Hilfe der Georeferenzierung wird einem indirekten Raumbezug in Form eines Ortsnamens, eines Straßennamens, einer postalischen Adresse, einer Gebietseinheit oder einem Grundstück ein direkter Raumbezug in Form einer Koordinate im amtlichen Bezugssystem ETRS89/UTM32 zugeordnet. Damit wird eine korrekte und eindeutige Positionierung (oder Verortung) einer oder mehrerer Adressen auf der Landkarte, in einem Geoinformationssystem oder einem Web-Portal ermöglicht. Auch umgekehrt können, ausgehend von einer Koordinate oder einem bestimmten Gebiet, Identifikatoren (z. B. postalische Adresse) ermittelt werden (reverse Geokodierung).

Nur georeferenzierte Informationen können unmittelbar räumlich analysiert und ausgewertet werden. Der Mehrwert entsteht somit dadurch, dass Daten über die Georeferenzierung verknüpft und Entscheidungen auf Grundlage räumlicher Bezüge solider getroffen werden können. Die Geokodierung von Daten ist von elementarer Bedeutung für die Digitalisierung von Prozessen.

Das Landesamt für Geoinformation und Landesvermessung Niedersachsen (LGLN) stellt allen nach § 9 NDIG zur Georeferenzierung von Registern Verpflichteten den vom Bundesamt für Kartographie und Geodäsie (BKG) betriebenen Geokodierungsdienst der Arbeitsgemeinschaft der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV) kostenfrei zur Verfügung. Damit wird auch die Verpflichtung zur Bereitstellung eines Basisdienstes nach § 12 Abs. 1 Satz 2 NDIG erfüllt.

Weitere Informationen finden Sie hier:

Anmeldung für die Nutzung des Geokodierungsdienstes über das LGLN (Hinweis: Anforderung der Nutzer-/innen-ID):

https://www.lgln.niedersachsen.de/startseite/online_angebote_amp_services/webdienste/geokodierungsdienst_vkv_adressservice/vkv-adressservice-185117.html

Zugang zum Geokodierungsdienst über das Geodatenzentrum des Bundesamtes für Kartographie und Geodäsie BKG:

https://sgs.geodatenzentrum.de/web_geocoder_uuid/?service=gdz_geokodierung&uuidfield=true

Benutzerhandbuch Geokodierungsdienst:

https://sgs.geodatenzentrum.de/web_geocoder_uuid/help/Hilfe_BKGGeocoder.html

Kontakt zum LGLN (Nutzer-/innen-ID):

kontraktmanagement@lgln.niedersachsen.de

10 Elektronische Aktenführung (§ 10 NDIG)

Ab dem 1.01.2023 müssen auf Arbeitsplätzen von Behörden des Landes, auf denen Verwaltungsleistungen über das Niedersächsische Verwaltungsportal erbracht werden, neu anzulegende Akten elektronisch geführt werden. Ab dem 1.01.2026 sollen neu anzulegende Akten in allen Behörden des Landes (im Geltungsbereich des NDIG) elektronisch geführt werden. Im Einvernehmen mit dem IT-Bevollmächtigten sind Fristverlängerungen möglich.

Das MI ist gemäß § 12 Abs. 1 Nr. 7 NDIG verpflichtet einen eAkte-Basisdienst bereitzustellen. Der Basisdienst ist von den Behörden des Landes im Geltungsbereich des NDIG[16] zu nutzen. Die übrigen Behörden können den Basisdienst nutzen. Das MI stellt als eAkte-Basisdienst die VIS-Suite der PDV GmbH bereit, welche von IT.N betrieben wird. Der eAkte-Basisdienst ermöglicht sowohl eine elektronische Ablage als auch eine Vorgangsbearbeitung nach den Vorgaben der Niedersächsischen Aktenordnung. In einer Arbeitsablage können potentiell aktenrelevante Inhalte gespeichert werden, z. B. Entwürfe oder Schriftstücke, deren Aktenrelevanz noch nicht geklärt ist.

Ordnungsgemäße elektronische Aktenführung

Das Rechtsstaatsprinzip aus Art. 19 Abs. 4 und Art. 20 Abs. 3 GG, der Amtsermittlungsgrundsatz (z. B. § 24 VwVfG, § 20 SGB X) und der Anspruch auf Akteneinsicht (z. B. § 29 VwVfG, § 25 SGB X) führen zu dem Grundsatz der Aktenmäßigkeit der Verwaltung. Dieser Grundsatz verpflichtet die Verwaltung Akten zu führen, in denen das Verwaltungshandeln vollständig, nachvollziehbar und transparent zu dokumentieren ist.

Daraus leiten sich Anforderungen ab, die zu einer ordnungsgemäßen Aktenführung gehören. Alle *bedeutsamen* Geschäftsvorfälle sind in mit eigenen Aktenzeichen bzw. Geschäftszeichen zu versehenden Akten oder Vorgängen zu dokumentieren und unveränderlich aufzubewahren. Sie müssen

[16] Ausnahmen finden sich in § 3 Abs. 4 NDIG

alle entscheidungserheblichen (*bedeutsamen*) Dokumente und Bearbeitungsschritte enthalten. Aktuelle und abgeschlossene Geschäftsvorfälle können vollständig und rechtssicher rekonstruiert werden. Das dient sowohl der Beweissicherung als auch der gegebenenfalls erforderlichen Beweisführung.

Die ordnungsgemäße Aktenführung erfordert eine sachliche Ordnung, die über einen – mit wenigen Ausnahmen (Steuerverwaltung, Justiz) einheitlichen Aktenplan gewährleistet wird. In Niedersachsen gibt es seit 1962 eine – mit wenigen Ausnahmen (Steuerverwaltung und Justiz) – einheitliche Aktenordnung (Nds. AktO), die seit 2006 auch die elektronische Aktenführung berücksichtigt. In Akten und Vorgängen geführte aktenrelevante Dokumente werden mit einem strukturierten Aktenzeichen bzw. Geschäftszeichen versehen. Bis zum Ablauf der Aufbewahrungsfristen sind sie recherchierbar und lesbar. Nach Ablauf der Aufbewahrungsfristen werden sie ausgesondert und dem Niedersächsischen Landesarchiv zur Übernahme angeboten.

In der elektronischen Aktenführung müssen inhaltliche Veränderungen an den aktenrelevanten Dokumenten ersichtlich sein. Sie müssen Änderungen und ihre Urheberschaft erkennen lassen. Der Geschäftsgang muss nachvollziehbar sein. Das bedeutet, dass Informationen und Prozessschritte (z. B. Sichtvermerke, Geschäftsgangvermerke, Mitzeichnungen), die den Bearbeitungszusammenhang, die Entscheidungsfindung und den chronologischen Ablauf der Bearbeitung betreffen, nachvollziehbar sein müssen. Das Recht und die Pflicht zur Remonstration (§ 36 BeamtStG) sowie die Beratungs- und Unterstützungspflicht gegenüber Vorgesetzten (§ 35 Abs. 1 Satz 1 BeamtStG) bedeuten zugleich, dass etwaige Bedenken der Mitarbeiterinnen und Mitarbeiter gegen dienstliche Anordnungen in die Akte aufzunehmen sind. Eben dies gilt für den Fall der begründeten Ablehnung einer Mitzeichnung oder einer Schlusszeichnung.

In Niedersachsen kommen EAkte-Systeme zum Einsatz, die diese Anforderungen erfüllen. Windows-Fileserver, Outlook-Ablagen, SharePoint-Systeme und ähnliche für die PC-Arbeit entwickelten Systeme sind dagegen für eine ordnungsgemäße *elektronische* Aktenführung nicht ausreichend.

Die Einführung der eAkte in der niedersächsischen Landesverwaltung erfolgt im Rahmen des Projekts P 8 des Programms DVN. Das Projekt P 8 hat einen Landesstandard entwickelt, der als Rahmen für einen vereinheitlichten Funktionsumfang und die entsprechende Konfiguration in den Behörden dient. Mit der weitgehenden Standardisierung zielt der Landesstandard auf einen einfachen übergreifenden Akten- und Dokumentenaustausch ab, u.a. im Rahmen einer Vorgangsbearbeitung, begrenzt zugleich die betrieblichen und wirtschaftlichen Aufwände für Pflege und Administration. Er wird nach den Anforderungen der Behörden weiterentwickelt. Im Rahmen des Projekts P 8 erfolgt die schrittweise Einführung der eAkte in den Behörden des Landes.

In § 10 Abs. 4 NDIG ist festgelegt, dass der Austausch elektronisch geführter Akten innerhalb einer Behörde und zwischen Behörden elektronisch erfolgen soll. Die Landesregierung kann hierfür technische Verfahren und Standards per Verordnung regeln, hat hiervon aber bislang keinen Gebrauch gemacht.

Es gibt aber untergesetzliche Regelungen, die einen Rahmen vorgeben. Der IT-Planungsrat Bund/Länder bzw. dessen Koordinierungsstelle für IT-Standards (KoSIT) hat ein Datenaustauschformat für Akten

oder sonstiges Schriftgut festgelegt. Dies ist der Standard XDOMEA, der aktuell in der Version 2.4.0 vorliegt, siehe:

https://www.xrepository.de/details/urn:xoev-de:xdomea:kosit:standard:xdomea

Da die Beschlüsse des IT-Planungsrats Bund/Länder zu fachübergreifenden Standards für die Länder verbindlich sind, ist dieses Format als Austauschformat „gesetzt".

Für die elektronische Übermittlung von Akten sollten ausreichend sichere Verfahren in Bezug auf Vertraulichkeit und Authentizität gewählt werden. Soweit dies nicht innerhalb eines gemeinsamen eAkte-Systems ohnehin erfüllt ist, bietet sich als Übermittlungsweg der Austausch über besondere Behördenpostfächer (beBPo) an, über die auch die Kommunikation mit Gerichten erfolgt. Jede Behörde sollte über mindestens ein beBPo verfügen. Diese Postfächer verwenden den Standard OSCI-Transport, der sowohl eine verschlüsselte Übertragung als auch einen sicheren Nachweis der absendenden und empfangenden Stelle ermöglicht. Die Anbringung von elektronischen Signaturen ist somit nicht erforderlich.

Weitere Informationen im Landesintranet finden Sie hier:

http://intra.it.niedersachsen.de/live/index.php?intranet_id=505478&_psmand=153

Kontakt zum Projekt P 8 des Programms DVN:

eMail: P8-DigitaleVerwaltung@it.niedersachsen.de

11 Ersetzendes Scannen (§ 11 NDIG)

§ 11 NDIG verpflichtet die Behörden des Landes, soweit sie Akten elektronisch führt, Papierdokumente einzuscannen und zur eAkte zu nehmen. Die Papierdokumente sollen vernichtet werden (ersetzendes Scannen), wenn eine Aufbewahrung nicht aus rechtlichen Gründen erforderlich ist.

Das Bundesamt für Sicherheit in der Informationstechnik hat die Richtlinie BSI TR-03138 (RESISCAN) veröffentlicht, die die Maßnahmen für eine zuverlässige technische Realisierung des Scannens beschreibt. Das NDIG schreibt zwar nicht vor, dass diese Maßnahmen eingehalten werden müssen. Sie können aber herangezogen werden, um Maßnahmen nach dem Stand der Technik festzulegen.

Ausnahmen vom ansonsten verpflichtenden Scannen sind durch § 11 NDIG zugelassen, entweder wenn es unverhältnismäßig aufwändig ist oder, wenn rechtliche Gründe gegen das Vernichten von Originalunterlagen sprechen.

Weitere Informationen zum ersetzenden Scannen finden Sie hier:

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html

Kontakt zum Thema ersetzendes Scannen im Projekt DVN:

eMail: P13-DigitaleVerwaltung@it.niedersachsen.de

12 Elektronische Basisdienste (§ 12 NDIG)

Ab dem 1.07.2021 hat das MI bestimmte Basisdienste bereitzustellen. § 12 NDIG regelt auch Nutzungspflichten zu den Basisdiensten. Die genaue Zuordnung kann den folgenden zwei Tabellen entnommen werden.

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 NDIG für Behörden des Landes			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
einfacher Zugang, z. B. eMail (ggf. QES)	Zugangseröffnung, § 4 Abs. 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
Nutzerkonto	Zugangseröffnung, § 4 Abs. 2 Satz 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
De-Mail oder anderer schriftformersetzender Dienst	Zugangseröffnung, § 4 Abs. 3	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	verpflichtend, § 12 Abs. 2 Satz 1
Identifizierung mit Personalausweis, Aufenthaltstitel	Identifizierung, § 4 Abs. 4	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 2	verpflichtend, § 12 Abs. 2 Satz 1
BUS (Allgemein)	Info-Bereitstellung, § 5 Abs. 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3	verpflichtend, § 12 Abs. 2 Satz 1
BUS (Leistungsbeschreibung) mit Formularserver	Info-Bereitstellung, § 5 Abs. 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3	verpflichtend, § 12 Abs. 2 Satz 1
Antragsverwaltungssystem	Verfahren bereitstellen, § 5 Abs. 5	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 4	verpflichtend, § 12 Abs. 2 Satz 1
Elektronisches Bezahlverfahren	Bereitstellung, § 6 Abs. 1 und 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 5	verpflichtend, § 12 Abs. 2 Satz 1
eRechnung	Empfang und Verarbeitung ab 18. April 2020, § 6 Abs. 3	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 6	verpflichtend, § 12 Abs. 2 Satz 1
Georeferenzierung	Angabe von Koordinaten nach § 9	durch das für Geobasisdaten zuständige Ministerium, § 12 Abs. 1 Satz 2	verpflichtend, § 12 Abs. 2 Satz 1
Elektronische Aktenführung	Stufenweise flächendeckende Einführung bis 1. Januar 2026, § 10 Abs. 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 7	verpflichtend, § 12 Abs. 2 Satz 1

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 NDIG für Kommunen und sonstigen Aufsicht des Landes unterstehenden juristischen Personen			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
einfacher Zugang, z. B. eMail (ggf. QES)	Zugangseröffnung, § 4 Abs. 1 Satz 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	

Verpflichtungen aus den §§ 4, 5, 6, 9, 10 und 12 NDIG für Kommunen und sonstigen Aufsicht des Landes unterstehenden juristischen Personen			
IT-Verfahren	**Verpflichtung**	**Bereitstellung Basisdienst**	**Verpflichtung Nutzung Basisdienst**
Nutzerkonto	Zugangseröffnung, § 4 Abs. 2 Satz 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1, kostenfrei, § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
De-Mail oder anderer schrift-formersetzender Dienst	Zugangseröffnung, § 4 Abs. 3	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 1	
Identifizierung mit Personalausweis, Aufenthaltstitel		durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 2	
BUS (Allgemein)	Info-Bereitstellung, § 5 Abs. 1	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3, kostenfrei § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
BUS (Leistungsbeschreibung) mit Formularserver	Info-Bereitstellung, § 5 Abs. 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 3, kostenfrei § 12 Abs. 3 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
Antragsverwaltungssystem	Verfahren bereitstellen, § 5 Abs. 5	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 4, kostenfrei § 12 Abs. 3 Satz 2	
Elektronisches Bezahlverfahren	Bereitstellung, § 6 Abs. 1 und 2	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 5	
eRechnung	Empfang und Verarbeitung ab 18.04.2020, § 6 Abs. 3	durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 6	
Georeferenzierung	Angabe von Koordinaten nach § 9	durch das für Geobasisdaten zuständige Ministerium, § 12 Abs. 1 Satz 2	verpflichtend, § 12 Abs. 3 Satz 1
Elektronische Aktenführung		durch IT-Ministerium, § 12 Abs. 1 Satz 1 Nr. 7	

Das MI stellt folgende Verfahren als Basisdienste bereit:

Basisdienst	**Vorgesehenes System**	**Bemerkung[17]**
einfacher Zugang, z. B. eMail (ggf. QES)	eMail-Server von IT.N auf Basis von Produkten der Microsoft Corporation	Bereitstellung durch IT.N

[17] Auf die Kostenfreiheit wird nur hingewiesen, wenn diese gesetzlich vorgeschrieben ist. In den übrigen Fällen entscheidet das bereitstellende Ministerium, ob und ggf. welche Kosten erhoben werden.

Basisdienst	Vorgesehenes System	Bemerkung[17]
Nutzerkonto	Nutzerkonto-Dienst der Dataport AöR	Bereitstellung über IT.N kostenfrei gemäß § 12 Abs. 3 Satz 2 NDIG
De-Mail oder anderer schriftformersetzender Dienst	De-Mail-Dienst eines De-Mail-Providers	Bereitstellung über IT.N Ggf. Ergänzung durch De-Mail-Gateway und Multimessenger-Dienst
Identifizierung mit Personalausweis, Aufenthaltstitel	eID-Service des Nutzerkonto-Dienstes der Dataport AöR	Bereitstellung über IT.N
BUS (Allgemein und Leistungsbeschreibung) mit Formularserver	Bürger- und Unternehmensservice (BUS) auf Basis des Systems Infodienste der Teleport GmbH	Bereitstellung durch IT.N Im Verbund Linie 6+[18] kostenfrei gemäß § 12 Abs. 3 Satz 2 NDIG
Antragsverwaltungssystem	Niedersächsisches Antragsverwaltungsverfahren Online (NAVO) auf Basis von GovOS der FJD Information Technologies AG	Bereitstellung durch IT.N kostenfrei gemäß § 12 Abs. 3 Satz 2 NDIG
Elektronisches Bezahlverfahren	pmPayment der GovConnect GmbH	Bereitstellung durch die GovConnect GmbH
eRechnung	ePoststelle für eRechnungen von IT.N	Bereitstellung durch IT.N
Georeferenzierung	Geokodierungsdienst des Bundesamts für Kartographie und Geodäsie (BKG)	Referenzierungsdienst der AG der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV);
Elektronische Aktenführung	VIS-Suite der PDV GmbH	Bereitstellung durch IT.N In Teilbereichen eGov-Suite der Fa. Fabasoft AG

13 Informationssicherheit

Die Nutzung von IT-Systemen, insbesondere die Kommunikation über das Internet, durchdringt die Gesellschaft zwischenzeitlich fast vollständig. Auch staatliches Handeln, insbesondere die Funktionsfähigkeit der Exekutive, wäre bereits heute ohne eine funktionierende Informationstechnologie erheblich beeinträchtigt. Die Verwaltung kommuniziert überwiegend per eMail, nutzt vermehrt Voice-Over-IP-Technologien und verarbeitet die zur Aufgabenerledigung erforderlichen, teils sensiblen Daten von Bürgerinnen und Bürgern auf ihren IT-Systemen.

[18] Die Linie 6+ ist ein Verbund der Länder Niedersachsen, Sachsen-Anhalt, Thüringen, Hessen, Rheinland-Pfalz, Schleswig-Holstein, Mecklenburg-Vorpommern und Brandenburg zur Weiterentwicklung eines elektronischen Behördenwegweisers.

Mit den §§ 4 bis 12 NDIG sind der Verwaltung in Niedersachsen eine Reihe von Verpflichtungen vorgegeben worden, die deren Leistungsfähigkeit steigern und ein modernes, zeitgemäßes Verwaltungshandeln ermöglichen. Zusammen mit der Umsetzung des OZG wird dies zu einer umfassenden Digitalisierung der Verwaltungsabläufe und damit zu einer weitgehenden Abkehr von der papiergebundenen Informationsverarbeitung führen. Dadurch entsteht allerdings eine nahezu vollständige Abhängigkeit der Funktionsfähigkeit der Verwaltung von der Verfügbarkeit der Informationstechnologie.

Angriffe auf Informations- und Kommunikationsinfrastrukturen – auch der öffentlichen Verwaltung – sind in den letzten Jahren immer zahlreicher und komplexer geworden; gleichzeitig ist eine zunehmende Professionalisierung der Angriffe zu verzeichnen. Hochentwickelte Schadsoftware, die vor einigen Jahren noch Geheimdiensten vorbehalten war, ist mittlerweile in einschlägigen Kreisen frei verfügbar und wird ständig weiterentwickelt. Dazu kommen ausgeklügelte Methoden der sozialen Manipulation und des Diebstahls von Identitäten.

Diese Angriffswellen, die sich auch gegen die IT-Systeme der Verwaltung in Niedersachsen richten, bedrohen zunehmend deren Funktionsfähigkeit und deren rechtmäßiges Handeln. So hat sich sogenannte „Ransomware“, das heißt Software, welche die Daten der betroffenen Computer durch eine Verschlüsselung von Dateien angreift, die nur durch Zahlung eines Lösegeldes entschlüsselt werden können und damit zum Gegenstand einer Erpressung gemacht werden, stark verbreitet. Prominente Beispiele sind die Angriffe mittels der Schadsoftware „EMOTET“ auf die IT der Verwaltung der Stadt Neustadt am Rübenberg, das Kammergericht Berlin sowie die Verwaltung der Medizinischen Hochschule Hannover (MHH).

Deshalb sind einhergehend mit den Zielen der Digitalisierung der Verwaltung eine Reihe von Maßnahmen zu treffen, um auch zukünftig die Funktionsfähigkeit der Verwaltung und den Schutz der Daten der Bürgerinnen und Bürger auf den IT-Systemen des Landes sicherzustellen. Der Dritte Teil des NDIG schafft daher insoweit die Ermächtigungsgrundlagen für die Implementierung IT-gestützter Anwendungen, um Gefahren für die Informationssicherheit abzuwenden und den Grundrechtsschutz der Bürgerinnen und Bürger zu gewährleisten. Abweichend vom Zweiten Teil des NDIG gilt der Dritte Teil ausschließlich für diejenigen Behörden und Institutionen, die in den jeweiligen Vorschriften unmittelbar berechtigt und verpflichtet werden.

14 Allgemeine Vorschriften zur Informationssicherheit

14.1 Der Sicherheitsverbund im Landesdatennetz

Die Vorschrift § 13 Abs. 1 Satz 1 NDIG stellt zunächst klar, dass die Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, Mitglieder eines Sicherheitsverbundes sind. Jedes Mitglied des Sicherheitsverbundes hat auf der Basis von Risikoanalysen eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit, auch im Hinblick auf andere Mitglieder des Sicherheitsverbundes, zu gewährleisten (§ 13 Abs. 1 Satz 2 NDIG). Der damit entstehende Solidarverbund und das gegenseitige Vertrauen auf Sicherheit gegenüber dem anderen erleichtern den Betrieb und die Nutzung von IT-Verfahren enorm. Allerdings erwächst daraus auch die Verpflichtung, diesem Vertrauen zu genügen. Jedes Mitglied des Sicherheitsverbundes hat

daher die nach § 13 Abs. 1 Satz 2 NDIG erforderlichen technischen und organisatorischen Maßnahmen unverzüglich zu veranlassen und regelmäßig zu überprüfen und anzupassen (§ 13 Abs. 1 Satz 3 NDIG).

Ein zentrales Element dieses Informationssicherheitsmanagementsystems der niedersächsischen Landesverwaltung ist das Handeln auf der Basis von Risikoanalysen. Das Erkennen und Behandeln von Risiken, nämlich deren Reduzierung, Vermeidung, Verschiebung oder letztlich deren Akzeptanz durch die verantwortlichen Behördenleitungen ermöglicht eine flexible und wirtschaftliche, dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit (§ 13 Abs. 1 Satz 2 NDIG).

Weitere Informationen im Landesintranet zum niedersächsischen Informationssicherheitsmanagement finden Sie hier:

http://intra.cio.niedersachsen.de/live/index.php?intranet_id=24496&_psmand=170

Kontakt zum Chief Information Security Officer (CISO):

Mail: ciso@mi.niedersachsen.de

14.2 Das N-CERT

Bei dem für die zentrale IT-Steuerung zuständigen Ministerium ist eine Zentralstelle für Informationssicherheit eingerichtet, vgl. § 14 NDIG. Dies ist zurzeit das N-CERT, d. h. das Niedersächsische Computer Emergency Response Team. Es ist als ein strategisch arbeitendes CERT auf der Ministerialebene angesiedelt und in der Stabsstelle CIO im MI organisiert.

Das N-CERT wertet arbeitstäglich laufend über 130 Informationsquellen zu Bedrohungen und Angriffen aus dem Cyberraum aus. Es steht mit allen CERTs im deutschsprachigen Raum in Europa im ständigen Kontakt. Dazu ist es Mitglied im Verwaltungs-CERT-Verbund sowie im Deutschen CERT-Verbund, in dem sich Unternehmen wie die Telekom, Volkswagen oder Siemens austauschen. Weiterhin steht es im ständigen Austausch mit den polizeilichen Ermittlungsbehörden und der Staatsanwaltschaft in Bezug auf Cyber-Delikte sowie dem Verfassungsschutz auf Landes- und Bundesebene. Durch die frühzeitige Detektion, Bewertung und Reaktion gegenüber Cyber-Bedrohungen trägt das N-CERT maßgeblich zur IT-Sicherheit in der Landesverwaltung bei.

Das N-CERT arbeitet sehr eng mit dem Security Operation Center des IT.N zusammen. Hier werden operative und forensische Untersuchungen zu Bedrohungen und Sicherheitsvorfällen durchgeführt und so gemeinsam Risiken bewertet und Sicherheitsmaßnahmen konzipiert. Diese Aufgaben sind im § 14 Abs.1 NDIG normiert worden.

Damit das N-CERT über eine aktuelle Sicherheitslage im Landesdatennetz verfügt, sind alle Mitglieder des Sicherheitsverbundes verpflichtet, Sicherheitsvorfälle gem. § 14 Abs. 2 NDIG dem N-CERT unverzüglich mitzuteilen. Ebenso benötigt das N-CERT die Kenntnis über sämtliche auf der Grundlage des Zweiten Abschnitts betriebenen IT-Systeme insbesondere über die IDS[19] und SIEM[20]-Systeme, die Hinweise auf Sicherheitsvorfälle geben können (§ 14 Abs. 3 NDIG).

[19] Intrusion Detection System
[20] Security Incident and Event Management

Das N-CERT steht daneben mit seiner Expertise allen Stellen der Landesverwaltung zur Verfügung. An den Warn- und Informationsdienst des N-CERT sind derzeit 104 Kommunen angeschlossen, die bedarfsspezifisch mit Informationen versorgt werden.

Weitere Informationen finden Sie hier:

https://www.mi.niedersachsen.de/startseite/themen/it_bevollmachtigter_der_landesregierung/niedersachsen_cert/niedersachsen-cert-150589.html

Kontakt zum N-CERT:

Mail: cert@mi.niedersachsen.de

14.3 Förderung der IT-Sicherheit (§ 15 NDIG)

Aufgrund der o. g. Gefahren obliegt es der das Landesdatennetz betreibenden Behörde (IT.N) und einer vom Justizministerium zu bestimmenden Stellen (Zentraler IT-Betreib Niedersächsische Justiz (ZIB) beim OLG Celle) gemäß § 15 Abs. 1 NDIG die IT-Sicherheit im Landesdatennetz bzw. im Netzabschnitt der Justiz zu fördern. Hierzu werden den Stellen jeweils für ihre Netzabschnitte oder auch das gesamte Landesdatennetz in den Absätzen 2 und 3 bestimmte Aufgaben zugewiesen. Um der Sonderstellung der Justiz gerecht zu werden, wurde der Netzabschnitt der Justiz als eigener definiert.

Zudem besteht für IT.N und den ZIB nach Absatz 4 die Verpflichtung, in den jeweiligen Netzabschnitten dem Stand der Technik entsprechende IT-Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit zu betreiben.

Nach dem derzeitigen Stand der Technik ist es insbesondere erforderlich, IDS und SIEM-Systeme einzusetzen. Bei IDS handelt es sich um IT-Systeme, die den Einbruch in andere IT-Systeme erkennen sollen. Ein Einbruch in ein IT-System liegt vor, wenn sich eine Person unberechtigt Zugriff zu einem IT-System verschafft. IDS sollen bestehende Sicherheitsmaßnahmen zur Verhinderung von Einbrüchen flankieren (und keinesfalls ersetzen), da allgemein davon ausgegangen wird, dass es keine zu 100 % sicheren Systeme gibt, mithin also immer damit gerechnet werden muss, dass ein Angreifer auch in geschützte Systeme eindringen kann. Ein IDS, dessen Betriebszweck die Erzeugung sicherheitsrelevanter Ereignisse ist, kann insoweit eine Datenquelle für ein SIEM-System darstellen.

Bei SIEM-Systemen handelt es sich um Systeme, die eine Echtzeitanalyse von sicherheitsrelevanten Ereignissen ermöglichen, die beim Betrieb von IT-Systemen und den darauf betriebenen Computerprogrammen einschließlich des Betriebssystems und seiner Dienste – in der Regel in Protokolldateien (sogenannte „log files“) – anfallen und gespeichert werden. Die SIEM-Systeme können außerdem durch die Speicherung der Ereignisse über einen längeren Zeitraum die Möglichkeit für eine Analyse eröffnen (z. B. von sich verändernden Angriffsverhalten und der Ermittlung neuer Angriffsvektoren). Diese ist typischerweise Gegenstand eines regelmäßigen Berichtswesens an die für die Informationssicherheit einer Organisation verantwortlichen Führungskräfte.

14.4 Maßnahmen zur Abwehr von Gefahren für die IT-Sicherheit

Der oder dem CIO wird in § 16 NDIG das Recht eingeräumt, bei einer gegenwärtigen Gefahr für die IT-Sicherheit, die zu einer Gefahr für die IT-Sicherheit bei anderen Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, führen kann, vorübergehende und unaufschiebbare Maßnahmen gegenüber Behörden und Gerichten des Landes anzuordnen, die zur Gewährleistung der IT-Sicherheit erforderlich sind. Dies gilt nur im Sicherheitsverbund des Landesdatennetzes und gegenüber Behörden des Landes. Auch dürfen die Maßnahmen nur vorübergehend angeordnet werden, da es sich quasi um Notstandsmaßnahmen handelt. Für die Definition der „gegenwärtigen Gefahr“ kann die Legaldefinition in § 2 Nr. 2 Niedersächsisches Polizei- und Ordnungsbehördengesetz (NPOG) herangezogen und modifiziert werden. Eine gegenwärtige Gefahr ist danach eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht. Wenn Angriffe auf die elektronische Verwaltungsinfrastruktur des Landes Niedersachsen drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, muss die Verfügbarkeit der Informationstechnik, insbesondere des Landesdatennetzes, entsprechend der Bedrohungslage und des Schadensrisikos vorübergehend eingeschränkt werden können. Im Interesse der Funktionsfähigkeit der gesamten Landesverwaltung und der Vertraulichkeit der Datenbestände ist der Schutz vor erheblichen Schäden vorrangig gegenüber der Funktionsfähigkeit einzelner Bereiche oder einzelner Dienste.

Etwaige Maßnahmen nach § 16 NDIG dürfen jedoch nur vorübergehend angeordnet werden, wenn eine Gefahr für die IT-Sicherheit oder ein gravierender Sicherheitsvorfall vorliegt oder unmittelbar bevorsteht und die Maßnahme daher unaufschiebbar ist. Ansonsten sollen solche Maßnahmen von den Behörden selbst getroffen werden, die für das jeweilige Verfahren zuständig sind - in Abstimmung mit den ansonsten betroffenen Behörden.

Zu beachten ist auch, dass die Anordnungsbefugnis nur gegenüber den Behörden des Landes greift. Allerdings kann eine Anordnung auch gegenüber dem zentralen IT-Dienstleister erfolgen. Inhalt könnte die Anordnung zum Abschalten einzelner Netzsegmente oder Basisdienste sein. Hiervon können auch die Kommunen betroffen sein, da diese das Landesdatennetz und bestimmte Basisdienste mit nutzen. Da es sich um ein Ultima-Ratio-Mittel handelt, wird dies jedoch nur im Ausnahmefall nach einer gründlichen Abwägung erfolgen.

15 Einsatz von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit

Die Befugnis, Maßnahmen nach dem Zweiten Abschnitt zu treffen, erhalten Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. Ein IT-System gilt im Sinne dieses Gesetzes mit dem Landesdatennetz verbunden, wenn es direkt oder über ein untergeordnetes behördeneigenes Netz (z. B. lokale Netze oder Datennetze der Kommunen) technisch angeschlossen ist. Nicht verbunden mit dem Landesdatennetz sind IT-Systeme, die nur über das Internet erreichbar sind. Netze von Verwaltungen außerhalb Niedersachsens einschließlich des Verbindungsnetzes zwischen den Landesdatennetzen sind im Sinne dieses Gesetzes nicht mit dem Landesdatennetz verbunden.

Die Ermächtigungen nach §§ 18 bis 23 NDIG unterliegen wegen des damit verbundenen Grundrechtseingriffs strengen Voraussetzungen, deren Einhaltung mit erheblichem technischen und vor allem auch organisatorischem Aufwand für eine Behörde verbunden ist, die solche IT-Systeme einsetzt. Daher hat der Gesetzgeber die Pflicht, diese Maßnahmen umzusetzen, nur den großen zentralen IT-Betrieben übertragen, vgl. § 15 NDIG. Alle anderen Behörden, die grundsätzlich von den Ermächtigungen nach §§ 18 bis 23 NDIG Gebrauch machen könnten, sollten sehr genau Nutzen und Aufwand für eine rechtssichere Umsetzung der gesetzlichen Vorgaben gegeneinander abwägen und ggf. eine zentrale Lösung bei den genannten IT-Betrieben suchen.

Kontakt bei Fragen zur zentralen IDS/SIEM-Lösung beim MI: cert@mi.niedersachsen.de, ciso@mi.niedersachsen.de

Im Folgenden sind diese Voraussetzungen exemplarisch an den §§ 18, 19, 20 und 21 NDIG dargestellt.

15.1 Automatisierte Auswertung eines Verzeichnis- und Berechtigungsdienstes (§ 18 NDIG)

§ 18 NDIG schafft eine Rechtsgrundlage für den Betrieb eines sogenannten Advanced Threat Analytics–System (ATA). Hierbei werden in dem System zusätzlich Metadaten aus dem Verzeichnisdienst Active Directory erhoben und ausgewertet. Diese dürfen nicht an Knoten- und Übergabepunkten, sondern am Verzeichnisdienst selbst erhoben werden. Als auffälliger Datenverkehr im Sinne dieser Vorschrift gelten z. B. ungewöhnlich häufige, direkt aufeinanderfolgende Anmeldeversuche, die nur von einer Kennung ausgehen, ungewöhnliche Bewegungsmuster durch Konten von Systemdiensten oder gleichzeitige Anmeldeversuche einer Kennung aus unterschiedlichen Subnetzen. Die Analyse des erhobenen Datenverkehrs und der Abgleich gegen den Normalzustand erfolgen vollständig automatisch. Wird eine Abweichung vom Normalzustand identifiziert, erfolgt die Auflösung der Meldung manuell. Ziel ist es, verdächtige Aktivitäten innerhalb des Netzwerks, und hier besonders im Verzeichnisdienst, zu identifizieren.

15.2 Automatisierte Auswertung von Ereignisdokumentationen und Datenverkehr (§ 19 NDIG)

Bei § 19 Abs. 1 NDIG handelt es sich um eine Zweckänderungsnorm, die es zulässt, bereits gespeicherte Datenbestände aus den aufgezählten Systemen auszuwerten. Nicht enthalten ist darin allerdings eine Ermächtigung zum Erheben dieser Daten, da eine derartige Ermächtigungsgrundlage gemäß § 3 NDSG und im Übrigen gemäß Artikel 6 Abs. 1 DSGVO bereits besteht. Aufgrund der strengen Zweckbindung dürfen die erhobenen Daten bisher nicht für den Zweck der IT-Sicherheit im Sinne dieses § 19 Abs. 1 NDIG verwendet werden. Die Zweckänderung in diesem Absatz lässt die Auswertung zu diesem Zweck nunmehr zu. Die Behörden dürfen die Daten zusammenführen und ausschließlich automatisiert auswerten, soweit dies zur Abwehr von Sicherheitslücken, Schadprogramme oder Angriffe und damit von

Gefahren für die IT-Sicherheit erforderlich ist. Im Vordergrund steht somit auch hier die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten. Absatz 1 S. 1 enthält daher selbst eine strenge Zweckbindung für die Verwendung der bereits auf anderer rechtlicher Grundlage erhobenen Daten.

Die Systeme, deren elektronische Ereignisdokumentationen automatisiert untersucht werden dürfen, sind in Absatz 1 S. 2 enumerativ aufgezählt. Automatisierte Ereignisdokumentationen sind die Protokolldaten, die in Protokolldateien, auch „log files“ genannt, automatisch abgelegt werden.

§ 19 Abs. 2 NDIG dient dazu, die Rechtsgrundlage zu schaffen, um den Datenverkehr im Landesdatennetz automatisiert nach Auffälligkeiten zu durchsuchen. Der Absatz stellt klar, dass es lediglich um die Daten geht, welche innerhalb der Informations- und Kommunikationsinfrastruktur des Landes verarbeitet und gespeichert werden und damit dem Verfügungsbereich des Landes unterliegen.

In Absatz 2 Satz 1 wird die strenge Zweckbindung normiert. Die Auswertung des Datenverkehrs hinsichtlich vorhandener Sicherheitslücken, Schadprogrammen oder Angriffen darf nur zur Abwehr von Gefahren für die IT-Sicherheit der Behörden erfolgen, somit gemäß § 1 Nr. 7 NDIG zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten. Angriffe sollen erkannt und deren Folgen beseitigt werden können, zudem soll Angriffen vorgebeugt werden. Die Suche nach Auffälligkeiten erfolgt an dieser Stelle ausschließlich automatisiert an den Übergabe- und Knotenpunkten der Behördennetze, die von der Behörde oder in deren Auftrag betrieben werden. Dazu dürfen die Daten automatisiert erhoben, entschlüsselt und unverzüglich, also ohne schuldhaftes Zögern, ausgewertet werden. Somit handelt es sich um eine Echtzeitanalyse des Datenverkehrs. Übergabe- und Knotenpunkte sind IT-Systeme, die den Datenverkehr mit einem anderen Netz sicherstellen oder ihn innerhalb des eigenen Netzes verteilen. Die Übergabe- und Knotenpunkte müssen gemäß § 1 Abs. 2 NDIG mit dem Landesdatennetz verbunden sein.

Die Auffälligkeiten im Datenverkehr ergeben sich aus einem Abweichen von dem festgelegten Normalzustand des Datenverkehrs und des Systemverhaltens sowie der Entdeckung von Schadsoftware.

Absatz 3 stellt klar, dass im Rahmen der automatisierten Verarbeitung nach Absatz 1 und 2 eine Auswertung der kommunikativen Bedeutung strikt untersagt ist. Auf dieser ersten Stufe dürfen lediglich vorher eingestellte und abgestimmte automatisierte Routinen verwendet werden, die eine solche Auswertung nicht vornehmen. Erst bei wenigstens zureichenden tatsächlichen Anhaltspunkten ist eine weitergehende Auswertung dieser Inhaltsdaten unter den strengen Voraussetzungen des § 21 möglich.

Sofern die Auswertung keine zureichenden tatsächlichen Anhaltspunkte ergab, regelt Absatz 4, dass die Daten unverzüglich, also ohne schuldhaftes Zögern, zu löschen sind. Dies gilt nicht für die nach Absatz 1 herangezogenen Datensätze, sofern diese noch für den ursprünglichen Verwendungszweck benötigt werden.

15.3 Weitere Auswertung ohne Inhaltsdaten in Verdachtsfällen (§ 20 NDIG)

§ 20 NDIG trifft Regelungen zur Auswertung aller Daten, die nicht Inhaltsdaten sind. § 20 Abs. 1 S. 1 NDIG lässt eine weitere einzelfallbezogene automatisierte Auswertung bestimmter Daten nach § 18 Abs. 1 oder 19 Abs. 1 oder 2 NDIG zu, sofern „zureichende tatsächliche Anhaltspunkte“ für eine Gefahr

vorliegen. Dabei dürfen die zusammengeführten Daten höchstens 30 Tage gespeichert werden. Der Begriff „zureichende tatsächliche Anhaltspunkte“ stammt aus dem strafprozessualen Bereich (§ 152 StPO). Es muss ein Anfangsverdacht für eine Gefahr für die IT-Sicherheit der Behörden durch Sicherheitslücken, Schadprogramme oder Angriffe vorliegen. Dies ist der Fall, wenn die Gefahr zumindest möglich erscheint.

§ 20 Absatz 2 NDIG sieht eine weitere Auswertung der Daten auch manuell durch eine natürliche Person vor sowie eine direkt personenbezogene Verarbeitung, sofern nunmehr hinreichende tatsächliche Anhaltspunkte im Sinne des § 170 StPO den Verdacht begründen, dass eine Gefahr für die IT-Sicherheit vorliegt. Dies ist der Fall, wenn es wahrscheinlicher ist, dass eine Gefahr vorliegt, als dass keine vorliegt. Die Abwägung, ob die Anhaltspunkte im jeweiligen Fall einen hinreichenden Verdacht begründen, muss durch die Behördenleitung und einer weiteren Beschäftigten oder einem weiteren Beschäftigten mit der Befähigung zum Richteramt erfolgen. Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen.

Absatz 2 bedeutet zudem eine Verlängerung der Speicherfrist, da die Daten zusätzlich gespeichert und ausgewertet werden dürfen, soweit und solange es zur Erkennung und Abwehr auch anderer Gefahren erforderlich ist.

15.4 Auswertung von Inhaltsdaten (§ 21 NDIG)

Absatz 1 lässt die weitere automatisierte Auswertung von Inhaltsdaten aus § 19 Abs. 1 oder 2 NDIG zu. Ausgewertet werden dürfen die Inhaltsdaten allerdings nur, soweit zureichende tatsächliche Anhaltspunkte auf Sicherheitslücken, Schadprogramme oder Angriffe bestehen. Hintergrund der Begrenzung auf die Daten nach § 19 Abs. 1 und 2 NDIG ist dabei, dass davon ausgegangen wird, dass Daten eines Verzeichnis- und Berechtigungsdienstes nach § 18 NDIG keine näher auszuwertenden Inhaltsdaten enthalten.

Absatz 1 Satz 1 regelt die Speicherfrist von höchstens 30 Tagen, wenn zureichende tatsächliche Anhaltspunkte vorliegen. Es muss insofern ein Anfangsverdacht im Sinne des § 152 StPO für eine Gefahr für die IT-Sicherheit der Behörden vorhanden sein

§ 21 Abs. 1 Satz 2 NDIG sieht eine automatisierte Pseudonymisierung der Daten vor, wenn die Daten nicht bereits mit einem Pseudonym versehen sind. Auch die weitere Auswertung der Inhaltsdaten nach Absatz 1 darf nur automatisiert erfolgen. Grund ist die besondere Sensibilität dieser Daten. Inhaltsdaten sind auch die Inhalte einer Kommunikation, sodass dort in hohem Maße Grundrechte betroffen sein können. Um die Grundrechtseingriffe bei diesem Verdachtsgrad so gering wie möglich zu halten, soll daher eine Erkennbarkeit der einzelnen Personen ausgeschlossen sein, ebenso eine manuelle Verarbeitung der Daten. Durch diese Erfordernisse wird eine natürliche Person nach diesem Absatz keine Kenntnis der Daten erhalten können. Zudem werden natürliche Personen, z. B. als Kommunikationsteilnehmende, durch die Pseudonymisierung nicht bekannt werden.

Aufgrund der besonderen Sensibilität von Inhaltsdaten ist bei einer Auswertung nach Absatz 1 eine unverzügliche nachträgliche Genehmigung der Behördenleitung im Einvernehmen mit einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt erforderlich. Auch hier

gilt wieder, sofern eine solche Person nicht Beschäftigt ist, tritt eine bei der Aufsichtsbehörde beschäftigte und dort dazu bestimmte Person an deren Stelle, § 21 Abs. 1 S. 4 NDIG. Wird diese Genehmigung verweigert, so sind sowohl die Daten als auch die bisherigen Auswertungsergebnisse unverzüglich zu löschen.

Diese Löschpflicht für die Daten und Auswertungsergebnisse besteht nach Absatz 1 S. 6 zudem, wenn die Auswertung keine hinreichenden tatsächlichen Anhaltspunkte geliefert haben.

Eine weitergehende Auswertung unter Personenbezug und mit einer Einsichtnahme oder manuellen Verarbeitung durch eine natürliche Person ist nach § 21 Abs. 2 NDIG nur dann zulässig, wenn eine vorherige Auswertung nach § 19 Abs. 1 oder 2 oder § 21 Abs. 1 NDIG hinreichende tatsächliche Anhaltspunkte im Sinne des § 170 StPO den Verdacht begründen, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr erforderlich sind. Diese Abwägung ist im Vorfeld zu treffen und es muss durch die Behördenleitung und eine weitere Beschäftigte oder einen weiteren Beschäftigten mit der Befähigung zum Richteramt eine vorherige Anordnung erfolgen. Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen. Nach Satz 4 dürfen die Daten soweit und solange gespeichert werden, wie dies zur Erkennung oder Abwehr einer anderen Gefahr erforderlich ist.

Absatz 3 gibt die Löschfrist für die Kopien der Daten, die Daten selbst und die Auswertungsergebnisse vor.

Absatz 4 schützt den Kernbereich der privaten Lebensgestaltung. Der Kernbereich kann die Kommunikation mit engen persönlichen Vertrauten wie u. a. Ehe- und Lebenspartnern und anderen engen Vertrauten oder Freunden sowie die Kommunikation mit Berufsgeheimnisträgern sein. Entscheidend ist diesbezüglich allerdings nicht in erster Linie der Kommunikationspartner, sondern vielmehr der Inhalt der Kommunikation, der dem höchstpersönlichen Bereich zugeordnet sein muss (LT-Drs. 15/3810, 30). Diese dürfen nach Satz 1 grundsätzlich nicht erhoben werden. Sollten dennoch auf der Grundlage der vorstehenden Absätze dieses Paragrafen Auswertungsergebnisse aus diesen geschützten Bereichen erlangt werden, so unterliegen diese einem Verwendungsverbot und sind daher auch unverzüglich, d. h. ohne schuldhaftes Zögern, zu löschen. Die Tatsache, dass es zu einer Auswertung der Daten kam und die Löschung der Daten ist zu dokumentieren. Auch wenn nicht in Gänze klar ist, ob die Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese bei Zweifeln zu löschen, da die Gefahr besteht, dass andernfalls in den durch Artikel 1 Abs. 1 des Grundgesetzes absolut geschützten Bereich eingegriffen wird.

15.5 Datensicherheit, Protokollierung (§ 25 NDIG)

In § 25 werden Vorgaben getroffen, die die Gewährleistung der Datensicherheit zum Ziel haben. Diese Vorgaben sind von allen Behörden zu erfüllen, die Gebrauch von den Ermächtigungen machen wollen. Die Vorgaben resultieren insbesondere aus der Rechtsprechung. Für die nach den voran beschriebenen Regeln verarbeiteten Daten müssen die notwendigen technischen und organisatorischen Maßnahmen ergriffen werden, um eine Kenntnisnahme unbefugter Dritter, eine Veränderung oder eine andere Verwendung als zu den in diesem Gesetz genannten Zwecken auszuschließen. Die Maßnahmen

müssen allesamt dem Stand der Technik entsprechen, wodurch Sicherheitslücken aufgrund veralteter Technik ausgeschlossen werden. Als Maßstab muss ein besonders zu sicherndes IT-System herangezogen werden und die Maßnahmen müssen an diesem Maßstab ausgerichtet werden. Die Umsetzung dieser Maßnahmen erfordert ein besonders hohes Maß an Datensicherheit. Die Maßnahmen, die sonst bei sensiblen Daten getroffen werden, reichen somit nicht aus. Ferner muss ein Sicherheitskonzept für die eingesetzten technischen Systeme aktenkundig gemacht werden, welches alle zwei Jahre einer Revision zu unterziehen ist. Schließlich muss jeder Zugriff auf die nach §§ 18 bis 23 verarbeiteten Daten sowie Auswertungsergebnisse protokolliert werden.

15.6 Weitere Regelungen

Weitere Regelungen aus dem zweiten Abschnitt beziehen sich u. a. auf Benachrichtigungs- und Dokumentationspflichten oder die Beteiligung der oder des Landesbeauftragten für den Datenschutz.