**Beschlussempfehlung**

Hannover, den 25.09.2019

Ausschuss für Inneres und Sport

**Entwurf eines Gesetzes zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes**

Gesetzentwurf der Landesregierung - Drs. 18/1598

Berichterstattung: Abg. Bernd Lynack (SPD)
(Es ist ein schriftlicher Bericht vorgesehen.)

Der Ausschuss für Inneres und Sport empfiehlt dem Landtag, den Gesetzentwurf mit den aus der Anlage ersichtlichen Änderungen anzunehmen.

Thomas Adasch
Vorsitzender

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

**Gesetz**
**zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes**

Artikel 1
Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)

Inhaltsübersicht



*Empfehlungen des Ausschusses für Inneres und Sport*

**Gesetz**
**zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes**

Artikel 1
Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)[*)]

Inhaltsübersicht



*) **§ 6 Abs. 3 und 4 dieses Gesetzes dient der Umsetzung der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen (ABl. EU Nr. L 133 S. 1).**

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

Zweiter Abschnitt
**Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit**

§ 17 Geltungsbereich, Wahrnehmung der Befugnisse nach diesem Abschnitt
§ 18 Allgemeine Bestimmungen
§ 19 Auswertung von gespeicherten Daten
§ 20 Erhebung und Auswertung des Datenverkehrs
§ 21 Auswertung ohne Inhaltsdaten
§ 22 Auswertung von Inhaltsdaten
§ 23 Gewährleistung der Datensicherheit
§ 24 Sicherheitskonzept
§ 25 Benachrichtigung der betroffenen Personen und Behörden
§ 26 Dokumentation
§ 27 Übermittlung personenbezogener Daten
§ 28 Einschränkung von Grundrechten

Erster Teil
**Allgemeines**

§ 1
Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes bedeutet:

1. Angriff:

ein Versuch, die IT-Sicherheit eines Computersystems unbefugt zu beeinflussen,

*Empfehlungen des Ausschusses für Inneres und Sport*

Zweiter Abschnitt
**Einsatz von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit**

§ 17 **Übertragung und Beschränkung** der Befugnisse nach diesem Abschnitt
§ 18 ***wird gestrichen***
**§ 18/1 Automatisierte Erhebung und Auswertung von Daten eines Verzeichnis- und Berechtigungsdienstes**
§ 19 **Automatisierte** Auswertung von **Ereignisdokumentationen und Datenverkehr**
§ 20 ***wird*** *(hier)* ***gestrichen*** *(jetzt in den §§ 18/1 und 19)*
§ 21 **Weitere** Auswertung ohne Inhaltsdaten **in Verdachtsfällen**
§ 22 **Weitere** Auswertung von Inhaltsdaten **in Verdachtsfällen**
**§ 22/1 Ergänzende Auswertung durch das Bundesamt für Sicherheit in der Informationstechnik**
**§ 22/2 Speicherung und Auswertung von Daten zur Abwehr einer dringenden Gefahr für die IT-Sicherheit**
**§ 22/3 Beseitigung von Schadprogrammen**
§ 23 _____ Datensicherheit**, Protokollierung**
§ 24 ***wird*** *(hier)* ***gestrichen*** *(jetzt in § 23)*
§ 25 Benachrichtigung der betroffenen Personen _____
§ 26 *unverändert*
**§ 26/1 Beteiligung der oder des Landesbeauftragten für den Datenschutz**
§ 27 **Zweckbindung,** Übermittlung personenbezogener Daten
§ 28 *unverändert*

Erster Teil
**Allgemeines**

§ 1
Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes bedeutet:

1. Angriff:

ein Versuch, die IT-Sicherheit _____ unbefugt zu beeinflussen,

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| 2. Basisdienst:<br><br>ein fachunabhängiges informationstechnisches Verfahren zur Unterstützung von Verwaltungsaufgaben, | 2. Basisdienst:<br><br>ein fachunabhängiges informationstechnisches Verfahren zur Unterstützung **bei der Wahrnehmung von Aufgaben der öffentlichen Verwaltung**, |
| 3. Behörde:<br><br>jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, | 3. Behörde:<br><br>jede Stelle **des Landes, einer Kommune oder einer sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts**, die Aufgaben der öffentlichen Verwaltung wahrnimmt, |
| 4. besondere Kategorien personenbezogener Daten:<br><br>personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, | 4. ***wird gestrichen*** |
| 5. elektronische Rechnung:<br><br>eine Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird, das ihre automatische und elektronische Verarbeitung ermöglicht, | 5. *unverändert* |
| | **5/1. Informationssicherheit:**<br><br>**die Vertraulichkeit, Verfügbarkeit und Integrität von Daten,** |
| 6. Informationstechnik:<br><br>technische Mittel zur elektronischen Verarbeitung oder Übertragung von Informationen, | 6. Informationstechnik **(IT)**:<br><br>technische Mittel zur ____ Verarbeitung oder Übertragung von Informationen, |
| 7. Inhaltsdaten:<br><br>Informationen, die bei einem Telekommunikationsvorgang übertragen werden und um derentwillen die Telekommunikation stattfindet und die keine Verkehrsdaten nach § 3 Nr. 30 des Telekommunikationsgesetzes sind, | 7. ***wird gestrichen*** |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| 8. IT-Sicherheit:<br><br>die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten, | 8. IT-Sicherheit:<br><br>die _____ Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten, |
| 9. Landesdatennetz:<br><br>eine Kommunikationsinfrastruktur, die eine Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird, | 9. Landesdatennetz:<br><br>eine **in Netzabschnitte gegliederte** Kommunikationsinfrastruktur, die eine Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden _____ ermöglicht und durch das Land _____ betrieben wird, |
| 10. Nutzerkonto:<br><br>eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung einer natürlichen oder juristischen Person oder einer Personengesellschaft zu Zwecken der Inanspruchnahme von Behördenleistungen, | 10. Nutzerkonto:<br><br>eine zentrale Identifizierungskomponente zur einmaligen oder dauerhaften Identifizierung **der Nutzerinnen und Nutzer** zu Zwecken der Inanspruchnahme von ____**L**eistungen **der öffentlichen Verwaltung**, |
| 11. Schadprogramm:<br><br>ein Computerprogramm, das bei Ausführung unbefugt die Vertraulichkeit, Verfügbarkeit oder Integrität der verarbeiteten Daten gefährden kann, oder ein Teil davon, | 11. Schadprogramm:<br><br>ein Computerprogramm, **dessen** Ausführung **die IT-Sicherheit** gefährden kann, oder ein Teil davon, |
| 12. Sicherheitsdomäne:<br><br>ein abgegrenzter Teil der Verwaltung mit einheitlichen Sicherheitsanforderungen oder einheitlicher Sicherheitsadministration, | 12. ***wird gestrichen*** |
| 13. Sicherheitsarchitektur:<br><br>die Gesamtheit der technischen und organisatorischen Maßnahmen für das Landesdatennetz, die zur Abwehr von Gefahren auf dieses dienen, | 13. ***wird*** *(hier)* ***gestrichen*** *(jetzt in § 12/2 Abs. 1)* |
| 14. Sicherheitslücken:<br><br>die Eigenschaften von Computerprogrammen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte gegen den Willen der Berechtigten Zugang zu diesen informationstechnischen Systemen verschaffen oder die Funktion dieser informationstechnischen Systeme beeinflussen können, | 14. Sicherheitslücken:<br><br>die Eigenschaften von Computerprogrammen oder sonstigen **IT-**Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte gegen den Willen der Berechtigten Zugang zu diesen **IT-**Systemen verschaffen oder die Funktion dieser **IT-**Systeme beeinflussen können, |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

15. Sicherheitsvorfall:

ein Ereignis, das die Vertraulichkeit, Verfügbarkeit oder Integrität der verarbeiteten Daten einschränkt oder beseitigt oder einschränken oder beseitigen könnte.

(2) Ein informationstechnisches System ist mit dem Landesdatennetz verbunden, wenn es direkt, über ein untergeordnetes behördeneigenes Netz oder über einen IT-Dienstleister an das Landesdatennetz angeschlossen ist.

§ 2
Die oder der IT-Bevollmächtigte der Landesregierung

[1]Die Landesregierung bestellt eine IT-Bevollmächtigte oder einen IT-Bevollmächtigten. [2]Sie oder er hat den Einsatz der Informationstechnik durch das Land und die Fortentwicklung der digitalen Verwaltung, die ihre geschäftlichen Prozesse durchgehend mithilfe der Informationstechnik durchführt, unter Berücksichtigung der fachlichen und organisatorischen Belange zu koordinieren.

Zweiter Teil
**Digitale Verwaltung**

§ 3
Geltungsbereich

(1) Dieser Teil gilt für die öffentlich-rechtliche Verwaltungstätigkeit des Landes, der Kommunen sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, soweit nicht besondere Rechtsvorschriften des Landes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(2) Dieser Teil gilt nicht für

1. die Hochschulen in staatlicher Verantwortung und Teile von Behörden des Landes, die mit Forschungsaufgaben betraut und deren informationstechnischen Systeme nicht mit dem Landesdatennetz verbunden sind,

*Empfehlungen des Ausschusses für Inneres und Sport*

15. Sicherheitsvorfall:

ein Ereignis, das die **IT-Sicherheit** einschränkt oder beseitigt oder einschränken oder beseitigen könnte.

(2) Ein **IT-**System ist mit dem Landesdatennetz verbunden, wenn es direkt, über ein untergeordnetes behördeneigenes Netz oder über einen IT-Dienstleister an das Landesdatennetz angeschlossen ist.

§ 2
Die oder der IT-Bevollmächtigte der Landesregierung

*unverändert*

Zweiter Teil
**Digitale Verwaltung**

§ 3
Geltungsbereich

(1) Dieser Teil gilt für die öffentlich-rechtliche Verwaltungstätigkeit **der Behörden**, soweit nicht besondere Rechtsvorschriften des Landes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

**(1/1) Dieser Teil gilt nicht für die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf- und Zivilsachen und für Maßnahmen des Richterdienstrechts.**

(2) Dieser Teil gilt nicht für

1. die Hochschulen in staatlicher Verantwortung _____ *(jetzt in Nummer 1/1)*,

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| | **1/1. die** Teile von Behörden des Landes, die mit Forschungsaufgaben betraut und deren **IT-**Systeme nicht mit dem Landesdatennetz verbunden sind**,** |
| 2. die Kirchen, Religionsgesellschaften und Weltanschauungsgemeinschaften sowie ihre Verbände und Einrichtungen, | 2. *unverändert* |
| 3. die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten, | 3. *unverändert* |
| 4. die landesunmittelbaren Körperschaften der gesetzlichen Kranken-, Renten- und Unfallversicherung sowie der sozialen Pflegeversicherung, | 4. *unverändert* |
| 5. Beliehene, | 5. *unverändert* |
| 6. den Norddeutschen Rundfunk und die Niedersächsische Landesmedienanstalt, | 6. *unverändert* |
| 7. die Nordwestdeutsche Forstliche Versuchsanstalt, | 7. *unverändert* |
| 8. die Schulen im Sinne des Niedersächsischen Schulgesetzes und die Schulen im Sinne des Niedersächsischen Gesetzes über Schulen für Gesundheitsfachberufe und Einrichtungen für die praktische Ausbildung, | 8. *unverändert* |
| 9. die den Landesbildungszentren angeschlossenen pädagogischen Bereiche, wenn deren informationstechnische Systeme nicht mit dem Landesdatennetz verbunden sind, | 9. die den Landesbildungszentren angeschlossenen pädagogischen Bereiche, wenn deren **IT-**Systeme nicht mit dem Landesdatennetz verbunden sind, **sowie** |
| 10. die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf-und Zivilsachen und für Maßnahmen des Richterdienstrechts sowie | 10. ***wird*** *(hier)* ***gestrichen*** *(jetzt in Absatz 1/1)* |
| 11. alle Einrichtungen im Sinne des § 1 Abs. 2 des Gesetzes über Tageseinrichtungen für Kinder. | 11. *unverändert* |
| (3) Für | (3) **Aus diesem Teil gilt nur § 10 Abs. 4** für |
| 1. das Justizministerium und seinen Geschäftsbereich, soweit diese nicht bereits von den Absätzen 1 und 2 erfasst sind, | 1. das Justizministerium und seinen Geschäftsbereich_____, |
| 2. die Verwaltungstätigkeit nach dem Zweiten Buch des Sozialgesetzbuchs, | 2. *unverändert* |
| 3. die Landtagsverwaltung, | 3. *unverändert* |
| 4. die Tätigkeit der Finanzbehörden nach der Abgabenordnung und dem Finanzverwaltungsgesetz, | 4. *unverändert* |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| 5. den Landesrechnungshof, | 5. *unverändert* |
| 6. die Vergabekammer Niedersachsen, | 6. *unverändert* |
| 7. die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde, | 7. *unverändert* |
| 8. die Wasser- und Bodenverbände, | 8. *unverändert* |
| 9. die Realverbände sowie die Forst- und die Jagdgenossenschaften und | 9. *unverändert* |
| 10. die Zweckverbände im Sinne des Niedersächsischen Gesetzes über die kommunale Zusammenarbeit sowie den Regionalverband „Großraum Braunschweig“ | 10. *unverändert* |
| gilt nur § 10 Abs. 4. | _____. |
| | **(3/1) Für die in den Absätzen 2 und 3 genannten Stellen und Tätigkeiten bleibt, soweit Bundesrecht ausgeführt wird, das E-Government-Gesetz (EGovG) in der am 31. Oktober 2019 geltenden Fassung vom 25. Juli 2013 (BGBl. I S. 2749), zuletzt geändert durch Artikel 1 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2206), unberührt.** |
| (4) Unabhängig von den Absätzen 1 bis 3 gilt § 6 Abs. 3 und 4 für | (4) **Abweichend** von den Absätzen **1/1** bis 3 gilt § 6 Abs. 3 und 4 für |
| 1. die niedersächsischen Auftraggeber im Sinne des § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) in Bezug auf Aufträge, die in den Anwendungsbereich des Teils 4 des Gesetzes gegen Wettbewerbsbeschränkungen fallen, und | 1. die niedersächsischen Auftraggeber im Sinne des § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) in Bezug auf **öffentliche** Aufträge **und Konzessionen**, die in den Anwendungsbereich des Teils 4 des Gesetzes gegen Wettbewerbsbeschränkungen fallen, und |
| 2. die öffentlichen Auftraggeber im Sinne des § 2 Abs. 5 des Niedersächsischen Tariftreue- und Vergabegesetzes in Bezug auf Aufträge, deren geschätzter Auftragswert den jeweils maßgeblichen Schwellenwert gemäß § 106 GWB nicht erreicht. | 2. die öffentlichen Auftraggeber im Sinne des § 2 Abs. 5 des Niedersächsischen Tariftreue- und Vergabegesetzes in Bezug auf **öffentliche** Aufträge, deren geschätzter Auftragswert den jeweils maßgeblichen Schwellenwert gemäß § 106 GWB nicht erreicht. |
| § 4<br>Elektronischer Zugang zur Verwaltung | § 4<br>Elektronischer Zugang zur Verwaltung |
| (1) [1]Die Behörden sind, auch wenn sie nicht Bundesrecht ausführen, verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente zu eröffnen. [2]Dies gilt unabhängig davon, ob die Dokumente mit einer qualifizierten elektronischen Signatur versehen sind. | (1) [1]**Jede** Behörde **ist verpflichtet**, auch wenn sie nicht Bundesrecht ausführt, _____ einen **§ 2 Abs. 1 EGovG entsprechenden** Zugang für die Übermittlung elektronischer Dokumente zu eröffnen. [2]_____ *(jetzt in Satz 1)* |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

(2) [1]Die Behörden sind verpflichtet, einen Zugang nach Absatz 1 auch über Nutzerkonten anzubieten. [2]Diese müssen die Bereitstellung und Entgegennahme von Daten zum Zweck der Inanspruchnahme von Behördenleistungen ermöglichen. [3]Sie sind durch technische und organisatorische Maßnahmen gegen den unberechtigten Zugriff Dritter zu schützen. [4]Die Behörden sollen die Nutzerkonten bei der Kommunikation in Verwaltungsverfahren nutzen.

(3) Die Behörden sind verpflichtet, einen Zugang nach Absatz 1 auch durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes oder einen anderen schriftformersetzenden Dienst anzubieten.

(4) Die Behörden des Landes sind verpflichtet, in elektronisch durchgeführten Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachtet wird, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes (PAuswG) oder nach § 78 Abs. 5 des Aufenthaltsgesetzes (AufenthG) anzubieten.

§ 5
Elektronische Informationen und Verwaltungsportal

(1) Die Behörden stellen, auch wenn sie nicht Bundesrecht ausführen, über öffentlich zugängliche Netze in allgemein verständlicher Sprache Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie ihre postalische, telefonische und elektronische Erreichbarkeit zur Verfügung.

(2) Die Behörden haben, auch wenn sie nicht Bundesrecht ausführen, über öffentlich zugängliche Netze in allgemein verständlicher Sprache über ihre nach außen wirkende öffentlich-rechtliche Tätigkeit, damit verbundene Gebühren, beizubringende Unterlagen, die zuständige Ansprechstelle und ihre Erreichbarkeit zu informieren sowie erforderliche Formulare bereitzustellen.

(3) Die Informationen nach den Absätzen 1 und 2 sowie nach § 3 Abs. 1 und 2 des E-Government-Gesetzes (EGovG) sind aktuell zu halten.

(4) [1]Die obersten Landesbehörden stellen sicher, dass die Informationen nach Absatz 2 und § 3 Abs. 2 EGovG für die Kommunen elektronisch bereitstehen, soweit diese für die Ausführung von Bundes- oder Landesrecht zuständig sind. [2]Die Kommunen können diese

*Empfehlungen des Ausschusses für Inneres und Sport*

(2) [1]**Jede** Behörde **ist** verpflichtet, einen Zugang **für die Übermittlung elektronischer Dokumente** auch über Nutzerkonten **zu eröffnen**. [2]**Die Nutzerkonten** müssen **eine Postfachfunktion enthalten, welche** die Bereitstellung und Entgegennahme von Daten _____ ermöglicht. [3]Sie sind durch technische und organisatorische Maßnahmen gegen den unberechtigten Zugriff Dritter zu schützen. [4]Die Behörden sollen die Nutzerkonten bei der Kommunikation in Verwaltungsverfahren nutzen.

(3) **Jede** Behörde **ist** verpflichtet, einen Zugang **für die Übermittlung elektronischer Dokumente** auch durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes oder einen anderen schriftformersetzenden Dienst **zu eröffnen**.

(4) **Jede** Behörde des Landes **ist** verpflichtet, in elektronisch durchgeführten Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen **hat** oder aus anderen Gründen eine Identifizierung für notwendig erachtet ____, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes (PAuswG) oder nach § 78 Abs. 5 des Aufenthaltsgesetzes (AufenthG) anzubieten.

§ 5
Elektronische Informationen und Verwaltungsportal

(1) **Jede** Behörde **stellt**, auch wenn sie nicht Bundesrecht **ausführt**, **entsprechend § 3 Abs. 1 EGovG** Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie ihre postalische, telefonische und elektronische Erreichbarkeit zur Verfügung.

(2) **Jede** Behörde **hat** _____ über öffentlich zugängliche Netze in allgemein verständlicher Sprache über ihre nach außen wirkende öffentlich-rechtliche Tätigkeit, damit verbundene Gebühren, beizubringende Unterlagen, die zuständige Ansprechstelle und ihre Erreichbarkeit zu informieren sowie erforderliche Formulare bereitzustellen.

(3) **Jede Behörde hat** die Informationen nach den Absätzen 1 und 2 sowie nach § 3 Abs. 1 und 2 _____EGovG____ aktuell zu halten.

(4) [1]Die obersten Landesbehörden stellen sicher, dass die **landeseinheitlichen** Informationen nach Absatz 2 _____ für die Kommunen elektronisch bereitstehen, soweit diese für die Ausführung von Bundes- oder Landesrecht zuständig sind. [2]Die Kommunen

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| Informationen für Zwecke nach Absatz 2 und § 3 Abs. 2 EGovG verwenden und dabei Ergänzungen vornehmen. | können diese Informationen **zur Erfüllung ihrer Pflichten** nach Absatz 2 _____ verwenden und dabei Ergänzungen vornehmen. |
| (5) [1]Zur Ausführung des § 1 des Onlinezugangsgesetzes stellt das für zentrale IT-Steuerung zuständige Ministerium ein niedersächsisches Verwaltungsportal bereit und verknüpft es mit dem Portalverbund von Bund und Ländern. [2]Die Behörden bieten ihre Verwaltungsleistungen auch über das niedersächsische Verwaltungsportal an. | (5) [1]Zur Ausführung des § 1 des Onlinezugangsgesetzes stellt das für zentrale IT-Steuerung zuständige Ministerium ein niedersächsisches Verwaltungsportal bereit und verknüpft es mit dem Portalverbund von Bund und Ländern. [2]**Jede** Behörde **bietet** ihre Verwaltungsleistungen auch über das niedersächsische Verwaltungsportal an. |
| § 6<br>Elektronische Bezahlmöglichkeiten und Rechnungen | § 6<br>Elektronische Bezahlmöglichkeiten und Rechnungen |
| (1) Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Verwaltungskosten oder sonstige Forderungen an, so muss die Behörde die Einzahlung dieser Verwaltungskosten oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren ermöglichen, auch wenn nicht Bundesrecht ausgeführt wird. | (1) _____ **Jede** Behörde **ist verpflichtet**, auch wenn **sie** nicht Bundesrecht ausführt**, § 4 EGovG entsprechende elektronische Bezahlmöglichkeiten zu schaffen**. |
| (2) Die Behörden sollen es ermöglichen, dass Zahlungen nach Absatz 1 so geleistet werden können, dass die Gutschrift sofort bei der empfangenden Behörde erkennbar ist, wenn die Höhe der Verwaltungskosten feststeht und die Verwaltungsleistung erst nach der Zahlung erbracht wird. | (2) **Jede** Behörde **soll**, wenn die Höhe der **Gebühren oder der sonstigen Forderungen** feststeht und die Verwaltungsleistung erst nach **deren** Zahlung erbracht wird**,** ____ ermöglichen, dass _____ nach Absatz 1 so **bezahlt** werden **kann**, dass die Gutschrift sofort bei der empfangenden Behörde erkennbar ist. |
| (3) Die Auftraggeber nach § 3 Abs. 4 stellen sicher, dass elektronische Rechnungen aufgrund von Aufträgen nach § 3 Abs. 4 nach Maßgabe der Verordnung nach Absatz 4 empfangen und verarbeitet werden können. | (3) **Jeder** Auftraggeber nach § 3 Abs. 4 **stellt** sicher, dass elektronische Rechnungen aufgrund von Aufträgen nach § 3 Abs. 4 nach Maßgabe der Verordnung nach Absatz 4 empfangen und verarbeitet werden können. |
| (4) [1]Die Landesregierung wird ermächtigt, durch Verordnung Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs zu erlassen. [2]Diese Vorschriften können sich beziehen auf | (4) [1]Die Landesregierung **erlässt** durch Verordnung Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs _____. [2]**In der Verordnung** können **bestimmt werden** |
| 1. die Art und Weise der Verarbeitung elektronischer Rechnungen, | 1. *unverändert* |
| 2. die Anforderungen an elektronische Rechnungen hinsichtlich der von diesen zu erfüllenden Voraussetzungen, den Schutz personenbezogener Daten, das zu verwendende Rechnungsdatenmodell und die Verbindlichkeit der elektronischen Form sowie | 2. *unverändert* |
| 3. Ausnahmen für sicherheitsspezifische Aufträge. | 3. *unverändert* |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| § 7<br>Nachweise | § 7<br>Nachweise |
| (1) [1]Wird ein Verwaltungsverfahren elektronisch durchgeführt, so können die vorzulegenden Nachweise, auch wenn nicht Bundesrecht ausgeführt wird, elektronisch eingereicht werden, es sei denn, dass durch Rechtsvorschrift etwas anderes bestimmt ist oder die Behörde für bestimmte Verfahren oder im Einzelfall die Vorlage eines Papieroriginals verlangt. [2]Die Behörde entscheidet nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist. | (1) [1]_____ Nachweise können, auch wenn nicht Bundesrecht ausgeführt wird, **entsprechend § 5 Abs. 1 EGovG** elektronisch eingereicht **oder von der zuständigen Behörde entsprechend § 5 Abs. 2 EGovG eingeholt** werden_____. [2]_____ *(jetzt in Satz 1)* |
| (2) [1]Die zuständige Behörde kann erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit der Einwilligung der Verfahrensbeteiligten direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen, auch wenn nicht Bundesrecht ausgeführt wird. [2]Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die erforderlichen personenbezogenen Daten verarbeiten, auch wenn nicht Bundesrecht ausgeführt wird. | (2) ***wird*** *(hier)* ***gestrichen*** *(jetzt in Absatz 1 Satz 1)* |
| § 8<br>Elektronische Formulare | § 8<br>Elektronische Formulare |
| [1]Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars, das ein Unterschriftsfeld vorsieht, vorgeschrieben, so wird allein dadurch nicht die Anordnung der Schriftform bewirkt, auch wenn nicht Bundesrecht ausgeführt wird. [2]Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld, auch wenn nicht Bundesrecht ausgeführt wird. | [1]**Für die Verwendung von Formularen gilt**, auch wenn nicht Bundesrecht ausgeführt wird**, § 13 EGovG entsprechend**. [2]_____ *(jetzt in Satz 1)* |
| § 9<br>Georeferenzierung | § 9<br>Georeferenzierung |
| (1) Wird ein elektronisches Register, das Angaben mit Bezug zu Grundstücken in Niedersachsen enthält, neu aufgebaut oder überarbeitet, so hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) auf der Grundlage der Angaben des amtlichen Vermessungswesens (Geobasisdaten) zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf das sich die Angaben beziehen. | (1) Wird ein elektronisches Register, das Angaben mit Bezug zu Grundstücken in Niedersachsen enthält, neu aufgebaut oder überarbeitet, so hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) auf der Grundlage der _____ amtlichen ____Geobasisdaten_ zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf das sich die Angaben beziehen. |
| (2) Register im Sinne dieses Gesetzes ist ein Verzeichnis, für das Daten aufgrund von Rechtsvorschriften des Landes erhoben oder gespeichert werden. | (2) Register im Sinne dieses Gesetzes **sind solche**, für **die** Daten aufgrund von Rechtsvorschriften des Landes erhoben oder gespeichert werden**; dies können öffentliche und nichtöffentliche Register sein**. |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

§ 10
Elektronische Aktenführung

(1) Die Behörden können ihre Akten elektronisch führen.

(2) [1]Die Behörden des Landes sollen neu anzulegende Akten ab dem 1. Januar 2026 elektronisch führen. [2]Jede oberste Landesbehörde stellt ab dem 1. Januar 2023 sicher, dass auf Arbeitsplätzen ihres Geschäftsbereichs, auf denen Verwaltungsleistungen über das Niedersächsische Verwaltungsportal erbracht werden, neu anzulegende Akten elektronisch geführt werden. [3]Bei Vorliegen besonderer Gründe können im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung jeweils spätere Termine nach den Sätzen 1 und 2 festgelegt werden. [4]Die oder der IT-Bevollmächtigte der Landesregierung kann das Einvernehmen verweigern, wenn die Terminverschiebung nicht ausreichend begründet ist und durch die Festlegung späterer Termine die flächendeckende Einführung der elektronischen Aktenführung erheblich beeinträchtigt würde.

(3) [1]Wird eine Akte elektronisch geführt, so sind die Einhaltung der Grundsätze der ordnungsgemäßen Aktenführung sowie die Lesbarkeit, die Integrität und Authentizität, die Verfügbarkeit und die Vertraulichkeit der Akte sicherzustellen. [2]Akten oder Aktenteile können weiterhin in Papierform geführt werden, wenn die Anforderungen nach Satz 1 nicht oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden können.

(4) [1]Der Austausch elektronisch geführter Akten innerhalb einer Behörde und zwischen Behörden soll auf elektronischem Wege erfolgen. [2]Die Landesregierung wird ermächtigt, technische Verfahren und Standards für den Austausch zwischen Behörden nach Satz 1 durch Verordnung zu regeln.

(5) Einsichtnahme in eine elektronisch geführte Akte wird gewährt, indem

1. ein Aktenausdruck zur Verfügung gestellt wird,
2. die elektronischen Dokumente auf einem Bildschirm wiedergegeben werden,
3. die elektronischen Dokumente übermittelt werden oder

*Empfehlungen des Ausschusses für Inneres und Sport*

§ 10
Elektronische Aktenführung

(1) **Jede** Behörde **kann** ihre Akten elektronisch führen.

(2) [1]**Jede** Behörde des Landes **soll** neu anzulegende Akten ab dem 1. Januar 2026 elektronisch führen. [2]Jede oberste Landesbehörde stellt ab dem 1. Januar 2023 sicher, dass auf Arbeitsplätzen ihres Geschäftsbereichs, auf denen Verwaltungsleistungen über das Niedersächsische Verwaltungsportal erbracht werden, neu anzulegende Akten elektronisch geführt werden. [3]**Jede in Satz 1 oder 2 genannte Behörde kann, wenn** besondere Gründe **vorliegen,** ____ im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung **von** den Sätzen 1 und 2 **abweichende** spätere Termine **festlegen**. [4]Die oder der IT-Bevollmächtigte der Landesregierung kann das Einvernehmen **nur dann** verweigern, wenn die Terminverschiebung nicht ausreichend begründet ist und durch die Festlegung späterer Termine die flächendeckende Einführung der elektronischen Aktenführung erheblich beeinträchtigt würde.

(3) [1]Wird eine Akte elektronisch geführt, so **ist** die Einhaltung der Grundsätze der ordnungsgemäßen Aktenführung**, insbesondere** die Lesbarkeit, die Integrität und Authentizität, die Verfügbarkeit und die Vertraulichkeit der Akte**, durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik** sicherzustellen. [2]Akten oder Aktenteile können weiterhin in Papierform geführt werden, wenn die Anforderungen nach Satz 1 nicht oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden können.

(4) [1]Der Austausch elektronisch geführter Akten innerhalb einer Behörde und zwischen Behörden soll auf elektronischem Wege erfolgen. [2]Die Landesregierung wird ermächtigt, technische Verfahren und Standards durch Verordnung zu regeln**, soweit dies** für den Austausch zwischen Behörden nach Satz 1 **erforderlich ist**.

(5) **Soweit ein Recht auf Akteneinsicht besteht, kann jede Behörde, die ihre Akten elektronisch führt, Akteneinsicht dadurch gewähren, dass sie**

1. ein**en** Aktenausdruck zur Verfügung **stellt**,
2. die elektronischen Dokumente auf einem Bildschirm **wiedergibt**,
3. die elektronischen Dokumente übermittelt ____ oder

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

4. der lesende Zugriff auf den Inhalt der Akte ermöglicht wird.

§ 11
Übertragen und Vernichten von Dokumenten in Papierform

(1) [1]Soweit die Behörden des Landes Akten elektronisch führen, übertragen sie die Dokumente, die in Papierform oder in anderer körperlicher Form vorliegen, erforderlichenfalls in elektronische Dokumente und speichern diese in einer elektronischen Akte. [2]Bei der Übertragung in elektronische Dokumente ist nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Dokumenten in Papierform oder in anderer körperlicher Form bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. [3]Von der Übertragung der Dokumente in Papierform oder anderer körperlicher Form in elektronische Dokumente kann abgesehen werden, wenn die Übertragung unverhältnismäßigen Aufwand erfordert.

(2) [1]Sind in Papierform oder in anderer körperlicher Form vorliegende Dokumente nach Absatz 1 übertragen und zur elektronischen Akte genommen worden, so sollen sie vernichtet oder zurückgegeben werden, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]Für Maßnahmen der Qualitätssicherung kann die Vernichtung von Dokumenten aufgeschoben werden.

(3) [1]Kommunen sowie sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts können in Papierform oder in anderer körperlicher Form vorliegende Dokumente, wenn sie übertragen und zu einer elektronischen Akte nach § 10 Abs. 1 genommen worden sind, vernichten oder zurückgeben, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]Absatz 2 Satz 2 gilt entsprechend.

§ 12
Basisdienste

(1) [1]Das für die zentrale IT-Steuerung zuständige Ministerium stellt den Behörden Basisdienste

1. für die Zugänge nach § 4 Abs. 1 bis 3,

*Empfehlungen des Ausschusses für Inneres und Sport*

4. **den** lesenden Zugriff auf den Inhalt der Akte ermöglicht ____.

§ 11
Übertragen und Vernichten von Dokumenten in Papierform

(1) [1]**Jede** Behörde des Landes **muss, soweit sie** Akten elektronisch führt, ____ die Dokumente, die in Papierform _____ vorliegen, ____ in elektronische Dokumente übertragen und diese in **der** elektronischen Akte speichern**; liegen Aktenbestandteile** in anderer körperlicher Form **vor, so ist deren elektronische Wiedergabe in der elektronischen Akte zu speichern**. [2]Bei der Übertragung **nach Satz 1** ist nach dem Stand der Technik sicherzustellen, dass die **gespeicherten Daten** mit den Dokumenten in Papierform oder **den Aktenbestandteilen** in anderer körperlicher Form bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. [3]Von der Übertragung **nach Satz 1** kann abgesehen werden, wenn die Übertragung unverhältnismäßigen Aufwand erfordert.

(2) [1]Sind **Dokumente** in Papierform oder **Aktenbestandteile** in anderer körperlicher Form nach Absatz 1 übertragen und zur elektronischen Akte genommen worden, so sollen sie vernichtet oder zurückgegeben werden, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]Für Maßnahmen der Qualitätssicherung kann die Vernichtung **oder Rückgabe** _____ aufgeschoben werden.

(3) [1]**Jede Behörde einer** Kommune **oder** sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts **kann, soweit sie Akten elektronisch führt, Dokumente** in Papierform oder **Aktenbestandteile** in anderer körperlicher Form **nach Maßgabe des Absatzes 1 Sätze 1 und 2** übertragen _____. **[1/1]Sind Dokumente in Papierform oder Aktenbestandteile in anderer körperlicher Form nach Satz 1 übertragen und zur** elektronischen Akte _____ genommen worden**, so können sie** vernichtet oder zurückgegeben **werden**, wenn eine Aufbewahrung aus rechtlichen Gründen nicht erforderlich ist. [2]_____

§ 12
Basisdienste

(1) [1]Das für die zentrale IT-Steuerung zuständige Ministerium stellt den Behörden Basisdienste

1. für die **elektronischen** Zugänge nach § 4 Abs. 1 bis 3 **dieses Gesetzes und § 2 Abs. 1 EGovG**,

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| 2. für den elektronischen Identitätsnachweis nach § 18 PAuswG oder nach § 78 Abs. 5 AufenthG, | 2. für den elektronischen Identitätsnachweis nach **§ 4 Abs. 4**, |
| 3. für die Zurverfügungstellung von Informationen und Bereitstellung von Formularen nach § 5 Abs. 1 und 2 dieses Gesetzes sowie § 3 Abs. 1 und 2 EGovG, | 3. für die Zurverfügungstellung von Informationen und Bereitstellung von Formularen **über das niedersächsische Verwaltungsportal** nach § 5 Abs. 1 und 2 dieses Gesetzes sowie § 3 Abs. 1 und 2 EGovG, |
| 4. für das Anbieten von Verwaltungsleistungen über das niedersächsische Verwaltungsportal nach § 5 Abs. 5 Satz 2, | 4. *unverändert* |
| 5. für eine Bezahlmöglichkeit nach § 6 Abs. 1 und 2, | 5. für eine **elektronische** Bezahlmöglichkeit nach § 6 Abs. 1 und 2 **dieses Gesetzes sowie § 4 EGovG**, |
| 6. für den Empfang und die Verarbeitung elektronischer Rechnungen nach § 6 Abs. 3 und | 6. für den Empfang und die Verarbeitung elektronischer Rechnungen nach § 6 Abs. 3 und **4 sowie** |
| 7. für die elektronische Aktenführung nach § 10 unter Berücksichtigung der Vorgangsbearbeitung | 7. *unverändert* |
| bereit. [2]Das für Geoinformation zuständige Ministerium stellt den Behörden einen Basisdienst für die Georeferenzierung bereit. [3]Basisdienste für die in den Sätzen 1 und 2 genannten Funktionen und für andere Funktionen können die Behörden des Landes nur im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung bereitstellen. [4]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit nicht erkennbar ist. [5]Die Behörden des Landes können sich bei der Bereitstellung von Basisdiensten Dritter bedienen. | bereit. [2]Das für Geoinformation zuständige Ministerium stellt den Behörden einen Basisdienst für die Georeferenzierung **nach § 9** bereit. [3]**Jede** Behörde des Landes **kann** im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung **andere** Basisdienste für die in den Sätzen 1 und 2 genannten Funktionen und **Basisdienste** für andere Funktionen _____ bereitstellen. [4]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit **des Basisdienstes** nicht erkennbar ist. [5]Die Behörden des Landes können sich bei der Bereitstellung von Basisdiensten Dritter bedienen. |
| (2) [1]Die Behörden des Landes haben ihre Verpflichtungen nach den §§ 4, 5 Abs. 1 und 2, den §§ 6, 9 und 10 Abs. 2 dieses Gesetzes sowie nach § 2 Abs. 1, § 3 Abs. 1 und 2 und den §§ 4 und 4 a EGovG mit den nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdiensten zu erfüllen. [2]Im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung können diese Verpflichtungen abweichend von Satz 1 mit einem nach Absatz 1 Satz 3 bereitgestellten Basisdienst oder über ein fachbezogenes informationstechnisches Verfahren erfüllt werden. [3]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit des Einsatzes in der Behörde nicht erkennbar ist. | (2) [1]**Jede** Behörde des Landes **hat** ihre Verpflichtungen nach den §§ 4, 5 Abs. 1 und 2, den §§ 6, 9 und 10 Abs. 2 dieses Gesetzes sowie nach § 2 Abs. 1, § 3 Abs. 1 und 2 und ____§ 4 ____ EGovG mit den nach Absatz 1 Sätze 1 und 2 bereitgestellten Basisdiensten zu erfüllen. [2]**Sie kann** im Einvernehmen mit der oder dem IT-Bevollmächtigten der Landesregierung ____ **ihre** Verpflichtungen **nach § 4 Abs. 1, 3 und 4 sowie den §§ 6 und 10 Abs. 2 dieses Gesetzes sowie nach § 2 Abs. 1 und § 4 EGovG** abweichend von Satz 1 mit einem nach Absatz 1 Satz 3 bereitgestellten Basisdienst oder über ein fachbezogenes informationstechnisches Verfahren **erfüllen**. [3]Das Einvernehmen kann nur verweigert werden, wenn die Zweckmäßigkeit oder Wirtschaftlichkeit des Einsatzes **des Basisdienstes oder des Verfahrens** in der Behörde nicht erkennbar ist. |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| (3) [1]Die Kommunen sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts haben ihre Verpflichtungen nach § 4 Abs. 2 mit dem nach Absatz 1 Satz 1 Nr. 1 bereitgestellten Basisdienst, ihre Verpflichtungen zur Zurverfügungstellung der Informationen nach § 5 Abs. 1 und 2 mit dem nach Absatz 1 Satz 1 Nr. 3 bereitgestellten Basisdienst und ihre Verpflichtungen nach § 9 mit dem nach Absatz 1 Satz 2 bereitgestellten Basisdienst zu erfüllen. [2]Die Basisdienste für<br><br>1. die Bereitstellung eines Zugangs über Nutzerkonten, die die Anforderungen nach § 4 Abs. 2 Sätze 2 und 3 erfüllen,<br><br>2. die Zurverfügungstellung der Informationen nach § 5 Abs. 1 und 2 dieses Gesetzes und nach § 3 Abs. 1 und 2 EGovG,<br><br>3. die Bereitstellung von erforderlichen Formularen nach § 5 Abs. 2 dieses Gesetzes und nach § 3 Abs. 2 EGovG sowie<br><br>4. das Anbieten von Verwaltungsleistungen über das niedersächsische Verwaltungsportal nach § 5 Abs. 4 Satz 2<br><br>werden den Kommunen und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts kostenfrei zur Nutzung bereitgestellt. | (3) [1]**Jede Behörde einer** Kommune **oder** sonstigen der Aufsicht des Landes unterstehenden juristischen Person des öffentlichen Rechts **hat** ihre Verpflichtungen nach § 4 Abs. 2**,** _____ § 5 Abs. 1 und 2 _____ und _____ § 9 **dieses Gesetzes sowie nach § 3 Abs. 1 und 2 EGovG** mit **den** nach Absatz 1 **Sätze 1 und** 2 bereitgestellten Basisdiensten zu erfüllen. [2]**Der** Basisdienst für **den elektronischen Zugang** über Nutzerkonten_____ nach § 4 Abs. 2 _____ **sowie die Basisdienste nach Absatz 1 Satz 1 Nrn. 3 und 4** werden den **in Satz 1 genannten Behörden** kostenfrei zur Nutzung bereitgestellt. |
| (4) Die Landesregierung wird ermächtigt, durch Verordnung<br><br>1. für die vom Land bereitgestellten Basisdienste weitere Nutzungsverpflichtungen und Verpflichtungen zur Bereitstellung zur Nutzung festzulegen und<br><br>2. die Ausgestaltung der Basisdienste zu regeln, insbesondere hinsichtlich<br><br>a) der Interoperabilitäts- und Informationssicherheitsstandards,<br><br>b) der Anforderungen, die der Qualitätssicherung dienen,<br><br>c) des Funktionsumfangs und des Inhalts der vom Land bereitgestellten Basisdienste, insbesondere der durch den jeweiligen Dienst zu verarbeitenden personenbezogenen Daten, sowie | (4) ***wird gestrichen*** |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

d) der Nutzung der vom Land bereitgestellten Basisdienste.

Dritter Teil
**Informationssicherheit**

Erster Abschnitt
**Gewährleistung der Informationssicherheit**

*Empfehlungen des Ausschusses für Inneres und Sport*

Dritter Teil
**Informationssicherheit**

Erster Abschnitt
**Allgemeine Vorschriften**

**§ 12/1**
Sicherheitsverbund_____

(1) [1]Die Behörden und Gerichte des Landes**, deren IT-Systeme mit dem Landesdatennetz verbunden sind, sind Mitglieder eines** Sicherheitsverbund**es**. [2]**Jedes** Mitglied des Sicherheitsverbund**es hat auf der Basis von Risikoanalysen** eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene **Informationssicherheit** _____, auch in Hinblick auf andere Mitglieder des Sicherheitsverbund**es**, zu gewährleisten. _____ *(jetzt in Satz 2)* [3]**Jedes Mitglied des Sicherheitsverbundes hat** die **nach Satz 2** erforderlichen technischen und organisatorischen Maßnahmen ____ unverzüglich zu veranlassen und regelmäßig zu überprüfen und anzupassen.

**(2)** Die das Landesdatennetz betreibende Behörde _____ **kann einer** Stelle, _____ **die** nicht Mitglied des Sicherheitsverbundes **ist**, **die Verbindung ihrer IT-**Systeme mit dem Landesdatennetz **gestatten**, **wenn sie sich** verpflichtet, die **in Absatz 1 Sätze 2 und 3 sowie in § 12/2 Abs. 2 genannten Pflichten einzuhalten**.

§ **12/2**
Zentralstelle für Informationssicherheit

(1) Bei dem für die zentrale IT-Steuerung zuständigen Ministerium ist eine Zentralstelle **für Informationssicherheit** eingerichtet, die

**1.** fortlaufend ein ____**S**icherheitslagebild über Bedrohungen **für** und Angriffe **auf IT-Systeme** erstellt**,**

**2.** **das Sicherheitslagebild** mit dem Ziel analysiert, Veränderungen der Gefahrenlage zu erkennen, **und aus dieser Analyse**, auch unter Berücksichtigung einer Gesamtschau der Risikoanalysen, Hinweise zur Anpassung der **Gesamtheit der technischen und organisatorischen IT-Sicherheitsmaßnahmen** entwickelt sowie

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

*Empfehlungen des Ausschusses für Inneres und Sport*

**3. die Mitglieder des Sicherheitsverbundes zu** Fragen der **IT-**Sicherheit _____ berät und bei ____ Sicherheitsvorfällen unterstützt.

(2) **Jedes Mitglied des Sicherheitsverbundes ist** verpflichtet, der Zentralstelle **für Informationssicherheit** ____ Sicherheitsvorfälle in einer von ihr vorgegebenen Form unverzüglich mitzuteilen, wenn diese geeignet sind, auch die **IT-**Sicherheit **bei** anderen **Stellen, deren IT-Systeme mit dem Landesdatennetz verbunden sind,** zu beeinträchtigen.

**(3) Jede Stelle, die Befugnisse nach dem zweiten Abschnitt wahrnimmt, ist verpflichtet, der Zentralstelle für Informationssicherheit den Betrieb von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit anzuzeigen.**

§ 13
Förderung der Sicherheit in der Informationstechnik

§ 13
Förderung der **IT-**Sicherheit _____

(1) [1]Die das Landesdatennetz betreibende Behörde fördert die Sicherheit der Informationstechnik im Landesdatennetz mit Ausnahme des Netzes des Geschäftsbereichs des Justizministeriums. [2]Im Netz des Geschäftsbereichs des Justizministeriums fördert eine vom Justizministerium bestimmte Stelle die Sicherheit der Informationstechnik.

(1) [1]Die das Landesdatennetz betreibende Behörde fördert die **IT-**Sicherheit _____ im Landesdatennetz mit Ausnahme des Netz**abschnitts** des Geschäftsbereichs des Justizministeriums. [2]Im Netz**abschnitt** des Geschäftsbereichs des Justizministeriums fördert eine vom Justizministerium bestimmte Stelle die **IT-**Sicherheit _____.

(2) Zu dem Zweck nach Absatz 1 haben die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle jeweils für ihren Bereich die Aufgabe,

(2) **Die in Absatz 1 genannten Stellen haben jeweils für ihren Netzabschnitt** die Aufgabe,

1. Gefahren für die IT-Sicherheit, die durch Sicherheitslücken, Schadprogramme oder Angriffe bestehen, abzuwehren,

1. ____ durch Sicherheitslücken, Schadprogramme oder Angriffe **verursachte** Gefahren für die IT-Sicherheit abzuwehren,

2. Informationen über Gefahren für die IT-Sicherheit und über Sicherheitsvorkehrungen zu sammeln, diese auszuwerten, die Sicherheitsrisiken zu analysieren und die gewonnenen Erkenntnisse den Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, zur Verfügung zu stellen,

2. Informationen über Gefahren für die IT-Sicherheit und über Sicherheitsvorkehrungen zu sammeln, diese auszuwerten, die Sicherheitsrisiken zu analysieren und die gewonnenen Erkenntnisse den Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, zur Verfügung zu stellen,

3. Sicherheitsvorkehrungen für das Landesdatennetz zu planen,

3. Sicherheitsvorkehrungen für das Landesdatennetz zu planen, **um künftige Gefahren für die IT-Sicherheit abwehren zu können,**

4. die Zentralstelle für IT-Sicherheit (§ 16 Abs. 1) nach deren Vorgaben zu unterstützen.

4. die Zentralstelle für **Informationssicherheit** _____ nach deren Vorgaben zu unterstützen.

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

(3) Zusätzlich hat die das Landesdatennetz betreibende Behörde, auch für das Netz des Geschäftsbereichs des Justizministeriums, die Aufgabe,

1. sicherheitstechnische Anforderungen an die von den Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, einzusetzende Informationstechnik und an die Verbindung von Netzen und informationstechnischen Systemen mit dem Landesdatennetz zu entwickeln und fortzuschreiben,

2. IT-Sicherheitsprodukte den Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, bereitzustellen,

3. die für Sicherheit der Informationstechnik Verantwortlichen der Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, in Abstimmung mit der Zentralstelle (§ 16 Abs. 1) zu unterstützen sowie

4. bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme von Stellen, deren informationstechnischen Systeme mit dem Landesdatennetz verbunden sind, in herausgehobenen Fällen zu unterstützen.

(4) Zur Wahrnehmung der Aufgaben nach den Absätzen 2 und 3 betreiben die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle dem jeweiligen Stand der Technik entsprechende informationstechnische Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme und Angriffe.

§ 14
Vorübergehende und unaufschiebbare Maßnahmen zur Gewährleistung der IT-Sicherheit

Die oder der IT-Bevollmächtigte der Landesregierung kann gegenüber Behörden und Gerichten des Landes 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 anordnen, die zur Gewährleistung der IT-Sicherheit erforderlich sind.

*Empfehlungen des Ausschusses für Inneres und Sport*

(3) Zusätzlich hat die das Landesdatennetz betreibende Behörde, auch für **den Netzabschnitt** des Geschäftsbereichs des Justizministeriums, die Aufgabe,

1. sicherheitstechnische Anforderungen an die von den Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, einzusetzende Informationstechnik und an die Verbindung von Netzen und **IT-**Systemen mit dem Landesdatennetz zu entwickeln und fortzuschreiben,

2. den Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, **informationstechnische Verfahren und Geräte für die IT-Sicherheit (**IT-Sicherheitsprodukte**)** bereitzustellen,

3. die _____ Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, **im Benehmen** mit der Zentralstelle **für Informationssicherheit** _____ **bei der Förderung der IT-Sicherheit** zu unterstützen sowie

4. **die** Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, in herausgehobenen Fällen bei der Wiederherstellung der **IT-**Sicherheit _____ zu unterstützen.

(4) **Die in Absatz 1 genannten Stellen sind verpflichtet, in ihrem jeweiligen Netzabschnitt** dem ____ Stand der Technik entsprechende **IT-**Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit _____ **zu betreiben**.

§ 14
Vorübergehende und unaufschiebbare Maßnahmen
_____

**[1]**Bei einer gegenwärtigen Gefahr für die IT-Sicherheit kann die oder der IT-Bevollmächtigte der Landesregierung **ein Mitglied des Sicherheitsverbundes anweisen,** vorübergehende und unaufschiebbare Maßnahmen **zu ergreifen**, die zur Gewährleistung der IT-Sicherheit bei anderen Stellen, deren **IT-**Systeme mit dem Landesdatennetz verbunden sind, erforderlich sind. **[2]Satz 1 gilt nicht für Maßnahmen nach dem Zweiten Abschnitt.**

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| § 15<br>Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen | § 15<br>Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen |
| (1) [1]Die Behörden und Gerichte des Landes betreiben ihre informationstechnischen Systeme in einem Sicherheitsverbund. [2]Die Mitglieder des Sicherheitsverbunds haben eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene IT-Sicherheit ihrer informationstechnischen Systeme, auch in Hinblick auf andere Mitglieder des Sicherheitsverbunds, zu gewährleisten. | ***wird*** *(hier)* ***gestrichen*** *(jetzt § 12/1)* |
| (2) [1]Die Informationssicherheit im Sicherheitsverbund ist von den Behörden und Gerichten des Landes auf der Basis von Risikoanalysen sicherzustellen. [2]Die zur Risikobehandlung erforderlichen technischen und organisatorischen Maßnahmen sind unverzüglich zu veranlassen und regelmäßig zu überprüfen und anzupassen. | |
| (3) Die das Landesdatennetz betreibende Behörde oder eine von ihr beauftragte Stelle hat Stellen, deren informationstechnische Systeme mit dem Landesdatennetz verbunden, aber nicht Mitglied des Sicherheitsverbundes sind, zur Einhaltung von bestimmten Sicherheitsmaßnahmen zu verpflichten, die dem Stand der Informationssicherheit im Sicherheitsverbund entsprechen. | |
| § 16<br>Zentralstelle für Informationssicherheit | § 16<br>Zentralstelle für Informationssicherheit |
| (1) Bei dem für die zentrale IT-Steuerung zuständigen Ministerium ist eine Zentralstelle eingerichtet, die fortlaufend ein Informationssicherheitslagebild über Bedrohungen und Angriffe erstellt und dieses mit dem Ziel analysiert, Veränderungen der Gefahrenlage zu erkennen, daraus, auch unter Berücksichtigung einer Gesamtschau der Risikoanalysen, Hinweise zur Anpassung der Sicherheitsarchitektur entwickelt sowie Behörden und Gerichte des Landes über Fragen der Sicherheit in der Informationstechnik berät und bei informationstechnischen Sicherheitsvorfällen unterstützt. | ***wird*** *(hier)* ***gestrichen*** *(jetzt § 12/2)* |
| (2) Die Behörden und Gerichte des Landes sind verpflichtet, der Zentralstelle informationstechnische Sicherheitsvorfälle in einer von ihr vorgegebenen Form unverzüglich mitzuteilen, wenn diese geeignet sind, auch die Informationssicherheit anderer Sicherheitsdomänen zu beeinträchtigen. | |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

Zweiter Abschnitt
**Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit**

§ 17
Geltungsbereich, Wahrnehmung der Befugnisse nach diesem Abschnitt

(1) [1]Dieser Abschnitt gilt für die Behörden, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind. [2]Dieser Abschnitt gilt entsprechend für Stellen aus dem Geschäftsbereich des Justizministeriums, die keine Aufgaben der öffentlichen Verwaltung wahrnehmen, soweit deren IT-Systeme mit dem Landesdatennetz verbunden sind.

(2) [1]Die das Landesdatennetz betreibende Behörde nimmt die Befugnisse nach diesem Abschnitt für das Landesdatennetz mit Ausnahme des Netzes für den Geschäftsbereich des Justizministeriums wahr. [2]Soweit der Landesrechnungshof, die von der oder dem Landesbeauftragten für den Datenschutz geleitete Behörde oder die Landtagsverwaltung betroffen ist, ist für die Wahrnehmung der Befugnisse deren Zustimmung erforderlich. [3]Im Netz für den Geschäftsbereich des Justizministeriums werden die Befugnisse nach diesem Abschnitt von einer vom Justizministerium zu bestimmenden Stelle wahrgenommen.

(3) Dieser Abschnitt gilt nicht für Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind.

§ 18
Allgemeine Bestimmungen

(1) Die Verwendungsbeschränkungen in diesem Abschnitt betreffen nur digitale Daten, die dem Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen oder einen Personenbezug aufweisen.

(2) Soweit die Auswertungen nach den §§ 19 bis 22 ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehindert werden.

*Empfehlungen des Ausschusses für Inneres und Sport*

Zweiter Abschnitt
**Einsatz von IT-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit**

§ 17
**Übertragung und Beschränkung** der Befugnisse nach diesem Abschnitt

(1) ***wird gestrichen***

(2) [1] ~~_____~~ **[1/1]Jede Behörde kann ihre Befugnisse nach diesem Abschnitt im Einvernehmen mit der das Landesdatennetz betreibenden Behörde auf diese übertragen; das Recht der kommunalen Zusammenarbeit bleibt unberührt.** [2 und 3] ~~_____~~
*(jetzt in den Absätzen 2/1 und 2/2)*

**(2/1)** Soweit der **Datenverkehr mit dem** Landesrechnungshof, **mit der** von der oder dem Landesbeauftragten für den Datenschutz geleiteten Behörde oder **mit der** Landtagsverwaltung betroffen ist, **dürfen die** Befugnisse **nach diesem Abschnitt nur im Einvernehmen mit dieser Behörde wahrgenommen werden**.

**(2/2)** Im **Netzabschnitt des** Geschäftsbereichs des Justizministeriums **und in den damit verbundenen lokalen Netzen der Stellen aus dem Geschäftsbereich des Justizministeriums** werden die Befugnisse nach diesem Abschnitt von einer vom Justizministerium **bestimmten** Stelle wahrgenommen.

(3) **Die Befugnisse nach** diesem Abschnitt **stehen den** Hochschulen und Einrichtungen des Landes, die mit Forschungsaufgaben betraut sind**, nicht zu**.

§ 18
Allgemeine Bestimmungen

***wird gestrichen***
*(Absatz 2 jetzt in § 22/3,*
*Absatz 3 jetzt in § 27 Abs. 0/1 Satz 1)*

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| (3) Personenbezogene Daten, die zum Zweck der Gewährleistung der IT-Sicherheit nach diesem Gesetz ausgewertet werden dürfen, dürfen nicht für andere Zwecke verarbeitet werden. | |
| | **§ 18/1**<br>**Automatisierte Erhebung und Auswertung von Daten eines Verzeichnis- und Berechtigungsdienstes** |
| | **(1) Jede Behörde kann** den **personenbezogenen** Datenverkehr eines Verzeichnis**- und Berechtigungs-**dienstes **auf einem von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-System automatisiert** erheben und auswerten**, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist**. |
| | **(2) Die nach Absatz 1 erhobenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie zu dem in Absatz 1 genannten Zweck nicht mehr erforderlich sind.** |
| § 19<br>Auswertung von gespeicherten Daten | § 19<br>**Automatisierte** Auswertung von **Ereignisdokumentationen und Datenverkehr** |
| (1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, die auf ihren mit dem Landesdatennetz verbundenen IT-Systemen zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten Daten automatisiert auszuwerten. [2]Für die Auswertung nach Satz 1 dürfen ausschließlich die automatisierten Ereignisdokumentationen von | (1) [1]**Jede** Behörde **kann auf den von** ihr **betriebenen,** mit dem Landesdatennetz verbundenen IT-Systemen **die dort** zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten **personenbezogenen** Daten **nach Maßgabe der Sätze 2 und 3** automatisiert auswerten**, soweit dies zu dem Zweck,** durch Sicherheitslücken, Schadprogramme oder Angriffe **verursachte** Gefahren für die IT-Sicherheit **abzuwehren, erforderlich ist**. [2]Für die Auswertung nach Satz 1 dürfen ausschließlich die automatisierten Ereignisdokumentationen von |
| 1. Firewall-Systemen und Systemen zum Netzwerkbetrieb, | 1. *unverändert* |
| 2. Systemen zur Erkennung und Beseitigung von Schadsoftware, | 2. *unverändert* |
| 3. Systemen zur Erkennung von unerwünschten Werbe-, Betrugs- oder schädlichen E-Mails, | 3. *unverändert* |
| 4. Servern von Datenbanken, Verzeichnisdiensten und Anwendungen und | 4. *unverändert* |
| 5. der Betriebssoftware von Computersystemen | 5. ____ Betriebssoftware **und Anwendungen** von Computersystemen |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

herangezogen werden. [3]Zum Zweck der Auswertung dürfen Daten gemäß Satz 2 zusammengeführt und gemeinsam verarbeitet werden.

(2) [1]Ergibt die automatisierte Auswertung nach Absatz 1, dass zureichende tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 nicht bestehen, so sind die Auswertungsergebnisse und gefertigte Kopien von Ereignisdokumentationen nach Absatz 1 Satz 2 unverzüglich zu löschen. [2]Die Speicherung und sonstige Verarbeitung nach dem ursprünglichen Verwendungszweck bleiben hiervon unberührt. [3]Eine Auswertung von Inhaltsdaten im Rahmen des Absatzes 1 ist nur unter den Voraussetzungen des § 22 zulässig. [4]Die Erstellung von personenbezogenen Profilen zur Vorhersage des Nutzungsverhaltens von natürlichen Personen ist untersagt.

§ 20
Erhebung und Auswertung des Datenverkehrs

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, an eigenen Übergabe- und Knotenpunkten, die mit dem Landesdatennetz verbunden sind, nach auffälligem Datenverkehr zu suchen. [2]Zu diesem Zweck darf der in diesen Übergabe- und Knotenpunkten anfallende Datenverkehr automatisiert erhoben und entschlüsselt werden. [3]Es dürfen

1. Erhebungszeitpunkt, IP-Adresse einschließlich Subnetzmaske, Präfixlänge, Port und Medienzugriffskontrolladresse (Media-Access-Control-Address — MAC-Adresse), vollständiger Domä-

*Empfehlungen des Ausschusses für Inneres und Sport*

herangezogen werden. [3]Zum Zweck der Auswertung dürfen **die in** Satz 2 **genannten** Daten _____ zusammengeführt und gemeinsam verarbeitet werden.

**(1/1)** [1]**Jede** Behörde **kann** an **den von ihr betriebenen,** mit dem Landesdatennetz verbunden**en** Übergabe- und Knotenpunkten **nach Maßgabe des Satzes 2** nach auffälligem Datenverkehr ____ suchen**, soweit dies zu dem Zweck,** durch Sicherheitslücken, Schadprogramme oder Angriffe **verursachte** Gefahren für die IT-Sicherheit **abzuwehren, erforderlich ist**. [2]_____ Der **an den** Übergabe- und Knotenpunkten anfallende **personenbezogene** Datenverkehr darf automatisiert erhoben**,** ____ entschlüsselt **und unverzüglich automatisiert ausgewertet** werden. _____ *(§ 20 Abs. 1 Satz 3 des Entwurfs jetzt in Satz 2, § 20 Abs. 1 Satz 4 des Entwurfs jetzt in § 18/1)*

**(1/2) Werden nach den Absätzen 1 und 1/1 Inhalte einer Telekommunikation (**Inhaltsdaten**) verarbeitet, so ist die** Auswertung **ihrer kommunikativen Bedeutung unzulässig**.

(2) [1]Ergibt die ____ Auswertung nach Absatz 1 **oder 1/1 keine** zureichenden tatsächlichen Anhaltspunkte für eine **durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte** Gefahr **für die IT-Sicherheit**, so sind die _____ nach Absatz 1 **oder 1/1 erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse** unverzüglich zu löschen. [2]Die Speicherung und sonstige Verarbeitung **der nach Absatz 1 ausgewerteten Daten** nach dem ursprünglichen Verwendungszweck bleiben **von Satz 1** unberührt. [3]_____ *(jetzt in Absatz 1/2)* [4]_____ *(jetzt in § 27 Abs. 0/1 Satz 2)*

§ 20
Erhebung und Auswertung des Datenverkehrs

***wird** (hier) **gestrichen***
*(jetzt in § 18/1 sowie § 19 Abs. 1/1 und 2)*

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

nenname sowie die Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen,

2. für ein- und ausgehende Verbindungen auf Basis des Hypertext-Übertragungsprotokolls (Hypertext Transfer Protocol — HTTP) sowie des verschlüsselten Hypertext-Übertragungsprotokolls (Hypertext Transfer Protokoll Secure — HTTPS) zusätzlich zu Nummer 1 der vollständige einheitliche Ressourcenzeiger (Uniform Resource Locator — URL) und die Kopfdaten (ohne Cookie),

3. für Verbindungen auf Basis des Domain-Name-Service Protokolls (DNS) alle Inhalte der DNS-Anfrage (DNS Query) sowie der DNS-Antwort (DNS Response)

unverzüglich automatisiert ausgewertet werden. [4]Ergänzend zu den Sätzen 1 bis 3 sind die Behörden zur Erkennung und Analyse auffälligen Datenverkehrs eines Verzeichnisdienstes befugt, den Datenverkehr eines Verzeichnisdienstes zu erheben und auszuwerten.

(2) [1]Ergibt die automatisierte Auswertung nach Absatz 1 Satz 3, dass zureichende tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 nicht bestehen, so sind die Daten einschließlich der Auswertungsergebnisse unverzüglich zu löschen. [2]Eine Auswertung von Inhaltsdaten im Rahmen des Absatzes 1 ist nur unter den Voraussetzungen des § 22 zulässig.

§ 21
Auswertung ohne Inhaltsdaten

(1) [1]Soweit die automatisierte Auswertung nach § 19 Abs. 1 oder § 20 Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zur Abwehr von Gefahren im Sinne des § 19 Abs. 1 Satz 1 oder des § 20 Abs. 1 Satz 1 erforderlich sind, dürfen diese weiter einzelfallbezogen automatisiert ausgewertet werden. [2]Für diesen Zweck dürfen diese Daten höchstens sieben Tage gespeichert werden und sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind.

*Empfehlungen des Ausschusses für Inneres und Sport*

§ 21
**Weitere** Auswertung ohne Inhaltsdaten
**in Verdachtsfällen**

(1) [1]**Ergibt eine** automatisierte Auswertung nach **§ 18/1 Abs. 1 oder** § 19 Abs. 1 oder **1/1** zureichende tatsächliche Anhaltspunkte **für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte** Gefahr **für die IT-Sicherheit**, **so kann die Behörde die nach § 18/1 Abs. 1 oder § 19 Abs. 1 und 1/1 erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse zusammenführen,** höchstens **30** Tage speichern **und in dieser Zeitspanne** weiter einzelfallbezogen automatisiert auswerten**, soweit dies** zur **Erkennung oder** Abwehr **der Gefahr** erforderlich **ist**. [2]**Die nach Satz 1 gespeicherten** Daten _____ sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind. [3]**Ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verur-**

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

(2) [1]Hat sich aus der weiteren Auswertung nach Absatz 1 ergeben, dass hinreichende tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die Daten nach § 19 Abs. 1 oder § 20 Abs. 1 durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, so dürfen die Daten auch nicht automatisiert ausgewertet und entpseudonymisiert werden. [2]Dies gilt nur, soweit und solange die Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder Angriffe erforderlich ist. [3]Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

(3) Die für die Zwecke der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie nicht mehr erforderlich sind.

§ 22
Auswertung von Inhaltsdaten

(1) [1]Zur Abwehr von Gefahren für die IT-Sicherheit des Landes durch Sicherheitslücken, Schadprogramme oder Angriffe sind die Behörden befugt, die in § 19 Abs. 1 und § 20 Abs. 1 angefallenen Inhaltsdaten automatisiert nach Hinweisen auf Schadprogramme oder Angriffe unverzüglich auszuwerten. [2]Die für die Zwecke der Auswertung nach Satz 1 erhobenen Daten sowie die Auswertungsergebnisse sind nach ihrer automatisierten

*Empfehlungen des Ausschusses für Inneres und Sport*

**sachte Gefahr für die IT-Sicherheit, so sind die gespeicherten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen.**

(2) [1]**Ergibt eine automatisierte Auswertung nach § 18/1 Abs. 1 oder § 19 Abs. 1 oder 1/1 oder eine** weitere **automatisierte** Auswertung nach Absatz 1 _____ hinreichende tatsächliche Anhaltspunkte für **eine durch eine Sicherheitslücke,** ein Schadprogramm **oder** einen Angriff **verursachte Gefahr für die IT-Sicherheit**, so dürfen die Daten **über den Ablauf der in Absatz 1 Satz 1 bestimmten Frist hinaus gespeichert,** auch nicht automatisiert ausgewertet und entpseudonymisiert werden**, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist**. [2]_____ *(jetzt in den Sätzen 1 und 6)* [3]Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Behördenleitung **im Einvernehmen mit** einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]**Wenn** eine solche Person nicht beschäftigt ist **oder aus anderen Gründen nicht zur Verfügung steht**, **tritt an deren Stelle** eine **bei** der Aufsichtsbehörde **beschäftigte und von deren Behördenleitung bestimmte Person** mit der Befähigung zum Richteramt _____. [5]_____ *(jetzt in Satz 4)* **[6]Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist; die Sätze 3 und 4 gelten entsprechend.**

**(2/1) Nach den Absätzen 1 und 2 dürfen keine Inhaltsdaten gespeichert oder ausgewertet werden.**

(3) **S**oweit **die nach Absatz 2 ausgewerteten** Daten sowie die Auswertungsergebnisse nicht mehr **für die dort genannten Zwecke oder eine Übermittlung nach § 27** erforderlich sind**,** sind **sie** unverzüglich zu löschen.

§ 22
**Weitere** Auswertung von Inhaltsdaten
**in Verdachtsfällen**

(1) ***wird*** *(hier)* ***gestrichen*** *(jetzt in § 19 Abs. 1, 1/1 und 2)*

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| Auswertung unverzüglich zu löschen, es sei denn, die nachfolgenden Absätze sehen eine weitere Verwendung vor. | |
| (2) [1]Soweit die automatisierte Auswertung nach Absatz 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass einzelne Daten zum Schutz vor Schadprogrammen oder Angriffen erforderlich sind, dürfen diese für höchstens sieben Tage gespeichert werden. [2]Diese Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies automatisiert möglich ist und sie nicht bereits pseudonym sind. [3]Die weitere, einzelfallbezogene Auswertung der Daten erfolgt nur automatisiert. [4]Die Speicherung nach Satz 1 bedarf der unverzüglichen Genehmigung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [5]Sofern eine solche Person nicht beschäftigt ist, ist die Genehmigung nach Satz 4 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [6]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen. | (2) [1]**Ergibt eine** automatisierte Auswertung nach **§ 19 Abs. 1 oder 1/1** zureichende tatsächliche Anhaltspunkte dafür ____, dass **die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein** Schadprogramm oder **einen** Angriff **verursachten Gefahr für die IT-Sicherheit** erforderlich sind, **so kann die Behörde abweichend von § 21 Abs. 2/1 auch Inhaltsdaten und Auswertungsergebnisse** höchstens **30** Tage speichern **und in dieser Zeitspanne** weiter einzelfallbezogen automatisiert auswerten**, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist; die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig**. [2]**Die nach Satz 1 gespeicherten** Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies **technisch** möglich ist und **die Daten** nicht bereits pseudonym sind. [3]_____ *(jetzt in Satz 1)* [4]Die Speicherung nach Satz 1 bedarf der unverzüglichen Genehmigung der Behördenleitung **im Einvernehmen mit** einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [5]**Wenn** eine solche Person nicht beschäftigt ist **oder aus anderen Gründen nicht zur Verfügung steht**, **tritt an deren Stelle** eine **bei** der Aufsichtsbehörde **beschäftigte und von deren Behördenleitung bestimmte Person** mit der Befähigung zum Richteramt _____. [6]_____ *(jetzt in Satz 5)* **[7]Wird die Genehmigung abgelehnt oder nicht unverzüglich erteilt, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse unverzüglich zu löschen. [8]Ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse unverzüglich zu löschen.** |
| (3) [1]Eine über die Absätze 1 und 2 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Auswertung der Daten nach Absatz 1 Satz 1 ist nur zulässig, soweit und solange hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass diese durch ein Schadprogramm oder einen Angriff verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben. [2]Dies gilt nur, soweit die Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen oder zur Erkennung und Abwehr | (3) [1]**Ergibt eine automatisierte Auswertung nach § 19 Abs. 1 oder 1/1 oder eine weitere automatisierte Auswertung nach Absatz 2** hinreichende tatsächliche Anhaltspunkte **dafür**, dass **die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke,** ein Schadprogramm oder einen Angriff verursachten **Gefahr für die IT-Sicherheit erforderlich sind, so dürfen die Daten über den Ablauf der in Absatz 2 Satz 1 bestimmten Frist hinaus gespeichert, auch** nicht automatisiert **ausgewertet und entpseudonymisiert werden,** soweit und solange **dies** |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| anderer Schadprogramme erforderlich ist. [3]Die Datenverarbeitung nach Satz 1 bedarf der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen. | **zur Erkennung oder** Abwehr **der** Gefahr_____ erforderlich ist**; die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig**. [2]_____ *(jetzt in den Sätzen 1 und 6)* [3]Die **weitere Auswertung** nach Satz 1 bedarf der Anordnung der Behördenleitung **im Einvernehmen mit** einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]**Wenn** eine solche Person nicht beschäftigt ist **oder aus anderen Gründen nicht zur Verfügung steht**, **tritt an deren Stelle** eine **bei** der Aufsichtsbehörde **beschäftigte und von deren Behördenleitung bestimmte Person** mit der Befähigung zum Richteramt _____. [5]_____ *(jetzt in Satz 4)* **[6]Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist; die Sätze 3 und 4 gelten entsprechend.** |
| (4) Die für den Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse sind unverzüglich zu löschen, soweit sie nicht mehr erforderlich sind. | (4) **S**oweit **die nach Absatz 3 ausgewerteten** Daten sowie die Auswertungsergebnisse nicht mehr **für die dort genannten Zwecke oder eine Übermittlung nach § 27** erforderlich sind**,** sind **sie** unverzüglich zu löschen. |
| (5) [1]Soweit möglich ist bei der Datenverarbeitung nach dieser Vorschrift technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen oder die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, nicht erhoben werden. [2]Werden dennoch aufgrund der Maßnahmen nach den Absätzen 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder besondere Kategorien personenbezogener Daten erlangt, so dürfen diese nicht verwendet werden. [3]Die zum Zweck der Auswertung vorhandenen Daten sowie die Auswertungsergebnisse, die den Kernbereich privater Lebensgestaltung betreffen oder die geeignet sind, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen, sind unverzüglich zu löschen. [4]Dies gilt auch in Zweifelsfällen. [5]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [6]Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung verwendet werden. [7]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt. | (5) [1]_____ [2]**Sind** nach ____ **Absatz 3 ausgewertete Daten** dem Kernbereich privater Lebensgestaltung oder besonderen Kategorien personenbezogener Daten **(Artikel 9 der Datenschutz-Grundverordnung) zuzurechnen oder geeignet, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen,** so dürfen diese nicht **gespeichert, verändert, genutzt oder übermittelt** werden**; sie sind unverzüglich zu löschen**. [3]_____ *(jetzt in Satz 2 Halbsatz 2)* [4]**Satz 2** gilt auch in Zweifelsfällen. [5]Die Tatsache**, dass in den Sätzen 2 und 4 genannte Daten ausgewertet wurden, und die** Löschung **dieser Daten sind** zu dokumentieren. [6]Die **in der** Dokumentation **enthaltenen Daten dürfen** ausschließlich **zur Datenschutzkontrolle** verwendet werden. [7]Sie **sind** zu löschen, wenn **seit einer Benachrichtigung nach § 25 Abs. 1 Satz 1 ein Jahr vergangen ist, frühestens jedoch zwei Jahre nach der Dokumentation, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden**. |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

*Empfehlungen des Ausschusses für Inneres und Sport*

**§ 22/1**
**Ergänzende Auswertung durch das Bundesamt für Sicherheit in der Informationstechnik**

**[1]Jede Behörde, die selbst IT-Systeme zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit betreibt, kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragen, den von ihr nach § 19 Abs. 1/1 erhobenen Datenverkehr, dessen automatisierte Auswertung keine zureichenden oder hinreichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit ergeben hat, ergänzend auszuwerten und den Datenverkehr zu diesem Zweck an das BSI übermitteln. [2]Der Auftrag darf nur erteilt werden, wenn**

**1. die ergänzende Auswertung durch das BSI nur nach Maßgabe der §§ 21 und 22 erfolgt und über die dabei erforderlichen Anordnungen oder Genehmigungen von der beauftragenden Behörde entschieden wird,**

**2. das BSI die Auswertungsergebnisse der beauftragenden Behörde unverzüglich zur Verfügung stellen wird,**

**3. eine Verwendung der personenbezogenen Daten durch das BSI zu anderen Zwecken als zur ergänzenden Auswertung unzulässig ist,**

**4. die Daten nach Maßgabe des § 23 verarbeitet sowie nach Abschluss der ergänzenden Auswertung unverzüglich gelöscht werden, und**

**5. das BSI in geeigneter Weise Nachweise dafür erbringen kann, dass die übermittelten Daten ordnungsgemäß verarbeitet und gelöscht werden.**

**[3]Die ergänzende Auswertung des BSI erfolgt ausschließlich nach Weisung der beauftragenden Behörde.**

**§ 22/2**
**Speicherung und Auswertung von Daten zur Abwehr einer dringenden Gefahr für die IT-Sicherheit**

**(1) [1]Jede Behörde kann den nach § 19 Abs. 1/1 erhobenen Datenverkehr zu dem Zweck, durch Schadprogramme oder Angriffe verursachte, im Hinblick auf das Ausmaß des zu erwartenden Scha-**

*Gesetzentwurf der Landesregierung - Drs. 18/1598* *Empfehlungen des Ausschusses für Inneres und Sport*

**dens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahren für die IT-Sicherheit im gesamten Landesdatennetz (dringende Gefahren für die IT-Sicherheit) abzuwehren, automatisiert speichern. [2]Die gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind; nach höchstens 30 Tagen sind die Daten zu löschen.**

**(2) [1]Soweit und solange es zur Abwehr einer dringenden Gefahr für die IT-Sicherheit unerlässlich ist, dürfen die nach Absatz 1 Satz 1 gespeicherten Daten automatisiert und nicht automatisiert ausgewertet, entpseudonymisiert sowie über den Ablauf der in Absatz 1 Satz 2 bestimmten Frist hinaus gespeichert werden; die Auswertung der kommunikativen Bedeutung von Inhaltsdaten ist unzulässig. [2]§ 22 Abs. 5 gilt entsprechend.**

**(3) [1]Maßnahmen nach Absatz 2 bedürfen der Anordnung des Amtsgerichts, in dessen Bezirk die Behörde ihren Sitz hat. [2]Im Antrag der Behörde sind der Sachverhalt und eine Begründung anzugeben. [3]Die Anordnung ergeht schriftlich. [4]Sie muss den Sachverhalt und die wesentlichen Gründe enthalten. [5]Für das gerichtliche Verfahren gilt § 19 Abs. 4 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) entsprechend. [6]Bei Gefahr im Verzug kann die Behördenleitung die Anordnung treffen; die Sätze 3 und 4 gelten entsprechend mit der Maßgabe, dass die Anordnung auch eine Begründung der Gefahr im Verzug enthalten muss. [7]Die richterliche Bestätigung der Anordnung ist unverzüglich zu beantragen. [8]Wird die Bestätigung abgelehnt, so tritt die Anordnung außer Kraft. [9]Die Daten und die Auswertungsergebnisse dürfen in diesem Fall nicht mehr verwendet werden und sind unverzüglich zu löschen; die Speicherung nach Absatz 1 bleibt unberührt.**

**(4) Soweit die nach Absatz 2 verarbeiteten Daten sowie die Auswertungsergebnisse nicht mehr für den dort genannten Zweck oder eine Übermittlung nach § 27 erforderlich sind, sind sie unverzüglich zu löschen; die Speicherung nach Absatz 1 bleibt unberührt.**

**§ 22/3**
**Beseitigung von Schadprogrammen**

[1]Soweit die Auswertungen nach den §§ **18/1** bis **22/2** ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehin-

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| | dert werden. [2]**Soweit Daten von dem Schadprogramm nicht oder nur mit unverhältnismäßigem Aufwand getrennt werden können, kann die Behörde diese Daten gemeinsam mit dem Schadprogramm löschen.** |
| § 23<br>Gewährleistung der Datensicherheit | § 23<br>_____ Datensicherheit**, Protokollierung** |
| (1) [1]Die nach den §§ 19 bis 22 erhobenen oder gespeicherten Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. [2]Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Datensicherheit zu gewährleisten. | (1) [1]Die nach den §§ **18/1** bis **22/2 verarbeiteten** Daten **sowie die Auswertungsergebnisse** sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. [2]Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Datensicherheit zu gewährleisten. |
| (2) Insbesondere | (2) Insbesondere |
| | **0/1.** sind der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch die jeweilige Behördenleitung hierzu besonders ermächtigt sind, ____ |
| 1. ist organisatorisch sicherzustellen, dass eine Kenntnisnahme der Daten nach den §§ 19 bis 22 durch andere als die dafür bestimmten Personen ausgeschlossen ist, | 1. ist organisatorisch sicherzustellen, dass eine Kenntnisnahme der ____ nach den §§ **18/1** bis **22/2 verarbeiteten Daten sowie der Auswertungsergebnisse** durch andere als die **nach Nummer 0/1 ermächtigten** Personen ausgeschlossen ist, |
| 2. sind die IT-Systeme für Datenverarbeitung nach den §§ 19 bis 22 von den für die üblichen betrieblichen Aufgaben vorgehaltenen IT-Systeme, insbesondere die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben vorgesehenen Speichereinrichtungen, zu trennen, | 2. **ist sicherzustellen, dass** die für Datenverarbeitung nach den §§ **18/1** bis **22/2 verwendeten** IT-Systeme von den für die üblichen betrieblichen Aufgaben **verwendeten** IT-Systemen **getrennt sind**, insbesondere die Speicherung in gesonderten _____ Speichereinrichtungen **erfolgt**, |
| 3. sind besondere Sicherungsmaßnahmen gegen den unberechtigten Zugriff aus anderen Netzen, insbesondere aus dem Internet, zu treffen, | 3. *unverändert* |
| 4. sind die personenbezogenen Daten frühestmöglich zu anonymisieren oder zu pseudonymisieren, | 4. ***wird gestrichen*** |
| 5. sind nach dem Stand der Technik als besonders sicher geltende Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit der gespeicherten Daten einzusetzen, | 5. *unverändert* |
| 6. sind der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch die jeweilige Behördenleitung hierzu besonders ermächtigt sind, und | 6. ***wird*** *(hier)* ***gestrichen*** *(jetzt in Nummer 0/1)* |

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

7. ist technisch und organisatorisch sicherzustellen, dass der Zugriff auf die Daten nur gemeinsam durch mindestens zwei hierzu besonders ermächtigte Personen erfolgen kann.

(3) [1]Zum Zweck der Datenschutzkontrolle ist jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren von den nach den §§ 19 bis 22 erhobenen oder gespeicherten Daten in einem Protokoll aufzunehmen. [2]Das Protokoll enthält Zeitpunkt und Art des Zugriffs, eine eindeutige Kennung der auf die Daten zugreifenden Personen sowie den Zweck des Zugriffs. [3]Das Protokoll darf ausschließlich zum Zweck der Rechtmäßigkeitskontrolle verwendet werden. [4]Die Einträge in das Protokoll sind zwölf Monate nach ihrer Aufnahme zu löschen.

(4) [1]Der zuständigen Aufsichtsbehörde für den Datenschutz ist einmal im Jahr eine Aufstellung über die nach den §§ 19 bis 22 und 25 erfolgten Verarbeitungen sowie die Dokumentation nach § 26 vorzulegen. [2]Satz 1 gilt nicht für den Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.

§ 24
Sicherheitskonzept

[1]Eine Behörde darf von den Ermächtigungen der §§ 19 bis 22 nur Gebrauch machen, wenn sie ein Sicherheitskonzept erstellt hat und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig gemacht hat. [2]Das Sicherheitskonzept ist vor jeder Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle zwei Jahre einer Revision zu unterziehen. [3]Für jede Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

*Empfehlungen des Ausschusses für Inneres und Sport*

7. ist technisch und organisatorisch sicherzustellen, dass der Zugriff auf die Daten nur gemeinsam durch mindestens zwei **nach Nummer 0/1** ermächtigte Personen erfolgen kann.

**(2/1)** [1]Eine Behörde darf von den Ermächtigungen der §§ **18/1** bis **22/2** nur Gebrauch machen, wenn sie ein Sicherheitskonzept **für die dazu eingesetzten technischen Systeme** erstellt ____ und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig gemacht hat. [2]Das Sicherheitskonzept ist _____ alle zwei Jahre einer Revision zu unterziehen. [3]Für jede Veränderung **der eingesetzten technischen Systeme** gilt Satz 1 entsprechend.

(3) [1]_____ **J**eder Zugriff, insbesondere das Lesen, Kopieren, Ändern, **Übermitteln,** Löschen und Sperren von ____ nach den §§ **18/1** bis **22/2 verarbeiteten** Daten **sowie von Auswertungsergebnissen** ist **zu protokollieren**. [2]Das Protokoll enthält Zeitpunkt**,** ____ Art **und Zweck** des Zugriffs **sowie** eine eindeutige Kennung der auf die Daten zugreifenden Person_____. [3]Das Protokoll darf ausschließlich **zur Datenschutzkontrolle** verwendet werden. [4]**Jeder** Eintrag in das Protokoll **ist zwei Jahre** nach **seiner** Aufnahme zu löschen**, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden**.

(4) ***wird*** *(hier)* ***gestrichen*** *(jetzt in § 26/1)*

§ 24
Sicherheitskonzept

***wird*** *(hier)* ***gestrichen*** *(jetzt in § 23 Abs. 2/1)*

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

§ 25
Benachrichtigung der betroffenen Personen und Behörden

[1]Die von Maßnahmen nach diesem Gesetz betroffenen Personen und Behörden sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. [2]Die Benachrichtigung kann unterbleiben,

1. solange hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die IT-Sicherheit gefährdet würde,

2. wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.

[3]Sofern eine Benachrichtigung unterbleiben soll, bedarf dies der Anordnung der Behördenleitung und einer oder eines weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]Sofern eine solche Person nicht beschäftigt ist, ist die Anordnung nach Satz 3 durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. [5]Die Person ist durch die Behördenleitung der Aufsichtsbehörde zu bestimmen.

§ 26
Dokumentation

[1]Anordnungen und Genehmigungen nach § 21 Abs. 2 Satz 3, § 22 Abs. 2 Satz 4 und Abs. 3 Satz 3 sowie § 25 Satz 3 sind zu dokumentieren. [2]Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung der Daten verwendet werden. [3]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens

*Empfehlungen des Ausschusses für Inneres und Sport*

§ 25
Benachrichtigung der betroffenen Personen
_____

**(1)** [1]Die von Maßnahmen nach **den §§ 18/1 bis 22/2 und 27** betroffenen Personen _____ sind **unverzüglich,** spätestens nach _____ der Abwehr **der durch eine Sicherheitslücke,** ein Schadprogramm **oder einen Angriff verursachten** Gefahr **für die IT-Sicherheit**, zu benachrichtigen _____. [2]**Satz 1 gilt nicht, soweit zur Durchführung der Benachrichtigung in unverhältnismäßiger Weise weitere Daten der betroffenen Personen erhoben werden müssten.**

**(2)** [1]Die Benachrichtigung kann unterbleiben,

1. solange **ihr ein in § 27 Abs. 1 Satz 1 genannter Zweck entgegensteht,**

**1/1. solange durch das mit der Benachrichtigung verbundene Bekanntwerden einer Sicherheitslücke** die IT-Sicherheit gefährdet würde **oder**

2. wenn die Person nur unerheblich betroffen **ist** und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.

**[2]Soll eine Benachrichtigung nach Satz 1 Nr. 1 oder 1/1 unterbleiben, so bedarf dies der Zustimmung des Amtsgerichts, in dessen Bezirk die Behörde ihren Sitz hat; für das gerichtliche Verfahren gilt § 19 Abs. 4 NPOG entsprechend.** [3]**Soll** eine Benachrichtigung **nach Satz 1 Nr. 2** unterbleiben ____, **so** bedarf dies der Anordnung der Behördenleitung **im Einvernehmen mit** einer oder einem weiteren Beschäftigten der Behörde mit der Befähigung zum Richteramt. [4]**Wenn** eine solche Person nicht beschäftigt ist **oder aus anderen Gründen nicht zur Verfügung steht**, **tritt an deren Stelle** eine **bei** der Aufsichtsbehörde **beschäftigte und von deren Behördenleitung bestimmte Person** mit der Befähigung zum Richteramt _____. [5]_____ *(jetzt in Satz 4)*

§ 26
Dokumentation

[1]Anordnungen**,** ____ Genehmigungen**, Bestätigungen und Zustimmungen** nach § 21 Abs. 2 Satz 3, § 22 Abs. 2 Satz 4 und Abs. 3 Satz 3**, § 22/2 Abs. 3 Sätze 1, 6 und 7,** § 25 **Abs. 2 Sätze 2 und** 3 sowie **§ 27 Abs. 1 Sätze 2 bis 6** sind zu dokumentieren. [2]Die **in der** Dokumentation **enthaltenen personenbezogenen Daten dürfen** ausschließlich **zur Datenschutzkontrolle**

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

*Empfehlungen des Ausschusses für Inneres und Sport*

verwendet werden. [3]Sie **sind** zu löschen, wenn **seit einer Benachrichtigung nach § 25 Abs. 1 Satz 1 ein Jahr vergangen ist, frühestens jedoch zwei Jahre nach der Dokumentation, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden**.

**§ 26/1**
**Beteiligung der oder des Landesbeauftragten für den Datenschutz**

[1]**Jede Behörde, die ihre Befugnisse nach diesem Abschnitt wahrnimmt, legt** der **oder dem Landesbeauftragten** für den Datenschutz ____ einmal **jährlich** eine Aufstellung über die **Datenverarbeitung** nach den §§ **18/1** bis **22/2,** ____ 25 **und 27 Abs. 1** _____ sowie die Dokumentation nach § 26 vor____. [2]Satz 1 gilt nicht für den Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten, soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.

§ 27
Übermittlung personenbezogener Daten

§ 27
**Zweckbindung,**
Übermittlung personenbezogener Daten

**(0/1)** [1]**Die nach den §§ 18/1 bis 22/2 verarbeiteten** personenbezogenen Daten **sowie die Auswertungsergebnisse** dürfen nicht **zu** anderen **als den dort genannten** Zwecken verarbeitet werden. [2]**Insbesondere** ist die Erstellung von personenbezogenen Profilen zur Vorhersage des Nutzungsverhaltens von natürlichen Personen untersagt.

(1) [1]Die Behörden sollen die Daten nach den §§ 21 und 22 übermitteln

(1) [1]**Jede** Behörde soll **abweichend von Absatz 0/1** die nach ____ § 21 **Abs. 2, §** 22 **Abs. 3 oder § 22/2 Abs. 2 ausgewerteten personenbezogenen** Daten _____ **sowie die Auswertungsergebnisse** übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100 a Abs. 2 der Strafprozessordnung bezeichneten Straftat,

1. an die Strafverfolgungsbehörden**, wenn dies** zur Verfolgung einer Straftat **erforderlich ist und die Strafverfolgungsbehörden die Daten mit einer Maßnahme nach** § 100 a **oder § 100 g** der Strafprozessordnung **(StPO) hätten erheben dürfen**,

2. an die Polizeibehörden zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person,

2. an die Polizeibehörden **des Bundes und der Länder, wenn dies** zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person **erforderlich ist**,

*Gesetzentwurf der Landesregierung - Drs. 18/1598*

3. an die Verfassungsschutzbehörde, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese zur planmäßigen Beobachtung und Aufklärung eines Beobachtungs- oder Verdachtsobjekts, das auf die Anwendung oder Vorbereitung von Gewalt gerichtet ist, oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 des Niedersächsischen Verfassungsschutzgesetzes erforderlich sind.

[2]Die Übermittlung nach Satz 1 Nrn. 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. [3]Für das Verfahren nach Satz 1 Nrn. 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [4]Für die Übermittlung der entsprechenden personenbezogenen Daten nach Satz 1 Nr. 3 gelten die §§ 9 bis 16 des Artikel 10-Gesetzes entsprechend.

(2) [1]Die Behörden können nach §§ 21 und § 22 verarbeitete personenbezogene Daten an die für den Betrieb der Informationstechnik der Behörden zuständigen Stellen oder damit beauftragte Betriebe übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die IT-Sicherheit der Behörden erforderlich ist. [2]Die das Landesdatennetz betreibende Behörde und die vom Justizministerium bestimmte Stelle können im Rahmen der Wahrnehmung ihrer Aufgaben nach § 13 Abs. 2 und 3 personenbezogene Daten an die an das Landesdatennetz angeschlossenen Behörden übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die IT-Sicherheit der Behörden erforderlich ist.

*Empfehlungen des Ausschusses für Inneres und Sport*

3. an die Verfassungsschutzbehörde **des Landes**, wenn **dies** zur Erfüllung der Aufgabe nach § 3 Abs. 1 ____ des Niedersächsischen Verfassungsschutzgesetzes erforderlich **ist und die Verfassungsschutzbehörde die Daten mit einer Maßnahme nach § 20 des Niedersächsischen Verfassungsschutzgesetzes oder § 3 des Artikel 10-Gesetzes hätte erheben dürfen**.

**[1/1]Die Übermittlung von Daten einer in § 53 oder § 53 a StPO genannten Person, über die diese das Zeugnis verweigern dürfte, ist unzulässig.** [2]**Eine** Übermittlung nach Satz 1 Nr. 1 **oder Nr.** 2 bedarf der vorherigen ____ Zustimmung **des Amtsgerichts, in dessen Bezirk die übermittelnde Behörde ihren Sitz hat;** für das **gerichtliche** Verfahren **gilt § 19 Abs. 4 NPOG** entsprechend. [3]_____ *(jetzt in Satz 2)* [4]**Eine** Übermittlung _____ nach Satz 1 Nr. 3 **bedarf der vorherigen Zustimmung der nach § 3 Abs. 1 Sätze 1 bis 4 des Niedersächsischen Gesetzes zur Ausführung** des Artikel 10-Gesetzes **(Nds. AG G 10) bestellten G 10-Kommission; § 3 Abs. 1 Sätze 5 bis 7 und Abs. 2 bis 4 Nds. AG G 10 gilt** entsprechend. **[5]Bei Gefahr im Verzug kann die Behördenleitung anordnen, dass die Daten vor der nach Satz 2 oder 4 erforderlichen Zustimmung übermittelt werden. [6]In diesem Fall ist unverzüglich die nachträgliche Zustimmung einzuholen. [7]Wird die nachträgliche Zustimmung abgelehnt, so tritt die Anordnung außer Kraft. [8]Die bereits übermittelten Daten dürfen in diesem Fall nicht verwendet werden und sind unverzüglich zu löschen; die empfangende Stelle ist darüber zu unterrichten.**

(2) [1]**Wurde durch Maßnahmen nach den §§ 18/1 bis 22/2 eine Sicherheitslücke, ein Schadprogramm oder ein Angriff festgestellt, so kann jede** Behörde **Auswertungsergebnisse, soweit erforderlich auch einschließlich der darin enthaltenen** personenbezogenen Daten**,** an _____ Stellen _____ übermitteln, **deren IT-Systeme mit dem Landesdatennetz verbunden sind,** wenn _____ dies zur Abwehr _____ von **durch die Sicherheitslücke, das Schadprogramm oder den Angriff verursachten** Gefahren für die IT-Sicherheit _____ erforderlich ist. [2]_____

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| § 28<br>Einschränkung von Grundrechten | § 28<br>Einschränkung von Grundrechten |
| Das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes wird durch die §§ 19 bis 22 und 27 eingeschränkt. | Das Fernmeldegeheimnis nach Artikel 10 **Abs. 1** des Grundgesetzes wird durch die §§ 19 bis **22/3** und 27 eingeschränkt. |
| Artikel 2<br>Änderung des Niedersächsischen Beamtengesetzes | Artikel 2<br>Änderung des Niedersächsischen Beamtengesetzes |
| Nach § 92 des Niedersächsischen Beamtengesetzes vom 25. März 2009 (Nds. GVBl. S. 72), zuletzt geändert durch Artikel 21 des Gesetzes vom 16. Mai 2018 (Nds. GVBl. S. 66), wird der folgende § 92 a eingefügt: | Nach § 92 des Niedersächsischen Beamtengesetzes vom 25. März 2009 (Nds. GVBl. S. 72), zuletzt geändert durch Artikel **2** des Gesetzes vom **18**. **Dezember** 2018 (Nds. GVBl. S. **317**), wird der folgende § 92 a eingefügt: |
| „§ 92 a<br>Verarbeitung von Personalaktendaten im Auftrag | „§ 92 a<br>Verarbeitung von Personalaktendaten im Auftrag |
| (1) [1]Die personalverwaltende Behörde darf gemäß Artikel 28 der Datenschutz-Grundverordnung Personalaktendaten im Auftrag nur für | (1) [1]Die personalverwaltende Behörde darf _____ nur **bei** |
| 1. die Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen und | 1. **der** Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen und |
| 2. die automatisierte Erledigung von Aufgaben für Zwecke nach § 88 Abs. 1 Satz 1 | 2. **der** automatisierten Erledigung von Aufgaben für Zwecke nach § 88 Abs. 1 Satz 1 |
| verarbeiten lassen. [2]Die personalverwaltende Behörde hat die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragsverarbeiter regelmäßig zu kontrollieren. | gemäß Artikel 28 der Datenschutz-Grundverordnung Personalaktendaten im Auftrag verarbeiten lassen. [2]_____ *(jetzt in Absatz 2/1)* [3]Eine nicht öffentliche Stelle darf nur beauftragt werden, wenn _____ bei **der personalverwaltenden Behörde** sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die **Verarbeitungsleistungen** erheblich kostengünstiger **erbringen** kann. |
| (2) Die Auftragserteilung und die Genehmigung einer Unterauftragserteilung bedürfen der vorherigen Zustimmung der obersten Dienstbehörde. | (2) *unverändert* |
| | **(2/1)** Die personalverwaltende Behörde hat die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den **oder die** Auftragsverarbeiter regelmäßig zu kontrollieren. |
| (3) Eine nicht öffentliche Stelle darf nur beauftragt werden, wenn die Beauftragung der Erfüllung von Aufgaben nach Absatz 1 Satz 1 dient und beim Verantwortlichen sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die übertragenen Aufgaben erheblich kostengünstiger erledigen kann.“ | (3) ***wird*** *(hier)* ***gestrichen*** *(jetzt in Absatz 1 Satz 3)* |

| *Gesetzentwurf der Landesregierung - Drs. 18/1598* | *Empfehlungen des Ausschusses für Inneres und Sport* |
|---|---|
| Artikel 3<br>Evaluation und Inkrafttreten | Artikel 3<br>Evaluation und Inkrafttreten |
| (1) Die Landesregierung überprüft zwei Jahre nach Inkrafttreten dieses Gesetzes die finanziellen Auswirkungen der Umsetzung auf die Kommunen. | *unverändert* |
| (2) [1]Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft. [2]Abweichend von Satz 1 tritt<br><br>1. Artikel 1 § 6 Abs. 3 und § 12 Abs. 1 Satz 1 Nr. 6 am 18. April 2020,<br><br>2. Artikel 1 § 4 Abs. 2 bis 4, § 5 Abs. 2, § 6 Abs. 1 und 2, § 12 Abs. 1 bis 3 am 1. Juli 2021 und<br><br>3. Artikel 1 § 5 Abs. 5 am 1. Januar 2023<br><br>in Kraft. | |



(Verteilt am 02.10.2019)