Niedersächsisches
Ministerialblatt

63. (68.) Jahrgang | Hannover, den 27. 11. 2013 | Nummer 44

INHALT

A. Staatskanzlei

B. Ministerium für Inneres und Sport

Gem. RdErl. 23. 10. 2013, Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) ... 864
20500

Gem. RdErl. 23. 10. 2013, Informationssicherheitsrichtlinie über die Abwehr von Schadsoftware (ISRL-Schadsoftware) 864

Gem. RdErl. 23. 10. 2013, Informationssicherheitsrichtlinie über die Datensicherung (ISRL-Datensicherung) ... 865

Gem. RdErl. 23. 10. 2013, Informationssicherheitsrichtlinie über die Nutzung des zentralen Internetzugangs und von Web-Angeboten (ISRL-Web-Nutzung) ... 868

Gem. RdErl. 23. 10. 2013, Informationssicherheitsrichtlinie über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender (ISRL-IT-Nutzung) ... 870

Bek. 1. 11. 2013, Vereinbarung gemäß § 81 NPersVG über die Durchführung einer Personalstrukturanalyse (PSA) in der niedersächsischen Landesverwaltung ... 873

Gem. RdErl. 8. 11. 2013, Zusammenarbeit von Staatsanwaltschaft und Polizei; Beschleunigung der Verfahrensabläufe insbesondere in sog. Umfangsverfahren ... 875
21021

Bek. 12. 11. 2013, Verleihung der Niedersächsischen Sportmedaille ... 876

C. Finanzministerium

RdErl. 12. 11. 2013, Lohnsteuerliche Behandlung von unentgeltlichen oder verbilligten Mahlzeiten der Arbeitnehmer ab Kalenderjahr 2014 ... 876

D. Ministerium für Soziales, Frauen, Familie, Gesundheit und Integration

RdErl. 1. 11. 2013, Hilfe zur Erziehung in Vollzeitpflege; Festsetzung der monatlichen Pauschalbeträge (Pflegegeld) 876
21130 00 00 07 017

RdErl. 19. 11. 2013, Richtlinie über die Gewährung von Zuwendungen zur Behebung der vom Hochwasser 2013 verursachten Schäden in Landkreisen, Städten und Gemeinden in Niedersachsen ... 877
23400

E. Ministerium für Wissenschaft und Kultur

F. Kultusministerium

G. Ministerium für Wirtschaft, Arbeit und Verkehr

H. Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz

RdErl. 1. 10. 2013, Tierschutz; Anforderungen an die Straußenhaltung ... 878
78530

I. Justizministerium

K. Ministerium für Umwelt, Energie und Klimaschutz

RdErl. 18. 11. 2013, Einführung des Programms Abwasserkataster Niedersachsen: Erfassung, Auswertung und Weiterleitung der Daten aus der behördlichen Einleiterüberwachung ... 878
28200

Landesamt für Bergbau, Energie und Geologie

Bek. 30. 10. 2013, Feststellung gemäß § 3 c UVPG (RWE Dea AG, Hamburg) ... 878

Landesamt für Geoinformation und Landentwicklung Niedersachsen

Bek. 14. 11. 2013, Feststellung gemäß § 6 NUVPG (Vereinfachte Flurbereinigung Dellien, Landkreis Lüneburg) ... 879

Landeswahlleiterin

Bek. 8. 11. 2013, Verzeichnis der Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Wahlperiode des 17. Niedersächsischen Landtages ... 879

Bek. 8. 11. 2013, Verzeichnis der Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Wahlperiode des 18. Deutschen Bundestages ... 879

Bek. 8. 11. 2013, Verzeichnis der Stadtwahlleiterinnen, Stadtwahlleiter, Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Europawahl 2014 ... 880

Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz

Bek. 8. 11. 2013, Veröffentlichung gemäß § 83 WHG; Anhörungsdokumente zu den wichtigen Fragen der Gewässerbewirtschaftung für die Flussgebietseinheiten Elbe, Weser, Ems und Rhein (niedersächsischer Anteil) ... 880

Bek. 27. 11. 2013, Vorläufige Sicherung des Überschwemmungsgebietes der Großen Hase, des Essener Kanals und der Überfallhase von der Einmündung des Hahnenmoorkanals (Fluss-km 47 + 500) bis zum Schützenhofwehr Quakenbrück (Fluss-km 79 + 200) in den Landkreisen Osnabrück, Cloppenburg und Emsland ... 881

Bek. 27. 11. 2013, Vorläufige Sicherung des Überschwemmungsgebietes der Hunte von der Grenze zum Landkreis Vechta (Fluss-km 120 + 250) bis zur Straße „Zur Römerbrücke“ in Nierhüsen (Fluss-km 137 + 630) in den Landkreisen Vechta und Osnabrück ... 881

Staatliches Gewerbeaufsichtsamt Braunschweig

Bek. 15. 11. 2013, Feststellung gemäß § 3 a UVPG (H. C. Starck GmbH, Goslar) ... 882

Staatliches Gewerbeaufsichtsamt Celle

Bek. 11. 11. 2013, Feststellung gemäß § 3 a UVPG (Biogasanlage Rehmsgas UG & Co. KG, Hermann Meine, Hambühren) 882

Staatliches Gewerbeaufsichtsamt Hannover

Bek. 27. 11. 2013, Immissionsschutzrechtliche Entscheidung gemäß § 16 Abs. 1 BImSchG (Smurfit Kappa Hoya Papier und Karton GmbH) ... 882

Staatliches Gewerbeaufsichtsamt Lüneburg

Bek. 18. 11. 2013, Planfeststellungsverfahren zur Errichtung und zum Betrieb der Deponie Haaßel — Anhörungsverfahren — (Kriete Kaltrecycling GmbH, Seedorf) ... 883

Staatliches Gewerbeaufsichtsamt Oldenburg

Bek. 5. 11. 2013, Feststellung gemäß § 3 a UVPG (ekn Gasvertrieb GmbH, Nordhorn) ... 890

Bek. 11. 11. 2013, Feststellung gemäß § 3 a UVPG (Biogas Lohe GmbH & Co. KG, Bakum) ... 890

Bek. 11. 11. 2013, Feststellung gemäß § 3 a UVPG (GF Bio-Energie-Hasetal GmbH, Löningen) ... 890

Bek. 12. 11. 2013, Genehmigungsverfahren nach dem BImSchG; Öffentliche Bekanntmachung (DMK Deutsches Milchkontor GmbH, Zeven) ... 890

Berichtigung ... 891

Stellenausschreibungen ... 891/892

B. Ministerium für Inneres und Sport

Leitlinie zur Gewährleistung der Informationssicherheit (ISLL)

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 23. 10. 2013 — CIO-02850-0007 —

— VORIS 20500 —

Bezug: Gem. RdErl. v. 12. 7. 2011 (Nds. MBl. S. 518) — VORIS 20500 —

Nummer 6.2 des Bezugserlasses wird mit Wirkung vom 1. 11. 2013 wie folgt geändert:

Nach Satz 1 werden die folgenden Sätze 2 und 3 eingefügt:

„Die zuständige oberste Landesbehörde kann abweichende Verantwortlichkeiten festlegen. Diese Leitlinie und die Informationssicherheitsrichtlinien sind in diesem Fall sinngemäß anzuwenden."

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 864

Informationssicherheitsrichtlinie über die Abwehr von Schadsoftware (ISRL-Schadsoftware)

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 23. 10. 2013 — CIO-02850/0110-0004 —

Bezug: Gem. RdErl. v. 12. 7. 2011 (Nds. MBl. S. 518), geändert durch Gem. RdErl. v. 23. 10. 2013 (Nds. MBl. S. 864) — VORIS 20500 —

1. Gegenstand und Geltungsbereich

Diese Informationssicherheitsrichtlinie über die Abwehr von Schadsoftware (ISRL-Schadsoftware) regelt auf Grundlage der Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) — Bezugserlass — in Form von Mindestanforderungen die Grundsätze der Abwehr von Schadsoftware und der Bewältigung bei einem tatsächlichen Schadsoftwarebefall von IT-Systemen der niedersächsischen Landesverwaltung.

Diese Informationssicherheitsrichtlinie gilt im gesamten Geltungsbereich der Leitlinie für die Gewährleistung der Informationssicherheit (Nummer 1.1 des Bezugserlasses).

2. Organisatorische und technische Maßnahmen der Behördenleitung

Die Behördenleitung ist im Rahmen ihrer Zuständigkeit für die Gewährleistung der Informationssicherheit verantwortlich. Zur Umsetzung dieser Informationssicherheitsrichtlinie sind durch die Behördenleitung die notwendigen organisatorischen und technischen Maßnahmen zu veranlassen. Die Sicherheitsanforderungen können auch dadurch erfüllt werden, dass die Behördenleitung einen Dritten (z. B. IT-Dienstleister, Landesbetrieb) mit der Umsetzung von Maßnahmen beauftragt. Entsprechende Vereinbarungen oder Verträge mit dem Dritten sind aktenkundig zu machen.

Soweit sichergestellt ist, dass die durch diese Informationssicherheitsrichtlinie festgelegten Mindestanforderungen vollständig umgesetzt werden, ist die weitere Ausgestaltung der Maßnahmen in Art und Umfang freigestellt.

3. Umsetzung

3.1 Die Umsetzung der Sicherheitsanforderungen (Nummer 5) soll vorrangig durch technische Maßnahmen erfolgen, die durch organisatorische Maßnahmen ergänzt werden.

3.2 Die Verantwortungsbereiche der einzelnen Anwenderinnen und Anwender sind eindeutig vom Verantwortungsbereich der Systemadministration abzugrenzen.

3.3 Zur organisatorischen Umsetzung der Sicherheitsanforderungen wird vorgeschlagen, dass die Anwenderinnen und Anwender über das Verhalten bei einem Verdacht auf Schadsoftwarebefall anhand der in der **Anlage** aufgeführten Inhalte informiert werden.

3.4 Es sind ggf. ergänzende organisatorische Maßnahmen zu ergreifen, insbesondere wenn sich Sicherheitsanforderungen unmittelbar an die Anwenderinnen und Anwender richten. Bei der Gestaltung organisatorischer Maßnahmen, insbesondere bei der Erstellung von Dienstanweisungen, ist zu beachten, dass diese auch für Anwenderinnen und Anwender ohne vertiefte IT-Kenntnisse verständlich und tatsächlich umsetzbar sind. Die spezifischen Sicherheitsmaßnahmen der einzelnen Sicherheitsdomänen müssen in einem angemessenen Verhältnis zur praktischen Handhabbarkeit durch die Anwenderinnen und Anwender stehen.

4. Innerbehördliche Zuständigkeit und Organisation

Die Behördenleitung legt die innerbehördlichen Zuständigkeiten (zuständigen Stellen) und ggf. die erforderlichen Prozesse für die Umsetzung der technischen und organisatorischen Maßnahmen aufgrund dieser Informationssicherheitsrichtlinie in eigener Zuständigkeit fest.

5. Sicherheitsanforderungen

5.1 Schutz vor Schadsoftware

5.1.1 Die Behördenleitung hat dafür Sorge zu tragen, dass grundsätzlich auf jedem Endgerät (z. B. Arbeitsplatzrechner, Tablet-Computer, Notebook) sowie auf jedem Serversystem eine Anti-Schadsoftware eingesetzt oder eine effektive Alternativmaßnahme zur Abwehr von Schadsoftware getroffen wird.

5.1.2 Die Behördenleitung entscheidet anhand einer Risikoanalyse, ob bestimmte Endgeräte (z. B. Smartphones) ohne Anti-Schadsoftware eingesetzt werden dürfen. Das Ergebnis der Risikoanalyse ist aktenkundig zu machen.

5.1.3 Die Behördenleitung gewährleistet, dass die eingesetzte Anti-Schadsoftware regelmäßig automatisiert aktualisiert wird. Die Aktualisierungsintervalle sind so klein wie nötig zu halten.

5.1.4 Der Status des Schutzes der IT-Systeme soll auf einem zentralen System erfasst werden.

5.1.5 Die Anti-Schadsoftware hat Dateien beim Zugriff zu untersuchen, unabhängig davon, auf welchem Datenträger oder Speichermedium die Dateien abgelegt sind. IT-Systeme sollen regelmäßig ohne Anlass vollständig auf Schadsoftware untersucht werden. Nach der Auslieferung vorinstallierter IT-Systeme oder der Durchführung von Wartungsarbeiten sollen die betroffenen IT-Systeme auf Schadsoftware untersucht werden.

5.2 Sensibilisierung und Information

5.2.1 Die Behördenleitung stellt sicher, dass alle Anwenderinnen und Anwender sowie die Systemadministration für von Schadsoftware ausgehende Gefahren und hinsichtlich der einzuhaltenden Sicherheitsmaßnahmen in angemessener Form und im notwendigen Umfang sensibilisiert und über aktuelle Veränderungen (z. B. Sicherheitshinweise) informiert werden.

5.2.2 Die Anwenderinnen und Anwender sind im erforderlichen Umfang und in geeigneter Weise zu informieren, wie sie sich bei einem Verdacht auf Schadsoftwarebefall verhalten sollen.

5.2.3 Die Systemadministration ist zu befähigen, auf Schadsoftwarebefall sachgerecht zu reagieren (z. B. Feststellung einer tatsächlichen Infektion, Ermittlung der Infektionsquelle und des Ausmaßes der Infektion, Beweissicherung, Ermittlung eines Datenverlustes oder -abflusses, Optimierung der Präventionsmaßnahmen).

5.3 Vorgehen bei Schadsoftwarebefall

5.3.1 Die Beseitigung von Schadsoftware soll grundsätzlich automatisiert erfolgen. Für den Fall, dass eine automatisierte Beseitigung fehlschlägt, sind die zur Beseitigung erforderlichen Zuständigkeiten und Abläufe von der Behördenleitung festzulegen.

5.3.2 Die Behördenleitung bestimmt, in welchen Fällen und auf welche Weise die zuständigen Stellen bei einem Schadsoftwarebefall zu informieren sind. Sie gewährleistet, dass die oder der Informationssicherheitsbeauftragte der Landesverwaltung in den gemäß Nummer 7.3.1 der ISLL vorgesehenen Fällen informiert wird.

6. Schlussbestimmung

Dieser Gem. RdErl. tritt am 1. 11. 2013 in Kraft.

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 864

Anlage

Inhalte für die Information der Anwenderinnen und Anwender über das Verhalten bei einem Verdacht auf Schadsoftwarebefall

1. Ausgangslage

Besteht der Verdacht, dass ein Endgerät oder eine Fachanwendung von Schadsoftware befallen sein könnte, so beachten Sie bitte die nachfolgenden Handlungsempfehlungen.

2. Meldestelle

Zuständige Meldestelle für einen Verdacht auf Schadsoftwarebefall ist [...].

3. Anhaltspunkte für einen Schadsoftwarebefall

Folgende Anhaltspunkte können auf einen Befall von IT-Systemen mit Schadsoftware hindeuten, wobei diese Anhaltspunkte nicht zwingend auf einen Schadsoftwarebefall zurückzuführen sein müssen und deshalb einer genauen Untersuchung bedürfen, die [die zuständige Stelle für die Betriebsverantwortung] für Sie durchführen wird:

— häufige Abstürze von Programmen,
— unerklärliches Systemverhalten,
— unerklärliche Fehlermeldungen,
— Zugriffsberechtigung für unbekannte Dienste oder Funktionen,
— unerklärliche Netzverbindungen,
— unerklärliche Veränderungen an Datei-Inhalten,
— unerklärliche Veränderungen an Dokumenteigenschaften,
— unerklärliche Veränderungen an Datei-Größen,
— ständige Verringerung des freien Speicherplatzes ohne tatsächliche Speicherung,
— Versand von E-Mails ohne Aktion der Anwenderin oder des Anwenders,
— nicht auffindbare Dateien,
— kein Zugriff auf einzelne Laufwerke,
— Probleme beim Starten des Rechners,
— unerklärliche Veränderung von Icons oder
— Probleme beim Abspeichern von Dateien oder Daten von Fachanwendungen.

4. Arbeitsschritte

4.1 Ruhe bewahren!

4.2 Auf keinen Fall dürfen Sie mit Ihrem Endgerät, auf dem Sie die Schadsoftware vermuten, weiterarbeiten.

4.3 Trennen Sie bei einem Verdacht auf einen Schadsoftwarebefall Ihr Endgerät sofort vom Netzwerk.

4.4 Besteht Ihrerseits der Verdacht, dass die Schadsoftware ein IT-System befallen hat, auf dem eine von Ihnen genutzte Fachanwendung bereitgestellt wird, so dürfen Sie auf keinen Fall mit dieser Fachanwendung weiterarbeiten! Melden Sie sich bitte sofort von der Fachanwendung ab.

4.5 Melden Sie sofort Ihren Verdacht auf einen Schadsoftwarebefall an [die zuständige Meldestelle]. Benennen Sie dabei das betroffene Endgerät (z. B. Arbeitsplatzrechner, Smartphone, Tablet-Computer, Notebook) eindeutig. Geben Sie möglichst auch den genauen Rechnernamen [siehe Aufkleber auf dem Gerät] an. Geben Sie ferner die festgestellten Symptome der o. a. Liste zu Nummer 3 an.

4.6 Warten Sie auf weitere Anweisungen der [zuständigen Meldestelle].

4.7 Ist die Quelle der Schadsoftware auf einen Datenträger zurückzuführen, der sich in Ihrem Besitz befindet, dürfen Sie diesen auf keinen Fall weiterbenutzen oder an andere Anwenderinnen und Anwender weitergeben. Händigen Sie diesen Datenträger bitte sofort der [zuständigen Meldestelle] aus.

4.8 Wenn noch andere Anwenderinnen oder Anwender auf Ihr Endgerät zugreifen, warnen Sie diese bitte ausdrücklich, dass ein Verdacht auf einen Schadsoftwarebefall besteht.

4.9 Setzen Sie Ihre Bearbeitung mit dem mutmaßlich befallenen Endgerät oder der Fachanwendung erst fort, wenn Ihnen die [zuständige Meldestelle] bestätigt hat, dass die Bereinigung des IT-Systems abgeschlossen ist.

4.10 Ändern Sie unverzüglich Ihr Anmelde-Kennwort.

Informationssicherheitsrichtlinie über die Datensicherung (ISRL-Datensicherung)

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 23. 10. 2013 — CIO-02850/0110-0005 —

Bezug: Gem. RdErl. v. 12. 7. 2011 (Nds. MBl. S. 518), geändert durch Gem. RdErl. v. 23. 10. 2013 (Nds. MBl. S. 864)
— VORIS 20500 —

1. Gegenstand und Geltungsbereich

Diese Informationssicherheitsrichtlinie über die Datensicherung (ISRL-Datensicherung) regelt auf Grundlage der Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) — Bezugserlass — in Form von Mindestanforderungen die Grundsätze der Datensicherung in der niedersächsischen Landesverwaltung. Diese Grundsätze gelten für alle elektronisch verarbeiteten Informationen (z. B. Dokumente in Dateiform, Inhaltsdaten der Fachanwendungen, Systemdaten, Protokolldaten).

Diese Informationssicherheitsrichtlinie gilt im gesamten Geltungsbereich der Leitlinie zur Gewährleistung der Informationssicherheit (Nummer 1.1 des Bezugserlasses).

2. Begriffsbestimmungen

Im Sinne dieser Informationssicherheitsrichtlinie ist

2.1 „Datensicherung“ das Kopieren von elektronisch gespeicherten Daten und erforderlichen Metainformationen, um sie im Fall eines Datenverlustes wiederherstellen zu können;

2.2 „Datenwiederherstellung“ die Rekonstruktion der elektronisch gespeicherten Daten in ihren vorherigen Kontext aus einer Datensicherung.

3. Organisatorische und technische Maßnahmen der Behördenleitung

Die Behördenleitung ist im Rahmen ihrer Zuständigkeit für die Gewährleistung der Informationssicherheit verantwortlich. Zur Umsetzung dieser Informationssicherheitsrichtlinie sind durch die Behördenleitung die notwendigen organisatorischen und technischen Maßnahmen zu veranlassen. Die Sicherheitsanforderungen können auch dadurch erfüllt werden, dass die Behördenleitung einen Dritten (z. B. IT-Dienstleister, Landesbetrieb) mit der Umsetzung von Maßnahmen beauftragt. Entsprechende Vereinbarungen oder Verträge mit dem Dritten sind aktenkundig zu machen.

Soweit sichergestellt ist, dass die durch diese Informationssicherheitsrichtlinie festgelegten Mindestanforderungen vollständig umgesetzt werden, ist die weitere Ausgestaltung der Maßnahmen in Art und Umfang freigestellt.

4. Umsetzung

4.1 Die Umsetzung der Sicherheitsanforderungen (Nummer 6) soll vorrangig durch technische Maßnahmen erfolgen, die durch organisatorische Maßnahmen ergänzt werden.

4.2 Zur organisatorischen Umsetzung der Sicherheitsanforderungen werden die Erstellung eines Anforderungskatalogs zur Datensicherung auf der Basis der in der **Anlage 1** dargestellten Checkliste sowie die Erstellung einer Datensicherungskonzeption auf der Basis der in der **Anlage 2** dargestellten Gliederung vorgeschlagen.

4.3 Es sind ggf. ergänzende organisatorische Maßnahmen zu ergreifen, insbesondere wenn sich Sicherheitsanforderungen unmittelbar an die Anwenderinnen und Anwender richten. Bei der Gestaltung organisatorischer Maßnahmen, insbesondere bei der Erstellung von Dienstanweisungen, ist zu beachten, dass diese auch für Anwenderinnen und Anwender ohne vertiefte IT-Kenntnisse verständlich und tatsächlich umsetzbar sind. Die spezifischen Sicherheitsmaßnahmen der einzelnen Sicherheitsdomänen müssen in einem angemessenen Verhältnis zur praktischen Handhabbarkeit durch die Anwenderinnen und Anwender stehen.

5. Innerbehördliche Zuständigkeit und Organisation

Die Behördenleitung legt die innerbehördlichen Zuständigkeiten (zuständige Stellen) und ggf. die erforderlichen Prozesse für die Umsetzung der technischen und organisatorischen Maßnahmen aufgrund dieser Informationssicherheitsrichtlinie in eigener Zuständigkeit fest.

6. Sicherheitsanforderungen

6.1 Grundsatz der zentralen Datenspeicherung

Die Datenspeicherung soll grundsätzlich zentral auf serverbasierten IT-Systemen der Dienststellen, einer Behörde, einer Fachverwaltung oder eines IT-Dienstleisters erfolgen.

6.2 Grundsätze zur Datensicherung

6.2.1 Die Datensicherung soll regelmäßig, automatisiert und zentral erfolgen.

6.2.2 Die gesicherten Daten sollen räumlich getrennt von den zu sichernden Daten aufbewahrt werden.

6.3 Anforderungen an die Datensicherung

6.3.1 Die Behördenleitung verantwortet die fachlichen Anforderungen an die Sicherung der Daten, einschließlich der Daten auf mobilen Endgeräten und Speichermedien. Es ist dabei unter Berücksichtigung der Risiken für die Verfügbarkeit der zu sichernden Daten sowie für die Vertraulichkeit und Integrität der gesicherten Daten und unter Wirtschaftlichkeitsaspekten zu bestimmen, welche Daten wie zu sichern und wie die Sicherungsdaten aufzubewahren sind. Der Anforderungskatalog ist aktenkundig zu machen.

6.3.2 Für die betriebliche Umsetzung der fachlichen Anforderungen hat die Behördenleitung eine Datensicherungskonzeption zu veranlassen, die mindestens die Festlegungen zur Datensicherung, zur Aufbewahrung der Sicherungsdaten, zur Datenwiederherstellung und zur Überprüfung der Wiederherstellbarkeit der gesicherten Daten umfasst.

6.4 Datenverlust

Die Behördenleitung stellt sicher, dass die oder der zuständige Informationssicherheitsbeauftragte im Fall eines Datenverlustes informiert wird.

6.5 Datenwiederherstellung

Die Entscheidung zur Datenwiederherstellung und zu deren Umfang ist ausschließlich von der dafür zuständigen Stelle zu treffen und aktenkundig zu machen.

6.6 Vertraulichkeit und Datenschutz

6.6.1 Die Vertraulichkeitsanforderung an die gesicherten Daten ergibt sich grundsätzlich aus der höchsten Vertraulichkeitsanforderung der zu sichernden Daten. Aus der Konzentration einer Vielzahl vertraulicher Daten kann sich eine höhere Vertraulichkeitsanforderung der gesicherten Daten ergeben.

6.6.2 Die Behördenleitung stellt sicher, dass Sicherungsmedien gelöscht oder vernichtet werden, sobald die Zweckbestimmung eine weitere Aufbewahrung der Sicherungsdaten nicht mehr erfordert.

6.7 Information der Anwenderinnen und Anwender

Die Anwenderinnen und Anwender sind über den Umfang der Datensicherung und das Verfahren zur Datenwiederherstellung zu informieren.

6.8 Sicherstellung der Wirksamkeit

Die Behördenleitung verantwortet die Überprüfung, ob

— sich die Anforderungen an die Datensicherung verändert haben,

— die getroffenen Maßnahmen zur Datensicherung den Anforderungen noch genügen und

— die implementierten Datensicherungsprozesse ordnungsgemäß funktionieren.

Die ordnungsgemäße Funktion der Datensicherungsprozesse ist insbesondere durch regelmäßige Überprüfungen der Wiederherstellbarkeit der gesicherten Daten festzustellen. Die Ergebnisse der Prüfungen sind aktenkundig zu machen.

7. Schlussbestimmung

Dieser Gem. RdErl. tritt am 1. 11. 2013 in Kraft.

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 865

Anlage 1

Checkliste
für einen Anforderungskatalog zur Datensicherung

1. Betroffener Datenbestand

1.1 Die Datensicherung soll folgende(s) Verfahren betreffen: […].

1.2 Es sollen die Daten des genannten Verfahrens gesichert werden, soweit sie in folgenden Systemumgebungen gespeichert sind:

— Produktionssystem,
— Testsystem,
— Referenzsystem,
— Schulungssystem.

1.3 Die Datensicherung soll folgende vom Verfahren genutzten IT-Systeme umfassen: […].

2. Spezifikation der zu sichernden Daten

Es ist festzulegen, für welche der folgenden gespeicherten Daten die Datensicherung durchzuführen ist:

— Anwendungssoftware für das Fachverfahren,
— Anwendungssoftware für die Büroarbeitsumgebung,
— Nutzdaten in Dateien auf File-Servern,
— Nutzdaten auf Datenbank-Servern,
— Nutzdaten auf Web-Servern,
— Nutzdaten auf Applikationsservern,
— Nutzdaten in den E-Mail-Postfächern,
— Struktur der Nutzdaten (z. B. Datenbankschemata),
— systemseitige Protokolldaten (z. B. der E-Mail-Server, der Web-Proxy),
— Systemdaten (z. B. Konfigurationsdateien, Passwortdateien, Zugriffsrechtedateien, Benutzerprofile),
— verfahrensseitige Protokolldaten (z. B. Eingaben, Änderungen, Löschungen von Inhaltsdaten).

3. Katalog der Anforderungen

3.1 Anforderungen an die Verfügbarkeit der zu sichernden Daten

Die Anforderungen an die Verfügbarkeit der zu sichernden Daten sind anhand der Schutzkategorien „normal“, „hoch“ oder „sehr hoch“ der Nummer 3.7 der ISLL zu beschreiben; dabei ist zu entscheiden,

— in welchem Umfang ein unwiederbringlicher Datenverlust akzeptabel ist und

— wie lange die Datenwiederherstellung dauern darf.

3.2 Anforderungen an die Integrität der gesicherten Daten

Die Anforderungen an die Integrität der Daten sind anhand der Schutzkategorien „normal“, „hoch“ oder „sehr hoch“ der Nummer 3.7 der ISLL für die Datensicherung, die Aufbewahrung der Sicherungsdaten und die Datenwiederherstellung zu beschreiben.

3.3 Anforderungen an die Vertraulichkeit der gesicherten Daten

Die Anforderungen an die Vertraulichkeit der Daten sind nach folgenden Maßstäben für die Datensicherung, die Aufbewahrung der Sicherungsdaten und die Datenwiederherstellung zu beschreiben:

— Schutzstufen gemäß Schutzstufenkonzept der oder des Landesbeauftragten für den Datenschutz Niedersachsen für personenbezogene Daten,
— Schutzkategorien „normal“, „hoch“ oder „sehr hoch“ der Nummer 3.7 der ISLL für sonstige vertrauliche Informationen und
— Geheimhaltungsgrade für Verschlusssachen gemäß Verschlusssachenanweisung für das Land Niedersachsen.

3.4 Einflussfaktoren für die Datensicherung

Festzulegen sind

— das zu sichernde Datenvolumen, um das Sicherungsvolumen und das geeignete Sicherungsmedium bestimmen zu können; als Maßeinheit kann Gigabyte (GB) benutzt werden;
— das Änderungsvolumen in einem bestimmten Zeitabschnitt, um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können; als Arbeitseinheit kann Gigabyte (GB)/Woche benutzt werden;
— die feststehenden, regelmäßig wiederkehrenden Zeitpunkte für die Datenänderungen, um die Sicherungsintervalle bestimmen zu können; es soll angegeben werden, ob die Daten täglich, wöchentlich, monatlich und/oder zu bestimmten Terminen geändert werden;
— die Aufbewahrungsfristen sowie das Mindestalter der Datensicherung, um die Anzahl der aufzubewahrenden Sicherungsgenerationen bestimmen zu können;
— die Löschfristen oder eine festgelegte maximale Generationenanzahl.

4. Beauftragung der Datensicherung

Mit der Datensicherung wird [...] beauftragt.

5. Beauftragung der Datenwiederherstellung

Die Datenwiederherstellung wird von [...] veranlasst und von [...] durchgeführt.

6. Beauftragung von Übungen

Die Wirksamkeit der Datensicherung wird monatlich/halbjährlich/jährlich/[...] mittels einer Übung überprüft.

7. Beauftragung von Kontrollen

[...] kontrolliert im Abstand von [...] die Konsistenz, Vollständigkeit, Lesbarkeit und Rekonstruierbarkeit der Sicherungsdaten.

Anlage 2

Gliederung
für eine Datensicherungskonzeption

1. Fachliche Vorgaben

Die fachlichen Vorgaben für eine Datensicherungskonzeption ergeben sich aus dem Anforderungskatalog zur Datensicherung:

1.1 betroffener Datenbestand;
1.2 Spezifikation der zu sichernden Daten;
1.3 Anforderungen an die Verfügbarkeit der Daten;
1.4 Anforderungen an die Vertraulichkeit der Daten;
1.5 Anforderungen an die Integrität der Daten;
1.6 fachliche Vorgaben zu folgenden Einflussfaktoren:
- — Datenvolumen,
- — Änderungsvolumen,
- — Änderungszeitpunkte der Daten,
- — Aufbewahrungsfristen,
- — Löschfristen.

2. Betriebliche Konzeption

Die Datensicherungskonzeption soll in strukturierter Form Festlegungen für die Datensicherung, die Aufbewahrung der Sicherungsdaten, die Datenwiederherstellung und für Übungen zur Datenwiederherstellung treffen, und zwar

— je Verfahren (z. B. Fachverfahren, Büroarbeitsumgebung),
— je Systemumgebung (z. B. Produktions-, Test-, Referenz-, Schulungssystem),
— je IT-System (z. B. Datenbank-, File-, Web-, Applikations-, E-Mail-Server),
— je Datenbestand (z. B. Betriebssystem, System-, Nutz-, Protokolldaten).

Insbesondere können folgende Festlegungen in Betracht kommen:

2.1 für die Datensicherung:
- — geeignetes Sicherungssystem,
- — geeignetes Sicherungsmedium,
- — Zugriffsschutz für das Sicherungsmedium,
- — Veränderungsschutz für das Sicherungsmedium,
- — Vertraulichkeitsschutz für das Sicherungsmedium,
- — Vertraulichkeitsschutz für die Datenübertragung (bei Bedarf „sicherer Kanal“),
- — Art der Datensicherung (z. B. differentielle, inkrementelle, Voll-Sicherung),
- — Zeitintervalle der Datensicherung (z. B. täglich, wöchentlich, monatlich),
- — zusätzliche ereignisgesteuerte Datensicherungstermine,
- — Zeitpunkte der Datensicherung (z. B. nachts, freitags abends),
- — Anzahl der aufzubewahrenden Sicherungsgenerationen,
- — Verantwortlichkeit für die Datensicherung,
- — Dokumentation der Datensicherung,
- — Vorgehensweise zur Überprüfung der Wirksamkeit (z. B. Überprüfung der Protokolle);

2.2 für die Aufbewahrung der Sicherungsdaten:
- — Aufbewahrungsort des Sicherungsmediums,
- — Transportmodalitäten für das Sicherungsmedium,
- — Mindestverwahrdauer der Sicherungsdaten,
- — Vorgehensweise zur Gewährleistung von Löschfristen für die Sicherungsdaten,
- — Vorgehensweise zur Wiederverwendung von Sicherungsmedien,
- — Vorgehensweise zur Entsorgung von Sicherungsmedien,
- — Vorgehensweise zur Kontrolle der Wiederherstellbarkeit der Daten (z. B. Kontrolle auf Konsistenz, Vollständigkeit, Lesbarkeit, Rekonstruierbarkeit),
- — Vorgehensweise zur Kontrolle der Funktionsfähigkeit des Sicherungsmediums oder Sicherungssystems (z. B. Kontrolle auf Überalterung, technische Defekte, falsche Parametrisierung),
- — Dokumentation zum Lebenszyklus der Sicherungsmedien,
- — Vorgehensweise zur Kontrolle der Datenträgerverwaltung,
- — Vorgehensweise zur Kontrolle der Bestandsverzeichnisse;

2.3 für die Datenwiederherstellung:
- — Kommunikationswege zur beauftragenden Stelle,
- — Verantwortlichkeit für die Datenwiederherstellung,
- — Zugriffsrechte zur Datenübertragung auf das Speichersystem für den Regelbetrieb,
- — Zeitbedarf für die Datenwiederherstellung,
- — Konsistenzprüfung nach der Datenwiederherstellung,
- — Dokumentation der Datenwiederherstellung;

2.4 für die Übungen zur Datenwiederherstellung:
- — Ziele der Übung,
- — Rollen,
- — Vorgehensweise zur Durchführung,
- — Zeitintervalle,
- — Zeitbedarf,
- — Vorbereitung,
- — Dokumentation,
- — Nachbereitung.

Informationssicherheitsrichtlinie über die Nutzung des zentralen Internetzugangs und von Web-Angeboten (ISRL-Web-Nutzung)

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 23. 10. 2013 — CIO-02850/0110-0006 —

Bezug: Gem. RdErl. v. 12. 7. 2011 (Nds. MBl. S. 518), geändert durch Gem. RdErl. v. 23. 10. 2013 (Nds. MBl. S. 864) — VORIS 20500 —

1. Gegenstand und Geltungsbereich

Diese Informationssicherheitsrichtlinie über die Nutzung des zentralen Internetzugangs und von Web-Angeboten (ISRL-Web-Nutzung) regelt auf Grundlage der Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) — Bezugserlass — in Form von Mindestanforderungen die Grundsätze zur Nutzung des zentralen Internetzugangs des Landes und von Web-Angeboten.

Diese Informationssicherheitsrichtlinie gilt im gesamten Geltungsbereich der Leitlinie für die Gewährleistung der Informationssicherheit (Nummer 1.1 des Bezugserlasses).

2. Begriffsbestimmungen

Im Sinne dieser Informationssicherheitsrichtlinie

2.1 ermöglichen „Web-Angebote“ den Anwenderinnen und Anwendern die Informationsbeschaffung und die Tätigung von Online-Transaktionen über die weltweit bereitgestellten Web-Seiten im Internet und über die Web-Seiten der niedersächsischen Landesverwaltung und anderer deutscher Verwaltungen;

2.2 ist eine „vertrauenswürdige“ Web-Seite eine Datenquelle, bei der keine tatsächlichen Anhaltspunkte vorliegen, die der Vertrauenswürdigkeit entgegenstehen. Anhaltspunkte, die einer Vertrauenswürdigkeit entgegenstehen, können sich z. B. aus dem Namen, der Adresse, dem Kontext, in dem die Web-Seite genannt oder verlinkt ist, den erwarteten Inhalten, den erwarteten Verantwortlichkeiten, dem Herkunftsland oder der Top-Level-Domäne (z. B. „.to“, „.ru“) des Web-Angebots ergeben;

2.3 ist ein „vertrauenswürdiges“ Server-Zertifikat die Bestätigung einer Zertifizierungsstelle, bei der keine tatsächlichen Anhaltspunkte vorliegen, die der Vertrauenswürdigkeit entgegenstehen. Anhaltspunkte, die einer Vertrauenswürdigkeit entgegenstehen, können sich z. B. aus der Ungültigkeit des Zertifikats oder aus einer inhaltlichen Abweichung zwischen der Web-Adresse und dem Zertifikat ergeben;

2.4 ist das „Landesnetz“ das Weitverkehrsnetzwerk, das sich ausschließlich in der Funktionsherrschaft des Landes Niedersachsen befindet.

3. Organisatorische und technische Maßnahmen der Behördenleitung

Die Behördenleitung ist im Rahmen ihrer Zuständigkeit für die Gewährleistung der Informationssicherheit verantwortlich. Zur Umsetzung dieser Informationssicherheitsrichtlinie sind durch die Behördenleitung die notwendigen organisatorischen und technischen Maßnahmen zu veranlassen. Die Sicherheitsanforderungen können auch dadurch erfüllt werden, dass die Behördenleitung einen Dritten (z. B. IT-Dienstleister, Landesbetrieb) mit der Umsetzung von Maßnahmen beauftragt. Entsprechende Vereinbarungen oder Verträge mit dem Dritten sind aktenkundig zu machen.

Soweit sichergestellt ist, dass die durch diese Informationssicherheitsrichtlinie festgelegten Mindestanforderungen vollständig umgesetzt werden, ist die weitere Ausgestaltung der Maßnahmen in Art und Umfang freigestellt.

4. Umsetzung

4.1 Die Umsetzung der Sicherheitsanforderungen (Nummer 6) soll vorrangig durch technische Maßnahmen erfolgen, die durch organisatorische Maßnahmen ergänzt werden.

4.2 Bei der Gestaltung organisatorischer Maßnahmen, insbesondere bei der Erstellung von Dienstanweisungen, ist zu beachten, dass diese auch für Anwenderinnen und Anwender ohne vertiefte IT-Kenntnisse verständlich und tatsächlich umsetzbar sind.

4.3 Die spezifischen Sicherheitsmaßnahmen der einzelnen Sicherheitsdomänen müssen in einem angemessenen Verhältnis zur praktischen Handhabbarkeit durch die Anwenderinnen und Anwender stehen.

4.4 Die Verantwortungsbereiche der einzelnen Anwenderinnen und Anwender sind eindeutig vom Verantwortungsbereich der Systemadministration abzugrenzen.

4.5 Zur organisatorischen Umsetzung der Sicherheitsanforderungen (Nummer 6) wird der Erlass einer Dienstanweisung nach dem in der **Anlage** dargestellten Muster (Musterdienstanweisung) vorgeschlagen. Dieser Umsetzungsvorschlag beschränkt sich auf Sicherheitsanforderungen, die sich unmittelbar an die Anwenderinnen und Anwender richten. Es sind ggf. ergänzende oder zusätzliche Maßnahmen zu ergreifen, die die Umsetzung dieser Informationssicherheitsrichtlinie durch die Behördenleitung und die innerbehördlich zuständige Stelle sicherstellen.

5. Innerbehördliche Zuständigkeit und Organisation

Die Behördenleitung legt die innerbehördlichen Zuständigkeiten (zuständigen Stellen) und ggf. die erforderlichen Prozesse für die Umsetzung der technischen und organisatorischen Maßnahmen aufgrund dieser Informationssicherheitsrichtlinie in eigener Zuständigkeit fest.

6. Sicherheitsanforderungen

6.1 Grundsatz der Nutzung des zentralen Internetzugangs des Landes

6.1.1 Grundsätzlich ist für die Nutzung des Internets der zentrale Internetzugang des Landes zu nutzen. Über Ausnahmen bei Endgeräten, die nicht mit dem Landesnetz gekoppelt sind, entscheidet die Behördenleitung anhand einer Risikoanalyse. Diese Entscheidung ist aktenkundig zu machen.

6.1.2 Die Behördenleitung stellt sicher, dass zwischen den Endgeräten, die mit dem Landesnetz gekoppelt sind, und dem Internet keine direkte Kommunikationsverbindung hergestellt wird (sog. Fremdnetzanschluss). Besteht aus fachlichen Gründen der Bedarf für den Zugang zum Landesnetz und zu einem öffentlichen Netz, ohne dass eine direkte Kommunikationsverbindung zwischen diesen Netzen besteht, entscheidet die Behördenleitung darüber anhand einer Risikoanalyse. Diese Entscheidung ist aktenkundig zu machen.

6.2 Sicherheitsanforderungen an die Nutzung des zentralen Internetzugangs

6.2.1 Der zentrale Internetzugang des Landes darf grundsätzlich nur für den Zugriff auf Web-Angebote mit den Protokollen http (englisch: hypertext transfer protocol) und https (englisch: hypertext transfer protocol secure) über die dafür vorgesehene Sicherheitsinfrastruktur (z. B. Proxyserver) genutzt werden.

6.2.2 Besteht aus fachlichen Gründen der Bedarf, das Protokoll http oder https für einen von Nummer 6.2.1 abweichenden Zweck zu verwenden (z. B. Fernwartung), entscheidet die Behördenleitung darüber anhand einer Risikoanalyse. Diese Entscheidung ist aktenkundig zu machen.

6.2.3 Besteht aus fachlichen Gründen der Bedarf, den zentralen Internetzugang des Landes für ein von Nummer 6.2.1 abweichendes Kommunikationsprotokoll zu nutzen, so bedarf dessen Zulassung der vorherigen Zustimmung der oder des Informationssicherheitsbeauftragten der Landesverwaltung. Die Behördenleitung hat dazu eine Risikoanalyse vorzulegen und Sicherheitsmaßnahmen vorzuschlagen, mit denen die Risiken infolge dieser zusätzlichen Kommunikationsverbindung mit dem Landesnetz begrenzt werden.

6.3 Sicherheitsanforderungen an die Nutzung von Web-Angeboten

6.3.1 Die Behördenleitung legt fest, wer Web-Angebote für welche Zwecke nutzen darf, und veranlasst die Sensibilisierung der Anwenderinnen und Anwender für Bedrohungen der Informationssicherheit durch die Nutzung von Web-Angeboten.

6.3.2 Die Behördenleitung entscheidet, ob und in welchem Umfang der Aufruf von verbotenen oder dienstlich nicht relevanten Web-Seiten durch eine Filterung unterbunden werden soll.

6.3.3 Die Behördenleitung veranlasst, dass Web-Seiten — soweit technisch möglich (z. B. mittels Überprüfung der DNSSEC-Signatur) — auf ihre Vertrauenswürdigkeit hin automatisiert überprüft und bei negativem Prüfergebnis geblockt werden.

6.3.4 Die Anwenderin oder der Anwender nimmt in eigener Verantwortung die Prüfung der nicht geblockten Web-Seiten auf Vertrauenswürdigkeit vor. Die Prüfung erfolgt im Rahmen der jeweiligen Kenntnisse und Qualifikation mit der gebotenen Sorgfalt. Der Aufruf nicht vertrauenswürdiger Web-Seiten ist grundsätzlich durch die Behördenleitung zu untersagen. Stellt sich eine Web-Seite nach ihrem Aufruf als nicht vertrauenswürdig heraus, sind die Weiterverarbeitung dieser Informationen und das Herunterladen von Dateien nicht zulässig.

6.3.5 Die Behördenleitung regelt, wie mit der Warnmeldung des Web-Browsers zu vermeintlich nicht vertrauenswürdigen Zertifikaten von Web-Servern umzugehen ist, die sich beim Aufbau einer verschlüsselten Verbindung (z. B. bei der Nutzung des Protokolls https) mittels Zertifikat ausweisen.

6.4 Funktionale Sicherheitsanforderungen

6.4.1 Die Behördenleitung hat Regelungen anhand einer Risikoanalyse zu treffen, ob und in welchem Umfang bestimmte Kategorien von Inhalten (z. B. Werbebanner, aktive Inhalte, Cookies) von Web-Seiten aktiviert bleiben dürfen und inwieweit der Web-Browser eine ausdrückliche Bestätigung der Anwenderin oder des Anwenders vor der Ausführung anfordern soll. Das Ergebnis der Risikoanalyse ist aktenkundig zu machen.

6.4.2 Die Behördenleitung legt anhand einer Risikoanalyse fest, ob und in welchem Umfang bestimmte Dateien mit ausführbarem Programmcode von den Web-Seiten heruntergeladen werden dürfen und inwieweit der Web-Browser eine ausdrückliche Bestätigung der Anwenderin oder des Anwenders vor der Ausführung anfordern soll. Das Ergebnis der Risikoanalyse ist aktenkundig zu machen.

6.4.3 Die Behördenleitung trifft Regelungen, unter welchen Rahmenbedingungen das Hochladen von Dateien auf Web-Angebote zulässig ist.

6.4.4 Die Behördenleitung stellt sicher, dass die Anwenderinnen und Anwender ein verschlüsseltes Protokoll (z. B. https) für den Aufruf der Web-Seite — sofern verfügbar — nutzen, falls Authentisierungsdaten (z. B. Kennwörter) über das Internet übertragen werden müssen. Soweit Web-Angebote über das verschlüsselte Protokoll https erreichbar sind, sollen die Anwenderinnen und Anwender davon Gebrauch machen. Eine Speicherung von Authentisierungsdaten im Web-Browser soll vermieden werden.

7. Schlussbestimmung

Dieser Gem. RdErl. tritt am 1. 11. 2013 in Kraft.

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 868

Anlage

Musterdienstanweisung über die Nutzung der Web-Angebote

1. Gegenstand und Geltungsbereich

Diese Dienstanweisung regelt die Grundsätze der dienstlichen Nutzung von Web-Angeboten durch die Beschäftigten. Sie ergänzt die Dienstanweisung über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender in der jeweils geltenden Fassung.

Diese Dienstanweisung gilt für alle Beschäftigten der [Behörde].

2. Begriffsbestimmungen

Im Sinne dieser Dienstanweisung

2.1 ermöglichen „Web-Angebote“ den Anwenderinnen und Anwendern die Informationsbeschaffung und die Tätigung von Online-Transaktionen über die weltweit bereitgestellten Web-Seiten im Internet und über die Web-Seiten der niedersächsischen Landesverwaltung und anderer deutscher Verwaltungen;

2.2 ist ein „Web-Browser“ ein Computerprogramm, das lokal auf dem Endgerät einer Anwenderin oder eines Anwenders ausgeführt wird und das dem Aufruf von Web-Seiten sowie der Darstellung der ankommenden Daten als Text oder Bild am Bildschirm dient;

2.3 ist eine „Web-Seite“ ein HTML-Dokument, in das Dateien, Grafiken, Videos, Werbebanner etc. eingebunden sein können;

2.4 ist eine „vertrauenswürdige“ Web-Seite eine Datenquelle, bei der keine tatsächlichen Anhaltspunkte vorliegen, die der Vertrauenswürdigkeit entgegenstehen. Anhaltspunkte, die einer Vertrauenswürdigkeit entgegenstehen, können sich z. B. aus dem Namen, der Adresse, dem Kontext, in dem die Web-Seite genannt oder verlinkt ist, den erwarteten Inhalten, den erwarteten Verantwortlichkeiten, dem Herkunftsland oder der Endung der Web-Adresse (z. B. „.to“, „.ru“) des Web-Angebots ergeben; nicht ausgeschlossen ist, dass es auch beim Aufruf vertrauenswürdiger Web-Seiten zu einem Schadsoftwarebefall kommen kann;

2.5 ist eine „Web-Adresse“ die Adresse einer Web-Seite, bestehend aus einem Protokoll und einem Adresspfad (beispielsweise: http://www.bsi.bund.de); Web-Seiten werden über das Protokoll http (englisch: hypertext transfer protocol) oder das Protokoll https (englisch: hypertext transfer protocol secure) zum Web-Browser übermittelt; wird das Protokoll https genutzt, ist der gesamte Datentransfer verschlüsselt und der Web-Server hat sich durch ein Zertifikat ausgewiesen;

2.6 ist ein „Server-Zertifikat“ die Bestätigung einer Zertifizierungsstelle, mit der sich der Web-Server beim Aufbau einer verschlüsselten Verbindung über das Protokoll https dem Web-Browser gegenüber ausweist;

2.7 ist ein „vertrauenswürdiges“ Server-Zertifikat die Bestätigung einer Zertifizierungsstelle, bei der keine tatsächlichen Anhaltspunkte vorliegen, die der Vertrauenswürdigkeit entgegenstehen. Anhaltspunkte, die einer Vertrauenswürdigkeit entgegenstehen, können sich z. B. aus der Ungültigkeit des Zertifikats oder aus einer inhaltlichen Abweichung zwischen der Web-Adresse und dem Zertifikat ergeben; nicht ausgeschlossen ist, dass eine Warnmeldung des Web-Browsers ein vertrauenswürdiges Server-Zertifikat fälschlicherweise als nicht vertrauenswürdig einstuft;

2.8 sind „Cookies“ Daten über besuchte Web-Seiten, die der Web-Browser beim Seitenaufruf in der Regel ohne Aufforderung auf dem Endgerät speichert und beim erneuten Besuch der Web-Seite ausliest.

3. Eigenverantwortung

Die Beschäftigten sind selbst für die sichere und rechtmäßige Nutzung der Web-Angebote verantwortlich, soweit sie hierauf Einfluss nehmen können. Es sind die einschlägigen Gesetze sowie die im Verkehr erforderliche Sorgfalt zu beachten. Bei Fragen oder Problemen im Zusammenhang mit der Web-Nutzung steht die [zuständige Stelle] zur Verfügung.

4. Grundsätze der Web-Nutzung

Die Nutzung von Web-Angeboten ist eine in [Behörde] etablierte Form der Informationsbeschaffung. Die Regelungen zur Aktenführung gelten unverändert auch für Informationen und Dateien, die aus einer Web-Seite heruntergeladen und gespeichert wurden. Es ist das [im Dokument] festgelegte Dokumentenmanagementsystem [(z. B. Fabasoft eGov-Suite)] zu nutzen.

5. Nutzungsumfang

5.1 Die Web-Seiten dürfen ausschließlich für dienstliche Zwecke aufgerufen werden. [*alternativ:* Die private Web-Nutzung richtet sich nach der Dienstvereinbarung über ...]

5.2 Das Herunterladen von Dateien ist auf das dienstlich erforderliche Maß zu beschränken.

5.3 Der Aufruf nicht vertrauenswürdiger Web-Seiten ist grundsätzlich untersagt. In begründeten Einzelfällen kann eine abweichende Regelung getroffen werden. Stellt sich eine Web-Seite nach ihrem Aufruf als nicht vertrauenswürdig heraus, sind die Weiterverarbeitung dieser Informationen und das Herunterladen von Dateien nicht zulässig.

5.4 Wird ein Web-Seiten-Aufruf aufgrund einer automatisierten Filterung nicht ausgeführt, und ist der Aufruf der betroffenen Web-Seite für die Aufgabenerledigung zwingend erforderlich, so nimmt den Bedarf zur Freischaltung die [zuständige Stelle] entgegen.

6. Allgemeine Sorgfaltspflichten

6.1 Die Beschäftigten nehmen in eigener Verantwortung die Prüfung der Web-Seiten auf Vertrauenswürdigkeit i. S. der Nummer 2.4 vor. Die Prüfung erfolgt im Rahmen der jeweiligen Kenntnisse und Qualifikation mit der gebotenen Sorgfalt. [Die Beschäftigten sollen ein Werkzeug,, das der zentrale IT-Dienstleister des Landes in seinem Intranet unter dem Register „Leistungen“ bereitstellt, bei ihrer Entscheidung zurate ziehen.]

6.2 Die Warnmeldung des Web-Browsers bei einer verschlüsselten Verbindung (z. B. Protokoll https), dass für den Web-Server kein vertrauenswürdiges Server-Zertifikat benutzt wird, darf erst von den Beschäftigten als unbegründet ignoriert werden, wenn ihre Prüfung keine Anhaltspunkte erbracht hat, die einer Vertrauenswürdigkeit des Server-Zertifikats i. S. der Nummer 2.7 entgegenstehen. Die Prüfung erfolgt im Rahmen der jeweiligen Kenntnisse und Qualifikation mit der gebotenen Sorgfalt. [Die Beschäftigten sollen ein Werkzeug,, das der zentrale IT-Dienstleister des Landes in seinem Intranet unter dem Register „Leistungen“ bereitstellt, bei ihrer Entscheidung zurate ziehen.]

7. Nutzung des Web-Browsers

7.1 Der Aufforderung des Web-Browsers, dem Ausführen bestimmter Inhalte (z. B. Werbebanner, aktive Inhalte, Cookies) zuzustimmen, darf erst nach kritischer Prüfung der Vertrauenswürdigkeit der Web-Seite nachgekommen werden, um die Wahrscheinlichkeit für eine Infektion mit Schadsoftware zu reduzieren.

7.2 Datensammlungen im Web-Browser (z. B. Listen kürzlich aufgerufener Web-Seiten) sollen regelmäßig [gemäß Anleitung] gelöscht werden, damit diese nicht zur Erstellung von persönlichen Profilen missbraucht werden können.

7.3 Die vom Web-Browser in einem Puffer-Speicher (Browser-Cache) gesammelten Daten sollen regelmäßig [gemäß Anleitung] gelöscht werden, damit diese nicht rekonstruiert und an unberechtigte Dritte gelangen können.

7.4 Die vom Web-Browser gespeicherten Cookies sollen regelmäßig [gemäß Anleitung] gelöscht werden, damit das „Surfverhalten“ nicht auswertbar ist und das Recht auf informationelle Selbstbestimmung gewahrt bleibt.

7.5 Der Aufforderung des Web-Browsers, dem Speichern von Cookies zuzustimmen, soll erst nach sorgfältiger Prüfung der Notwendigkeit dieses Web-Seiten-Aufrufs nachgekommen werden.

7.6 Soweit Web-Angebote über das verschlüsselte Protokoll https erreichbar sind, haben die Anwenderinnen und Anwender davon Gebrauch zu machen.

7.7 Falls Authentisierungsdaten (z. B. Kennwörter) über das Internet übertragen werden müssen, hat der Aufruf der Web-Seite über das verschlüsselte Protokoll https — sofern verfügbar — zu erfolgen.

7.8 Eine Speicherung des Benutzernamens und des Kennworts im Web-Browser ist nicht zulässig.

8. Daten-Import und Daten-Export

8.1 Eine besonders sorgfältige Prüfung der Web-Seiten auf Vertrauenswürdigkeit gemäß Nummer 6.1 ist erforderlich, bevor

a) Dateien mit der Endung „.pdf“,

b) komprimierte Dateien (z. B. mit den Endungen „.zip“ und „.rar“),

c) Dateien, die Makros enthalten können (z. B. mit der Endung „.docx“), oder

d) Dateien unterschiedlicher Bilddateiformate (z. B. mit den Endungen „.bmp“, „.gif“, „.jpg“, „.jpeg“, „.png“ und „.tif“)

heruntergeladen werden.

8.2 Es dürfen grundsätzlich keine Dateien mit offensichtlich ausführbarem Programmcode von einer Web-Seite heruntergeladen werden. Dies trifft insbesondere auf Dateien mit den Endungen „.bat“, „.com“, „.exe“, „.scr“, „.vbs“ und „.wsh“ zu. Es gilt das Verbot zur Installation von Computerprogrammen gemäß Nummer 2.3 der Dienstanweisung über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender. In begründeten Einzelfällen kann eine abweichende Regelung getroffen werden.

8.3 Dateien mit offensichtlich ausführbarem Programmcode i. S. der Nummer 8.2 dürfen nicht auf Web-Seiten hochgeladen werden. Für das Hochladen sonstiger Dateien auf Web-Seiten kann in begründeten Fällen von der [zuständigen Stelle] eine Zustimmung erteilt werden, soweit Anforderungen an die Vertraulichkeit dem nicht entgegenstehen.

9. Ausnahmen

[Die zuständige Stelle] kann [im Einvernehmen mit der oder dem Informationssicherheitsbeauftragten] nach pflichtgemäßem Ermessen im Einzelfall Ausnahmen von den Regelungen dieser Dienstanweisung zulassen. Die Ausnahmen sind zu dokumentieren und durch Ersatzmaßnahmen abzusichern.

10. Inkrafttreten

Diese Dienstanweisung tritt am Tag nach ihrer Bekanntgabe in Kraft.

Informationssicherheitsrichtlinie über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender (ISRL-IT-Nutzung)

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 23. 10. 2013 — CIO-02850/0110-0001 —

Bezug: Gem. RdErl. v. 11. 6. 2013 (Nds. MBl. S. 480)

Der Bezugserlass wird mit Wirkung vom 1. 11. 2013 wie folgt geändert:

1. In Nummer 3.5 Satz 1 wird nach dem Wort „Anlage“ die Zahl „1“ eingefügt.
2. Nummer 5.6.1 wird wie folgt geändert:
   a) In Satz 2 wird der Klammerzusatz „(Individualvereinbarung oder Dienstvereinbarung)“ gestrichen.
   b) Es wird der folgende Satz angefügt:
   „Sofern die private Nutzung zugelassen werden soll, wird der Abschluss einer Dienstvereinbarung nach dem in der Anlage 2 dargestellten Muster (Musterdienstvereinbarung) vorgeschlagen.“
3. Die bisherige Anlage wird Anlage 1 und wie folgt geändert:
   Nummer 5.1 erhält folgende Fassung:
   „5.1 Verbot der privaten Nutzung von IT-Systemen [*alternativ:* Private Nutzung von IT-Systemen]
   Eine private Nutzung der IT-Systeme des Landes Niedersachsen durch die Anwenderinnen und Anwender ist untersagt. Dies gilt insbesondere auch für die private Nutzung von Web-Angeboten und des E-Mail-Dienstes. [*Alternativ:* Die private Nutzung der IT-Systeme des Landes Niedersachsen richtet sich nach der Dienstvereinbarung über die private Nutzung von dienstlichen IT-Systemen.]“.
4. Es wird die in der **Anlage** abgedruckte Anlage 2 angefügt.

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 870

Anlage

„Anlage 2

Musterdienstvereinbarung
über die private Nutzung von dienstlichen IT-Systemen

Zwischen der/dem [Behörde] (nachfolgend: [Kürzel])
und dem Personalrat der/des [Kürzel] (nachfolgend: Personalrat)
wird auf Grundlage von § 78 NPersVG die folgende Dienstvereinbarung über die private Nutzung von dienstlichen IT-Systemen abgeschlossen:

Präambel

Die Verhandlungspartner stimmen darin überein, dass in einer modernen Verwaltung die private Nutzung dienstlicher IT-Systeme in geringfügigem Umfang zugelassen werden kann. Dabei sind sich die Verhandlungspartner der Tatsache bewusst, dass die Dienststelle auch bei Zulassung der privaten Nutzung die Informationssicherheit und die Sicherheit der IT-Systeme gewährleisten muss und zu diesem Zweck technische Systeme betreibt, die dazu dienen, die Nutzung der IT-Systeme, gespeicherte Daten und Inhalte von Kommunikationsvorgängen zu analysieren.

1. Geltungsbereich und Zweckbestimmung

1.1 Diese Dienstvereinbarung regelt die Grundsätze für die private Nutzung von Web-Angeboten und des E-Mail-Dienstes [ggf. weitere Anwendungen einfügen] sowie für die damit möglicherweise verbundene Speicherung privater Dateien auf von [Kürzel] betriebenen IT-Systemen. Sie gilt für alle Beschäftigten.

1.2 Diese Dienstvereinbarung legt Nutzungsbedingungen für die dienstlichen IT-Systeme fest. Sie ermöglicht damit die informierte Einwilligung der Beschäftigten in die Bedingungen der privaten Nutzung. Sie lässt [ggf. vorhandene Regelungen (z. B. Dienstanweisung über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender) einfügen] unberührt.

2. Begriffsbestimmungen

2.1 Eine „dienstliche Nutzung“ von dienstlichen IT-Systemen liegt vor, wenn die Verwendung von IT-Systemen der Aufgabenerfüllung der oder des jeweiligen Beschäftigten dient.

2.2 „Geringfügig“ ist eine gelegentliche Nutzung von kurzer Dauer, die nur wenig Datenverkehr verursacht und wenig Speicherplatz in Anspruch nimmt. In diesem Sinne geringfügig sind beispielsweise:

— der Aufruf von Webseiten, um Öffnungszeiten, Telefonnummern, die aktuelle Verkehrslage oder allgemeine Informationen der Gewerkschaften und ihrer Spitzenorganisationen zu erfahren,
— das Versenden einer E-Mail, um sich zum Mittagessen zu verabreden oder mitzuteilen, dass man später als verabredet nach Hause kommt,
— das Lesen von per E-Mail übersandten Informationen der Gewerkschaften und ihrer Spitzenorganisationen und die Weiterleitung an andere Gewerkschaftsmitglieder in der Dienststelle und
— [sofern die private Nutzung weiterer Anwendungen zugelassen wird, bieten sich weitere Beispiele an].

Nicht in diesem Sinne geringfügig sind beispielsweise:

— die Nutzung von Internet-Telefonie und Streaming-Diensten,
— die Nutzung der dienstlichen E-Mail-Adresse für den Empfang von Newslettern mit Ausnahme der Newsletter der Gewerkschaften und deren Spitzenorganisationen und
— der Versand von E-Mails mit großen Dateianhängen [größer als X Megabyte], wie beispielsweise Videodateien.

2.3 „Inhalte des Kommunikationsvorgangs“ sind die bei einem Kommunikationsvorgang übermittelten Daten.

2.4 Eine „private Nutzung“ von dienstlichen IT-Systemen ist eine Verwendung von IT-Systemen, die nicht der Aufgabenerfüllung dient, sondern im Interesse der oder des jeweiligen Beschäftigten oder von Dritten erfolgt.

2.5 „Protokollierung“ ist die automatisierte Speicherung von Zustandsinformationen über den Betrieb und die Nutzung eines IT-Systems sowie über den Zugang zu einem IT-System.

2.6 „Verkehrsdaten“ sind Daten über Umstände der Kommunikation, wie die Teilnehmerinnen oder Teilnehmer und die Dauer eines Kommunikationsvorganges.

3. Zulässigkeit der Nutzung

3.1 Die private Nutzung von Web-Angeboten und des E-Mail-Dienstes [ggf. weitere Anwendungen einfügen] ist unter dem Vorbehalt des Widerrufs in geringfügigem Umfang zulässig,

— wenn die oder der jeweilige Beschäftigte zuvor seine Einwilligung in die Protokollierung von Verkehrsdaten, in die (automatisierte) Analyse der Inhalte von Kommunikationsvorgängen und in die (automatisierte) Analyse von gespeicherten Dateien (z. B. mittels Anti-Schadsoftware) gemäß dem A n h a n g erklärt hat und
— soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und
— soweit die private Nutzung nicht einer Nebentätigkeit dient, es sei denn, die private Nutzung wird zu diesem Zweck durch [zuständige Stelle] ausdrücklich genehmigt.

3.2 Funktionspostfächer dürfen nicht für die private Kommunikation genutzt werden.

3.3 Verlässt eine Beschäftigte oder ein Beschäftigter das [Kürzel], steht ihr oder ihm ihre oder seine dienstliche E-Mail-Adresse nicht mehr zur Verfügung. Gespeicherte E-Mails werden nach dem Ausscheiden der oder des Beschäftigten aus dem [Kürzel] gelöscht.

4. Eigenverantwortung

Die Beschäftigten sind selbst für den sicheren und rechtmäßigen Einsatz der dienstlichen IT-Systeme verantwortlich, soweit sie hierauf Einfluss nehmen können.

5. Verhaltensgrundsätze

5.1 Die Beschäftigten haben jede Nutzung dienstlicher IT-Systeme zu unterlassen, die erkennbar geeignet ist, den Interessen des [Kürzel] oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit der IT-Systeme zu beeinträchtigen, oder die gegen geltende Rechtsvorschriften [und die Dienstanweisung über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender] verstößt.

5.2 Die Beschäftigten nutzen den E-Mail-Dienst so, dass die Empfängerin oder der Empfänger erkennen kann, ob es sich um eine dienstliche oder private E-Mail handelt.

5.3 Die Beschäftigten nutzen dienstliche IT-Systeme insbesondere nicht, um gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßende Inhalte abzurufen, zu speichern oder zu verbreiten.

5.4 Unabhängig von der gesetzlichen Zulässigkeit ist es den Beschäftigten im Rahmen der privaten Nutzung dienstlicher IT-Systeme verboten, verfassungsfeindliche, rassistische, Gewalt verherrlichende oder pornografische Inhalte abzurufen, zu speichern oder zu verbreiten.

6. Information und Schulung der Beschäftigten

[Kürzel] sensibilisiert die Beschäftigten, die dienstliche IT-Systeme nutzen, für die damit verbundenen Gefahren für die Informationssicherheit durch geeignete Maßnahmen wie beispielsweise Handzettel, elektronische Rundschreiben oder Schulungen.

7. Sicherstellung der Erreichbarkeit

[Die folgenden Varianten können alternativ oder kumulativ verwandt werden.]

[Variante 1:]

Die Beschäftigten stellen sicher, dass Eingänge auch während ihrer Abwesenheit bearbeitet werden können, indem sie den Ordner „Posteingang“ für die jeweilige Vertretung freigeben.

[Variante 2:]

Bei vorhersehbarer Abwesenheit informieren die Beschäftigten die Absenderinnen und die Absender von E-Mails mittels des Abwesenheitsassistenten über [die voraussichtliche Dauer der Abwesenheit und] die Möglichkeiten, die Vertretung zu erreichen.

[Variante 3:]

Bei unvorhersehbarer Abwesenheit von mehr als [Zeitraum] lässt die oder der Vorgesetze durch [zuständige Stelle] während der Abwesenheit eingegangene E-Mails an die Vertretung weiterleiten und ggf. eine Abwesenheitsnachricht einrichten. Dies gilt nicht für die E-Mail-Postfächer der Mitglieder des Personalrates, der Gleichstellungsbeauftragten, der oder des Suchtbeauftragten oder von anderen Funktionsträgerinnen und Funktionsträgern, deren Tätigkeit ein vergleichbares Maß an Vertraulichkeit erfordert.

8. Protokollierung

8.1 Bei der Nutzung von Web-Angeboten werden protokolliert:

[Die Details richten sich nach der jeweiligen technischen Ausgestaltung in der Dienststelle oder ggf. nach einer Vereinbarung mit dem IT-Dienstleister. Typisch sind beispielsweise:

— Datum und Uhrzeit,
— IP- Adresse des verwendeten Endgerätes,
— aufgerufene Webseiten (URL bis zum ersten Parameter) und
— übertragene Datenmenge.]

8.2 Bei der Nutzung des E-Mail-Dienstes werden protokolliert:

[Die Details richten sich nach der jeweiligen technischen Ausgestaltung in der Dienststelle oder ggf. nach einer Vereinbarung mit dem IT-Dienstleister. Typisch sind beispielsweise:

— Datum und Uhrzeit,
— Absenderin oder Absender,
— Empfängerin oder Empfänger,
— Inhalt der Betreffzeile und
— Größe der E-Mail.]

8.3 [Bei der Nutzung von [Software/IT-System] werden protokolliert:

[Inhalte der Protokolldatei].]

9. Analyse von gespeicherten Daten und der Inhalte von Kommunikationsvorgängen

9.1 Auf IT-Systemen des [Kürzel] bzw. des [IT-Betrieb] gespeicherte Daten werden durch technische Maßnahmen (z. B. Einsatz einer Anti-Schadsoftware) zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme (automatisiert) analysiert.

9.2 Alle eingehenden E-Mails werden durch technische Maßnahmen (z. B. Einsatz einer Firewall, eines Spam-Filters und einer Anti-Schadsoftware) zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme (automatisiert) analysiert.

9.3 Die Inhalte von Kommunikationsvorgängen im Landesnetz und am Übergang zwischen dem Landesnetz und dem Internet werden zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme (automatisiert) analysiert.

10. Zweckbindung und Löschungsfrist

10.1 Eine Unterscheidung von dienstlicher und privater Nutzung ist auf technischem Weg nicht möglich. Die Protokollierung von Verkehrsdaten (Nummer 8), die (automatisierte) Untersuchung von gespeicherten Dateien (Nummer 9), die (automatisierte) Analyse der Inhalte von Kommunikationsvorgängen (Nummer 9) und die Kontrolle gemäß Nummer 11 dieser Dienstvereinbarung erstrecken sich auch auf die private Nutzung der IT-Systeme.

10.2 Diese Dienstvereinbarung erlaubt es nur, die Protokolldaten nach Nummer 8 und die Ergebnisse der automatisierten Analyse nach Nummer 9 ausschließlich zu Zwecken der Missbrauchskontrolle und Missbrauchsverfolgung nach Nummer 11 zu verwenden. Im Übrigen findet eine Verhaltens- oder Leistungskontrolle nicht statt. Die Verwendung der Daten zu anderen Zwecken bedarf einer eigenen Rechtsgrundlage.

10.3 Die Protokolldaten werden spätestens nach 180 Tagen automatisch gelöscht. Sofern ein Missbrauchsverdacht nach Nummer 11 dieser Dienstvereinbarung besteht, dürfen die erforderlichen Daten für den erforderlichen Zeitraum gespeichert werden.

11. Maßnahmen bei Missbrauchsverdacht

11.1 Bestehen zureichende tatsächliche Anhaltspunkte für eine missbräuchliche oder unerlaubte Nutzung der IT-Systeme durch eine Beschäftigte oder einen Beschäftigten kann [zuständige Stelle] Protokolldaten nach Nummer 8 dieser Dienstvereinbarung oder von der oder dem Beschäftigten gespeicherte Daten, insbesondere E-Mails, überprüfen. Die oder der Beschäftigte kann an der Überprüfung teilnehmen, ein Mitglied des Personalrates oder eine Rechtsanwältin oder einen Rechtsanwalt hinzuziehen.

11.2 Im Übrigen gelten die einschlägigen Regelungen des Disziplinar- bzw. Tarifrechts. Ein Verstoß gegen diese Dienstvereinbarung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

11.3 Ist aufgrund von nicht-personenbezogenen Analysen, insbesondere der Auswertung des Datenvolumens, eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung der IT-Systeme zu erkennen, so werden die Beschäftigten per E-Mail an die Regelungen dieser Dienstvereinbarung erinnert. Ergeben weitere nicht-personenbezogene Analysen keine Änderung des Nutzungsverhaltens in einem Zeitraum von einem Monat, der auf die Erinnerung nach Satz 1 folgt, werden die Protokolldaten der folgenden zwei Wochen durch die [zuständige Stelle] stichprobenartig personenbezogen ausgewertet. Absatz 1 ist entsprechend anzuwenden.

11.4 [Zuständige Stelle] behält sich vor, bei Verstößen gegen diese Dienstvereinbarung die private Nutzung dienstlicher IT-Systeme im Einzelfall zu untersagen.

12. Inkrafttreten

Diese Dienstvereinbarung tritt mit Ablauf des TT. MM. JJJJ in Kraft.

13. Kündigung dieser Dienstvereinbarung

Im Fall einer Kündigung dieser Dienstvereinbarung ist die private Nutzung von dienstlichen IT-Systemen bis zum Abschluss einer neuen Dienstvereinbarung untersagt.

.....
Datum, Unterschrift Behördenleitung

.....
Datum, Unterschrift Personalrat

Anhang

Erklärung zur privaten Nutzung dienstlicher IT-Systeme

.....
(Vorname, Nachname)

Ich habe die „Dienstvereinbarung über die private Nutzung von dienstlichen IT-Systemen“ zur Kenntnis genommen und möchte dienstliche IT-Systeme in dem nach der Dienstvereinbarung erlaubten Umfang zukünftig auch privat nutzen.

Mir ist bekannt, dass technisch nicht zwischen dienstlicher und privater Nutzung unterschieden wird. Ich bin daher damit einverstanden, dass

— die in Nummer 8 der Dienstvereinbarung genannten Daten protokolliert werden,
— die gemäß Nummer 9 der Dienstvereinbarung auf IT-Systemen der/des [Kürzel] bzw. des [IT-Betrieb] gespeicherten Daten durch technische Maßnahmen (z. B. Einsatz einer Anti-Schadsoftware) zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme analysiert werden,
— alle eingehenden E-Mails durch technische Maßnahmen (z. B. Einsatz einer Firewall, eines Spam-Filters und einer Anti-Schadsoftware) zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme analysiert werden, und
— die Inhalte von Kommunikationsvorgängen im Landesnetz und am Übergang zwischen dem Landesnetz und dem Internet automatisiert zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme analysiert werden.

Insoweit willige ich in einen Eingriff in das Fernmeldegeheimnis nach Artikel 10 Abs. 1 des Grundgesetzes für die Bundesrepublik Deutschland und § 88 Abs. 1 des Telekommunikationsgesetzes ein.

Ich habe Kenntnis von der Tatsache, dass

— Protokolldaten oder von mir gespeicherte Daten (insbesondere E-Mails) unter den Voraussetzungen der Nummer 11 der Dienstvereinbarung personenbezogen ausgewertet werden können,
— meine Vertreterin oder mein Vertreter und meine Vorgesetze oder mein Vorgesetzter zu Zwecken des Dienstbetriebes in mein E-Mail-Postfach Einsicht nehmen können und dabei möglicherweise von privaten E-Mails Kenntnis erlangen und

— die Vertraulichkeit, Verfügbarkeit und Integrität der auf dienstlichen IT-Systemen gespeicherten Informationen nur im Umfang der dienstlichen Erfordernisse gewährleistet wird und damit die Kenntnisnahme meiner Daten durch Dritte, der Ausfall von IT-Systemen oder die Veränderung von Daten nicht ausgeschlossen werden können.

.....
Datum, Unterschrift“.

Vereinbarung gemäß § 81 NPersVG über die Durchführung einer Personalstrukturanalyse (PSA) in der niedersächsischen Landesverwaltung

Bek. d. MI v. 1. 11. 2013 — 14.15-03008 —

1. Die LReg und die Spitzenorganisationen der Gewerkschaften haben eine Vereinbarung gemäß § 81 NPersVG über die Durchführung einer Personalstrukturanalyse (PSA) in der niedersächsischen Landesverwaltung abgeschlossen. Diese Vereinbarung vom 8./31. 10. 2013 wird in der **Anlage** bekannt gemacht.

2. Der Präsident des LT, der Präsident des LRH sowie der LfD haben ihr Einvernehmen gemäß § 81 Abs. 5 bis 7 NPersVG erklärt.

An die
Dienststellen der Landesverwaltung

— Nds. MBl. Nr. 44/2013 S. 873

Anlage

Vereinbarung gemäß § 81 NPersVG über die Durchführung einer Personalstrukturanalyse (PSA) in der niedersächsischen Landesverwaltung

Zwischen

der Niedersächsischen Landesregierung, vertreten durch das Niedersächsische Ministerium für Inneres und Sport, einerseits

und

dem Deutschen Gewerkschaftsbund — Bezirk Niedersachsen—Bremen—Sachsen-Anhalt —,

dem Niedersächsischen Beamtenbund und Tarifunion (NBB),

dem Niedersächsischen Richterbund — Bund der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte (NRB) —

andererseits

wird gemäß § 81 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) in der Fassung vom 22. 1. 2007 (Nds. GVBl. S. 11), zuletzt geändert durch Artikel 3 des Gesetzes vom 30. 6. 2011 (Nds. GVBl. S. 210), folgende Vereinbarung geschlossen:

Präambel

Als größter Arbeitgeber in Niedersachsen beschäftigt das Land im Jahr 2012 rund 200 000 Mitarbeiterinnen und Mitarbeiter. Diese erbringen gegenüber den Bürgerinnen und Bürgern sowie gegenüber den Unternehmen des Landes öffentliche Dienstleistungen auf hohem Niveau. Damit sind sie der wichtigste Garant für eine leistungsstarke und zukunftsfähige niedersächsische Landesverwaltung.

Die Landesverwaltung hat sich infolge der Verwaltungsmodernisierung als einem kontinuierlichen und sehr grundlegenden Reformprozess strukturell bereits stark verändert. Weitere substanzielle Veränderungen werden sich aufgrund des demografischen Wandels für die Landesverwaltung ergeben. Eine zahlenmäßig kleinere und durchschnittlich ältere Bevölkerung wird die öffentlichen Dienstleistungen künftig anders in Anspruch nehmen als bisher. Organisation und Aufgabenwahrnehmung der Landesverwaltung sind kontinuierlich hieran anzupassen. Parallel zur Bevölkerungsentwicklung werden auch in der Landesverwaltung durchschnittlich ältere Mitarbeiterinnen und Mitarbeiter tätig sein, die professionell auf diese Herausforderungen vorbereitet werden müssen.

Vor diesem Hintergrund hat die Landesregierung zunächst im August 2010 Eckpunkte für ein demografiesicheres und ressourcenbewusstes Personalmanagement in Niedersachsen beschlossen und ein ressortübergreifendes Projekt initiiert. Im Oktober 2012 hat die Landesregierung als Ergebnis dieses Projekts das Personalmanagementkonzept der niedersächsischen Landesverwaltung vorgelegt. Dieses Konzept umfasst u. a. die Themenbereiche Nachwuchsgewinnung, Führungskräftequalifizierung und Fortbildung, Vereinbarkeit von Beruf und Familie sowie Gesundheit am Arbeitsplatz.

Wichtige Grundlage für ein demografiesicheres Personalmanagement ist es, einen detaillierten Gesamtüberblick über die Alters- und Qualifikationsstruktur der Landesverwaltung zu erhalten. Zu diesem Zwecke soll periodisch eine systematische und EDV-basierte Personalstrukturanalyse durchgeführt und in einem Bericht veröffentlicht werden.

Mit der vorliegenden Vereinbarung wollen die Vertragspartner Rechtssicherheit für Mitarbeiterinnen und Mitarbeiter der niedersächsischen Landesverwaltung im Hinblick auf die für die Personalstrukturanalyse erforderliche Verarbeitung der Beschäftigtendaten schaffen. Beide Seiten sind sich einig, dass die durch die Personalstrukturanalyse gewonnenen Erkenntnisse notwendig sind, um die im Personalmanagementkonzept dargelegten Bausteine für ein demografiesicheres und ressourcenbewusstes Personalmanagement zielgerecht umsetzen zu können.

Im gemeinsamen Dialog möchten die Vertragspartner den Prozess zur Umsetzung des Personalmanagementkonzepts der niedersächsischen Landesverwaltung weiter begleiten. Sie werden dazu einen regelmäßigen, mindestens einmal jährlich stattfindenden Erfahrungsaustausch durchführen.

1. Regelungsgegenstand und Geltungsbereich

1.1 Für die Landesverwaltung wird eine Personalstrukturanalyse (PSA) durchgeführt.

1.2 Die Vereinbarung regelt die Datenverarbeitung, die Zulässigkeit von Auswertungen sowie die Rechte der Personalvertretungen.

Die Vereinbarung dient der ordnungsgemäßen Durchführung der PSA sowie auch als Schutzmaßnahme für die Beschäftigten, z. B. vor unbefugten Auswertungen.

1.3 Die Vereinbarung gilt für alle Dienststellen der niedersächsischen Landesverwaltung, die in die PSA einbezogen werden. Die Vereinbarung gilt auch für den Landtag, den Landesrechnungshof und den Landesbeauftragten für den Datenschutz, wenn der Präsident oder die Präsidentin, der Landesbeauftragte oder die Landesbeauftragte ihr Einvernehmen erklären.

2. Begriffsbestimmungen

2.1 Personalstrukturanalyse

Mit dem Begriff Personalstrukturanalyse (PSA) wird das Verfahren zur Ermittlung und Auswertung von Strukturdaten der Beschäftigten in der niedersächsischen Landesverwaltung bezeichnet. Bei ca. 200 000 Beschäftigten ist eine elektronische Datenverarbeitung notwendig.

2.2 Datenverarbeitung

Datenverarbeitung ist gemäß § 3 Abs. 2 Satz 1 NDSG das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. Personenbezogene Daten sind gemäß § 3 Abs. 1 NDSG Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen.

2.3 Datenstruktur

Für jeden Personalfall wird ein Datensatz erfasst, der in Datenfelder gegliedert ist. Feldname, Feldlänge und Datentyp (numerisch oder alphanumerisch) sind festgelegt. Die Datenfelder enthalten die konkreten Informationen (Daten im allgemeinen Sprachgebrauch, aus technischer Sicht Feldinhalte), die für die Analyse erforderlich sind.

3. Ziele und Grundsätze der Personalstrukturanalyse

3.1 Im Hinblick auf ein demografiesicheres und ressourcenbewusstes Personalmanagement in Niedersachsen sollen durch eine PSA Grundlagen für eine belastbare Personalplanung geliefert werden.

3.2 Dazu wird jährlich ein Bericht zur PSA mit Stichtag 30. 6. vorgelegt und fortgeschrieben. Dieser Personalstrukturbericht enthält Standardauswertungen bis zur Ebene der Kapitel. Zusätzliche ressortspezifische Auswertungen sind mit MI und dem jeweiligen Hauptpersonalrat, den Hauptrichterräten oder dem Hauptstaatsanwaltsrat abzustimmen.

3.3 Um den Erhebungsaufwand für die PSA zu minimieren sind vorhandene Datenbestände zu nutzen. Dieses sind das Bezügeverfahren KIDICAP PPay und perspektivisch das Personalmanagementverfahren (PMV).

4. Datenverarbeitung im Rahmen der PSA

4.1 In Anlehnung an die Datensatzstrukturen der Personalstandstatistik (PSS), die zum Stichtag 30. 6. jeden Jahres erhoben wird, werden in pseudonymisierter Form Datensätze durch die für die Auszahlung der Bezüge und Versorgung zuständige Landesbehörde aus KIDICAP exportiert und in der Landesstatistikbehörde ausgewertet.

4.2 Durch die Pseudonymisierung wird der Name der Beschäftigten oder des Beschäftigten durch die Personalnummer ersetzt, um die Identifizierung der Betroffenen oder des Betroffenen auszuschließen bzw. wesentlich zu erschweren.

4.3 Auswertungen, die Rückschlüsse auf einzelne Personen ermöglichen sollen, sind unzulässig.

4.4 Der Datenexport erfolgt monatlich, um zusätzlich zu den stichtagsbezogenen Bestandsdaten die monatlichen Veränderungen zu ermitteln.

4.5 Von der Landesstatistikbehörde werden die Daten in einer Datenbank für maximal 13 Monate gespeichert, um die letzten 12 Veränderungsläufe (d. h. den Abgleich des Bestandes mit dem Vormonat) ggf. wiederholen zu können. Im Anschluss daran werden sie unwiderruflich gelöscht.

5. Zugriffsrechte, Datenauswertung und -weitergabe;

Zugriff auf die Datenbank in der Landesstatistikbehörde haben nur die unmittelbar mit dieser Aufgabe betrauten Mitarbeiterinnen und Mitarbeiter. Die Bearbeitung erfolgt mithilfe der dort vorhandenen Standardprogramme (SAS-System). Die statistischen Ergebnisse werden in Tabellen zusammengefasst und den obersten Landesbehörden zu Zwecken der Planung übermittelt, auch soweit Tabellenfelder nur einen einzigen Fall ausweisen. Die gewerkschaftlichen Spitzenorganisationen werden über die Liste der Tabellen und ggf. erfolgte Änderungen zeitnah unterrichtet.

6. Datenschutz

Die Bestimmungen des Niedersächsischen Datenschutzgesetzes sowie die datenschutzrechtlichen Spezialnormen und des Niedersächsischen Statistikgesetzes sind einzuhalten.

Die Verarbeitung von personenbezogenen Daten ist so zu gestalten, dass sie Unbefugten nicht zur Kenntnis gelangen können.

7. Rechte der Personalvertretungen, der Richtervertretungen und der Staatsanwaltsvertretungen

Die Personalvertretungen, die Richtervertretungen und die Staatsanwaltsvertretungen haben nach Maßgabe des § 60 NPersVG, § 16 Abs. 2 sowie § 74 NRiG das Recht, zur Unterstützung ihrer Arbeit im Rahmen ihrer Zuständigkeit eigene Auswertungen in Abstimmung mit dem zuständigen Ressort über MI anzufordern.

8. Detailregelungen

Folgende A n l a g e zu dieser Regelung wird im Einzelnen vereinbart:

Datenstruktur der Personalstrukturanalyse vom 1. 12. 2012.

9. Schlussbestimmung

9.1 Die Vereinbarung tritt am 1. 11. 2013 in Kraft.

9.2 Bei Veränderungen am Verfahren sowie bei Änderungen der Anlage zur Datenstruktur werden die an der Vereinbarung beteiligten gewerkschaftlichen Spitzenorganisationen rechtzeitig vorher beteiligt. Einvernehmliche Änderungen der Vereinbarung einschließlich der Anlagen sind jederzeit möglich und werden als schriftliche Ergänzung hinzugefügt.

9.3 Die Vereinbarung kann mit einer Frist von drei Monaten zum Ende eines Kalenderjahres schriftlich gekündigt werden.

A n l a g e

(zur Vereinbarung gemäß § 81 NPersVG über die Durchführung einer Personalstrukturanalyse — PSA — in der niedersächsischen Landesverwaltung)

Datenstruktur der Personalstrukturanalyse (PSA)

Der Satzaufbau orientiert sich an der Datensatzbeschreibung des Statistischen Bundesamtes (DSB-PS010-2011) für die Personalstandstatistik.

Datenfeld	Feldname	Typ/Stelligkeit	Bemerkung	Quelle, EF-Nr. in Personalstandstatistik
1	PersonalID	Text (12)	Lfd. Nummer der oder des Beschäftigten	Text; aus EF 4
2 a	Berichtsstelle	Text (7)	Berichtsstellen-Nr.	Text; aus EF 3
2 b	Dienstort	Text (8)	Regionalschlüssel der Dienststelle	Text; aus EF 14
3	Geschlecht	Text (1)	Geschlecht (m, w)	Schlüsseltabelle; aus EF 7
4	GebJG	Text (4)	Geburtsjahrgang (z. B. 1965)	Text; aus EF 9
5	BeschUmfang	Text (1)	Beschäftigungsumfang	Schlüsseltabelle; aus EF 10
6	BeschDauer	Text (1)	Beschäftigungsdauer	Schlüsseltabelle; aus EF 11
7	BeschArt	Text (2)	Art des Beschäftigungsverhältnisses	Text; aus EF 12
8	Einstufung	Text (3)	Besoldungsgruppe/Entgeltgruppe (z. B. BesGr. A 12/EntgeltGr. 11)	Text; aus EF 13
9	EplKap	Text (4)	Einzelplan/Kapitel (z. B. 03 01)	Text; aus EF 16U1
10	ArbZeitIst	Text (4)	in Prozent (%)	Text; aus EF 21
11	ArbZeitSoll	Text (4)	in Stunden (z. B. 39,8)	Text; aus EF 47
12[1])	Unterbrechung	Text (2)		Schlüsseltabelle neu
13[1])	Unterbrechung — von	Datum		Freitext, aus KIDICAP
14[1])	Unterbrechung — bis	Datum		Freitext, aus KIDICAP
15[2])	Abgang	Text (2)	endgültiger Abgang	Schlüsseltabelle neu
16[3])	Zugang	Text (2)	Zugang	Schlüsseltabelle neu

[1]) Diese drei Felder können mehrfach aufgeführt werden (maximal für die zwölf zurückliegenden Monate). Der Schlüssel aus KIDICAP für Unterbrechungen wird durch die für die Auszahlung der Bezüge und Versorgung zuständige Landesbehörde exportiert und von der Landesstatistikbehörde umgesetzt.

[2]) Der Schlüssel für Abgänge aus KIDICAP wird durch die für die Auszahlung der Bezüge und Versorgung zuständige Landesbehörde exportiert und von der Landesstatistikbehörde umgesetzt.

[3]) Die Schlüsselvergabe für Zugänge erfolgt durch die Landesstatistikbehörde.

Zusammenarbeit von Staatsanwaltschaft und Polizei; Beschleunigung der Verfahrensabläufe insbesondere in sog. Umfangsverfahren

Gem. RdErl. d. MI u. d. MJ v. 8. 11. 2013 — 23.11-01447/5 —

— VORIS 21021 —

Bezug: a) Gem. RdErl. d. MJ u. d. MI v. 16. 9. 1996 (Nds. Rpfl. S. 262)
b) AV d. MJ v. 22. 11. 1976 (Nds. Rpfl. S. 250), zuletzt geändert durch AV v. 6. 3. 2012 (Nds. Rpfl. S. 199)
— VORIS 33300 00 00 00 003 —
c) Gem. RdErl. v. 23. 1. 2006 (Nds. MBl. S. 86, Nds. Rpfl. S. 118)
— VORIS 21021 —

1. Allgemeines, Begriffsbestimmung und -eingrenzung

Staatsanwaltschaft und Polizei werden regelmäßig mit umfangreichen, (rechtlich) schwierigen und mit hohem Ermittlungs- und Hauptverhandlungsaufwand behafteten Ermittlungsverfahren konfrontiert, insbesondere im Bereich der Wirtschafts-, Landwirtschafts-, Steuer- oder Zollkriminalität, der Korruptionsdelinquenz, des Betäubungsmittelhandels, der gewerbs- und bandenmäßigen Schleusung oder des Menschenhandels, des Bandendiebstahls oder der Cybercrime.

Aufgrund begrenzter personeller und finanzieller Ressourcen, aber auch der besonders zeit- und personalintensiven, über Länder- und Staatsgrenzen hinausgreifenden Ermittlungen in sog. Umfangsverfahren werden zur Zusammenarbeit von Staatsanwaltschaft und Polizei und zur Beschleunigung (der Abläufe) dieser Verfahren die nachstehenden Regelungen getroffen.

Umfangsverfahren i. S. dieses Gem. RdErl. sind Verfahren, die durch

— eine Vielzahl der zu verfolgenden Straftaten und/oder Tatverdächtigen,
— den Umfang der auszuwertenden Beweismittel sowie
— eine prognostizierte Ermittlungsdauer von mehr als sechs Monaten

gekennzeichnet sind und somit den für durchschnittliche Ermittlungsverfahren aufzuwendenden Einsatz an personellen und sachlichen Mitteln bei Polizei und Staatsanwaltschaft nicht unerheblich übersteigen.

Sie sind in der Regel der Organisierten Kriminalität und/oder den o. g. Kriminalitätsfeldern zuzuordnen und erfordern regelmäßig einen Bearbeitungsaufwand von mehr als sechs Monaten.

2. Handlungsrahmen

Die Strafverfolgungsbehörden sind dem Legalitätsprinzip (§ 152 Abs. 2, § 163 Abs. 1 StPO) verpflichtet, das ihnen zum einen gebietet, Strafverfolgung gleichmäßig zu betreiben (Willkürverbot, Artikel 3 Abs. 1 GG), ihnen zum anderen aber auch aufgibt, bei grundrechtsrelevanten Eingriffen in Rechte der betroffenen Bürgerin oder des betroffenen Bürgers das Verhältnismäßigkeitsprinzip zu beachten. Umgekehrt verpflichtet das GG — als Ausfluss von Rechtsstaats- und Sozialstaatsprinzip — den Staat zu effektiver Strafverfolgung.

Das Gebot effektiven Staatshandelns kann aber auch bedeuten, dass Prioritäten gesetzt und Schwerpunkte gebildet werden, wenn eine gleichmäßige Verfolgung aller Straftaten, für die ein Anfangsverdacht besteht, effektiv nicht gewährleistet werden kann. Eine solche Schwerpunktbildung ist in den §§ 154, 154 a, 430 StPO sowie in § 143 Abs. 4 GVG geregelt.

3. Beschleunigung der Verfahrensabläufe durch verfahrenssteuernde Absprachen, Strategieentwicklung und Konzeptionserstellung

3.1 Ziele

Mit dem Ziel einer effektiven Strafverfolgung unter Nutzung der vorhandenen Ressourcen haben Polizei und Staatsanwaltschaft

— frühzeitig einen wechselseitigen Austausch über das mögliche Entstehen eines Umfangsverfahrens herzustellen und das Vorliegen eines derartigen Falles festzustellen,
— Einvernehmen bezüglich der Übernahme eines solchen Verfahrens zu erzielen und
— über juristische und kriminalistische Auswertungs- und Analyseergebnisse eine Ermittlungskonzeption festzulegen, die insbesondere die einzusetzenden Personalressourcen, die wesentlichen Ermittlungsphasen und den Zeitrahmen bestimmt.

Dabei ist in allen Phasen des Verfahrens ein intensiver Informationsaustausch, der auch verfahrenssteuernde Absprachen beinhaltet, sicherzustellen.

Dieser Gem. RdErl. bezweckt eine planvolle und die Ressourcen schonende Steuerung des polizeilichen Personaleinsatzes sowie die Beschleunigung der Ermittlungen in Umfangsverfahren. Die Sachleitungsbefugnis der Staatsanwaltschaft im Strafverfahren (§ 152 Abs. 1 GVG, § 161 Abs. 1 Satz 2 StPO) bleibt hiervon unberührt. Sie wird insbesondere nicht durch die nach Nummer 3.2 herbeizuführende Verständigung eingeschränkt, von der die Staatsanwaltschaft abzuweichen berechtigt ist, wenn ihr dies sachlich geboten erscheint.

3.2 Verfahrensbeschreibung

Zur Zielerreichung und unter Beachtung des Legalitätsprinzips treffen Polizei und Staatsanwaltschaft folgende Maßnahmen oder verständigen sich über folgende Punkte:

— Die Polizei stellt Straftaten, Strafzusammenhänge und Täterbeziehungen sowie kriminalistische Bewertungen, insbesondere zum prognostizierbaren oder zu erwartenden Umfang und Schwerpunkt eines Verfahrens (Nummer 26 RiStBV — siehe Bezugs-AV zu b), möglichst in Form eines Analyseberichts oder einer vorläufigen Ermittlungskonzeption, dar und legt diesen oder diese frühzeitig der Staatsanwaltschaft zwecks Abstimmung der weiteren Verfahrensweise vor.
— Die Staatsanwaltschaft prüft zeitnah die Übernahme komplexer und überregionaler Ermittlungsverfahren mit unterschiedlichen staatsanwaltschaftlichen Zuständigkeiten und teilt ihre Entscheidung der Polizei mit.
— Die Polizei stellt die vorhandenen personellen und materiellen Ressourcen dar.
— Staatsanwaltschaft und Polizei bestimmen einen zeitlichen Rahmen für die Durchführung des Ermittlungsverfahrens und unterscheiden dabei nach verdeckter und offener Ermittlungsphase für die Bearbeitung, bis hin zur Anklageerhebung.
— Vor Aufnahme der Ermittlungen sind grundsätzlich von Polizei und Staatsanwaltschaft gemeinsam erarbeitete und abgestimmte Ermittlungskonzepte zu fertigen und regelmäßig und/oder anlassbezogen fortzuschreiben.
— Die Staatsanwaltschaft legt die sachbearbeitende Dezernentin oder den sachbearbeitenden Dezernenten einschließlich der Stellvertreterin oder des Stellvertreters fest und gibt die jeweiligen Erreichbarkeiten bekannt.
— Bei der Erledigung umfangreicher Ermittlungsverfahren prüft die Staatsanwaltschaft, ob von der Möglichkeit der Übertragung der staatsanwaltschaftlichen Zuständigkeit (§ 145 GVG) Gebrauch gemacht werden kann.
— Staatsanwaltschaft und Polizei treffen frühzeitig Absprachen bezüglich des Aktenaufbaus und legen die für die Täterermittlung zwingend erforderlichen Ermittlungshandlungen fest.
— Staatsanwaltschaft und Polizei treffen frühzeitige Absprachen zum Umfang der Sicherstellung und Beschlagnahme von Beweismitteln und der Auswertetiefe.
— Staatsanwaltschaft und Polizei prüfen sorgfältig die Notwendigkeit von personal- und kostenintensiven Ermittlungshandlungen zu Beginn der operativen Ermittlungsphase (Ermittlungstiefe) mit Blick auf weniger belastende Maßnahmen zur Stützung des Tatverdachts oder zur Bestimmung des Kreises der Tatverdächtigen.
— Staatsanwaltschaft und Polizei verständigen sich darüber, ob im Fall durchgeführter Telekommunikationsüberwachungsmaßnahmen von der Protokollierung solcher Telefongespräche abgesehen werden kann, die von vornherein erkennbar nicht dazu geeignet sind, den Tatvorwurf zu verifizieren.
— Die Staatsanwaltschaft trifft frühzeitig die Entscheidung zur gezielten Ermittlung von Teilkomplexen.

— Die Staatsanwaltschaft prüft eine Anwendung der §§ 154 und 154 a StPO unter Beachtung des § 430 StPO und des § 143 Abs. 4 GVG bereits während der laufenden Ermittlungen.

— Die Staatsanwaltschaft trifft frühzeitige Entscheidungen zu verfahrensbeschränkenden Maßnahmen (Abtrennungen, Abgaben und Einstellungen nach § 154 StPO wie z. B. Entscheidungen über den Umgang mit Randerkenntnissen).

— Die Polizei strebt an, dass die zur Bewältigung eines Umfangsverfahrens eingerichtete polizeiliche Besondere Aufbauorganisation (BAO) so lange mit angemessener Personalstärke bestehen bleibt, bis die staatsanwaltschaftlichen Ermittlungen weitestgehend abgeschlossen sind.

Alle angesprochenen Möglichkeiten zur frühzeitigen Strukturierung der Ermittlungen in Umfangsverfahren und Begrenzung des damit verbundenen Ermittlungsaufwands bedingen eine möglichst frühzeitige Abstimmung zwischen Staatsanwaltschaft und Polizei. Sie hat am Anfang, nicht erst am Ende der Ermittlungen zu stehen und sich auf alle verfahrensrelevanten Aspekte zu erstrekken. Dabei sollte nicht nur Einvernehmen darüber bestehen, innerhalb welcher Zeit die Ermittlungen nach Möglichkeit abgeschlossen werden sollen, sondern vor allem auch darüber, wie mit anfallenden, einem zügigen Verfahrensabschluss entgegenstehenden Gesichtspunkten oder Ermittlungsergebnissen umgegangen werden soll.

Wesentliche verfahrenssteuernde und ggf. -beschränkende Absprachen sowie Aussagen oder Entscheidungen zu relevanten Rahmenbedingungen sind in allen Phasen schriftlich festzulegen, jedoch nicht zu den Verfahrensakten zu nehmen.

4. Erfahrungsaustausch, Überprüfung der Zielerreichung

Die Behörden von Staatsanwaltschaft und Polizei überprüfen die Zielerreichung in ihrem Zuständigkeitsbereich und erörtern diese im Rahmen der regelmäßigen Zusammenkünfte auf allen staatsanwaltschaftlichen und polizeilichen Entscheidungsebenen (vgl. Bezugserlass zu a).

5. Schlussbestimmungen

Dieser Gem. RdErl. tritt am 1. 12. 2013 in Kraft und mit Ablauf des 31. 12. 2018 außer Kraft. Der Bezugserlass zu c tritt mit Ablauf des 30. 11. 2013 außer Kraft.

An die
Polizeibehörden und -dienststellen
Justizbehörden

— Nds. MBl. Nr. 44/2013 S. 875

Verleihung der Niedersächsischen Sportmedaille

Bek. d. MI v. 12. 11. 2013 — 64.3-11 219/1 (2013) —

Bezug: Beschl. d. LM v. 1. 8./18. 12. 1984 (Nds. MBl. 1985 S. 202)
— VORIS 11430 00 00 03 011 —

Der Herr Ministerpräsident hat am 14. 6. 2013 nachstehenden Persönlichkeiten und Vereinen die Niedersächsische Sportmedaille verliehen:

a) für hohe sportliche Leistungen:
Sandra Auffarth, Ganderkesee,
Bernd Jeffré, Barmissen,
Vico Merklein, Babenhausen-Langstadt,
Dimitri Peters, Hannover;

b) für Verdienste um die Förderung des Sports:
Bianca Grewe, Walsrode,
Brigitte Just, Wennigsen,
Benno Bögershausen, Cloppenburg,
Antonino Spatola, Wolfsburg;

c) für beispielgebenden Beitrag für die Weiterentwicklung der Sportangebote:
Turnverein Dinklage von 1904 e. V.,
BC Tigers Salzgitter e. V.,
TV Jahn Schneverdingen e. V.,
Turngemeinschaft Wiesmoor von 1930 e. V.

— Nds. MBl. Nr. 44/2013 S. 876

C. Finanzministerium

Lohnsteuerliche Behandlung von unentgeltlichen oder verbilligten Mahlzeiten der Arbeitnehmer ab Kalenderjahr 2014

RdErl. d. MF v. 12. 11. 2013 — S 2334-35-3332 —

Bezug: RdErl. v. 20. 12. 2012 (Nds. MBl. 2013 S. 32)

Mahlzeiten, die arbeitstäglich unentgeltlich oder verbilligt an die Arbeitnehmer abgegeben werden, sind mit dem anteiligen amtlichen Sachbezugswert nach der SvEV zu bewerten. Dies gilt ab 1. 1. 2014 gemäß § 8 Abs. 2 Satz 8 EStG auch für Mahlzeiten, die dem Arbeitnehmer während einer beruflich veranlassten Auswärtstätigkeit oder im Rahmen einer doppelten Haushaltsführung vom Arbeitgeber oder auf dessen Veranlassung von einem Dritten zur Verfügung gestellt werden, wenn der Preis der Mahlzeit 60 EUR nicht übersteigt. Die Sachbezugswerte ab Kalenderjahr 2014 sind — teilweise — durch die Sechste Verordnung zur Änderung der Sozialversicherungsentgeltverordnung vom 21. 10. 2013 (BGBl. I S. 3871) festgesetzt worden. Demzufolge beträgt der Wert für Mahlzeiten, die ab Kalenderjahr 2014 gewährt werden,

a) für ein Mittag- oder Abendessen 3,00 EUR,

b) für ein Frühstück 1,63 EUR.

Im Übrigen wird auf R 8.1 Abs. 7 und 8 LStR sowie auf das BMF-Schreiben zur Reform des steuerlichen Reisekostenrechts vom 30. 9. 2013 (BStBl I S. 1279) hingewiesen.

Dieser RdErl. ergeht im Einvernehmen mit dem Bundesministerium der Finanzen und den obersten Finanzbehörden der anderen Länder. Er entspricht dem BMF-Schreiben vom 12. 11. 2013 — IV C 5-S 2334/13/10002 —, das im BStBl I veröffentlicht wird.

An die
Oberfinanzdirektion Niedersachsen
Finanzämter

— Nds. MBl. Nr. 44/2013 S. 876

D. Ministerium für Soziales, Frauen, Familie, Gesundheit und Integration

Hilfe zur Erziehung in Vollzeitpflege; Festsetzung der monatlichen Pauschalbeträge (Pflegegeld)

RdErl. d. MS v. 1. 11. 2013 — 305.13–51 212 —

— VORIS 21130 00 00 07 017 —

Bezug: RdErl. d. MK v. 29. 3. 1996 (Nds. MBl. S. 593), zuletzt geändert durch RdErl. v. 1. 11. 2012 (Nds. MBl. S. 974)
— VORIS 21130 00 00 07 017 —

Die Anlage zum Bezugserlass erhält ab 1. 1. 2014 folgende Fassung:

„**Anlage**

Monatliche Pauschalbeträge bei Vollzeitpflege

	Altersstufe (Jahre)	Materielle Aufwendungen (EUR)	Kosten der Erziehung (EUR)	Gesamtbetrag (EUR)
I.	0 bis 5	504	235	739
II.	6 bis 11	584	235	819
III.	ab 12	671	235	906“.

An
die Region Hannover, Landkreise, kreisfreien Städte und kreisangehörigen Gemeinden
das Niedersächsische Landesamt für Soziales, Jugend und Familie

— Nds. MBl. Nr. 44/2013 S. 876

Richtlinie über die Gewährung von Zuwendungen zur Behebung der vom Hochwasser 2013 verursachten Schäden in Landkreisen, Städten und Gemeinden in Niedersachsen

RdErl. d. MS v. 19. 11. 2013 — 501.1 —

— VORIS 23400 —

1. Zuwendungszweck, Rechtsgrundlage

1.1 Das Land gewährt nach Maßgabe dieser Richtlinie und der VV-Gk zu § 44 LHO Zuwendungen für die Beseitigung von Hochwasserschäden für den Wiederaufbau der zerstörten Infrastruktur in den Gemeinden im Rahmen der zwischen dem Bund und den Ländern geschlossenen Verwaltungsvereinbarung „Aufbauhilfe“.

1.2 Ein Rechtsanspruch des Antragstellers auf Gewährung einer Zuwendung besteht nicht, vielmehr entscheidet die Bewilligungsstelle aufgrund ihres pflichtgemäßen Ermessens im Rahmen der verfügbaren Haushaltsmittel.

2. Gegenstand der Förderung

2.1 Gefördert werden Maßnahmen zur Beseitigung von hochwasserbedingten Schäden im Einzugsgebiet des Flussgebiets der Elbe einschließlich ihrer Nebenflüsse, die im Zeitraum vom 18. 5. 2013 bis zum 4. 7. 2013 entstanden sind. Darüber hinaus werden Schäden in den niedersächsischen Gebieten ersetzt, in denen Soforthilfen nach § 2 Abs. 2 Satz 2 des Aufbauhilfefonds-Errichtungsgesetzes (AufbhG) vom 15. 7. 2013 (BGBl. I S. 2401) geleistet wurden.

Unter hochwasserbedingte Schäden fallen Schäden durch Hochwasser sowie Schäden durch wild abfließendes Wasser, Sturzflut, aufsteigendes Grundwasser, überlaufende Regenwasser- und Mischkanalisation und die Folgen von Hangrutsch, soweit sie jeweils unmittelbar durch das Hochwasser verursacht sind. Berücksichtigt werden auch unmittelbare Schäden durch Einsatzkräfte und Einsatzfahrzeuge.

Nicht berücksichtigt werden Schäden, die wegen Verstoßes gegen Vorschriften zum Schutz vor Hochwassergefahren in festgesetzten oder vorläufig gesicherten Überschwemmungsgebieten eingetreten sind.

2.2 Es werden Maßnahmen in Landkreisen, Städten und Gemeinden in folgenden Bereichen gefördert:

2.2.1 Städtebauliche Infrastruktur, einschließlich der Wiederherstellung von historischen Innenstädten, Kultureinrichtungen, Denkmälern, das Stadtbild prägenden Gebäuden (soweit sie nicht aus dem kulturellen Hilfsprogramm des Beauftragten der Bundesregierung für Kultur und Medien gefördert werden). Zur städtebaulichen Infrastruktur gehören auch die administrative Infrastruktur und Erschließungsanlagen wie Straßen, Wege, Plätze und Brücken sowie Parkflächen und Grünanlagen.

2.2.2 Soziale Infrastruktur, wie Anlagen zur Kinderbetreuung, Schulen, Krankenhäuser, Alten- und Pflegeheime, Einrichtungen der Behindertenhilfe sowie der Grundversorgung dienende Freizeitinfrastruktur wie Sportstätten und Gemeinschaftseinrichtungen in Kleingartenanlagen.

2.2.3 Verkehrliche Infrastruktur einschließlich der unbeweglichen ÖPNV-Infrastruktureinrichtungen, soweit sie nicht der Förderung im Rahmen der Gemeinschaftsaufgabe „Verbesserung der regionalen Wirtschaftsstruktur“ unterliegt. Zur verkehrlichen Infrastruktur gehören auch außerörtliche überwiegend öffentliche Straßen und Wege sowie Brücken.

2.2.4 Im Rahmen der Schadensbeseitigung können in begründeten Fällen auch Maßnahmen der Modernisierung gefördert werden, soweit hierfür eine Rechtspflicht besteht oder sie zwingend erforderlich sind.

2.2.5 Förderfähig sind auch Maßnahmen zur Beseitigung von hochwasserbedingten Schäden an Gebäuden und Einrichtungen in nicht kommunaler Trägerschaft, die zur Infrastruktur i. S. der Nummern 2.2.1 bis 2.2.4 gehören.

2.3 Die Kumulierung von Mitteln aus der Verwaltungsvereinbarung „Aufbauhilfe“ mit Mitteln aus anderen Förderprogrammen ist zulässig. Eine mehrfache Geltendmachung desselben Schadens in verschiedenen Programmen, die mit Mitteln des AufbhG finanziert werden, sowie eine Überkompensation sind unzulässig.

2.4 Eine früher gewährte Förderung für dasselbe Objekt mit Mitteln aus öffentlichen Haushalten schließt eine nochmalige Förderung von Maßnahmen im Rahmen dieses Programms nicht aus.

2.5 Nicht förderfähig sind

2.5.1 Maßnahmen, deren Kosten der Bund zu tragen hat,

2.5.2 Maßnahmen, deren Kosten das Land zu tragen hat.

3. Zuwendungsempfänger

Zuwendungsempfänger sind Landkreise, Städte und Gemeinden. Sie können die Zuwendung im Rahmen der VV-Gk Nr. 12 zu § 44 LHO als Erstempfänger an einen Letztempfänger weiterleiten. Letztempfänger sind andere als kommunale Träger von Einrichtungen i. S. der Nummern 2.2.1 bis 2.2.4.

4. Zuwendungsvoraussetzungen

4.1 Die Höhe der Hochwasserschäden an der Infrastruktur in den Hochwassergebieten ist von den betroffenen Gemeinden auf Basis einer Kostenschätzung oder -berechnung und unter Beifügung einer Karte des Überschwemmungsgebietes bei der Bewilligungsstelle anzumelden.

4.2 Versicherungsleistungen sind ebenso wie zweckgebundene Spenden oder sonstige Leistungen Dritter auf die Förderung anzurechnen. In den Fällen, in denen Versicherungsschutz besteht oder zweckgebundene Spenden oder sonstige Leistungen Dritter zu erwarten sind, kann die Höhe der Förderung zunächst auch ohne Berücksichtigung solcher späteren Leistungen vorläufig festgesetzt werden. Dabei sind bereits erfolgte Abschlagszahlungen zu berücksichtigen. Nach abschließender Regulierung des Schadens durch die Versicherung erfolgt die endgültige Festsetzung der Förderhöhe unter Berücksichtigung der Versicherungsleistungen durch einen Schlussbescheid. Gleiches gilt für die Berücksichtigung zweckgebundener Spenden oder sonstiger Leistungen Dritter.

Bewilligungen, die im Hinblick auf spätere Versicherungsleistungen zunächst nur vorläufig erfolgen, sind nur unter der Voraussetzung möglich, dass der Zuwendungsempfänger seine Versicherungsansprüche bis zur Höhe der Förderung an das Land abtritt. Die abschließende Festsetzung der Förderhöhe erfolgt nach Maßgabe des Satzes 1.

5. Art und Umfang, Höhe der Zuwendung

5.1 Die Zuwendung wird als nicht rückzahlbarer Zuschuss im Rahmen der Projektförderung als Vollfinanzierung bis zu 100 % gewährt.

5.2 Förderfähig sind Ausgaben für

5.2.1 vorbereitende Arbeiten,

5.2.2 Leistungen von Beauftragten für die Vorbereitung und Durchführung der Maßnahmen,

5.2.3 den Abriss,

5.2.4 den Ersatzbau, auch für den Ersatzneubau an anderer Stelle bis zur Höhe des tatsächlich entstandenen Schadens,

5.2.5 wesentliche funktionsbezogene Einrichtungsgegenstände.

5.3 Bei den Modernisierungsmaßnahmen gemäß Nummer 2.2.4 werden nur die unrentierlichen Ausgaben gefördert.

6. Anweisungen zum Verfahren

6.1 Für die Bewilligung, Auszahlung und Abrechnung der Zuwendung sowie für den Nachweis und die Prüfung der Verwendung und die ggf. erforderliche Aufhebung des Zuwendungsbescheides und die Rückforderung der gewährten Zuwendung gelten die VV-Gk zu § 44 LHO, soweit nicht in dieser Richtlinie abweichende Regelungen getroffen sind.

6.2 Zuständige Bewilligungsstelle ist die Investitions- und Förderbank Niedersachsen (NBank), Günther-Wagner-Allee 12—16, 30177 Hannover.

6.3 Der Antrag auf Gewährung einer Zuwendung ist bei der Bewilligungsstelle schriftlich zu stellen. Hierbei ist der von der NBank bereit gehaltene Vordruck zu verwenden.

6.4 Sofern Zuwendungen an Dritte nach Nummer 3 weitergeleitet werden, stellt der Erstempfänger den Antrag auf Förderung auf der Grundlage der Anträge der Letztempfänger. Der Erstempfänger bestätigt das Vorliegen der Fördervoraussetzungen.

6.5 Anträge sind spätestens bis zum 30. 6. 2015 bei der NBank zu stellen.

6.6 Die Auszahlung der Fördermittel erfolgt nach Abrechnung der Maßnahme. Bei Abrechnung einzelner Bauabschnitte wird die Auszahlung von Fördermitteln hierfür zugelassen.

6.7 Für die Gewährung von Zuwendungen nach dieser Richtlinie gilt eine Ausnahme vom Verbot des vorzeitigen Maßnahmebeginns. Frühester Maßnahmebeginn ist der 18. 5. 2013.

7. Schlussbestimmungen

Dieser RdErl. tritt mit Wirkung vom 18. 5. 2013 in Kraft und mit Ablauf des 31. 12. 2015 außer Kraft.

An die
Städte, Landkreise und Gemeinden in den betroffenen Gebieten
Investitions- und Förderbank Niedersachsen (NBank)

— Nds. MBl. Nr. 44/2013 S. 877

H. Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz

Tierschutz; Anforderungen an die Straußenhaltung

RdErl. d. ML v. 1. 10. 2013 — 204.1-42507/86-12 —

— VORIS 78530 —

Bezug: RdErl. v. 12. 11. 2008 (Nds. MBl. S. 1228)
— VORIS 78530 —

Der Bezugserlass wird mit Wirkung vom 1. 12. 2013 wie folgt geändert:

In Nummer 2 Satz 1 wird das Datum „31. 12. 2013“ durch das Datum „31. 12. 2015“ ersetzt.

An
die Region Hannover, Landkreise, kreisfreien Städte
den Zweckverband Jade-Weser

Nachrichtlich:
An
die Arbeitsgemeinschaft der kommunalen Spitzenverbände
das Niedersächsische Landesamt für Verbraucherschutz und Lebensmittelsicherheit

— Nds. MBl. Nr. 44/2013 S. 878

K. Ministerium für Umwelt, Energie und Klimaschutz

Einführung des Programms Abwasserkataster Niedersachsen: Erfassung, Auswertung und Weiterleitung der Daten aus der behördlichen Einleiterüberwachung

RdErl. d. MU v. 18. 11. 2013 — 22-62415/11 —

— VORIS 28200 —

Bezug: RdErl. v. 11. 1. 2006 (Nds. MBl. S. 93)
— VORIS 28200 —

Nummer 3 des Bezugserlasses wird mit Wirkung vom 1. 12. 2013 wie folgt geändert:

Die Angabe „1. Februar“ wird durch die Angabe „1. April“ ersetzt.

An die
Dienststellen der Wasserwirtschaftsverwaltung
unteren Wasserbehörden
staatlich anerkannten Untersuchungsstellen

— Nds. MBl. Nr. 44/2013 S. 878

Landesamt für Bergbau, Energie und Geologie

Feststellung gemäß § 3 c UVPG (RWE Dea AG, Hamburg)

Bek. d. LBEG v. 30. 10. 2013
— L1.4/L67007/03-08 02/2013-0017 —

Die Firma RWE Dea AG, Überseering 40, 22297 Hamburg, plant in der Gemeinde Kirchlinteln, Ortsteil Odeweg, im Land Niedersachsen, den Bau einer Nassgasleitung zwischen der Bohrung Weißenmoor Z 2 und der GTA Weißenmoor Z 1. Die DN 150 Duplex-Stahl-Leitung mit Kunststoffummantelung wird eine Länge von 1 100 m haben.

Die geplante Leitung befindet sich nordöstlich der Ortschaft Odeweg in der Gemeinde Kirchlinteln, Landkreis Verden, im Land Niedersachsen.

Aufgrund der Dimensionierung fällt die Rohrleitung unter die Vorprüfungspflicht UVPG. Es war eine standortbezogene Vorprüfung erforderlich.

Im Rahmen des Genehmigungsverfahrens war gemäß § 3 c i. V. m. Nummer 19.3.3 der Anlage 1 UVPG in der derzeit geltenden Fassung durch eine Vorprüfung des Einzelfalles zu ermitteln, ob für das beantragte Vorhaben die Durchführung einer Umweltverträglichkeitsprüfung erforderlich ist.

Diese nach den Vorgaben der Anlage 2 UVPG vorgenommene standortbezogene Vorprüfung des Einzelfalles hat ergeben, dass eine Umweltverträglichkeitsprüfung für das o. g. Vorhaben nicht erforderlich ist.

Diese Feststellung wird hiermit öffentlich bekannt gemacht. Sie ist nach § 3 a UVPG nicht selbständig anfechtbar.

— Nds. MBl. Nr. 44/2013 S. 878

Landesamt für Geoinformation und Landentwicklung Niedersachsen

Feststellung gemäß § 6 NUVPG (Vereinfachte Flurbereinigung Dellien, Landkreis Lüneburg)

Bek. d. LGLN v. 14. 11. 2013 — GB 3-33-611-1937-Dellien —

Die Regionaldirektion Lüneburg des LGLN hat dem Geschäftsbereich 3 des LGLN die 2. Änderung zum Wege- und Gewässerplan mit landschaftspflegerischem Begleitplan nach § 41 FlurbG für das vereinfachte Flurbereinigungsverfahren Dellien, Landkreis Lüneburg, vorgelegt. Auf der Grundlage des geänderten Wege- und Gewässerplans mit landschaftspflegerischem Begleitplan erfolgt der Ausbau der gemeinschaftlichen und öffentlichen Anlagen.

Auf der Grundlage der 2. Änderung des Wege- und Gewässerplans mit landschaftspflegerischem Begleitplan ist gemäß § 6 NUVPG nach einer allgemeinen Vorprüfung des Einzelfalles gemäß § 5 NUVPG festzustellen, ob für diese Änderung des Vorhabens — Bau der gemeinschaftlichen und öffentlichen Anlagen i. S. des FlurbG — eine Umweltverträglichkeitsprüfung durchzuführen ist.

Diese allgemeine Vorprüfung hat für das vereinfachte Flurbereinigungsverfahren Dellien ergeben, dass von dieser Änderung des Vorhabens keine erheblichen nachteiligen Umweltauswirkungen zu erwarten sind.

Gemäß § 6 NUVPG wird hiermit festgestellt, dass für diese Änderung des Vorhabens keine Verpflichtung zur Durchführung einer Umweltverträglichkeitsprüfung besteht.

— Nds. MBl. Nr. 44/2013 S. 879

Landeswahlleiterin

Verzeichnis der Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Wahlperiode des 17. Niedersächsischen Landtages

Bek. d. Landeswahlleiterin v. 8. 11. 2013 — LWL 11411/2.3.7 —

Bezug: Bek. v. 8. 8. 2012 (Nds. MBl. S. 147), zuletzt geändert durch Bek. v. 3. 1. 2013 (Nds. MBl. S. 39)

Die Nummern 1 bis 3 des Verzeichnisses der Bezugsbekanntmachung erhalten folgende Fassung:

Wahlkreis Nr.	Name	Kreiswahlleiterin/ Kreiswahlleiter	Stellvertreterin/ Stellvertreter	Dienststelle der Wahlleiterin/ des Wahlleiters a = Telefon b = Telefax c = E-Mail
„1 2 3	Braunschweig-Nord Braunschweig-Süd Braunschweig-West	Stadtrat Ruppert	Baudirektor Klein	38100 Braunschweig Reichsstraße 3 a: 0531 470-1 b: 0531 470-4141, -944101 c: wahlen@braunschweig.de“.

— Nds. MBl. Nr. 44/2013 S. 879

Verzeichnis der Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Wahlperiode des 18. Deutschen Bundestages

Bek. d. Landeswahlleiterin v. 8. 11. 2013 — LWL-11401/2.2.9 —

Bezug: Bek. v. 22. 6. 2012 (Nds. MBl. S. 502), zuletzt geändert durch Bek. v. 24. 4. 2013 (Nds. MBl. S. 332)

Die Nummer 50 des Verzeichnisses der Bezugsbekanntmachung erhält folgende Fassung:

Wahlkreis Nr.	Name	Kreiswahlleiterin oder Kreiswahlleiter	Stellvertreterin oder Stellvertreter	Dienststelle der Wahlleiterin oder des Wahlleiters a = Telefon b = Telefax c = E-Mail
„50	Braunschweig	Stadtrat Ruppert	Baudirektor Klein	Stadt Braunschweig Reichsstraße 3 38100 Braunschweig a: 0531 470-1 b: 0531 470-94 4101, -4141 c: wahlen@braunschweig.de“.

— Nds. MBl. Nr. 44/2013 S. 879

Verzeichnis der Stadtwahlleiterinnen, Stadtwahlleiter, Kreiswahlleiterinnen und Kreiswahlleiter sowie ihrer Stellvertretungen für die Europawahl 2014

Bek. d. Landeswahlleiterin v. 8. 11. 2013 — LWL 11431/2.8 —

Bezug: Bek. v. 16. 8. 2013 (Nds. MBl. S. 603)

Im Verzeichnis der Bezugsbekanntmachung erhalten die Stadt Braunschweig, der Landkreis Osterholz und die Stadt Osnabrück folgende Fassung:

Kreisfreie Stadt (St) Landkreis (LK)	Stadtwahlleiterin/ Stadtwahlleiter Kreiswahlleiterin/ Kreiswahlleiter	Stellvertreterin oder Stellvertreter	Dienststelle der Wahlleiterin oder des Wahlleiters a = Telefon b = Telefax c = E-Mail
„St Braunschweig	Stadtrat Ruppert	Baudirektor Klein	38100 Braunschweig Reichsstraße 3 a: 0531 470-1 b: 0531 470-4141, c: wahlen@braunschweig.de
LK Osterholz	Landrat Lütjen	Erste Kreisrätin Schumacher	27711 Osterholz-Scharmbeck Osterholzer Straße 23 a: 04791 930-0 b: 04791 930-358 c: wahl@landkreis-osterholz.de
St Osnabrück	Oberbürgermeister Griesert	Stadträtin Rzyski	49076 Osnabrück Natruper-Tor-Wall 5 a: 0541 323-3063 b: 0541 323-4361 c: wahlen@osnabrueck.de“.

— Nds. MBl. Nr. 44/2013 S. 880

Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz

**Veröffentlichung gemäß § 83 WHG;
Anhörungsdokumente zu den wichtigen Fragen der Gewässerbewirtschaftung für die Flussgebietseinheiten Elbe, Weser, Ems und Rhein (niedersächsischer Anteil)**

Bek. d. NLWKN v. 8. 11. 2013 — L34.62004-2.11 —

Hiermit werden die Anhörungsdokumente zu den wichtigen Fragen der Gewässerbewirtschaftung für die Flussgebietseinheiten

— Elbe,

— Weser,

— Ems und

— Rhein (niedersächsischer Anteil)

gemäß § 83 Abs. 4 Satz 1 Nr. 2 WHG vom 31. 7. 2009 (BGBl. I S. 2585), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. 4. 2013 (BGBl. I S. 734), bekannt gemacht.

Die Anhörungsdokumente sind im Internetangebot des NLWKN unter www.nlwkn.niedersachsen.de veröffentlicht und liegen in der Zeit vom 22. 12. 2013 bis zum 22. 6. 2014 bei der Direktion des NLWKN und den nachfolgend genannten NLWKN-Betriebsstellen während der Dienststunden (montags bis donnerstags von 8.00 bis 16.30 Uhr, freitags von 8.00 bis 12.30 Uhr) zur Einsichtnahme und zur Stellungnahme aus.

Flusseinzugsgebiete Elbe

NLWKN — Direktion:	Am Sportplatz 23, 26506 Norden,
NLWKN — Betriebsstelle Lüneburg:	Adolph-Kolping-Straße 6 21337 Lüneburg,
NLWKN — Betriebsstelle Stade:	Harsefelder Straße 2, 21680 Stade,
NLWKN — Betriebsstelle Süd:	Standort Braunschweig: Rudolf-Steiner-Straße 5, 38120 Braunschweig, Standort Göttingen: Alfa-Myrdal-Weg 2, 37085 Göttingen,
NLWKN — Betriebsstelle Verden:	Bürgermeister- Münchmeyer-Straße 6, 27283 Verden.

Flusseinzugsgebiet der Weser

NLWKN — Direktion:	Am Sportplatz 23, 26506 Norden,
NLWKN — Betriebsstelle Aurich:	Oldersumer Straße 48, 26603 Aurich,
NLWKN — Betriebsstelle Brake-Oldenburg:	Standort Brake: Heinestraße 1, 26919 Brake, Standort Oldenburg: Ratsherr-Schulze- Straße 10, 26122 Oldenburg,
NLWKN — Betriebsstelle Cloppenburg:	Drüdingstraße 25, 49661 Cloppenburg,
NLWKN — Betriebsstelle Hannover-Hildesheim:	Standort Hannover: Göttinger Chaussee 76 A, 30453 Hannover, Standort Hildesheim: An der Scharlake 39, 31135 Hildesheim,

NLWKN — Betriebsstelle Lüneburg:	Adolph-Kolping-Straße 6, 21337 Lüneburg,
NLWKN — Betriebsstelle Stade:	Harsefelder Straße 2, 21680 Stade,
NLWKN — Betriebsstelle Sulingen:	Am Bahnhof 1, 27232 Sulingen,
NLWKN — Betriebsstelle Süd:	Standort Braunschweig: Rudolf-Steiner-Straße 5, 38120 Braunschweig,
	Standort Göttingen: Alfa-Myrdal-Weg 2, 37085 Göttingen,
NLWKN — Betriebsstelle Verden:	Bürgermeister-Münchmeyer-Straße 6, 27283 Verden.

Flusseinzugsgebiet der Ems

NLWKN — Direktion:	Am Sportplatz 23, 26506 Norden,
NLWKN — Betriebsstelle Aurich:	Oldersumer Straße 48, 26603 Aurich,
NLWKN — Betriebsstelle Brake-Oldenburg:	Standort Brake: Heinestraße 1, 26919 Brake,
	Standort Oldenburg: Ratsherr-Schulze-Straße 10, 26122 Oldenburg,
NLWKN — Betriebsstelle Cloppenburg:	Drüdingstraße 25, 49661 Cloppenburg,
NLWKN — Betriebsstelle Meppen:	Haselünner Straße 78, 49716 Meppen.

Flusseinzugsgebiet des Rheins

NLWKN — Direktion:	Am Sportplatz 23, 26506 Norden,
NLWKN — Betriebsstelle Meppen:	Haselünner Straße 78, 49716 Meppen.

Stellungnahmen können auch vom 22. 12. 2013 bis zum 22. 6. 2014 auf dem Postweg an den Niedersächsischen Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz, Direktion GB III, Am Sportplatz 23, 26506 Norden, oder per E-Mail an poststelle@nlwkn-nor.niedersachsen.de geschickt werden.

— Nds. MBl. Nr. 44/2013 S. 880

Vorläufige Sicherung des Überschwemmungsgebietes der Großen Hase, des Essener Kanals und der Überfallhase von der Einmündung des Hahnenmoorkanals (Fluss-km 47 + 500) bis zum Schützenhofwehr Quakenbrück (Fluss-km 79 + 200) in den Landkreisen Osnabrück, Cloppenburg und Emsland

Bek. d. NLWKN v. 27. 11. 2013 — 62023/206,138,523/13 —

Der NLWKN hat den Bereich der Landkreise Osnabrück, Cloppenburg und Emsland, der von einem hundertjährlichen Hochwasser der Großen Hase, des Essener Kanals und der Überfallhase überschwemmt wird, ermittelt und in Arbeitskarten dargestellt.

Die Arbeitskarten werden hiermit öffentlich bekannt gemacht. Das Überschwemmungsgebiet gilt ab dem Tag nach dieser Bek. nach § 115 Abs. 5 NWG vom 19. 2. 2010 (Nds. GVBl. S. 64), zuletzt geändert durch § 87 Abs. 3 des Gesetzes vom 3. 4. 2012 (Nds. GVBl. S. 46), bis zur Festsetzung durch die zuständige untere Wasserbehörde nach § 115 Abs. 2 NWG als festgesetzt. Das Überschwemmungsgebiet ist nach § 78 WHG freizuhalten; es bestehen besondere Verbote und Genehmigungsvorbehalte nach § 78 Abs. 6 WHG.

Das Überschwemmungsgebiet erstreckt sich auf das Gebiet der Gemeinde Herzlake, Gemeinde Menslage, Stadt Löningen, Gemeinde Essen und der Stadt Quakenbrück und ist in den mitveröffentlichten Übersichtskarten **(Anlagen 1 und 2)** im Maßstab 1 : 40 000 (TK 25 Blatt-Nummer 3211, 3212, 3213, 3311, 3312, 3313, 3314) dargestellt. Die Arbeitskarten im Maßstab 1 : 5 000 (11 Blätter) werden beim

Landkreis Osnabrück,
Am Schölerberg 1,
49082 Osnabrück,

beim

Landkreis Cloppenburg,
Eschstraße 29,
49661 Cloppenburg,

und beim

Landkreis Emsland,
Ordeniederung 1,
49716 Meppen

aufbewahrt und können ab dem Tag nach dieser Bek. während der Dienststunden dort kostenlos eingesehen werden. In den Arbeitskarten ist die Grenze des nach § 115 Abs. 5 NWG vorläufig gesicherten Überschwemmungsgebietes mit einer roten Linie gekennzeichnet; das vom NLWKN ermittelte Überschwemmungsgebiet selbst ist blau dargestellt.

Anordnung der sofortigen Vollziehung

Gemäß § 80 Abs. 2 Nr. 4 VwGO i. d. F. vom 19. 3. 1991 (BGBl. I S. 686) in der derzeit geltenden Fassung wird die sofortige Vollziehung der vorläufigen Sicherung des Überschwemmungsgebietes angeordnet.

Die Begründung der Anordnung der sofortigen Vollziehung kann ebenfalls bei den Landkreisen Cloppenburg, Emsland und Osnabrück eingesehen werden.

Hinweis:

Die Karten sind außerdem auf der Internetseite des NLWKN eingestellt unter: www.nlwkn.niedersachsen.de/Hochwasser- & Küstenschutz/Hochwasserschutz/Überschwemmungsgebiete/ zu den Überschwemmungsgebietskarten.

— Nds. MBl. Nr. 44/2013 S. 881

Die Anlagen sind auf den Seiten 884—887 dieser Nummer des Nds. MBl. abgedruckt.

Vorläufige Sicherung des Überschwemmungsgebietes der Hunte von der Grenze zum Landkreis Vechta (Fluss-km 120 + 250) bis zur Straße „Zur Römerbrücke“ in Nierhüsen (Fluss-km 137 + 630) in den Landkreisen Vechta und Osnabrück

Bek. d. NLWKN v. 27. 11. 2013 — 62023/259,260/13 —

Der NLWKN hat den Bereich der Landkreise Vechta und Osnabrück, der von einem hundertjährlichen Hochwasser des Gewässers Hunte überschwemmt wird, ermittelt und in Arbeitskarten dargestellt.

Die Arbeitskarten werden hiermit öffentlich bekannt gemacht. Das Überschwemmungsgebiet gilt ab dem Tag nach dieser Bek. nach § 115 Abs. 5 NWG vom 19. 2. 2010 (Nds. GVBl. S. 64), zuletzt geändert durch § 87 Abs. 3 des Gesetzes vom 3. 4. 2012 (Nds. GVBl. S. 46), bis zur Festsetzung durch die zuständige untere Wasserbehörde nach § 115 Abs. 2 NWG als festgesetzt. Das Überschwemmungsgebiet ist nach § 78 WHG freizuhalten; es bestehen besondere Verbote und Genehmigungsvorbehalte nach § 78 Abs. 6 WHG.

Das Überschwemmungsgebiet erstreckt sich auf das Gebiet der Gemeinden Bohmte, Damme und Steinfeld und ist in der mitveröffentlichten Übersichtskarte **(Anlage)** im Maßstab 1 : 50 000

(TK 25 Blatt-Nummern 3415, 3416, 3515) dargestellt. Die Arbeitskarten im Maßstab 1 : 5 000 (Blätter 1 bis 5) werden beim

Landkreis Vechta,
Ravensberger Straße 20,
49377 Vechta,

und

beim Landkreis Osnabrück,
Am Schölerberg 1,
49082 Osnabrück,

aufbewahrt und können ab dem Tag nach dieser Bek. während der Dienststunden dort kostenlos eingesehen werden. In den Arbeitskarten ist die Grenze des nach § 115 Abs. 5 NWG vorläufig gesicherten Überschwemmungsgebietes mit einer roten Linie gekennzeichnet; das vom NLWKN ermittelte Überschwemmungsgebiet selbst ist blau dargestellt.

Hinweis:

Die Karten sind außerdem auf der Internetseite des NLWKN eingestellt unter: www.nlwkn.niedersachsen.de/Hochwasser- & Küstenschutz/Hochwasserschutz/Überschwemmungsgebiete/ zu den Überschwemmungsgebietskarten.

— Nds. MBl. Nr. 44/2013 S. 881

Die Anlage ist auf den Seiten 888/889 dieser Nummer des Nds. MBl. abgedruckt.

Staatliches Gewerbeaufsichtsamt Braunschweig

Feststellung gemäß § 3 a UVPG (H. C. Starck GmbH, Goslar)

Bek. d. GAA Braunschweig v. 15. 11. 2013 — G/13/039 —

Die Firma H. C. Starck GmbH, Im Schleeke 78—91, 38642 Goslar, hat mit Schreiben vom 26. 8. 2013 die Erteilung einer Änderungsgenehmigung gemäß § 16 Abs. 2 BImSchG in der derzeit geltenden Fassung für die Erweiterung der Anlage zur Herstellung von Wolfram und Wolframverbindungen beantragt. Die Erweiterung besteht in der Aufstellung einer zweiten Feststoffextraktionsanlage und der Erweiterung der Kapazität der Anlage auf die Herstellung von 8 000 t/a Wolframoxid.

Im Rahmen dieses Genehmigungsverfahrens ist gemäß § 3 c i. V. m. Nummer 4.2 der Anlage 1 UVPG durch eine allgemeine standortbezogene Vorprüfung des Einzelfalles zu ermitteln, ob für das beantragte Vorhaben die Durchführung einer Umweltverträglichkeitsprüfung erforderlich ist.

Diese Vorprüfung hat ergeben, dass eine Umweltverträglichkeitsprüfung für das o. g. Verfahren nicht erforderlich ist.

Es wird darauf hingewiesen, dass diese Feststellung nicht selbständig anfechtbar ist.

— Nds. MBl. Nr. 44/2013 S. 882

Staatliches Gewerbeaufsichtsamt Celle

Feststellung gemäß § 3 a UVPG (Biogasanlage Rehmsgas UG & Co. KG, Hermann Meine, Hambühren)

Bek. d. GAA Celle v. 11. 11. 2013 — CE002999986-13-219-02 ar —

Die Rehmsgas UG & Co. KG, Hermann Meine, Im Dorfe 13, 29313 Hambühren, hat mit Schreiben vom 30. 9. 2013 die Erteilung einer Genehmigung gemäß § 16 Abs. 1 BImSchG in der derzeit geltenden Fassung für die wesentliche Änderung einer Biogasanlage mit Verbrennungsmotoranlage am Standort in 29313 Hambühren, Gemarkung Hambühren, Flur 3, Flurstück 10/3, beantragt.

Im Rahmen dieses Genehmigungsverfahrens ist gemäß § 3 c i. V. m. Nummer 1.11.1.1 der Anlage 1 UVPG in der derzeit geltenden Fassung durch eine Vorprüfung des Einzelfalles zu ermitteln, ob für das beantragte Vorhaben die Durchführung einer Umweltverträglichkeitsprüfung erforderlich ist.

Die Vorprüfung hat ergeben, dass eine Umweltverträglichkeitsprüfung in diesem Verfahren nicht erforderlich ist.

Diese Feststellung wird hiermit öffentlich bekannt gemacht. Sie ist nicht selbständig anfechtbar.

— Nds. MBl. Nr. 44/2013 S. 882

Staatliches Gewerbeaufsichtsamt Hannover

Immissionsschutzrechtliche Entscheidung gemäß § 16 Abs. 1 BImSchG (Smurfit Kappa Hoya Papier und Karton GmbH)

Bek. d. GAA Hannover v. 27. 11. 2013 — H027720166-H-12-111 —

Der Firma Smurfit Kappa Hoya Papier und Karton GmbH, Von-dem-Bussche-Straße 1, 27318 Hoya, wurde auf ihren Antrag vom 9. 12. 2009 gemäß § 16 i. V. m. § 10 BImSchG vom GAA Hannover als zuständiger Genehmigungsbehörde am 11. 11. 2013 die Genehmigung zur wesentlichen Änderung ihrer Anlage zur Herstellung von Papier, Karton oder Pappe mit einer Produktionsleistung von 20 Tonnen oder mehr je Tag entsprechend Nummer 6.2.1 (G/E) der 4. BImSchV erteilt.

Der verfügende Teil der Genehmigung und die Rechtsbehelfsbelehrung werden in der **Anlage** bekannt gemacht. Auf Maßgaben und Nebenbestimmungen in Abschnitt II des Bescheides wird hingewiesen.

Der vollständige Genehmigungsbescheid einschließlich der Begründung liegt in der Zeit

vom 28. 11. bis 11. 12. 2013 (einschließlich)

a) bei der Genehmigungsbehörde, dem Staatlichen Gewerbeaufsichtsamt Hannover, 30177 Hannover, Am Listholze 74, Foyer,

montags bis donnerstags	7.30 bis 16.00 Uhr,
freitags	7.30 bis 13.30 Uhr,

b) bei der Samtgemeinde Grafschaft Hoya, Schloßplatz 2, 27318 Hoya/Weser, Fachbereich Bauen, 2. Etage, Zimmer 37,

montags bis mittwochs	8.00 bis 16.30 Uhr,
donnerstags	8.00 bis 18.00 Uhr,
freitags	8.00 bis 13.00 Uhr,

c) bei der Gemeinde Dörverden, Rathaus, Große Straße 80, 27313 Dörverden, EG, Flur des Fachbereichs Bauen,

montags bis mittwochs	8.30 bis 16.00 Uhr,
donnerstags	8.30 bis 18.00 Uhr,
freitags	8.30 bis 12.00 Uhr,

und außerhalb der Dienststunden nach telefonischer Vereinbarung (Tel. 04234 399-60, -61),

öffentlich aus und kann dort während der vorgenannten Dienststunden von jedermann eingesehen werden.

Mit Ablauf des **11. 12. 2013** gilt der Bescheid gegenüber den Einwenderinnen und Einwendern und Dritten, die keine Einwendungen erhoben haben, als zugestellt.

In der Zeit vom **28. 11. 2013 bis 11. 1. 2014** (einschließlich) kann der vollständige Genehmigungsbescheid von allen Personen, die Einwendungen erhoben haben, beim GAA Hanno-

ver schriftlich angefordert werden. Der vollständige Genehmigungsbescheid sowie die Bezeichnung des maßgeblichen BVT-Merkblattes sind im Internet unter www.gewerbeaufsicht.niedersachsen.de über den Pfad „Wir über uns — Aktuelles lokal > öffentliche Bekanntmachung > Hannover—Hildesheim“ einsehbar.

Die maßgeblichen Vorschriften zur Öffentlichkeitsbeteiligung ergeben sich aus § 10 BImSchG und dem Vierten Abschnitt der 9. BImSchV.

— Nds. MBl. Nr. 44/2013 S. 882

Anlage

I. Entscheidung

1. Gemäß § 16 Abs. 1 des Bundes-Immissionsschutzgesetzes (BImSchG) i. V. m. Nr. 6.2.1 G/E des Anhangs der 4. BImSchV wird der Firma

Smurfit Kappa Hoya Papier und Karton GmbH,
Von-dem-Bussche-Str. 1,
27318 Hoya,

die Genehmigung zur wesentlichen Änderung ihrer

Anlage zur Herstellung von Papier und Karton

erteilt.

Standort der Anlage ist das Grundstück:

Straße:	Von-dem-Bussche-Straße 1
Postleitzahl und Ort:	27318 Hoya
Gemarkung:	Hoya
Flur:	3
Flurstücke:	35, 13/31, 13/24, 13/28, 32.

2. Im Einzelnen wird genehmigt:

— Umbau Papiermaschine PM 2 in mehreren Schritten zur Kapazitätserhöhung auf 450 000 t/a,

— Kapazitätserhöhung der Kartonmaschine PM 4 auf 100 000 t/a,

— Ausschöpfung der vollen installierten Leistung von 80,1 MW des bestehenden Kraftwerks der PM 2 (Kraftwerksnebenanlage 1),

— Begrenzung der Gasturbine 1 mit der Zusatzfeuerung (Kessel 5) auf eine max. Feuerungswärmeleistung von 47,1 MW,

— Errichtung der Kraftwerksnebenanlage 2 mit einer Feuerungswärmeleistung von 32,4 MW zur Versorgung der PM 2,

— Ausbau der innerbetrieblichen Gleisanlage und Bau einer Bahnübergangssicherungsanlage.

3. Die Antragsunterlagen (Anlage 1*) sind Bestandteil dieser Genehmigung.

4. Die Anlage ist entsprechend der Antragsunterlagen (Anlage 1*) zu errichten und zu betreiben, soweit durch die in Abschnitt II aufgeführten Nebenbestimmungen nichts anderes bestimmt wird.

5. Diese Genehmigung erlischt für alle Anlagenteile dieses Bescheides, die nicht innerhalb von drei Jahren nach Eintritt der Rechtskraft der Genehmigung in Betrieb genommen wurden.

6. Diese Genehmigung schließt folgende Genehmigungen ein:

— die Baugenehmigung des Landkreises Nienburg,

— die eisenbahnrechtliche Plangenehmigung der Gesellschaft für Landeseisenbahnaufsicht mbH,

— die Genehmigung im Sinne des § 4 Abs. 1 des Treibhausgas-Emissionshandelsgesetzes (TEHG). Sie berechtigt zur Freisetzung von Treibhausgasen im Rahmen der genehmigten Tätigkeit (Anlage nach § 2 TEHG, Anhang I, Tätigkeit XV: Anlage zur Herstellung von Papier, Karton oder Pappe mit einer Produktionsleistung von mehr als 20 Tonnen je Tag).

7. Weitere bisher für die Anlage erteilte Entscheidungen (Genehmigungen, Anordnungen, Anzeigen usw.) behalten weiterhin ihre Gültigkeit, soweit sie durch diese Genehmigung keine Änderung erfahren.

Dies gilt insbesondere für die mit Bescheid der Bezirksregierung Hannover vom 14. 9. 1988 (Az. 204a-40500/4/6.2/1) erteilte Genehmigung für die PM 2 und die Dampfkesselanlage sowie die Anzeige gem. § 67 BImSchG vom 20. 3. 1986 für die PM 4 sowie deren nachfolgende Genehmigungen, die der vorliegenden Genehmigung zugrunde liegen.

8. Der Antragsteller hat die Kosten dieses Genehmigungsverfahrens zu tragen.

II. Nebenbestimmungen*)

III. Begründung*)

IV. Rechtsbehelfsbelehrung

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch erhoben werden. Der Widerspruch ist schriftlich oder mündlich zur Niederschrift beim Staatlichen Gewerbeaufsichtsamt Hannover, Am Listholze 74, 30177 Hannover, einzulegen.

*) Hier nicht abgedruckt.

Staatliches Gewerbeaufsichtsamt Lüneburg

Planfeststellungsverfahren zur Errichtung und zum Betrieb der Deponie Haaßel
— Anhörungsverfahren —
(Kriete Kaltrecycling GmbH, Seedorf)

Bek. d. GAA Lüneburg v. 18. 11. 2013
— 4.1LG000034351-61 ar —

1. Im Rahmen des Anhörungsverfahren beginnt der Erörterungstermin am

11. 12. 2013, um 10.00 Uhr,
im Hotel Selsinger Hof,
Bahnhofstraße 1,
27446 Selsingen.

2. Der Einlass erfolgt ab ca. 60 Minuten vor Beginn des Termins. Eine Tagesordnung wird vor Ort ausgelegt.

3. Kann der Erörterungstermin am 11. 12. 2013 nicht abgeschlossen werden, wird er an den folgenden Werktagen bis einschließlich 13. 12. 2013 am selben Ort fortgesetzt. Ob und inwieweit die Folgetermine in Anspruch genommen werden und wann sie beginnen, entscheidet die Verhandlungsleitung jeweils am Schluss eines Verhandlungstages.

4. Im Termin werden die rechtzeitig erhobenen Einwendungen und Stellungnahmen mit der Vorhabenträgerin, den Behörden, den Betroffenen sowie denjenigen, die Einwendungen erhoben oder Stellungnahmen abgegeben haben, erörtert.

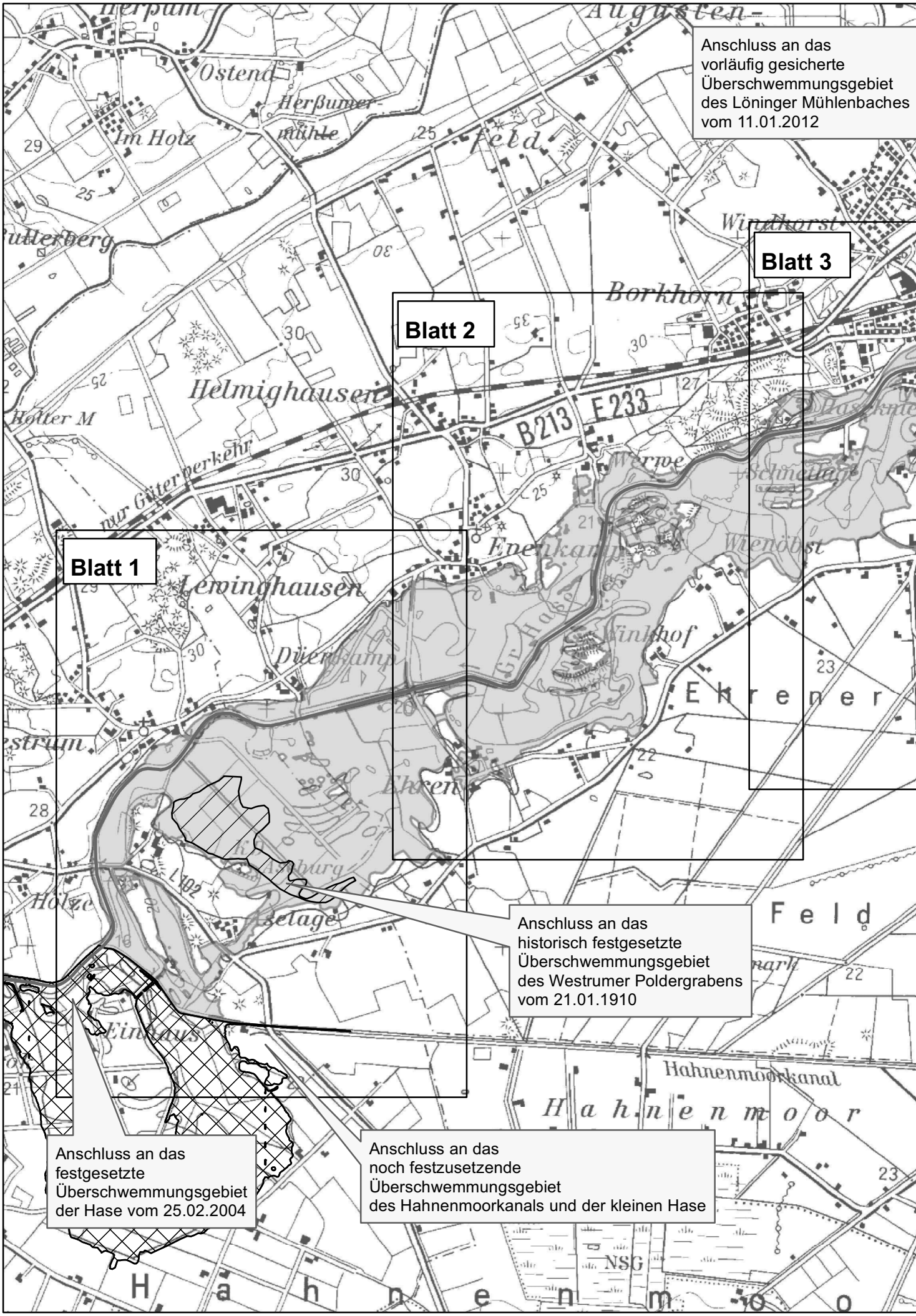
5. Die Teilnahme am Termin ist jeder oder jedem, deren oder dessen Belange durch das Vorhaben berührt werden, freigestellt. Die Vertretung durch eine Bevollmächtigte oder einen Bevollmächtigten ist möglich. Diese oder dieser hat ihre oder seine Bevollmächtigung durch eine schriftliche Vollmacht nachzuweisen und diese zu den Akten der Anhörungsbehörde zu geben. Es wird darauf hingewiesen, dass bei Ausbleiben einer oder eines Beteiligten auch ohne sie oder ihn verhandelt werden kann, dass verspätete Einwendungen ausgeschlossen sind und dass das Anhörungsverfahren mit Schluss der Verhandlung beendet ist.

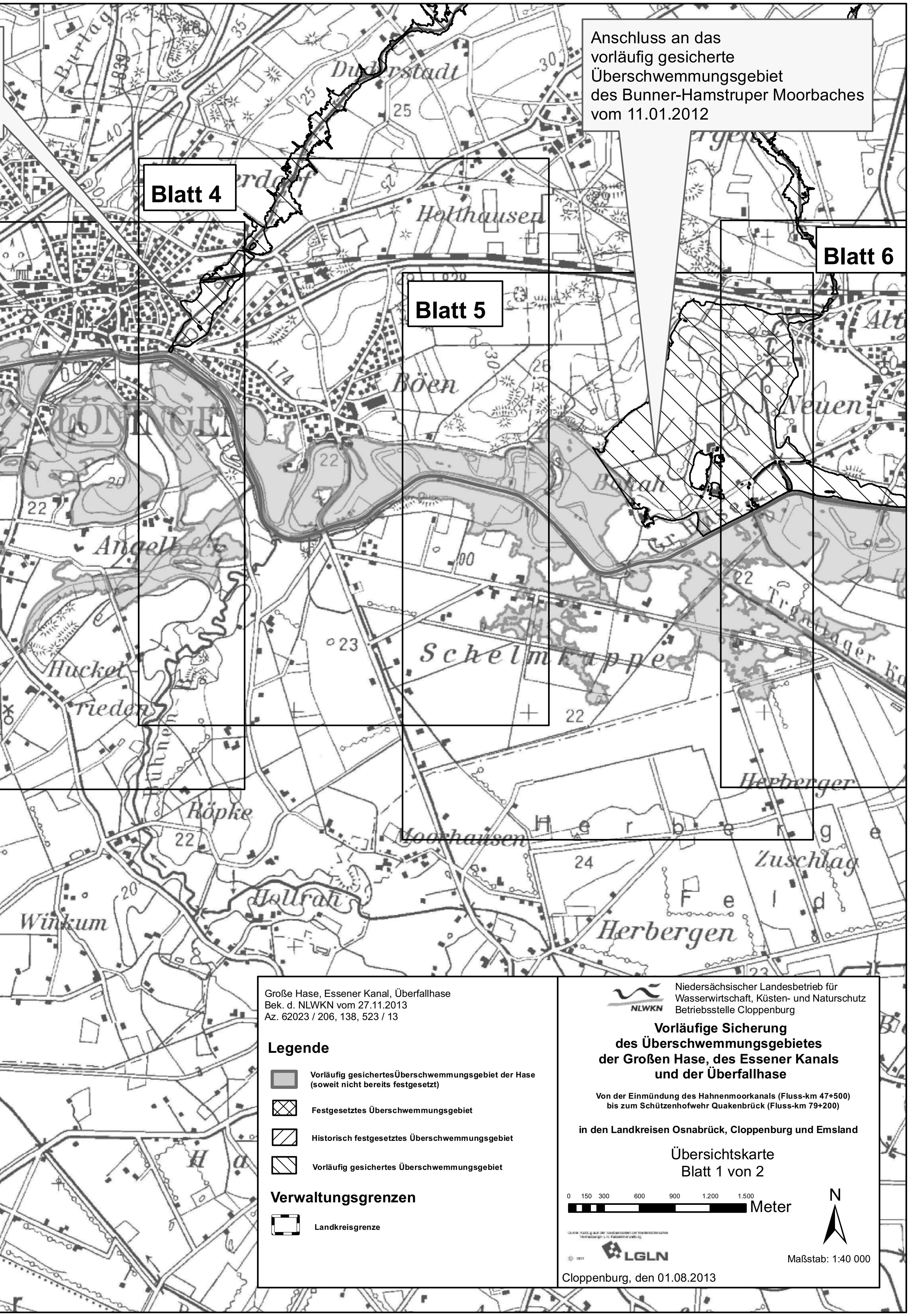
6. Durch die Teilnahme am Erörterungstermin oder durch Vertreterbestellung entstehende Kosten werden nicht erstattet.

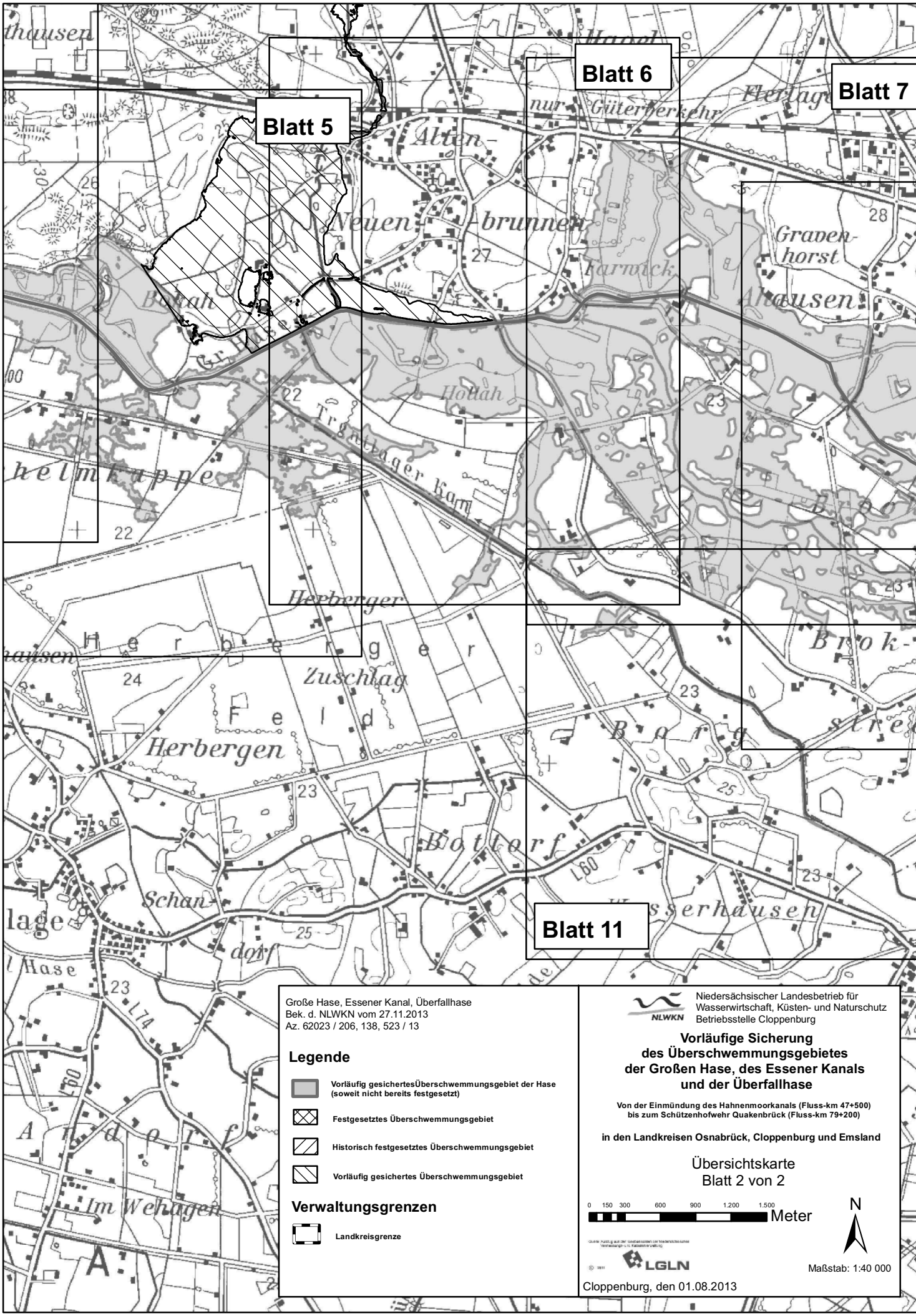
7. Sofern Einwenderinnen oder Einwender nicht am Erörterungstermin teilnehmen, gelten die von ihnen erhobenen Einwendungen als aufrechterhalten und werden im weiteren Verfahren entsprechend berücksichtigt.

8. Der Erörterungstermin ist nicht öffentlich.

— Nds. MBl. Nr. 44/2013 S. 883


Anschluss an das vorläufig gesicherte Überschwemmungsgebiet des Löninger Mühlenbaches vom 11.01.2012
Blatt 3
Blatt 2
Blatt 1
Anschluss an das historisch festgesetzte Überschwemmungsgebiet des Westrumer Poldergrabens vom 21.01.1910
Anschluss an das festgesetzte Überschwemmungsgebiet der Hase vom 25.02.2004
Anschluss an das noch festzusetzende Überschwemmungsgebiet des Hahnenmoorkanals und der kleinen Hase
Ostend
Herßumer-mühle
Im Holz
Feld
Windhorst
Borkhorn
Helmighausen
B213
E233
Holter M
nur Güterverkehr
Werwe
Schnettage
Wienöbst
Lewinghausen
Winkhof
Ehrener
Ehren
Aselage
Hölze
Einhaus
Hahnenmoorkanal
Hahnenmoor
NSG


Anschluss an das
vorläufig gesicherte
Überschwemmungsgebiet
des Bunner-Hamstruper Moorbaches
vom 11.01.2012
Blatt 4
Blatt 5
Blatt 6
Holthausen
Böen
Löningen
Angelbeck
Huckelrieden
Schelmkappe
Röpke
Moorhausen
Herberger Feld
Zuschlag
Herbergen
Hollrah
Winkum
Neuen
Große Hase, Essener Kanal, Überfallhase
Bek. d. NLWKN vom 27.11.2013
Az. 62023 / 206, 138, 523 / 13
Legende
Vorläufig gesichertesÜberschwemmungsgebiet der Hase (soweit nicht bereits festgesetzt)
Festgesetztes Überschwemmungsgebiet
Historisch festgesetztes Überschwemmungsgebiet
Vorläufig gesichertes Überschwemmungsgebiet
Verwaltungsgrenzen
Landkreisgrenze
Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz Betriebsstelle Cloppenburg
NLWKN
Vorläufige Sicherung des Überschwemmungsgebietes der Großen Hase, des Essener Kanals und der Überfallhase
Von der Einmündung des Hahnenmoorkanals (Fluss-km 47+500) bis zum Schützenhofwehr Quakenbrück (Fluss-km 79+200)
in den Landkreisen Osnabrück, Cloppenburg und Emsland
Übersichtskarte
Blatt 1 von 2
0 150 300 600 900 1.200 1.500
Meter
N
LGLN
Maßstab: 1:40 000
Cloppenburg, den 01.08.2013



Große Hase, Essener Kanal, Überfallhase
Bek. d. NLWKN vom 27.11.2013
Az. 62023 / 206, 138, 523 / 13

Legende

- Vorläufig gesichertesÜberschwemmungsgebiet der Hase (soweit nicht bereits festgesetzt)
- Festgesetztes Überschwemmungsgebiet
- Historisch festgesetztes Überschwemmungsgebiet
- Vorläufig gesichertes Überschwemmungsgebiet

Verwaltungsgrenzen

- Landkreisgrenze

Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz
Betriebsstelle Cloppenburg

NLWKN

Vorläufige Sicherung des Überschwemmungsgebietes der Großen Hase, des Essener Kanals und der Überfallhase

Von der Einmündung des Hahnenmoorkanals (Fluss-km 47+500) bis zum Schützenhofwehr Quakenbrück (Fluss-km 79+200)

in den Landkreisen Osnabrück, Cloppenburg und Emsland

Übersichtskarte
Blatt 2 von 2

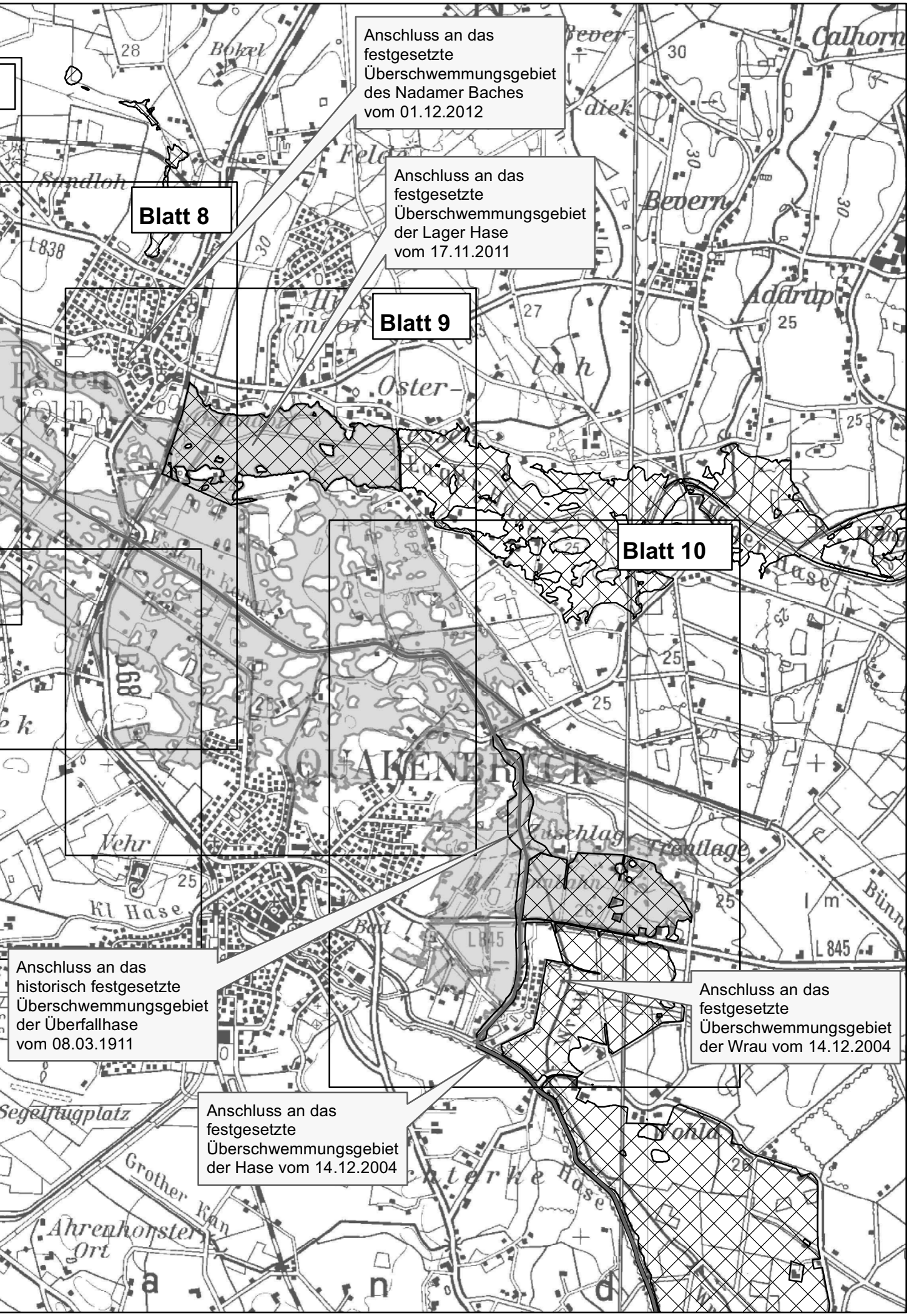
0 150 300 600 900 1.200 1.500 Meter

N

LGLN

Maßstab: 1:40 000

Cloppenburg, den 01.08.2013


Anschluss an das festgesetzte Überschwemmungsgebiet des Nadamer Baches vom 01.12.2012
Anschluss an das festgesetzte Überschwemmungsgebiet der Lager Hase vom 17.11.2011
Blatt 8
Blatt 9
Blatt 10
Anschluss an das historisch festgesetzte Überschwemmungsgebiet der Überfallhase vom 08.03.1911
Anschluss an das festgesetzte Überschwemmungsgebiet der Wrau vom 14.12.2004
Anschluss an das festgesetzte Überschwemmungsgebiet der Hase vom 14.12.2004
Bokel
Calhorn
Bevern
Addrup
Oster-
Essen
QUAKENBRÜCK
Vehr
Kl Hase
Trentlage
Segelflugplatz
Grother Kan
Ahrenhorster Ort
Wohld
L 845
L 838
B 68