Gesetz- und Verordnungsblatt

FÜR DAS LAND NORDRHEIN-WESTFALEN

76. Jahrgang	Ausgegeben zu Düsseldorf am 26. Juli 2022	Nummer 34

203013

Zweite Verordnung zur Änderung der Ausbildungsverordnung Laufbahngruppe 1 allgemeiner Verwaltungsdienst Gemeinden

Vom 14. Juli 2022

Auf Grund des § 7 Absatz 2 des Landesbeamtengesetzes vom 14. Juni 2016 (GV. NRW. S. 310, ber. S. 642) verordnet das Ministerium für Heimat, Kommunales, Bau und Digitalisierung im Einvernehmen mit dem Ministerium des Innern und dem Ministerium der Finanzen:

Artikel 1

Die Ausbildungsverordnung Laufbahngruppe 1 allgemeiner Verwaltungsdienst Gemeinden vom 9. September 2014 (GV. NRW. S. 501), die durch Verordnung vom 4. Juli 2018 (GV. NRW. S. 360) geändert worden ist, wird wie folgt geändert:

1. In § 5 Absatz 2 wird das Wort „soll“ durch das Wort „kann“ ersetzt.
2. Dem § 10 werden folgende Absätze 4 und 5 angefügt:

   „(4) Der Vorbereitungsdienst kann entsprechend der gesetzlichen Regelung auch in Teilzeit mit einem bis auf 75 Prozent der regelmäßigen Arbeitszeit reduzierten Umfang der Tätigkeit abgeleistet werden. Der tatsächliche Umfang der Reduzierung erfolgt im Einvernehmen mit dem Dienstherrn. Eine Ausbildung in Teilzeit ist an den Tagen der theoretischen Ausbildung nicht möglich. Die praktische Ausbildung ist im Umfang der Reduzierung entsprechend anzupassen. Der Ausbildungsverlauf bleibt unberührt.

   (5) Für Beamtinnen und Beamte, die einem olympischen, paralympischen oder deaflympischen Bundes- oder Landeskader angehören oder Mitglied einer entsprechenden Auswahlmannschaft sind und eine Empfehlung des Sportfachverbandes vorlegen, kann die Ausbildung um die mit dem Sportfachverband abgestimmte Trainings- und Wettkampfzeit bis zur Höchstausbildungszeit auf höchstens drei Jahre verlängert werden.“
3. § 15 Absatz 2 wird wie folgt gefasst:

   „(2) Für die Entscheidung über die Zulassung zur Abschlussprüfung sind nur die ersten vier fachpraktischen Ausbildungsabschnitte zu berücksichtigen. Die Zulassung kann nur erfolgen, wenn mindestens drei Ausbildungsabschnitte mit der Note „ausreichend“ oder einer besseren Bewertung abgeschlossen wurden und im Rahmen der vier fachpraktischen Ausbildungsabschnitte mindestens ein Durchschnittswert von „ausreichend“ erreicht wird.“
4. § 17 Absatz 5 wird wie folgt geändert:

   a) In Satz 1 werden die Wörter „Leistungsnachweise in Form von schriftlichen Übungsarbeiten (Klausurarbeiten) und sonstige Leistungen (zum Beispiel mündliche Leistungen, Tests, Hausarbeiten)“ durch die Wörter „schriftliche Leistungsnachweise (Klausurarbeiten)“ ersetzt.

   b) In Satz 2 werden die Wörter „sowie die sonstigen Leistungen“ gestrichen.

   c) In Satz 5 wird die Angabe „und 2“ durch die Angabe „bis 3“ ersetzt.
5. Dem § 19 wird folgender Absatz 7 angefügt:

   „(7) Entscheidungen über Widersprüche in Prüfungsangelegenheiten trifft der Prüfungsausschuss. Dieser kann die Aufgabe der Studienleitung übertragen.“
6. § 20 Absatz 2 wird wie folgt geändert:

   a) In Satz 1 werden die Wörter „im Lehrgang erbrachten Klausurarbeiten und sonstigen Leistungen“ durch die Wörter „theoretischen Ausbildung“ ersetzt.

   b) Satz 2 wird aufgehoben.
7. § 28 Absatz 2 wird wie folgt gefasst:

   „(2) In der Wiederholungsprüfung ist der Prüfling auf Antrag von der Prüfung in einzelnen Bereichen zu befreien, wenn seine Leistungen in diesen Prüfungsbereichen bei der zurückliegenden Prüfung mindestens mit der Note „ausreichend“ bewertet wurden. Der Antrag ist rechtzeitig vor der Wiederholungsprüfung zu stellen. Bei der Festsetzung des Ausbildungspunktwertes nach § 20 Absatz 2 sind auch die Noten der Beurteilungen über den verlängerten Vorbereitungsdienst und die Noten der während der Zeit im Unterricht gefertigten Klausurarbeiten in die Berechnung einzubeziehen.“
8. § 30 Absatz 1 wird wie folgt gefasst:

   „(1) Beamtinnen und Beamte des feuerwehrtechnischen Dienstes der Laufbahngruppe 1 ab dem zweiten Einstiegsamt, die nach § 26 Absatz 2 Satz 3 des Beamtenstatusgesetzes vom 17. Juni 2008 (BGBl. I S. 1010), das zuletzt durch Artikel 2 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250) geändert worden ist, an Maßnahmen zum Erwerb einer neuen Befähigung teilzunehmen haben, erwerben die Befähigung für die Laufbahn des allgemeinen Verwaltungsdienstes in den Gemeinden und Gemeindeverbänden des Landes Nordrhein-Westfalen der Laufbahngruppe 1 ab dem zweiten Einstiegsamt durch die erfolgreiche Teilnahme an

   1. dem für diese Laufbahn eingerichteten Vorbereitungsdienst oder
   2. einer Ausbildung für Verwaltungsfachangestellte nach der APO Verwaltungsfachangestellte vom 11. Juni 2014 (GV. NRW. S. 325) in der jeweils geltenden Fassung.

   Dies setzt voraus, dass die Teilnehmenden sowohl im Lehrgang als auch in der praktischen Ausbildung mindestens einen Durchschnittspunktwert von 5,00 erhalten. Das zuständige Studieninstitut für kommunale Verwaltung stellt die erfolgreiche Teilnahme entsprechend Satz 1 Nummer 1 oder Nummer 2 fest. Eine Prüfung darf nicht gefordert werden.“
9. Die Anlage 4 erhält die aus dem Anhang zu dieser Verordnung ersichtliche Fassung.

Artikel 2

Diese Verordnung tritt am 1. August 2022 in Kraft.

Düsseldorf, den 14. Juli 2022

Die Ministerin
für Heimat, Kommunales, Bau und Digitalisierung
des Landes Nordrhein-Westfalen

Ina S c h a r r e n b a c h

Anlage 4
(zu § 17 Absatz 5,
§ 20 Absatz 5)

Studieninstitut für kommunale Verwaltung _____

Nachweisung des Ausbildungspunktwertes

für_____

1. Ergebnis der praktischen Ausbildung im

1.1 Ausbildungsabschnitt 1: _____
1.2 Ausbildungsabschnitt 2: _____
1.3 Ausbildungsabschnitt 3: _____
1.4 Ausbildungsabschnitt 4: _____

Summe_____: 4 = _____ (Punktwert der praktischen Ausbildung*)

2. Ergebnis der theoretischen Ausbildung im Unterrichtsfach:

		Klausurarbeiten	
2.1	Staats- und Europarecht	Punktzahl	_____
2.2	Allgemeines Verwaltungsrecht	Punktzahl	_____
2.3	Kommunalrecht	Punktzahl	_____
2.4	Recht der Gefahrenabwehr	Punktzahl	_____
2.5	Sozialrecht	Punktzahl	_____
2.6	Bürgerliches Recht	Punktzahl	_____
2.7	Beamtenrecht	Punktzahl	_____
2.8	Arbeits- und Tarifrecht	Punktzahl	_____
2.9	Verwaltungsorganisation	Punktzahl	_____
2.10	Betriebswirtschaftslehre mit Bezügen zur Volkswirtschaftslehre	Punktzahl	_____
2.11	Kosten- und Leistungsrechnung	Punktzahl	_____
2.12	Kommunale Buchführung	Punktzahl	_____
2.13	Kommunale Abgaben	Punktzahl	_____
2.14	Kommunales Finanzmanagement	Punktzahl	_____
		Summe	_____

Summe aller Punktzahlen der Klausurarbeiten _____ : _____ (Zahl der Klausurarbeiten) =

_____ (Punktwert der theoretischen Ausbildung*)

Anlage 4
(zu § 17 Absatz 5
§ 20 Absatz 5)

3. Ausbildungspunktwert

Summe der Punktwerte für

3.1 praktische Ausbildung _____
und

3.2 theoretische Ausbildung _____x 2

Summe _____: 3

= Ausbildungspunktwert*) _____

Damit ist die Beamtin/der Beamte zur Prüfung nicht zugelassen/zugelassen (§ 20 Absatz 3 VAP 1.2 allgVerw - Gem).

_____, den _____

_____
(Unterschrift Studienleitung)

Von der vorstehenden Berechnung habe ich Kenntnis genommen.

_____, den _____

_____
(Unterschrift Beamtin/Beamter)

---

*) Bruchwerte sind ohne Rundung bis zur zweiten Dezimalstelle zu errechnen.

2254

Bekanntmachung des Inkrafttretens des Zweiten Staatsvertrages zur Änderung medienrechtlicher Staatsverträge (Zweiter Medienänderungsstaatsvertrag)

Nachdem am 29. Juni 2022 alle Ratifikationsurkunden bei der Staatskanzlei des Landes Nordrhein-Westfalen, Vorsitzland der Ministerpräsidentenkonferenz, hinterlegt waren, ist der Staatsvertrag gemäß seines Artikels 3 Absatz 2 Satz 1 am 30. Juni 2022 in Kraft getreten.

Düsseldorf, 5. Juli 2022

Der Ministerpräsident
des Landes Nordrhein-Westfalen

Hendrik W ü s t

– GV. NRW. 2022 S. 831

45

Verordnung über die elektronische Kommunikation und Aktenführung in Angelegenheiten der strafrechtlichen Zusammenarbeit mit dem Ausland im Land Nordrhein-Westfalen (ERVVO RHSt)

Vom 7. Juni 2022

Auf Grund des § 77b des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), dessen Satz 2 bis 4 durch Artikel 1 Nummer 4 des Gesetzes vom 18. Oktober 2010 (BGBl. S. 1408) eingefügt und dessen Satz 1 zuletzt durch Artikel 163 der Verordnung vom 31. August 2015 (BGBl. I S. 1474) geändert worden ist, in Verbindung mit § 1 Absatz 2 Satz 1 des Justizgesetzes Nordrhein-Westfalen vom 26. Januar 2010 (GV. NRW. S. 30), der zuletzt durch Gesetz vom 23. Februar 2022 (GV. NRW. S. 254) geändert worden ist, verordnet das Ministerium der Justiz:

§ 1
Zulassung der elektronischen Kommunikation im Bereich der Rechtshilfe in Strafsachen

Gerichte und Behörden können nach Maßgabe der nachfolgenden Vorschriften elektronische Nachrichten zum Zweck der internationalen Rechtshilfe in Strafsachen von ausländischen Gerichten und Behörden empfangen oder an diese übermitteln. Die an dem elektronischen Nachrichtenverkehr teilnehmenden Behörden sowie der Zeitpunkt, ab dem sie daran teilnehmen, werden in der Anlage 1 bezeichnet.

§ 2
Übermittlung von Nachrichten

Die Übermittlung von Nachrichten nach § 1 erfolgt über den deutschen e-Justice Communication via Online Data Exchange-Zugangspunkt, im Folgenden e-CODEX-Zugangspunkt, unter Nutzung des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP) oder des e-Evidence Digital Exchange Systems (eEDES).

§ 3
Arten und Formate der zu übermittelnden Dokumente

(1) Nachrichten nach § 1 bestehen aus einem Dokument im Portable Document Format, im Folgenden PDF, und maschinenlesbaren Daten im Format Extensible Markup Language (XML). Das Dokument enthält das an die empfangende Behörde zu übermittelnde, das Rechtshilfeersuchen betreffende Anschreiben. Das Beifügen von Anhängen ist zulässig.

(2) Die übermittelnde Behörde ist dafür verantwortlich, dass das Dokument und die Anhänge schädliche aktive Komponenten, wie beispielsweise Viren, Trojaner oder Würmer, nicht enthalten.

§ 4
Gewährleistung der Authentizität von an das Ausland zu übermittelnden Dokumenten und der Integrität von zu übermittelnden Dokumenten und Nachrichten

(1) Eine Mehrfertigung des Dokuments ist durch eine in Nummer 9 Absatz 1 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten in der Fassung der Bekanntmachung vom 23. Dezember 2016 (BAnz AT 12.10.2017 B1) in der jeweils geltenden Fassung bezeichnete Person zu unterzeichnen. Die unterzeichnete Mehrfertigung ist zu den Akten zu nehmen. Das Dokument ist elektronisch als PDF zu speichern und mit einer qualifizierten elektronischen Signatur nach der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2005, S. 19; L 155 vom 14.6.2016, S. 44) in der jeweils geltenden Fassung zu versehen.

(2) Die qualifizierte elektronische Signatur kann durch ein anderes sicheres Verfahren im Sinne des § 77a Absatz 2 des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist, ersetzt werden. Bei Übermittlung über einen e-CODEX-Zugangspunkt stellt die Beifügung des „Trust-OK-Tokens“ nach Maßgabe des sich aus Anlage 2 ergebenden europäischen Standards ein solches sicheres Verfahren dar.

(3) Dem Dokument beizufügende Anhänge sind, sofern sie nicht schon elektronisch vorliegen, durch Einscannen in die elektronische Form zu übertragen. Ist ein beizufügendes Schriftstück mit einem Beglaubigungsvermerk versehen, ist im Dokument die bildliche und inhaltliche Übereinstimmung des auf dem beigefügten Schriftstück angebrachten Beglaubigungsvermerks zu bestätigen. Die Übertragung hat nach dem Stand der Technik zu erfolgen. Sie genügt dieser Anforderung insbesondere, wenn den Anforderungen der Technischen Richtlinie 03138 Ersetzendes Scannen (RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnik vom 23. April 2020 genügt wird. Eingescannte Leerseiten werden nicht übersandt.

(4) Abweichend von Nummer 9 Absatz 3 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten bedarf es der Beifügung eines Abdrucks des Dienstsiegels nicht.

§ 5
Prüfung der Authentizität und Integrität von aus dem Ausland übermittelten Dokumenten und Nachrichten

(1) Sofern nach dem Gesetz über die internationale Rechtshilfe in Strafsachen für die Leistung von Rechtshilfe die Einreichung schriftlicher Unterlagen einschließlich Originalen oder beglaubigten Abschriften vorgesehen ist, ist die Vorlage elektronischer Dokumente zulässig, die mit qualifizierter elektronischer Signatur versehen sind.

(2) Die qualifizierte elektronische Signatur kann durch ein anderes sicheres Verfahren im Sinne des § 77a Absatz 2 des Gesetzes über die internationale Rechtshilfe in Strafsachen ersetzt werden. Bei Übermittlung über einen e-CODEX-Zugangspunkt stellt die Beifügung des „Trust-OK-Tokens“ nach Maßgabe des sich aus Anlage 2 ergebenden europäischen Standards ein solches sicheres Verfahren dar.

(3) Sofern eine qualifizierte elektronische Signatur nach der Verordnung (EU) Nr. 910/2014 verwendet wird, müssen diese und das ihr zugrunde liegende Zertifikat durch das adressierte Gericht oder durch eine andere von der Landesjustizverwaltung mit der automatisierten Überprüfung beauftragte Stelle prüfbar sein.

(4) Ist ein übermitteltes elektronisches Dokument zur Bearbeitung nicht geeignet, ist dies der absendenden Stelle unter Angabe der geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.

§ 6

Weitere Bearbeitung eingehender elektronischer Nachrichten aus dem Ausland

(1) Soweit die elektronische Aktenführung noch nicht eingeführt ist, ist von eingehenden elektronischen Dokumenten, soweit es sich nicht um maschinenlesbare Dateien handelt, ein Ausdruck für die Akten zu fertigen. Im Übrigen bleiben die Vorschriften der Allgemeinen Verwaltungsvorschriften des Justizministeriums „Anweisungen für die Verwaltung des Schriftguts bei den Geschäftsstellen der Gerichte und Staatsanwaltschaften des Landes Nordrhein-Westfalen“ vom 27. April 1967 (JMBl. NRW S. 109), die zuletzt durch die Allgemeine Verwaltungsvorschrift vom 16. Dezember 2019 (JMBl. NRW S. 3) geändert worden sind, unberührt.

(2) Soweit die elektronische Aktenführung eingeführt ist, gilt die eAkten-Verordnung Strafverfahren vom 19. August 2020 (GV. NRW. S. 761) in der jeweils geltenden Fassung.

§ 7

Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt die Verordnung über die elektronische Kommunikation und Aktenführung in Angelegenheiten der strafrechtlichen Zusammenarbeit mit dem Ausland im Lande Nordrhein-Westfalen vom 24. März 2015 (GV. NRW. S. 324) außer Kraft.

Düsseldorf, den 7. Juni 2022

Der Minister der Justiz
des Landes Nordrhein-Westfalen

Peter B i e s e n b a c h

Anlage 1

I. Am elektronischen Rechtshilfeverkehr in Strafsachen unter Nutzung des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP) teilnehmende Gerichte und Behörden, Zeitpunkt der Teilnahme

Staatsanwaltschaften	**Zeitpunkt**
Aachen, Düsseldorf	ab 01.02.2015
Duisburg, Krefeld, Kleve, Köln, Mönchengladbach	ab 01.09.2015
Arnsberg, Bielefeld, Bochum, Bonn, Detmold, Dortmund, Essen, Hagen, Münster, Paderborn, Siegen, Wuppertal	ab 01.12.2015

Gerichte	**Zeitpunkt**
./.	./.
./.	./.

II. Am elektronischen Rechtshilfeverkehr in Strafsachen unter Nutzung des e Evidence Digital Exchange Systems (eEDES) teilnehmende Gerichte und Behörden, Zeitpunkt der Teilnahme

Staatsanwaltschaften	**Zeitpunkt**
Köln, Kleve und Dortmund	ab 01.11.2021
Aachen, Arnsberg, Bielefeld, Bochum, Bonn, Detmold, Duisburg, Essen, Hagen, Krefeld, Kleve, Mönchengladbach, Münster, Paderborn, Siegen, Wuppertal	ab 01.05.2022

Gerichte	**Zeitpunkt**
./.	./.
./.	./.

III. e-CODEX-Zugangspunkt (e-Codex-Gateway)

Landesbetrieb
Information und Technik Nordrhein-Westfalen (IT.NRW)
Mauerstraße 51
40476 Düsseldorf

Anlage 2

e-CODEX
Agreement on a Circle of Trust

e-CODEX making justice faster.eu

e-CODEX
Agreement on a Circle of Trust

Adopted by the e-CODEX General Assembly on the 20th of February 2013

Definitions

Advanced Electronic Signature	An advanced electronic signature as defined by Article 2 (2) of Directive 1999/93 EC
Advanced Electronic System	An electronic system as outlined in Article 1.2.1.
Authentication-based Advanced Electronic System	A system meeting the requirements set out in Annex 2
Connector	The Connector is a piece of software which implements the interface between (i) the national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal, and (ii) the Gateway of such Party.
Contact Points	Natural and/or legal persons designated by a Party to be responsible for operational and technical matters related to or in connection with the functioning of the e-CODEX System
Document	Any kind of electronic file, such as PDF, XML files, graphics files.
e-CODEX System	The technological and organisational infrastructure, which includes the e-delivery platform (e.g. the e-CODEX Service Provider, the e-CODEX Connector and the e-CODEX Gateway).
Gateway	The technical and organisational infrastructure provided by a Party for incoming and outgoing cross border electronic communication with such Party within the e-CODEX System
Message	An electronic message sent or received by a Gateway via the e-CODEX System, consisting of at least one or

	more Documents, accompanied by a Trust-ok Token.
Original Country of Trust	The state in which the Sending Connector is located that first received the Document, or the state identified by the European E-Justice-Portal.
Party/Parties	The parties to this agreement
Qualified Electronic Signature	An Advanced Electronic Signature based on a qualified certificate and created by a secure signature-creation device, as defined by Article 5 (1) of Directive 1999/93 EC
Receiving State	The state of the Party whose Receiving Gateway receives a Message, or, in the case of the European E-Justice-Portal, the state of the Recipient in each case including the subdivisions and administrative and judicial bodies of that state.
Receiving Party	The Party whose Receiving Gateway receives a Message forwarded from the Sending Gateway via the e-CODEX System
Receiving Connector	The Connector receiving a Message from the Receiving Gateway for forwarding to the Recipient and meeting the requirements set out in Annex 4
Receiving Gateway(s)	The Gateway(s) receiving a Message from the Sending Gateway and meeting the requirements set out in Annex 4
Recipient	The User receiving a Message
Sender	The User indicated as the author of a Message
Sending Party	The Party from whose Sending Gateway a Message is forwarded to the Receiving Gateway(s) via the e-CODEX System
Sending Connector	The Connector first receiving a Message from the sender for forwarding to the Sending Gateway(s) and meeting the requirements set out in Annex 4
Sending Gateway	The Gateway first receiving a Message from the Sending Connector for forwarding to the Receiving Gateway(s) and meeting the requirements set out in Annex 4
Signature-based Advanced Electronic System	An Advanced Electronic System using a Qualified Electronic Signature or an Advanced Electronic

e CODEX making justice faster.eu

	Signature
Time Evidence	A discrete set of electronic data generated by an electronic system, providing information about the occurrence of a particular event, as further detailed in Annex 5
Trust-ok Token	A software token as described in Article 1.3. and further specified in Annex 3
User	Any party (including courts and public authorities) to a judicial proceeding and/or exchange of information carried out via the e-CODEX System

e CODEX making justice faster.eu

Preamble: Nature of the Present Agreement

The present Agreement is a document by which the Parties intend to define and establish a Circle of Trust for the cross border exchange of documents and data within all e-CODEX use cases for the duration of the pilots.

The Agreement will firstly be adopted by the General Assembly of the e-CODEX project. When Partners are ready to join a pilot they must declare to the e-CODEX Coordinator that they comply with the terms of this Agreement (declaration of accession).

Annex 1[1] lists the Parties who have acceded to this Agreement and in which pilot(s) they are participating.

This preamble forms part of the Present Agreement.

1. Principle of a Circle of Trust

1.1.
For the purpose of this Agreement, the principle of a Circle of Trust is understood as the mutual recognition between Member States of an electronic document within the existing legal framework.

1.2.
In order to fall within the scope of the Circle of Trust, the Document must:

1.2.1.
originate from an Advanced Electronic System, which is an electronic system with the following characteristics:

- The Document is uniquely linked to the User,
- The system is capable of identifying the User,
- The Document is created using means that the User can maintain under his control and any subsequent change of the data is detectable.

[1] Annex 1 will be maintained by the e-CODEX Coordinator.

1.2.2.
be accompanied by a Trust-ok Token issued by the Sending Connector, as described in 1.3. indicating whether the Document is considered as trusted (SUCCESSFUL) or untrusted (UNSUCCESSFUL) in the Original Country of Trust.

1.3.
The characteristics of a Trust-ok Token are specified in Annex 3. In particular, the Trust-ok Token consists of two parts (the token data and the report) as outlined below:

- The content of the report has to be mapped to the content of the token data.
- Based on the content of this report, an assessment must be given about whether or not the document is trusted by the sending party of this Agreement (SUCCESSFUL or UNSUCCESSFUL) in accordance with its policies.

1.4.
There are Signature-based and Authentication-based Advanced Electronic Systems.

- When using a Signature-based Advanced Electronic System the token data must also (i) contain information on whether the signature has been validated successfully, (ii) indicate whether a Qualified Electronic Signature or an Advanced Electronic Signature was applied and (iii) indicate the name of the signatory.

- When using an Authentication-based Advanced Electronic System the token data must also contain information on the identity of the User and on the authentication mechanisms applied by the system.

1.5.
Each Sending Party undertakes to issue a Trust-ok Token for any Document sent via its Sending Gateway.

2. National Contact points

2.1.
The Parties agree and undertake to use all their best efforts to cooperate effectively and in a timely way to strengthen the functioning of the e-CODEX System.

2.2.
For this purpose, the Parties undertake to appoint Contact Points who shall be responsible for operational and technical matters related to or in connection with the functioning of the e-CODEX System.

3. Reliability and Availability

3.1.
The Sending Connector and the Sending Gateway and the Receiving Gateway and the Receiving Connector must meet the requirements set out in Annex 4.

3.2.
The Parties undertake to set up their Gateways within the e-CODEX System and to communicate and exchange information in order to avoid any risks associated with non-receiving or non-sending of Messages or the partial or total failure of the e-CODEX System. Particularly each Party must inform the e-CODEX Coordinator and the other Parties without undue delay about any changes to or incidents at its Connectors, Gateways or Advanced Electronic Systems which lead or have led to a default of their obligations in meeting the requirements set out in this Agreement or which may otherwise have an adverse effect on the reliability of the Circle of Trust.

3.3.
For each Message, each of the Sending Connector and the Receiving Connector shall issue Time Evidences as further detailed in Annex 5 in order to allow the Sender and the Recipient to identify the points of time that are legally relevant.

3.4.
The Parties will agree on measures to avoid risks of system failure.

4. Effects of the Trust-ok Token

Upon receipt of a Message from the Sending Gateway, the Receiving Gateway shall forward the Message to the Receiving Connector without requesting further authentication from the Sender. The Receiving Connector shall process the Message in accordance with the laws of the Receiving State. In relation to the Sending Party, the Receiving State shall have no obligation to carry out a verification of the authenticity and integrity of the Document(s) but may rely on the information provided by the Trust-ok Token.

e CODEX making justice faster.eu

5. Data Protection and Security Issues

The Parties, through their Contact Points and in compliance with data protection laws at European and national level, shall adopt all necessary technical and organisational measures to guarantee personal data security and prevent the alteration or loss of, or unauthorised processing of or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).

Such measures in the application of the criminal pilot should address as a minimum the provisions of Council Framework Decision 2008/977/JHA[2], Art 22 § 2.

6. Amendments

Any amendments to this Agreement (including its Annexes) require the prior approval of the e-CODEX General Assembly.

They enter into force with binding effect for all Parties two months after the approval by the e-CODEX General Assembly. The Parties' right to terminate their participation pursuant to Art. 7 remains unaffected.

However, amendments to Annex 1 do not require the approval of the e-CODEX General Assembly. The e-CODEX Coordinator will, without undue delay, maintain Annex 1 and inform existing Parties of the accession of any new Party or the termination by a Party.

7. Termination

If a Party wants to stop participating in one or more of the pilots it must inform the e-CODEX Coordinator at least one month in advance. Two months after having declared so, the Party will not be bound any more to this Agreement for such pilot(s).

---

2 To be replaced by the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:HTML

e CODEX making justice faster.eu

Annex 1 to the Agreement on a Circle of trust

List of Parties who have acceded to this Agreement

(This list will be maintained by the Coordinator.)

e CODEX making justice faster.eu

Annex 2 to the Agreement on a Circle of trust

Authentication-based Advanced Electronic System

An Authentication-based Advanced Electronic System is an electronic system as outlined in Article 1.2.1. of the Agreement (Advanced Electronic System) which meets the following requirements:

Registration

All users have to undergo a registration process requiring identification. For specific roles e.g. lawyers, notaries, the registration process checks with the help of the organisation legally representing this user-group (e.g. national bar association), if the user is really a member of this user-group.

Authenticity

The user is (b) authenticated using an electronic software- certificate plus user-id and password. So the system can (a) uniquely link each created document to the sending user. All documents are created (c) with means, which are under the control of the user (using the own IT-System of the user).

Integrity

The user's system is connected via a Clearing House to the national electronic filing system. A Clearing House has to undergo a certification procedure by or on behalf of or supervised by the Member State's authorities before interconnecting to the National Electronic Legal Communication System (i.e. the national electronic communication system provided by the respective Member State for communication with the courts and linked to the National Connector).

The connections between the user's system and the Clearing House and the connection between the Clearing House and the central components of the National Electronic Legal Communication System are encrypted and secured by electronic certificates. Both the Clearing House and the central components log the whole content of the incoming and outgoing messages at the earliest possible time immediately after receipt resp. before sending. The logs of the Clearing House together with the logs of the Electronic Legal Communication system ensure to follow the trace of any document sent. The logs of the Clearing House and of the central components must be kept at least for 3 months from the date of the message.

Validation modules with extensive checks at the receiving side make sure that only valid applications are received by the courts.

Any subsequent change of a document can be at least manually detected by comparing the messages logged at the sender and receiver side.

e CODEX making justice faster.eu

Annex 3 to the Agreement on a Circle of trust

Characteristics of the Trust-ok Token

General

The "Trust-OK"-Token will be a PDF-File generated by the sending Connector to provide a human readable document. It contains either the result of the signature and certificate validation or information regarding the authentication process of the user. Additionally, a machine readable form (XML file) will be generated to support future developments.

Content

The token itself will be divided into three parts:

- The first part consists of basic information necessary for the receiving party to recognise documents as trustworthy which includes information on the advanced electronic system and an evaluation of the legal trust level. The legal trust level is stated either as "successful" or "unsuccessful".
- The second part gives a technical assessment of the documents signature (signature-based advanced electronic system) or the authentication information (authentication-based advanced electronic system). This assessment consists of a standardised summary of the original validation data and a technical trust level based on this summary. Furthermore, it displays the results as traffic lights:
  - **For an signature-based advanced electronic system:**
    - Green: The document has been signed with a Qualified or an Advanced Electronic Signature and every necessary validation has been passed.
    - Orange: The document has been signed with a valid Qualified or Advanced Electronic Signature. Within the process of validation, not every service for the validation was accessible, e.g. due to technical problems.
    - Red: The document has not been signed or the signature is invalid.
  - **For an authentication-based advanced electronic system:**
    - Green: The document originates from an authentication-based advanced electronic system, which has authenticated the sender successfully.
    - Red: In any other case.
- The third part will be made of the original validation report provided by either the national solution itself or by the DSS validation tool.

All in all the "Trust OK"-Token will contain:

- Information on the used advanced electronic system
- Information on the time the documents have been filed Basic Information on applied signatures and used certificates or the identity of the user

- Evaluation of the technical trust level (red / orange / green)
- Evaluation of the legal trust level (successful / unsuccessful)
- Original validation report provided by the national solution or the DSS validation tool

Human Readable Token (PDF)

As mentioned above, the human readable token will consist of three parts.

The first part presented on the first page of the actual token includes general information on the advanced electronic system and a legal assessment of the business document. In addition, a national disclaimer and a "validation stamp" showing the legal validation result (successful/unsuccessful) are shown at the bottom of the page.

The second page provides a standardised technical overview of the information from the original validation report -. Depending on the Advanced Electronic System (authentication- or signature-based), the information given by the technical overview varies.

Similar to the first page, the bottom of this page consists of a stamp in the color of the documents technical validation result (green/orange/red) and a short description, e.g. providing additional information about why a document received a orange technical assessment.

The third part of the document consists of the original validation report as it has been created by the issuing member states' validation software.

Machine Readable Token (XML)

This paragraph provides the XML schema that defines the structure of the XML version of the "Trust Ok"-Token.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">

<xsd:element name="TrustOkToken" type="TokenType" />

<xsd: simpleType name="AdvancedSystemEnum">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Signature-based" />
        <xsd:enumeration value="Authentication-based" />
    </xsd:restriction>
```

```
</xsd:simpleType>

<xsd:simpleType name="TechnicalTrustLevelEnum">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="FAIL" />
        <xsd:enumeration value="SUFFICIENT" />
        <xsd:enumeration value="SUCCESSFUL" />
    </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="LegalTrustLevelEnum">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="SUCCESSFUL" />
        <xsd:enumeration value="NOT_SUCCESSFUL" />
    </xsd:restriction>
</xsd:simpleType>

<xsd: complexType name="IssuerType">
    <xsd:sequence>
        <xsd:element name="ServiceProvider" type="xsd:string" />
        <xsd:element name="Country" type="xsd:string" />
        <xsd:element name="AdvancedElectronicSystem" type="AdvancedSystemEnum" />
    </ xsd:sequence>
</xsd: complexType>

<xsd:complexType name=" DocumentType">
    <xsd:sequence>
        <xsd:element name="Filename" type="xsd:string" />
        <xsd:element name="Type" type="xsd:string" />
        <xsd:element name="Digest" type="xsd:string" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name=" SourceType ">
    <xsd:sequence>
        <xsd:any minOccurs="0" maxOccurs="unbounded" />
    </xsd:sequence>
```

e CODEX making justice faster.eu

```
</xsd: complexType>

<xsd:complexType name="SignatureInformationType">
    <xsd:sequence>
        <xsd:element name="SignatureVerification" type="xsd:boolean" />
        <xsd:element name="StructureVerification" type="xsd:boolean" />
        <xsd:element name="SignatureFormat" type="xsd:string" />
        <xsd:element name="SignatureLevel" type="xsd:string" minOccurs="0" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="CertificateInformationType">
    <xsd:sequence>
        <xsd:element name="Issuer" type="xsd:string" />
        <xsd:element name="CertificateVerification" type="xsd:boolean" />
        <xsd:element name="ValidityAtSigningTime" type="xsd:boolean" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="AuthenticationInformationType">
    <xsd:sequence>
        <xsd:element name="IdentityProvider" type="xsd:string" />
        <xsd:element name="UsernameSynonym" type="xsd:string" />
        <xsd:element name="TimeOfAuthentication" type="xsd:dateTime" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="SignatureDataType">
    <xsd:sequence>
        <xsd:element name="SigningTime" type="xsd:dateTime" />
        <xs:element name="SignatureInformation" type="SignatureInformationType" />
        <xs:element name="CertificateInformation" type="CertificateInformationType" />
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="VerificationDataType">
    <xsd:choice>
```

```
            <xsd:sequence>
                <xsd:element name="SignatureData" type="SignatureDataType"
minOccurs="1" />
                <xsd:element name="AuthenticationData"
type="AuthenticationInformationType" minOccurs="0" />
            </xsd:sequence>
            <xsd:sequence>
                <xsd:element name="SignatureData" type="SignatureDataType"
minOccurs="0" />
                <xsd:element name="AuthenticationData"
type="AuthenticationInformationType" minOccurs="1" />
            </xsd:sequence>
        </xsd:choice>
</xsd:complexType>

<xsd:complexType name="TechnicalResultType">
    <xsd:sequence>
        <xsd:element name="TrustLevel" type="TechnicalTrustLevelEnum" />
        <xsd:element name="Comments" type="xsd:string" minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="LegalResultType">
    <xsd:sequence>
        <xsd:element name="TrustLevel" type="LegalTrustLevelEnum" />
        <xsd:element name="Disclaimer" type="xsd:string" minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ValidationType">
    <xsd:sequence>
        <xs:element name="VerificationTime" type="xsd:dateTime" />
        <xs:element name="VerificationData" type="VerificationDataType" />
        <xs:element name="Result" type="ResultType" />
        <xs:element name="OriginalValidationReport" type="SourceType" />
    </xsd:sequence>
</xsd: complexType>
```

```
<xsd:complexType name="TokenType">
    <xsd:sequence>
        <xsd:element name="Issuer" type="IssuerType" />
        <xsd:element name="Document" type="DocumentType“ />
        <xsd:element name="Validation" type="ValidationType“ />
    </xsd:sequence>
</xsd:complexType>

</xsd:schema>
```

e CODEX making justice faster.eu

Annex 4 to the Agreement on a Circle of trust

Requirements for Connectors

Set up of a Connector

A Connector needs to be set up in a secure and protected domain. The Connector has to use an electronic certificate provided by an official trust authority (officially accredited trust service provider of the respective state) for signing the ASICS container which is sent from the Connector to the Gateway(s). The certificate shall be compliant to the X.509 standard.

The underlying operating system has to be kept up to date with regard to necessary updates and patches, especially those with regard to security.

Authenticity and Integrity

The Receiving Connector has to process the document(s) and the Trust-ok Token in accordance with the laws of the Receiving State.

Only authorized and authenticated persons (by means of a strong and properly administered user-Id and password) must have access to the Connector.

The operating authority of a Connector must monitor the performance of their Connector as established by their normal business hours. In case of any failure the operating authority must put into place measures to address this failure as fast as is reasonably possible.

Requirements for Gateways

Set up of a Gateway

An e-CODEX Gateway needs to be set up in a secure and protected domain. Only dedicated point to point internet connections secured by electronic certificates provided by an official trust authority between 2 Gateways must be allowed. The certificates shall be compliant to the X.509 standard.

The recommended software of the Gateway is the one provided by the e-CODEX project published via http://joinup.ec.europa.eu/. The operating authority has to take care that the Gateway is always updated according to the published software version of the Gateway.

The underlying operating system has to be kept up to date with regards to necessary updates and patches, especially those with regards to security.

Authenticity and Integrity

The exchange of Messages and other information between the Gateways has to be done encrypted by SSL encryption. An e-CODEX Gateway has to be monitored by the operating authority so that any risk of non-receiving, non-sending of a Message and any risk of data loss can be avoided.

Only authorized and authenticated persons (by means of a strong and properly administered user-Id and password) must have access to the Gateway.

The operating authority of a Gateway must monitor performance of their Connector as established by their normal business hours. In case of any failure the operating authority must put into place measures to address this failure as fast as is reasonably possible.

e CODEX making justice faster.eu

Annex 5 to the Agreement on a Circle of trust

List of Time Evidences

- The description of the time evidences may include:
  - **What** XML, PDF, or any other electronic support of the time evidence
  - **Why** the fact that triggers the time evidence production
  - **When** the moment or step of the process at which the time evidence is generated
  - **Where** the point in which the time evidence is created (system, application...)
  - **Who** electronic (or even human) actor accountable for the time evidence
  - **How** a short explanation of the way the time evidence is produced
- e-CODEX time evidences are generated by the Sending or Receiving Connector (in particular by the EvidenceBuilder) based on the ETSI REM standard

List of time evidences

Details given in this list are: the name of the evidence in the technical workflow; detail description in form of What, Why, When, Where, Who and How; what happen if the evidence is positive ☑ or negative ☒.

Submission Evidence // SubmissionAcceptanceRejection()

- **What** REM ETSI evidence
- **Why** the Message has been successfully processed (transformation, AsicsContainer and TrustOkToken) in order to be sent by the Sending Connector
- **When** a Message is first received by the Sending Connector
- **Where** EvidenceBuilder module of the Sending Connector
- **Who** Owner of the Sending Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [SubmissionAcceptance] It is (1) added to the Message to be submitted from the Sending Connector to the Sending Gateway and (2) sent to the Sender after the Message has been submitted to the Sending Gateway

☒ [SubmissionRejection] If there is an error it is only sent to the Sender immediately.

RelayREMMD Evidence // RelayREMMDAcceptanceRejection ()

- **What** REM ETSI evidence
- **Why** the Message has arrived at the Receiving Gateway (and Connector)
- **When** the Message has been received by the Receiving Connector
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [RelayREMMD Acceptance] confirm the arrival of the Message in the Receiving Connector

☒ [RelayREMMD Rejection] The Sending Connector starts a timer at the moment of sending the message. If the period of time expired without receiving a RelayREMMD Acceptance from the Receiving Connector, a Relay REMMD Rejection is generated.

Delivery Evidence // DeliveryNonDeliveryToRecipient ()

- **What** REM ETSI evidence
- **Why** the Message has been delivered to the Recipient's mailbox
- **When** after the Message has arrived in the Recipient's mailbox and corresponding evidence from the national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal (in each case if available) has been received.
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [deliveryEvidence Acceptance] the Message has been successfully delivered to the Recipient's mailbox

☒ [deliveryEvidence Rejection] the Message delivery to the Recipient's mailbox has not been achieved

Retrieval Evidence // RetrievalNonRetrievalToRecipient ()

- **What** REM ETSI evidence
- **Why** the the Recipient's national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal, communicates to the Receiving Connector that the Recipient has successfully retrieved – according to the applicable national rules – the message to the Recipient. This is when the Recipient really opens his mailbox.
- **When** according to the applicable national rules
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [retrievalEvidence Acceptance] the Recipient has successfully retrieved the Message.

☒ [retrievalEvidence Rejection] the Recipient has not been able to retrieve the Message

e-CODEX making justice faster.eu

Declaration of Accession:

The subscribing e-CODEX partner hereby declares to the e-CODEX Coordinator that he complies with the terms of this Agreement and its annexes for his e-CODEX piloting activities.

Name of legal entity: _____
(full name of the e-CODEX partner)

Name of legally authorised representative: _____
(written out in full)

Title of legally authorised representative: _____

Signature of legally authorised representative: _____

Place: _____ Date: _____

Stamp of the organisation:

– GV. NRW. 2022 S. 831

75

Verordnung über die Zuständigkeit zur Gewährung eines einmaligen Heizkostenzuschusses an Wohngeld beziehende Personen (Heizkostenzuschuss-Zuständigkeitsverordnung – HkzZVO)

Vom 5. Juli 2022

Auf Grund des § 3 Absatz 1 Satz 2 des Heizkostenzuschussgesetzes vom 29. April 2022 (BGBl. I S. 698) verordnet die Landesregierung:

§ 1
Zuständigkeit

Die Gemeinden sind zuständig für die Gewährung eines einmaligen Heizkostenzuschusses an den in § 1 Absatz 1 des Heizkostenzuschussgesetzes genannten Personenkreis.

§ 2
Inkrafttreten und Außerkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft. Sie tritt am 31. Mai 2032 außer Kraft.

Düsseldorf, 5. Juli 2022

Die Landesregierung Nordrhein-Westfalen

Der Ministerpräsident
Hendrik W ü s t

Für die Ministerin für Heimat, Kommunales, Bau und Digitalisierung
Der Minister des Innern
Herbert R e u l

– GV. NRW. 2022 S. 856

77

Änderung der Satzung über den Wasserverband Eifel-Rur

Vom 13. Dezember 2021

Die Verbandsversammlung hat aufgrund der §§ 10 Abs. 1, 11 und 14 Abs. 1 des Gesetzes über den Wasserverband Eifel-Rur (Eifel-RurVG) vom 7. Februar 1990 (GV. NW. S. 106), zuletzt geändert durch Artikel 26 des Gesetzes vom 1. Februar 2022 (GV. NRW. S. 122), am 13. Dezember 2021 beschlossen, die Satzung des Wasserverbandes Eifel-Rur vom 4. Oktober 1993 (GV. NRW. S. 976), zuletzt geändert durch Beschluss der Verbandsversammlung vom 9. Dezember 2019 (GV. NRW. 2020 S. 197), wie folgt zu ändern:

1. Dem § 6 wird folgender Absatz 5 angefügt:

   „Abstimmungen zu Beschlüssen und Wahlen sind in offener Form durchzuführen, solange kein Delegierter eine geheime Abstimmung oder Wahl beantragt. Der Antrag auf geheime Abstimmung oder Wahl muss zu Beginn des betreffenden Tagesordnungspunktes gestellt werden."

2. Nach § 6 werden folgender § 6a und § 6b eingefügt:

   „**§ 6 a**

   Virtuelle Verbandsversammlung (§ 15 Abs. 11 Eifel-RurVG)

   (1) Für den Fall, dass unter den Voraussetzungen des § 15 Abs. 11 Eifel-RurVG eine Verbandsversammlung als virtuelle Verbandsversammlung stattfindet, wird diese über ein vom Vorstand zu bestimmendes Videokonferenzsystem durchgeführt, das den Anforderungen nach § 15 Abs. 11 Satz 1 Ziff. 1 bis 3 Eifel-RurVG entspricht. Dieses System soll verfügbar sein, ohne zusätzliche Software installieren zu müssen.

   (2) Der Verband stellt das System zur Verfügung und gewährleistet seine generelle Funktionsfähigkeit. Er übernimmt keine Gewähr dafür, dass der individuelle technische Zugang zu diesem System, wie etwa eine ausreichende Übertragungsbandbreite, im Einzelfall möglich ist. Erforderliche Hard- oder Software zur Ermöglichung der Sitzungsteilnahme wird vom Verband nicht zur Verfügung gestellt.

   (3) In der Einladung zu der virtuellen Verbandsversammlung ist den Delegierten und den Vertretern nach § 15 Abs. 8 Eifel-RurVG der Internet-Link zu der virtuellen Verbandsversammlung einschließlich der entsprechenden Zugangsdaten mitzuteilen. Die Delegierten und die Vertreter nach § 15 Abs. 8 Eifel-RurVG haben diese Zugangsdaten vertraulich zu behandeln.

   (4) Die Beteiligung der Öffentlichkeit erfolgt in der Weise, dass Interessierte den öffentlichen Teil der Verbandsversammlung über einen Live-Stream verfolgen können, wenn sie sich über die Homepage des WVER hierzu angemeldet haben, und ihnen der Internet-Link sowie die Zugangsdaten zur Verfügung gestellt wurden. Die Möglichkeit der Beteiligung der Öffentlichkeit wird in dem Bekanntmachungstext über die Sitzung der Verbandsversammlung kenntlich gemacht. Soweit nach § 6 Abs. 2 dieser Satzung in der Verbandsversammlung Angelegenheiten behandelt werden, die nicht öffentlich sind, wird bei der Behandlung dieser Tagesordnungspunkte der Live-Stream unterbrochen.

   § 6 b

   Beschlussfassung und Wahlen im Umlaufverfahren (§ 15 Abs. 12 Eifel-RurVG)

   (1) Für den Fall, dass unter den Voraussetzungen des § 15 Abs. 11 Eifel-RurVG anstelle einer virtuellen Verbandsversammlung eine Beschlussfassung oder Wahlen der Delegierten im Wege eines Umlaufverfahrens durch schriftliche Stimmabgabe gemäß § 15 Abs. 12 Eifel-RurVG erfolgen sollen, fragt die oder der Vorsitzende des Verbandsrates in einem kombinierten Abstimmungsvorgang zunächst das Einverständnis der Delegierten zu diesem Vorgehen ab. Sodann erfolgt – unter dem Vorbehalt, dass mindestens die Hälfte der Delegierten ihr Einverständnis zur schriftlichen Stimmabgabe erklärt hat – eine schriftliche Stimmabgabe in der Sache.

   (2) Die Abfrage des Einverständnisses zur Durchführung des Umlaufverfahrens und die Stimmabgabe auf schriftlichem Weg erfolgen in der Weise, dass den Delegierten die Einverständniserklärung und die Beratungsunterlagen einschließlich der Stimmabgabezettel auf postalischem Weg übermittelt werden. Die Stimmabgabezettel sind in einem vom Verband zur Verfügung gestellten frankierten Rückumschlag innerhalb einer Frist von zwei Kalenderwochen an die oder den Vorsitzenden des Verbandsrates zurückzusenden.

   (3) Nach Ablauf der in Abs. 2 genannten Frist stellt die oder der Vorsitzende des Verbandsrates zunächst fest, ob sich mindestens die Hälfte der Delegierten mit der Durchführung des Umlaufverfahrens einverstanden erklärt hat. Im Anschluss an diese Feststellung stellt die oder der Vorsitzende gegebenenfalls das Ergebnis der Beschlussfassung bzw. der Wahlen fest und unterrichtet die Delegierten und die Vertreter nach § 15 Abs. 8 Eifel-RurVG innerhalb von zwei Kalenderwochen nach Ablauf der in Abs. 2 genannten Frist über die festgestellten Ergebnisse."

3. Nach § 9 werden folgende §§ 9a, 9b und 9c eingefügt:

   „**§ 9 a**

   Sitzungen des Verbandsrates (§ 18 Eifel-RurVG)

   (1) Die Sitzungen des Verbandsrates sind grundsätzlich nicht öffentlich.

(2) Über Gegenstände, die nicht auf der mit der Einladung versandten Tagesordnung stehen, aber keinen Aufschub dulden, kann nur mit Zustimmung der Mehrheit der anwesenden Mitglieder beraten und beschlossen werden.

(3) Abstimmungen zu Beschlüssen und Wahlen sind in offener Form durchzuführen, solange kein Mitglied eine geheime Abstimmung oder Wahl beantragt. Der Antrag auf geheime Abstimmung oder Wahl muss zu Beginn des betreffenden Tagesordnungspunktes gestellt werden.

§ 9 b

Virtuelle Verbandsratssitzung (§ 18 Abs. 8 Eifel-RurVG)

Für den Fall, dass unter den Voraussetzungen des § 15 Abs. 11 Eifel-RurVG eine virtuelle Verbandsratssitzung stattfindet, wird diese über ein vom Vorstand zu bestimmendes Konferenzsystem durchgeführt, das den Anforderungen nach § 15 Abs. 11 Satz 1 Ziff. 1 bis 3 Eifel-RurVG entspricht, wobei auf eine Bildübertragung verzichtet werden kann. Das Konferenzsystem soll verfügbar sein, ohne zusätzliche Software installieren zu müssen. § 6 a Abs. 2 und 3 gelten entsprechend.

§ 9 c

Beschlussfassung und Wahlen im Umlaufverfahren (§ 18 Abs. 8 Eifel-RurVG)

(1) Für den Fall, dass unter den Voraussetzungen des § 15 Abs. 11 Eifel-RurVG anstelle einer virtuellen Verbandsratssitzung eine Beschlussfassung oder Wahlen im Wege eines Umlaufverfahrens durch schriftliche Stimmabgabe gemäß § 18 Abs. 12 Eifel-RurVG erfolgen sollen, fragt die oder der Vorsitzende des Verbandsrates in einem einheitlichen Abstimmungsvorgang zunächst das Einverständnis der Mitglieder zu diesem Vorgehen ab. Sodann erfolgt – unter dem Vorbehalt, dass mindestens Zweidrittel der Mitglieder ihr Einverständnis zur schriftlichen Stimmabgabe erklärt hat – eine schriftliche Stimmabgabe in der Sache.

(2) Die Abfrage des Einverständnisses zur Durchführung des Umlaufverfahrens und die Stimmabgabe auf schriftlichem Weg erfolgen in der Weise, dass den Mitgliedern die Einverständniserklärung und die Beratungsunterlagen einschließlich der Stimmabgabezettel auf postalischem Weg übermittelt werden. Die Stimmabgabezettel sind in einem vom Verband zur Verfügung gestellten vorfrankierten Rückumschlag innerhalb einer Frist von zwei Kalenderwochen an die oder den Vorsitzenden des Verbandsrates zurückzusenden.

(3) Nach Ablauf der in Abs. 2 genannten Frist stellt die oder der Vorsitzende des Verbandsrates zunächst fest, ob sich mindestens Zweidrittel der Mitglieder mit der Durchführung des Umlaufverfahrens einverstanden erklärt hat. Im Anschluss an diese Feststellung stellt sie oder er gegebenenfalls das Ergebnis der Beschlussfassung bzw. der Wahlen fest und unterrichtet die Mitglieder innerhalb von zwei Kalenderwochen nach Ablauf der in Abs. 2 genannten Frist über die festgestellten Ergebnisse.“

Hinweis

Es wird darauf hingewiesen, dass eine Verletzung von Verfahrens- und Formvorschriften des Eifel-RurVG gegen die Satzung nach Ablauf eines Jahres seit dieser Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn,

a) eine vorgeschriebene Genehmigung fehlt,

b) die Satzung ist nicht ordnungsgemäß öffentlich bekannt gemacht worden,

c) der Vorstand hat den Beschluss der Verbandsversammlung vorher beanstandet oder

d) der Form- oder Verfahrensmangel ist gegenüber dem Verband vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt.

Genehmigung

Die vorstehende Satzungsänderung wurde vom Ministeriums für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen mit Schreiben vom 13. Juni 2022, Az.: IV-1 61.01.04.03, gemäß § 11 Abs. 2 Eifel-RurVG genehmigt.

Düren, den 22. Juni 2022

Wasserverband Eifel-Rur
Der Vorstand
Dr. Joachim R e i c h e r t

– GV. NRW. 2022 S. 856

Einzelpreis dieser Nummer 6,20 Euro
zuzügl. Porto- und Versandkosten

Bestellungen, Anfragen usw. sind an den A. Bagel Verlag zu richten. Anschrift und Telefonnummer wie folgt für
Abonnementsbestellungen: Grafenberger Allee 82, Fax (02 11) 96 82/2 29, Tel. (02 11) 96 82/2 38 (8.00–12.30 Uhr), 40237 Düsseldorf

Bezugspreis halbjährlich 38,50 Euro (Kalenderhalbjahr). Jahresbezug 77,– Euro (Kalenderjahr), zahlbar im Voraus. Abbestellungen für Kalenderhalbjahresbezug müssen bis zum 30. 4. bzw. 31. 10., für Kalenderjahresbezug bis zum 31. 10. eines jeden Jahres beim A. Bagel Verlag vorliegen.
Reklamationen über nicht erfolgte Lieferungen aus dem Abonnement werden nur innerhalb einer Frist von vier Wochen nach Erscheinen anerkannt.

In den Bezugs- und Einzelpreisen ist keine Umsatzsteuer i. S. d. § 14 UStG enthalten.

Einzelbestellungen: Grafenberger Allee 82, Fax (02 11) 96 82/2 29, Tel. (02 11) 96 82/2 41, 40237 Düsseldorf

Von Vorabeinsendungen des Rechnungsbetrages – in welcher Form auch immer – bitten wir abzusehen. Die Lieferungen erfolgen nur auf Grund schriftlicher Bestellung gegen Rechnung. Es wird dringend empfohlen, Nachbestellungen des Gesetz- und Verordnungsblattes für das Land Nordrhein-Westfalen möglichst innerhalb eines Vierteljahres nach Erscheinen der jeweiligen Nummer beim A. Bagel Verlag vorzunehmen, um späteren Lieferschwierigkeiten vorzubeugen. Wenn nicht innerhalb von vier Wochen eine Lieferung erfolgt, gilt die Nummer als vergriffen. Eine besondere Benachrichtigung ergeht nicht.

Herausgeber: Im Namen der Landesregierung, das Ministerium des Innern NRW, Friedrichstr. 62–80, 40217 Düsseldorf.

Herstellung und Vertrieb im Namen und für Rechnung des Herausgebers: A. Bagel Verlag, Grafenberger Allee 82, 40237 Düsseldorf

Druck: TSB Tiefdruck Schwann-Bagel, Düsseldorf und Mönchengladbach

ISSN 0177-5359