

Anlage 3:

**Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische
Maßnahmen**

betreffend die OZG-Verwaltungsleistung:

**Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm
(OZG-Leistung: Förderung ehrenamtlicher Tätigkeit)**

Zwischen der

- nachstehend „**Auftraggeber**“ genannt –
(Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO)

und

d-NRW AöR

vertreten durch Dr. Roger Lienenkamp

Freie-Vogel-Str. 387
44269 Dortmund

- nachstehend „**Auftragnehmer**“ genannt –
(Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO)

- beide nachstehend gemeinsam „**Vertragsparteien**“ genannt -

Präambel

Zwischen dem Auftraggeber (Leistungsbezieher gem. der Rahmenvereinbarung zur Nachnutzung von OZG-Verwaltungsleistungen über den Kommunalvertreter.NRW) und dem Auftragnehmer (Leistungserbringer, Kommunalvertreter gem. der Rahmenvereinbarung zur Nachnutzung von OZG-Verwaltungsleistungen über den Kommunalvertreter.NRW) wird mit Vertragsschluss des Einzelabrufs die folgende Vereinbarung zur Auftragsverarbeitung (auch Klauseln) zum Einzelabruf für den Bezug einer OZG-Verwaltungsleistung (094-24-073) betreffend die OZG-Verwaltungsleistung „Förderung ehrenamtlicher Tätigkeit“: als Anlage 3 (nachstehend „**Einzelabruf**“) geschlossen.

Die OZG-Verwaltungsleistung „Förderung ehrenamtlicher Tätigkeit“ besteht aus zwei Komponenten, nämlich aus der mobilen Anwendung „Ehrenamtskarte“ (auch „App“) und dem dazugehörigen Verwaltungsprogramm. Die mobile Anwendung „Ehrenamtskarte“ stellt ein länderübergreifender Onlinedienst i.S.v. §§ 8a Abs. 1, 2 Abs. 8 OZG dar und dient u.a. der Ausfüllung, Zwischenspeicherung, Übermittlung der Anträge an die jeweils zuständige Stelle (sog. Antragservice). Das Verwaltungsprogramm ist aus technischer Sicht ein Online-Dienst, der das Fachverfahren abbildet, und gilt somit nicht als ein länderübergreifender Onlinedienst i.S.v. §§ 8a Abs. 1, 2 Abs. 8 OZG. Die vorliegende Vereinbarung zur Auftragsverarbeitung bezieht sich ausschließlich auf das Verwaltungsprogramm.

Die Vertragsparteien bezwecken mit dieser Vereinbarung zur Auftragsverarbeitung das datenschutzrechtliche Verhältnis zwischen dem Auftraggeber (Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO) und dem Auftragnehmer (Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO) für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm“ der OZG-Verwaltungsleistung „Förderung ehrenamtlicher Tätigkeit“, der als Fachverfahren gilt, im Hinblick auf die Vorgaben der europäischen Datenschutz-Grundverordnung („DSGVO“), des Bundesdatenschutzgesetzes („BDSG“) des Datenschutzgesetzes Nordrhein-Westfalen („DSG NRW“) sowie der ggf. weiteren einschlägigen Landesdatenschutzgesetze in der jeweils gültigen Fassung zu konkretisieren. Der Auftraggeber setzt das Verwaltungsprogramm zum Zwecke der Durchführung des Verfahrens gem. § 8a Abs. 4 S. 2 OZG ein.

Vor diesem Hintergrund vereinbaren die Vertragsparteien was folgt.

§ 1 Zweck und Anwendungsbereich

- a) Mit dieser Vereinbarung zur Auftragsverarbeitung soll die Einhaltung von Art. 28 Abs. 3, 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) sichergestellt werden.
- b) Der Auftraggeber und der Auftragnehmer haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 3, 4 DSGVO zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang I.
- d) Die Anhänge I bis III sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Auftraggeber und der Auftragnehmer gemäß der DSGVO unterliegen.

§ 2 Änderungen der Vereinbarung zur Auftragsverarbeitung

a) Änderungen dieser Vereinbarung zur Auftragsverarbeitung sind nur durch ausdrückliche, übereinstimmende, beweissicher dokumentierte Erklärungen beider Parteien in Textform zulässig. Soweit in dieser Vereinbarung von Textform die Rede ist, ist Textform gem. § 126b BGB gemeint.

b) Dies hindert die Parteien nicht daran, diese Vereinbarung in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden. Insoweit sind die Parteien auch nicht daran gehindert, Verträge neben dieser Vereinbarung zur Auftragsverarbeitung zu schließen.

§ 3 Auslegung

a) Werden in diesen Klauseln, die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

§ 4 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Verträge, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

§ 5 Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Auftraggebers verarbeitet werden, sind in Anhang I aufgeführt.

§ 6 Weisungsbefugnisse des Auftraggebers

a) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung (Textform) des Auftraggebers, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftraggeber kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass vom Auftraggeber erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber mit mindestens 14-tägiger Frist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

c) Der Auftraggeber setzt dem Auftragnehmer eine angemessene Frist zur Umsetzung der Weisungen. Er wird bei der Fristsetzung und Abfassung seiner Weisungen berücksichtigen, dass der Auftragnehmer Weisungen anderer Auftraggeber unterliegen kann, und anstreben, sich, unbeschadet seiner gesetzlichen Rechte, mit anderen Auftraggebern abzustimmen.

d) Sollte der Auftragnehmer wider Erwarten eine Weisung des Auftraggebers nicht innerhalb der gesetzten Frist umsetzen können, ist er verpflichtet, den Auftraggeber unverzüglich hierüber mit Angabe ihn verhindernder Gründe zu informieren.

e) Der Auftraggeber hat hinsichtlich der Datenverarbeitung ein umfassendes Weisungsrecht. Mündliche Weisungen sind unverzüglich in einem elektronischen Format zu bestätigen. Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind zwischen den Parteien abzustimmen und zu dokumentieren. Weisungsberechtigt sind dabei die zeichnungsbefugten Angehörigen der gemäß Geschäftsverteilungsplan zuständigen Organisationseinheit des Auftraggebers.

§ 7 Zweckbindung

Der Auftragnehmer verarbeitet die personenbezogenen Daten nur für den/die in Anhang I genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Auftraggebers erhält.

§ 8 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragnehmer nur für die in Anhang II angegebene Dauer verarbeitet.

§ 9 Ort der Verarbeitung personenbezogener Daten

a) Die Verarbeitung der personenbezogenen Daten aus dem Anhang I durch den Auftragnehmer findet ausschließlich in Mitgliedstaaten der Europäischen Union ("EU") oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum ("EWR") statt. Eine Datenverarbeitung außerhalb der EU oder des EWR, auch im Wege der Gewährung des Zugriffs auf die Daten, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Datenverarbeitung in Ländern, die weder Mitgliedstaat der EU oder Vertragsstaat des EWR sind (nachfolgend „Drittländer“ genannt) dürfen nur dann und soweit erfolgen, dass die Voraussetzungen der Art. 44 ff. DSGVO zur Zufriedenheit des Auftraggebers erfüllt sind.

§ 10 Sicherheit der Verarbeitung

a) Der Auftragnehmer ergreift mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung dieser Vereinbarung unbedingt erforderlich ist. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

c) Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

§ 11 Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragnehmer bearbeitet Anfragen des Auftraggebers bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Auftraggebers gestattet der Auftragnehmer ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Auftraggeber einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.

Der Nachweis solcher Maßnahmen, die nicht nur die vorliegende Vereinbarung zur Auftragsverarbeitung betreffen, sondern das Datenschutzniveau beim Auftragnehmer im Allgemeinen, kann erfolgen durch

- 1. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- 2. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, insbesondere solche gemäß Art. 42 DSGVO;
- 3. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- 4. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

d) Der Auftraggeber kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragnehmers umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt. Der Auftraggeber wird seine Prüftätigkeiten und Inspektionen mit Auftraggebern gleicher oder vergleichbarer Verarbeitungstätigkeiten mit Unterstützung des Auftragnehmers abstimmen, um die Belastung für die Geschäftsabläufe des Auftragnehmers zu begrenzen. Dies kann insbesondere auch die gemeinschaftliche Beauftragung eines unabhängigen Prüfers beinhalten. Der Auftragnehmer kann zu diesem Zweck den Kontakt zwischen Auftraggebern herstellen. Der Auftragnehmer ist berechtigt, Inspektionen mehrerer Auftraggeber zu einem Termin zusammenzufassen. Der Auftraggeber wird durch die vorstehenden Regelungen nicht in seinen Kontrollrechten beschränkt. Er kann jederzeit, insbesondere, wenn der Anlass der Kontrolle oder Risiken für betroffene Personen dies erforderlich machen, von einer Abstimmung mit anderen Auftraggebern absehen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Prüftätigkeiten und Inspektionen nicht häufiger als alle 12 Monate statt.

e) Die Parteien stellen den zuständigen Aufsichtsbehörden die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 12 Einsatz von Unterauftragsverarbeitern

a) Der Auftragnehmer besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern, die in Anhang III aufgeführt sind. Der Auftragnehmer unterrichtet den Auftraggeber mindestens sechs Wochen im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Auftraggeber damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände

gegen diese Änderungen erheben zu können. Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Beide Parteien müssen jederzeit den Nachweis führen können, welche Unterauftragsverarbeiter zu welchem Zeitpunkt genehmigt waren.

b) Beauftragt der Auftragnehmer einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Auftraggebers), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter und dessen Unterauftragsverarbeitern dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragnehmer gemäß diesen Klauseln gelten. Der Auftragnehmer stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragnehmer entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

c) Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragnehmer den Wortlaut der Untervergabevereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragnehmer haftet gegenüber dem Auftraggeber in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß der mit dem Auftragsverarbeiter geschlossenen Vereinbarung nachkommt. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

§ 13 Vertraulichkeit geschäftlicher Unterlagen

a) Die Parteien behandeln Unterlagen und Informationen, die sie im Rahmen dieser Vereinbarung erhalten, über § 10 dieser Vereinbarung hinaus auch dann vertraulich, wenn ihre Verarbeitung nicht Vereinbarungsgegenstand ist oder sie keinen Personenbezug aufweisen.

b) Diese Verpflichtungen bleiben auch nach Beendigung dieser Vereinbarung bestehen.

§ 14 Unterstützung des Auftraggebers

a) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Auftraggeber dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragnehmer die Weisungen des Auftraggebers.

c) Abgesehen von der Pflicht des Auftragnehmers, den Auftraggeber gemäß § 14 lit. b zu unterstützen, unterstützt der Auftragnehmer unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber zudem bei der Einhaltung der folgenden Pflichten:

1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Auftraggeber keine Maßnahmen zur Eindämmung des Risikos trifft;

3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragnehmer den Auftraggeber unverzüglich unterrichtet,

wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4. Verpflichtungen gemäß Art. 32 DSGVO: Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in Textform abstimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

d) Die Parteien legen in Anhang II die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Auftraggebers durch den Auftragnehmer bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

§ 15 Meldung von Verletzungen des Schutzes personenbezogener Daten

a) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat innerhalb von 24 Stunden nach Kenntnisaufnahme des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen.

Sie muss mindestens folgende Angaben enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

b) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach Art. 33 oder 34 DSGVO) auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der personenbezogenen Daten gem. Anhang I zu minimieren und zu beseitigen, die Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

c) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

§ 16 Haftung

- a) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- b) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Beschäftigten bzw. die von ihm mit der Durchführung dieser Vereinbarung Beauftragten oder die von ihm eingesetzten Unterauftragsverarbeiter im Zusammenhang mit der Erbringung der beauftragten Leistung schuldhaft verursachen.

§ 17 Löschen oder Rückgabe von personenbezogenen Daten

- a) Überlassene Daten(-sätze) und Datenträger verbleiben im Eigentum des Auftraggebers.
- b) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- c) Nach Beendigung dieser Vereinbarung löscht der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag des Auftraggebers verarbeiteten personenbezogenen Daten und bescheinigt dem Auftraggeber, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Auftraggeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser Klauseln. Der Auftragnehmer ist verpflichtet, die Rückgabe bzw. Löschung auch bei Unterauftragsverarbeitern herbeizuführen.
- d) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 18 Außerkrafttreten der zuvor geschlossenen Auftragsverarbeitungsverträge zum Online-Dienst

Mit Inkrafttreten dieser Vereinbarung zur Auftragsverarbeitung treten sämtliche zuvor zwischen den Parteien geschlossenen Auftragsverarbeitungsverträge im Zusammenhang mit der OZG-Leistung „Förderung ehrenamtlicher Tätigkeit“ außer Kraft und finden keine Anwendung mehr.

§ 19 Verstöße gegen die Klauseln und Beendigung der Vereinbarung zur Auftragsverarbeitung

- a) Falls der Auftragnehmer seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Auftraggeber – unbeschadet der Bestimmungen der DSGVO – den Auftragnehmer anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder die Vereinbarung beendet ist. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Der Auftraggeber ist berechtigt, diese Vereinbarung zur Auftragsverarbeitung zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 1. der Auftraggeber die Verarbeitung personenbezogener Daten durch den Auftragnehmer gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 2. der Auftragnehmer in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;

3. der Auftragnehmer einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.

c) Der Auftragnehmer ist berechtigt, diese Vereinbarung zu kündigen, soweit sie die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Auftraggeber auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragnehmer darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß § 6 lit. b verstoßen.

d) Diese Vereinbarung wird auf unbestimmte Zeit geschlossen. Sie kann von beiden Vertragsparteien jederzeit in Textform mit einer Frist von acht Monaten zum Ende eines Nachnutzungszeitraums beendet werden.

e) Die vorliegende Vereinbarung bleibt über das Ende der Hauptvereinbarung, Einzelabruf für den Bezug einer OZG-Verwaltungsleistung (094-24-073), hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

f) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

g) Diese Vereinbarung unterliegt deutschem Recht. Als Gerichtsstand wird der Sitz des Auftragnehmers bestimmt.

Anhänge:

Anhang I: Beschreibung der Datenverarbeitung für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Anhang II: Beschreibung der TOM für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Anhang III: Liste der Unterauftragsverarbeiter für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Ort, Datum, Unterschrift
Für den Auftraggeber

Ort, Datum, Unterschrift
Für den Auftragnehmer

Anhang I: Beschreibung der Datenverarbeitung für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Begriffsbestimmungen zur Darstellung der Datenverarbeitungen:

1. Verwaltungsprogramm ist ein digitaler Dienst, der zur Verwaltung von Antragsinformationen im Rahmen des Verfahrens „Ehrenamtskarte“ dient.
2. Webportal für Organisationsbestätigung ist aus technischer Sicht Teil des Verwaltungsprogramms. Über das Webportal wird die Bestätigung der Organisation eingeholt, dass die antragstellende Person die bei der Antragstellung auf Erteilung der Ehrenamtskarte angegebene ehrenamtliche Tätigkeit tatsächlich ausübt.

Bemerkungen:

Die als „gegebenenfalls“ ausgewiesenen Daten, werden verarbeitet, sofern diese vom Verantwortlichen und/oder den Betroffenen zur Verfügung gestellt werden.

Datenverarbeitungen:

1 Bearbeitung des Antrags auf Erteilung der Ehrenamtskarte im Verwaltungsprogramm

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Antragstellende,
- ggf. Erziehungsberechtigte,
- ggf. Ansprechpersonen der Organisation der ehrenamtlichen Tätigkeit

Kategorien personenbezogener Daten, die verarbeitet werden:

- Stammdaten,
- Adressdaten,
- Kontaktdaten,
- zeitlicher Umfang der ehrenamtlichen Tätigkeit,
- ehrenamtliche Tätigkeitsbereiche,
- weitere für Antragsbearbeitung relevante Informationen (Freitext),
- Angaben zur Organisation der ehrenamtlichen Tätigkeit,
- Angaben zur Wahrheitstreue,
- Auswahlmöglichkeit der Ehrenamtskarte per Post,
- ggf. Einwilligungen,
- Bestätigungen (bspw. keine Aufwandsentschädigung),
- Bearbeitungsstatus des Antrags,

- Informationen zur neu erteilten Ehrenamtskarte (bspw. Kartenummer),
- Angaben zur Gültigkeit der Ehrenamtskarte,
- Metadaten (bspw. Antrags-ID, Zeitpunkt des Antragseingangs ins Verwaltungsprogramm)

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Das Verfahren Ehrenamtskarte richtet sich nicht auf die Verarbeitung und/oder Auswertung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO aus. Unter bestimmten Umständen kann aber insbesondere die Bezeichnung der Organisation der ehrenamtlichen Tätigkeit indirekte Hinweise auf besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO liefern. Ob der Anwendungsbereich des Art. 9 DSGVO unter konkreten Umständen eröffnet ist, entscheidet der Verantwortliche.

Art der Verarbeitung:

- Im Verwaltungsprogramm steht der Antrag zur Bearbeitung zur Verfügung, insbesondere kann der Antrag durch den Verantwortlichen angesehen, genehmigt, abgelehnt, gespeichert, gelöscht werden. Sollte aus verschiedenen Gründen ein Antrag nicht auf dem elektronischen Wege gestellt werden können, so ist es immer noch möglich, den Antrag analog ins Verwaltungsprogramm aufzunehmen.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Die Daten werden zum Zwecke der Ermöglichung der Durchführung des Verfahrens zur Erteilung der Ehrenamtskarte verarbeitet.

Dauer der Verarbeitung:

- Die Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

2 Bearbeitung des Antrags zur Einbindung der analogen Ehrenamtskarte im Verwaltungsprogramm

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Antragstellende

Kategorien personenbezogener Daten, die verarbeitet werden:

- Stammdaten,
- Adressdaten,
- Kontaktdaten,
- Angaben zur Stelle, die Ehrenamtskarte erteilt hat,
- Angaben zur bestehenden Ehrenamtskarte,
- weitere für Antragsbearbeitung relevante Informationen,

- ggf. Einwilligungen,
- Bearbeitungsstatus des Antrags,
- Angaben zur Gültigkeit der Ehrenamtskarte,
- Metadaten (bspw. Antrags-ID, Zeitpunkt des Antragseingangs ins Verwaltungsprogramm)

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Im Verwaltungsprogramm steht der Einbindungsantrag zur Bearbeitung zur Verfügung, insbesondere kann er durch den Verantwortlichen angesehen, genehmigt, abgelehnt, gespeichert, gelöscht werden.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Die Daten werden zum Zwecke der Ermöglichung der Einbindung der analogen Ehrenamtskarte und der anschließenden Bereitstellung der digitalen Ehrenamtskarte verarbeitet.

Dauer der Verarbeitung:

- Die Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

3 Datenverarbeitungen bei Einholung der Organisationsbestätigung mittels des Webportals

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Antragstellende,
- ggf. Ansprechpersonen der Organisation der ehrenamtlichen Tätigkeit

Kategorien personenbezogener Daten, die verarbeitet werden:

- Es können personenbezogene Stammdaten und Kontaktdaten der Ansprechperson der Organisation verarbeitet werden, sofern die Daten von der Person, die das Formular zur Organisationsbestätigung ausfüllt, angegeben werden. Es können personenbeziehbare Metadaten von der Person, die das Formular zur Organisationsbestätigung ausfüllt, verarbeitet werden (bspw. Datum und Uhrzeit des Abrufs; Name des aufgerufenen Internetdienstes, der aufgerufenen Ressource und der verwendeten Aktion; IP-Adresse; Abfrage, die der Client gestellt hat; übertragene Datenmenge; Meldung, ob der Abruf erfolgreich war; Browser-Identifikation (enthält in der Regel die Browserversion sowie das Betriebssystem)). Es werden außerdem folgende Daten der auf Erteilung der Ehrenamtskarte antragsstellenden Person verarbeitet: Angaben zur Organisation der ehrenamtlichen Tätigkeit, Stammdaten, Adressdaten, zeitlicher Umfang der ehrenamtlichen Tätigkeit, weitere für Antragsbearbeitung relevante Informationen (Freitext).

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Das Verfahren Ehrenamtskarte richtet sich nicht auf die Verarbeitung und/oder Auswertung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO aus. Unter bestimmten Umständen kann aber insbesondere die Bezeichnung der Organisation der ehrenamtlichen Tätigkeit indirekte Hinweise auf besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO liefern. Ob der Anwendungsbereich des Art. 9 DSGVO unter konkreten Umständen eröffnet ist, entscheidet der Verantwortliche.

Art der Verarbeitung:

- Die antragstellende Person versendet in eigener Verantwortung eine in der mobilen Anwendung „Ehrenamtskarte“ verfügbare vorformulierte E-Mail an die Organisation, wo die ehrenamtliche Tätigkeit erbracht wird. Die E-Mail enthält u. a. einen Link zum Webportal des Verwaltungsprogramms, wo die Organisation die Angaben der antragstellenden Person bestätigen kann.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Die aufgrund der Einwilligung seitens der Ansprechperson der Organisation bereitgestellten Daten werden verarbeitet, um dem Verantwortlichen die Verwendung der Daten zur direkten Ansprache zu ermöglichen. Die Daten der Antragstellenden werden verarbeitet, um dem Verantwortlichen die Einholung der Organisationsbestätigung auf dem elektronischen Wege zu ermöglichen. Die Metadaten werden zur Bereitstellung der bestimmungsgemäßen Funktionalität des elektronischen Webportals verarbeitet.

Dauer der Verarbeitung:

- Die Metadaten werden gelöscht, sobald das Webportal geschlossen wird. Alle anderen Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

4 Statistische Auswertung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Antragstellende

Kategorien personenbezogener Daten, die verarbeitet werden:

- Bearbeitungsstatus des Antrags,
- Metadaten (bspw. Zeitpunkt des Antragseingangs ins Verwaltungsprogramm),
- ggf. Antragsdaten

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Die Anonymisierung erfolgt ohne menschliches Mitwirken, d.h. automatisch, durch die Komponente des Verwaltungsprogramms.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Anonymisierung der Daten zum Zwecke der Erstellung der statistischen Auswertungen.

Dauer der Verarbeitung:

- Personenbezogene Daten werden nur im Rahmen des Anonymisierungsvorgangs verarbeitet.

5 Nutzung des Verwaltungsprogramms im Rahmen der Aufgabenwahrnehmung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Nutzende des Verwaltungsprogramms, ggf. inkl. Beschäftigte des Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden:

- Anmeldedaten (bspw. E-Mail-Adresse, Passwort),
- Stammdaten,
- Kontaktdaten,
- Statusinformationen des Accounts (aktiv/deaktiviert),
- Rolle,
- Berechtigungen,
- interne Vermerke,
- ggf. Metadaten beim Aufruf der Webseite des Verwaltungsprogramms (bspw. Datum und Uhrzeit des Abrufs; Name des aufgerufenen Internetdienstes, der aufgerufenen Ressource und der verwendeten Aktion; IP-Adresse; Abfrage, die der Client gestellt hat; übertragene Datenmenge; Meldung, ob der Abruf erfolgreich war; Browser-Identifikation (enthält in der Regel die Browserversion sowie das Betriebssystem))

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Die betroffenen Personen rufen das Verwaltungsprogramm über einen Webbrowser auf. Sie verwenden das Verwaltungsprogramm zur Erledigung der ihnen zugewiesenen Aufgaben.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Verarbeitung der Daten, um den betroffenen Personen die Erledigung der ihnen zugewiesenen Aufgaben zu ermöglichen.

Dauer der Verarbeitung:

- Die Metadaten werden gelöscht, sobald das Verwaltungsprogramm geschlossen wird. Alle anderen Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

6 Nutzerverwaltung im Verwaltungsprogramm

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Nutzende des Verwaltungsprogramms, ggf. inkl. Beschäftigte des Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden:

- Stammdaten,
- Kontaktdaten,
- Anmeldedaten,
- Statusinformationen des Accounts (aktiv/deaktiviert),
- Rolle,
- Berechtigungen

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Im Verwaltungsprogramm werden die Rollen und Rechte verwaltet.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Die Verarbeitung der Daten erfolgt zu Zwecken der Ermöglichung der Zuweisung der Rollen und Rechte, die für die Erfüllung der vom Verantwortlichen zugewiesenen Aufgaben, erforderlich sind.

Dauer der Verarbeitung:

- Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

7 Bearbeitung der Informationen zur Antragstellung und digitalen Ehrenamtskarte im Verwaltungsprogramm, die den Antragstellenden in der mobilen Anwendung „Ehrenamtskarte“ bereitgestellt werden

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Antragstellende

Kategorien personenbezogener Daten, die verarbeitet werden:

- Bearbeitungsstatus des Antrags,
- Stammdaten und Angaben zur Gültigkeit der Ehrenamtskarte auf der digitalen Ehrenamtskarte

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Der Verantwortliche hat die Möglichkeit die Informationen im Zusammenhang mit der Antragstellung bzw. der digitalen Ehrenamtskarte im Verwaltungsprogramm zu bearbeiten, um diese den Antragstellenden in der mobilen Anwendung „Ehrenamtskarte“ bereitzustellen.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Im Verwaltungsprogramm können die Informationen zur Antragstellung und digitalen Ehrenamtskarte zum Zwecke deren Bereitstellung in der mobilen Anwendung „Ehrenamtskarte“ bearbeitet werden.

Dauer der Verarbeitung:

- Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

8 Bearbeitung der Informationen über Ansprechpersonen für Antragsbearbeitung im Verwaltungsprogramm, die in der mobilen Anwendung „Ehrenamtskarte“ bereitgestellt werden

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Ansprechpersonen für Antragsbearbeitung

Kategorien personenbezogener Daten, die verarbeitet werden:

- ggf. Stammdaten,
- Kontaktdaten

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Der Verantwortliche hat die Möglichkeit die Informationen über die Ansprechpersonen für Antragsbearbeitung im Verwaltungsprogramm zu bearbeiten, um diese in der mobilen Anwendung „Ehrenamtskarte“ bekannt zu geben.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Im Verwaltungsprogramm können die Informationen über die Ansprechpersonen für Antragsbearbeitung zum Zwecke deren Bekanntgabe in der mobilen Anwendung „Ehrenamtskarte“ bearbeitet werden.

Dauer der Verarbeitung:

- Die Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

9 Protokollierung der Tätigkeiten im Verwaltungsprogramm

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Nutzende des Verwaltungsprogramms, ggf. inkl. Beschäftigte des Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden:

- Daten der geloggten sicherheitsrelevanten Ereignisse (insbesondere ausgeführte sicherheitsrelevante Tätigkeit, Zeitpunkt der Tätigkeit, E-Mail-Adresse)

Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO:

- Keine

Art der Verarbeitung:

- Die sicherheitsrelevanten Ereignisse werden geloggt.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Die Protokollierung der sicherheitsrelevanten Daten erfolgt zum Zwecke der Sicherstellung der Sicherheit des technischen Systems und der Datenverarbeitungen.

Dauer der Verarbeitung:

- Daten werden gelöscht, sobald die Speicherung durch den Verantwortlichen nicht mehr für den verfolgten Zweck erforderlich ist.

Anhang II: Beschreibung der TOM für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

I. Die d-NRW AöR hat nextgov iT GmbH mit der technischen Bereitstellung des Verwaltungsprogramms beauftragt. Die nextgov iT GmbH betreibt somit vollumfänglich den Online-Dienst und setzt die notwendigen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten um. Die Maßnahmen gewährleisten einen angemessenen Schutz für die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO, falls beim Verantwortlichen solche Verarbeitung eintreten sollte. Die technischen und organisatorischen Maßnahmen der nextgov iT GmbH gestalten sich wie folgt:

1. Überblick

Die nachfolgenden technisch-organisatorischen Maßnahmen werden durch die nextgov iT GmbH umgesetzt. Für ggf. eingebundene Subunternehmer gelten sachlich vergleichbare Verpflichtungen. Aus diesem Grunde werden die jeweiligen technisch-organisatorischen Maßnahmen differenziert dargestellt.

2. Technische und organisatorische Maßnahmen

2.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern - (räumlich) vorhanden

- Elektronische Zutrittscodekarten/ Zutrittstransponder
- Begleitung von Besucherzutritten durch eigene Mitarbeiter
- Auslagerung von Servern in Rechenzentren

b. Zugangskontrolle

Verhindern des Eindringens Unbefugter in die DV-Systeme oder deren unbefugter Nutzung

- Verschlüsselung von Netzwerken
- Verwendung von verschlüsselten Zugriffskanälen auf Kundenserver und Unternehmensdaten (VPN, SSH, https)
- Passwortsicherung von Bildschirmarbeitsplätzen
- Verwendung von individuellen Passwörtern
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern
- Passwort-Policy mit Mindestvorgaben zur Passwortkomplexität
- Rollenbasierte Rechtevergabe für Produktionssysteme
- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern

- Verpflichtung zur Vertraulichkeit

c. Zugriffskontrolle

Verhinderung von unerlaubten Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen

- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Daten und Datenbanken

d. Trennungskontrolle

Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten

- Trennung von Kunden (Mandantenfähigkeit oder Separierung des verwendeten Systems)
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
- Trennung von Entwicklungs-, Test- und Produktivsystem

2.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a. Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln

- Weitergabe personenbezogener Daten nur auf expliziter vertraglicher oder rechtlicher Grundlage
- Datenaustausch über gesicherte Verbindung
- Verschlüsselung vertraulicher Datenträger

b. Eingabekontrolle

Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege

- Festlegung von Benutzerberechtigungen (Profile)
- Differenzierte Benutzerberechtigungen - Lesen, Ändern, Löschen
- Teilzugriff auf Daten bzw. Funktionen
- Verpflichtung auf das Datengeheimnis

2.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Verfügbarkeitskontrolle

Schutz gegen zufällige Zerstörung oder Verlust

- Datensicherungs- und Backupkonzepte
- Durchführung der Datensicherungs- und Backupkonzepte
- Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung

von Anschlägen, Absturz, Erdbeben)

Generelle Maßnahmen Belastbarkeit

- Härtung von Systemen
- Durchführung von automatisierten Schwachstellenscans
- Regelmäßige Patchzyklen
- Bedarfsorientierte Durchführung von Penetrationstests

b. Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Fähigkeit des Umgangs mit risikobedingten Veränderungen, Toleranz und Ausgleichsfähigkeit gegenüber Störungen

- Abgrenzung kritischer Komponenten
- Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
- Auslagerung von Datensicherungen

Unverzögliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates:

- Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen
- Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen

Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst:

- Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten
- Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit
- Externe Auftragsverarbeiter und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a. Kontrollverfahren

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen

- Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert
- Meldung neuer / veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen. Bei negativem Verlauf der zuvor genannten Überprüfung werden die

Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt.

b. Auftragskontrolle

Sicherstellung der weisungsgemäßen Datenverarbeitung durch Dienstleister

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
- Regelmäßige Kontrollen beim Auftragsverarbeiter nach Vertragsbeginn (während Vertragsdauer)
- Überprüfung des Datensicherheitskonzepts beim Auftragsverarbeiter
- Sichtung vorhandener IT-Sicherheitszertifikate der Auftragsverarbeiter

2.5 Hosting und Verschlüsselung der Daten

Die nextgov iT GmbH hat regio iT gesellschaft für informationstechnologie mbh mit dem Hosting des Online-Dienstes beauftragt. Das Hosting bezeichnet das Bereitstellen von Speicherplatz für den Online-Dienst. Dementsprechend werden die Daten verschlüsselt in den Rechenzentren der regio iT gesellschaft für informationstechnologie mbh in Deutschland gespeichert. Die Rechenzentren sind nach ISO 27001 zertifiziert. Die regio iT gesellschaft für informationstechnologie mbh verschlüsselt Daten auf Datenhaltungssystemen gemäß als sicher anerkannter Verfahren und Schlüssellängen, entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI).

Anhang III: Liste der Unterauftragsverarbeiter für den Online-Dienst „Förderung ehrenamtlicher Tätigkeit“: Verwaltungsprogramm

Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: nextgov iT GmbH

Anschrift: Lombardenstraße 24, 52070 Aachen

Telefon: +49 241 942609 00

E-Mail: info@nextgovit.de

Beauftragt durch: d-NRW AöR

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):

Technische Bereitstellung des Online-Dienstes und damit Verarbeitung sämtlicher, vorstehend genannter personenbezogener Daten.

2. Name: regio iT gesellschaft für informationstechnologie mbh

Anschrift: Lombardenstraße 24, 52070 Aachen

Telefon: +49 241 413 59

E-Mail: info@regioit.de

Beauftragt durch: nextgov iT GmbH

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):

Hosting des Online-Dienstes und damit Verarbeitung und Speicherung sämtlicher, vorstehend genannter personenbezogener Daten in Rechenzentren in Deutschland.