Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Auftraggeber (Verantwortlicher):

Die natürliche Person, juristische Person, juristische Person des öffentlichen Rechts, öffentlich-rechtliches Sondervermögen, Stadt, Gemeinde, politische Partei, politische Fraktion, oder eine sonstige vergleichbare Organisation oder Einrichtung, welche das BürgerStimme Service-System über die Webstelle (https://web.buerger-stimme.com) gebucht hat.

Auftragnehmer (Auftragsverarbeiter):

NTQ Solutions GmbH, Hölderlinstraße 12, 74074 Heilbronn

---

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst die Erhebung, Speicherung und Verarbeitung von - u.a. personenbezogenen - Daten der Nutzer des Auftraggebers mit dem Ziel der vollfunktionalen Bereitstellung des BürgerStimme Service-Systems, einschließlich sämtlicher Funktionen und Möglichkeiten, welche über dieses angeboten werden und mit dem Auftraggeber in expliziter Absprache vereinbart wurden.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung in ein Drittland ist zulässig, sofern für dieses ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO vorliegt (z.B. EU-US Data Privacy Framework) oder wenn geeignete Garantien gemäß Art. 46 DSGVO vorgesehen sind (insbesondere durch den Abschluss der EU-Standardvertragsklauseln). Jede darüber hinausgehende Verlagerung der Dienstleistung, die nicht durch diese Maßnahmen gedeckt ist, bedarf der vorherigen Zustimmung des Auftraggebers.

Der Vertrag beginnt mit der Buchung des BürgerStimme Service-Systems über die Webstelle der BürgerStimme und wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt einen Monat.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die konkreten Details zu Art und Zweck der Verarbeitung der erhobenen Daten können dem Vertrag über die Bereitstellung des BürgerStimme Service-Systems im Rahmen der Übersicht der Leistungen entnommen werden.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):
Die Verarbeitung umfasst im Wesentlichen die Erhebung, Speicherung, Organisation, Übermittlung und Löschung von Daten. Dies beinhaltet die Zuordnung der personenbezogenen Daten zu Datensätzen, welche im Rahmen der Nutzung des BürgerStimme Service-Systems generiert wurden. Dies dient vornehmlich dem Zwecke der Identifikation, der Kommunikation sowie der systeminternen Verknüpfung zur Bereitstellung der Funktionalität.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
Gegenstand der Verarbeitung sind folgende Datenarten/Kategorien:
- Bestands- und Kontaktdaten (z. B. Name, Adresse, Geburtsdatum, E-Mail-Adresse)
- Inhaltsdaten (z.B. Texteingaben, Meldungen, Kommentare, hochgeladene Fotos, geteilte Standortdaten)
- Nutzungs- und Metadaten (z.B. IP-Adressen, Geräte-Informationen, Zugriffszeiten, Logfiles, Identifikations-Token)

Ausschluss besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO):
Das BürgerStimme Service-System ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (z.B. Gesundheitsdaten, Daten zum Sexualleben, genetische/biometrische Daten, religiöse Überzeugungen oder politische Meinungen) ausgelegt.
Der Auftraggeber verpflichtet sich, keine solchen Daten in das System einzupflegen oder durch das System verarbeiten zu lassen, sofern dies nicht ausdrücklich und schriftlich als gesonderter Vertragsgegenstand mit einem darauf abgestimmten Sicherheitskonzept vereinbart wurde. Sollten Nutzer des Auftraggebers (z.B. Bürger in Freitextfeldern) unaufgefordert Daten dieser Kategorie eingeben, wirkt der Auftraggeber auf eine unverzügliche Löschung oder Schwärzung hin, sobald er Kenntnis davon erlangt.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
Bei den betroffenen Personen handelt es sich um:
- Nutzer des Dienstes (z.B. Bürger/Einwohner)
- Beschäftigte oder Beauftragte des Auftraggebers (sofern diese das System administrieren oder nutzen)
- Interessenten oder Kontaktpersonen

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

Gehen Anträge oder Anfragen von betroffenen Personen (z. B. auf Auskunft oder Löschung) direkt beim Auftragnehmer ein, wird dieser die Anfrage nicht selbstständig beantworten, sondern sie unverzüglich an den Auftraggeber weiterleiten. Dies gilt nicht, wenn sich die Anfrage auf eine technische Funktion bezieht (z. B. automatisierte Kontolöschung oder Export von gesammelten Daten), für die der Auftraggeber durch die Nutzung der Software-Funktionalität bereits eine generelle Weisung erteilt hat.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel in Textform (z.B. E-Mail) oder in einem dokumentierten elektronischen Format.

Weisungen können auch durch die Vornahme von Einstellungen oder Aktionen innerhalb der bereitgestellten Software (z.B. Lösch- oder Konfigurationsbefehle im Admin-Bereich) erteilt werden. Mündliche Weisungen

sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Änderungen des Verarbeitungsgegenstandes sind gemeinsam abzustimmen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt, vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der vertraglichen Pflichten zu überzeugen.

Informations- und Vertraulichkeitspflichten: Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und spezifischen Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:
Sofern der Auftraggeber keine andere weisungsberechtigte Person explizit nennt, ist diese gleich der vom Auftraggeber als Ansprechpartner eingetragene Person auf der Webstelle (https://web.buerger-stimme.com).

Weisungsempfänger beim Auftragnehmer sind:
Die Geschäftsführung sowie die Leitung des Bereichs Technischer Support / Customer Success.

Für Weisung zu nutzende Kommunikationskanäle:
NTQ Solutions GmbH, Hölderlinstraße 12, 74074 Heilbronn, E-Mail: support@buerger-stimme.com.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Die Daten, welche über das BürgerStimme Service-System verarbeitet werden, werden gesammelt auf der von Firebase gemanagten Datenbank für das System hinterlegt.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere zu überprüfen, dass die gespeicherten personenbezogenen Daten in seinem Bereich geschützt und die eingebauten Sicherheitsstufen intakt sind. Ein Verdacht auf etwaige Kompromittierung ist unverzüglich zu untersuchen und entsprechende Abhilfemaßnahmen sind einzuleiten.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben, welche nicht über die hierfür eingerichtete Webstelle autonom entnommen werden können, auf Anfrage jeweils unverzüglich an den Auftraggeber weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu kontrollieren.
Da der Auftragnehmer Cloud-Infrastrukturdienste nutzt, erfolgt der Nachweis der Datensicherheit vorrangig durch die Vorlage aktueller Testate, Berichte oder Zertifizierungen unabhängiger Instanzen (z. B. ISO 27001, SOC 2, ISAE 3402) des Auftragnehmers oder seiner Unterauftragnehmer. Vor-Ort-Kontrollen in Rechenzentren der Unterauftragnehmer (z.B. Google) sind in der Regel ausgeschlossen und werden durch die genannten Zertifikate ersetzt.
Sonstige Vor-Ort-Kontrollen in den Geschäftsräumen des Auftragnehmers erfolgen nur nach vorheriger Terminvereinbarung, zu üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht

und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist ein Datenschutzbeauftragter bestellt:
Erreichbar unter: datenschutz@buerger-stimme.com Postanschrift: NTQ Solutions GmbH, z. Hd. Datenschutzbeauftragter, Hölderlinstraße 12, 74074 Heilbronn

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer informiert den Auftraggeber unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten (im Sinne von Art. 4 Nr. 12 DSGVO) bekannt wird, die Daten des Auftraggebers betrifft. Dies gilt auch bei einem begründeten Verdacht auf einen solchen Vorfall.
Die Meldung an den Auftraggeber muss mindestens folgende Informationen enthalten (soweit zum Zeitpunkt der Meldung bereits verfügbar):

- Beschreibung der Art der Verletzung (wenn möglich mit Kategorien und ungefährer Anzahl der betroffenen Personen/Datensätze),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung,
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Der Auftragnehmer unterstützt den Auftraggeber bestmöglich bei dessen Pflichten zur Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und zur Benachrichtigung der betroffenen Personen (Art. 34 DSGVO).
Eigene Meldungen des Auftragnehmers an Aufsichtsbehörden oder Betroffene, die im Namen des Auftraggebers erfolgen, sind nur nach vorheriger expliziter Weisung gemäß Ziff. 3 dieses Vertrages zulässig.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Der Auftraggeber stimmt der Beauftragung des folgenden Haupt-Unterauftragnehmers zur Erbringung der Cloud-Infrastruktur- und Hosting-Leistungen ausdrücklich zu: Google Cloud EMEA Limited, 70 Sir John Rogerson’s Quay, Dublin 2, Irland (sowie deren verbundene Unternehmen, insb. Google LLC, USA).

Die primäre Speicherung der Inhaltsdaten (Datenbanken, Datei-Uploads) und die Verarbeitung durch Server-Logik erfolgen in ISO-27001-zertifizierten Rechenzentren der Google Cloud EMEA Limited in der Region Frankfurt am Main, Deutschland (europe-west3).
Der Auftraggeber nimmt zur Kenntnis, dass einzelne technische Infrastruktur-Dienste (insb. Content Delivery Networks zur Auslieferung der Web-App oder Routing-Dienste für Push-Benachrichtigungen) aufgrund ihrer technischen Natur global verteilt arbeiten können. Soweit hierbei Daten (z.B. IP-Adressen oder technische Metadaten) über Server außerhalb der EU/EWR geleitet werden, erfolgt dies auf Grundlage des EU-US Data Privacy Frameworks (DPF), für welches der Unterauftragnehmer zertifiziert ist, oder auf Basis von Standardvertragsklauseln (SCCs). Der Auftragnehmer sichert zu, durch technische Maßnahmen (z. B. „Data

Residency“-Einstellungen) die Datenmenge in Drittländern auf das technisch notwendige Minimum zu reduzieren.

Der Auftragnehmer ist berechtigt, weitere Unterauftragnehmer hinzuzuziehen oder bestehende zu ersetzen (Allgemeine Genehmigung gem. Art. 28 Abs. 2 DSGVO).
Der Auftragnehmer informiert den Auftraggeber in Textform (z. B. per E-Mail oder über das Admin-Dashboard) rechtzeitig vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern. Dem Auftraggeber steht ein Einspruchsrecht zu. Erfolgt kein Einspruch innerhalb von vier Wochen nach Information, gilt die Änderung als genehmigt. Im Fall eines begründeten Einspruchs werden die Parteien eine einvernehmliche Lösung suchen; ist dies nicht möglich, steht dem Auftraggeber ein Sonderkündigungsrecht zu.
Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern gelten. Es müssen mit dem Unterauftragnehmer Bestimmungen vereinbart werden, die ein gleichwertiges Datenschutzniveau gewährleisten.

Da eine Vor-Ort-Kontrolle in den Hochsicherheits-Rechenzentren der Cloud-Anbieter (z.B. Google) vertraglich und faktisch ausgeschlossen ist, wird vereinbart, dass die Kontrolle der Eignung der technischen und organisatorischen Maßnahmen dieser Unterauftragnehmer vorrangig durch die Einsichtnahme in aktuelle Testate, Berichte oder Zertifizierungen unabhängiger Instanzen (z. B. ISO 27001, SOC 2, BSI C5) erfolgt. Der Auftragnehmer stellt diese Nachweise auf Anfrage zur Verfügung (bzw. verweist auf die Download-Portale der Anbieter).

8. Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

Vorbemerkung zur Infrastruktur:
Das BürgerStimme Service-System wird als Software-as-a-Service (SaaS) auf der Cloud-Infrastruktur der Google Cloud EMEA Limited (Google Cloud / Firebase) betrieben. Die physische Sicherheit der Rechenzentren und der Netzwerkinfrastruktur obliegt dem Unterauftragnehmer Google, welcher nach weltweit anerkannten Standards (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2) zertifiziert ist.

Der Auftragnehmer hat ergänzend dazu folgende eigene Maßnahmen implementiert:

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

a) Zutrittskontrolle (Physischer Zugang)
- Kein physischer Zugang zu Servern: Der Auftragnehmer unterhält keine eigenen Serverräume. Die Datenverarbeitung erfolgt ausschließlich in den Hochsicherheits-Rechenzentren von Google (Standort: Frankfurt, europe-west3).
- Sicherung der Arbeitsplätze: Die Geschäftsräume des Auftragnehmers sind gegen unbefugten Zutritt gesichert (abschließbare Türen, Kontrolle von Besuchern).
- Mobile Arbeit: Bei Remote-Arbeit wird sichergestellt, dass Dritte keine Einsicht in Bildschirme oder sensible Daten nehmen können (z.B. Sperren des Bildschirms bei Abwesenheit).

b) Zugangskontrolle (Systemzugriff)
- Starke Authentifizierung: Zugriff auf Administrations-Oberflächen (z.B. Firebase Console, Google Cloud Platform) ist durch komplexe Passwörter und zwingende Zwei-Faktor-Authentifizierung (2FA/MFA) gesichert.

- Verschlüsselung: Alle Arbeitsgeräte (Laptops/Smartphones) des Auftragnehmers sind festplattenverschlüsselt (z.B. BitLocker, FileVault).
- Virenschutz & Firewall: Einsatz aktueller Sicherheitssoftware und Firewalls auf allen Endgeräten.

c) Zugriffskontrolle (Datenzugriff)
- Berechtigungskonzept (Least Privilege): Mitarbeiter haben nur Zugriff auf jene Daten, die sie für ihre Aufgabenerfüllung zwingend benötigen.
- Firebase Security Rules: Der Zugriff auf die Datenbanken ist durch serverseitige Sicherheitsregeln (Firestore Security Rules) so beschränkt, dass Nutzer nur auf ihre eigenen Daten oder öffentlich freigegebene Daten zugreifen können.
- Protokollierung: Administrative Zugriffe auf die Cloud-Infrastruktur werden durch Google Cloud Audit Logs protokolliert.

d) Trennungskontrolle
- Logische Mandantentrennung: Die Daten des Auftraggebers werden logisch strikt von Daten anderer Kunden getrennt verarbeitet (z.B. softwareseitige Zugriffsbeschränkungen).
- Trennung von Systemen: Produktiv-, Test- und Entwicklungsumgebungen sind voneinander getrennt.

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

a) Weitergabekontrolle
- Verschlüsselung bei Übertragung (Encryption in Transit): Jeglicher Datenverkehr zwischen der App/Web-App (Nutzer) und den Servern sowie zwischen dem Auftragnehmer und den Servern erfolgt ausschließlich verschlüsselt.

b) Eingabekontrolle
- Nachvollziehbarkeit: Änderungen an den Daten durch den Auftraggeber werden im System protokolliert
- Code-Sicherheit: Änderungen am Quellcode der Software werden über Versionierungssysteme (z.B. Git) nachvollzogen und vor dem Deployment geprüft.

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

a) Verfügbarkeitskontrolle
- Redundanz: Nutzung der Google Cloud Infrastruktur gewährleistet hohe Ausfallsicherheit durch redundante Systeme und Stromversorgung.
- Backups: Durchführung regelmäßiger automatisierter Backups der Datenbanken. Die Backups werden geo-redundant oder in einer anderen Verfügbarkeitszone gespeichert.
- DDoS-Schutz: Nutzung der globalen Google-Infrastruktur zur Abwehr von Distributed-Denial-of-Service Angriffen.

b) Wiederherstellbarkeit
- Es existiert ein Notfallplan zur Wiederherstellung der Systeme im Falle eines physischen oder technischen Zwischenfalls (Disaster Recovery).

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)
- Datenschutz-Management: Regelmäßige Überprüfung der Einhaltung der Datenschutzvorschriften und der Wirksamkeit der getroffenen Maßnahmen.
- Software-Updates: Regelmäßiges Einspielen von Sicherheitsupdates für verwendete Bibliotheken und Frameworks.

- Auftragsverarbeitung: Regelmäßige Kontrolle der Unterauftragnehmer (insb. Google) durch Prüfung derer aktueller Sicherheitszertifikate.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten oder früherer Beendigung des Auftrags hat der Auftragnehmer sämtliche in seinen Besitz gelangte personenbezogene Daten sowie erstellte Verarbeitungs- oder Nutzungsergebnisse nach Wahl des Auftraggebers entweder herauszugeben (z. B. durch Bereitstellung einer Export-Funktion in einem gängigen Format) oder datenschutzgerecht zu löschen.

Erfolgt keine explizite Weisung des Auftraggebers zur Herausgabe, werden die Daten spätestens 30 Tage nach Vertragsbeendigung gelöscht.

Die Löschung ist dem Auftraggeber auf Anfrage schriftlich oder in einem dokumentierten elektronischen Format (Textform) zu bestätigen.

Ausnahmen von der Löschpflicht:

- Gesetzliche Aufbewahrungspflichten: Von der Löschung ausgenommen sind Daten, zu deren Aufbewahrung der Auftragnehmer gesetzlich verpflichtet ist (z. B. aus steuer- oder handelsrechtlichen Gründen) oder die zur Nachweisführung der ordnungsgemäßen Auftragsverarbeitung erforderlich sind.
- Backups: Daten, die sich in routinemäßigen Datensicherungsdateien (Backups) befinden, werden durch den regulären Überschreibungszyklus der Backups (Rotation) endgültig gelöscht. Eine sofortige selektive Löschung aus Backup-Archiven ist technisch nicht geschuldet, sofern die Wiederherstellung dieser Daten organisatorisch ausgeschlossen wird.

10. Vergütung

Eine gesonderte Vergütung oder Kostenerstattung für die Tätigkeit im Rahmen dieses Auftragsverarbeitungsvertrages wird nicht vereinbart. Die Leistungen des Auftragnehmers sind mit der Vergütung für die Hauptleistung (Bereitstellung des BürgerStimme Service-Systems) abgegolten.

11. Haftung

Die Parteien haften gegenüber betroffenen Personen gemäß der Regelung des Art. 82 DSGVO. Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer richtet sich die Haftung nach den Bestimmungen des Hauptvertrages (AGB bzw. Vertrag zur Bereitstellung des BürgerStimme Service-Systems). Soweit der Hauptvertrag Haftungsbeschränkungen vorsieht, gelten diese auch für die Haftung aus diesem Auftragsverarbeitungsvertrag, sofern dem nicht zwingende gesetzliche Vorschriften entgegenstehen.

12. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend entsprechend der gesetzlichen Aufbewahrungsfristen aufzubewahren.

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung oder der Vereinbarung in einem dokumentierten elektronischen Format (Textform, z. B. E-Mail oder Admin-Dashboard), und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen und die Dritten auf die Eigentums- und Hoheitsrechte des Auftraggebers hinzuweisen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem gewollten wirtschaftlichen und rechtlichen Zweck am nächsten kommt.

Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Geschäftssitz des Auftragnehmers, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

13. Gültigkeit

Dieser Vertrag wird elektronisch geschlossen. Er tritt mit dem Abschluss des Vertrages über die Hauptleistung (Buchung des BürgerStimme Service-Systems über die Webstelle https://web.buerger-stimme.com oder durch Annahme eines Angebots) in Kraft.

Gemäß Art. 28 Abs. 9 DSGVO bedarf dieser Vertrag keiner handschriftlichen Unterzeichnung, sofern er in einem dokumentierten elektronischen Format geschlossen wird. Mit der Buchung und der Anerkennung der AGB und dieses AVV durch den Auftraggeber gilt der Vertrag als wirksam geschlossen.