Zwischen der Firma
VoteWorks GmbH
Königswinterer Str. 27
53639 Königswinter
DEUTSCHLAND
– Nachfolgend „**Auftragnehmer**“ genannt –

und
Firma:
Name:
Straße, Hausnummer:
Postleitzahl, Ort:
Deutschland
Kundennummer:
Auftragsnummer: VW

– Nachfolgend „**Auftraggeber**“ genannt –

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Einzelvertrag (nachstehend „Vertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte, personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten.
Diese Anlage ist nur gültig in Verbindung mit einem aktiven Vertrag über ein Vote@Home Produkt, das im Zusammenhang mit einem der nachfolgenden IONOS bzw. weiteren Produkten steht:
Managed Cloud, vServer (VPS), Cloud Server, Dedicated Server, Dynamic Cloud Server, Virtual Server, Webhosting, sowie Jimdo Website und Adressbuch.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1) Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Gegenstand dieser Anlage ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Als Hosting Dienstleister und Administrator von Server-Systemen kann auf Seiten des Auftragnehmers ein Zugriff auf personenbezogene Daten allerdings nicht ausgeschlossen werden.
2) Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr.7 DS-GVO).

2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format („Textform“) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden („Einzelweisung“).

§ 3 Pflichten des Auftragnehmers

1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Art. 28 Abs. 3 lit. a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Die Durchführung von rechtswidrigen Weisungen darf der Auftragnehmer ablehnen.
2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
Erfolgt eine solche Datenverarbeitung in Privatwohnungen, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
3) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.
4) Die Beschreibung technischer und organisatorischen Maßnahmen gemäß *Anhang TOMs* ist Bestandteil dieser Vereinbarung. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer unterstützt soweit erforderlich den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.
5) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Schweigepflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.
6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
7) Für alle im Rahmen dieser Anlage anfallenden Datenschutzfragen ist der Ansprechpartner:
VoteWorks GmbH
Der Datenschutzbeauftragte
Königswinterer Str. 27
53639 Königswinter
datenschutz@vote-at-home.de

8) Der Auftragnehmer stellt sicher, seinen Pflichten nach Art. 32 Abs.1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Lösung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

1) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezgl. datenschutzrechtlicher Bestimmungen feststellt.
2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 11 dieser Anlage entsprechend.

§ 5 Anfragen betroffener Personen

1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet bei Erfüllung seiner Pflichten nicht dafür, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
2) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 1 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese

Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Drittstaatentransfer

1) Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

1) Mit der Hinzuziehung von verbundenen und fremden Unternehmen zur Wartung, Pflege der Rechenzentrumsstruktur, Telekommunikationsdienstleistungen und Benutzerservice durch den Auftragnehmer ist der Auftraggeber einverstanden.
Der Auftraggeber hat das Recht innerhalb von zwei Wochen ab Kenntnis der Information über den Subdienstleister aus wichtigem Grund schriftlich beim Auftragnehmer Einspruch gegen den Einsatz des Subunternehmers einzulegen. Erfolgt kein Einspruch innerhalb der genannten Frist, gilt dies als Zustimmung des Auftraggebers zum Einsatz dieses Subdienstleisters. Der Auftragnehmer ist zur außerordentlichen Kündigung berechtigt, sofern der Auftraggeber der Beauftragung eines Subunternehmers dieses Vertrages widerspricht und keine Einigung erreicht werden kann.

2) Die in Anhang 3 aufgeführten Unterauftragnehmer sind vom Auftraggeber genehmigt.

3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die vom Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

§ 9 Informationspflichten, Schriftformklausel, Rechtswahl

1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich drüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.
2) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit dieser Anlage zum Datenschutz im Übrigen nicht.
3) Es gilt deutsches Recht.
4) Diese Anlage ersetzt alle vorangegangenen Vereinbarungen dieser Art.

§ 10 Haftung und Schadensersatz

1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Dieser Vertrag wird elektronisch geschlossen und ist ohne Unterschrift und nur mit Anerkennung der folgenden Anhänge gültig:

Anhang TOMs
Anhang Konkretisierung des Vertragsinhalts und
Anhang Übersicht der Unterauftragsverhältnisse

VoteWorks® GmbH
+49 22 44 8777-0, Fax -15
Königswinterer Str. 27
D-53639 Königswinter

Amtsgericht Siegburg HRB 12778
Steuernr.: 222/5720/1637
USt.-IdNr. DE293042893
Geschäftsführer: Bernd Nixdorf

info@voteworks.de
Sparkasse Köln-Bonn
BLZ 370 501 98
Konto 193 182 3429

Anhang TOMs: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO, die auch im Zusammenhang mit einem der vom Auftragnehmer und Auftraggeber genutzten IONOS Produkte stehen können

Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. Der allgemeine Teil beschreibt technische und organisatorische Maßnahmen, die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In diesem Anhang sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Vertraulichkeit

Vertraulichkeit ist die Eigenschaft, die verfügt, dass personenbezogene Daten unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Zutrittskontrolle: Empfangs- und Sicherheitsdienst, individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Karten, Transponder und Schlüssel), Mitarbeiter- und Besucherausweise, Besucher dürfen sich grundsätzlich nur in Begleitung eines Mitarbeiters im Gebäude aufhalten. Alarm- und Einbruchmeldeanlage, Büroräume sind außerhalb der Arbeitszeit verschlossen.
Zugangskontrolle: Formale Benutzer- und Berechtigungsverfahren, Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung; systemisch forcierte Passwortrichtlinien, VPN bei Remotezugriff und durch vom Verantwortlichen verwaltete Geräte
Mobile Device Management: Mobile Datenträger sind verschlüsselt; automatische Sperre von Desktops nach wenigen Minuten Inaktivität, Clean Desk-Policy
Zugriffskontrolle: Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation, Nutzung kryptografischer Verfahren (z.B. Verschlüsselung), Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip, Trennung von Anwendungs- und Administrationszugängen, Protokollierung von Zugriffsversuchen, Einrichtung von Administratorarbeitsplätzen, minimale Anzahl an Administratoren, Nutzung von Dokumentenvernichtung.
Pseudonymisierung: Sofern möglich oder erforderlich werden personenbezogene Daten pseudonymisiert verarbeitet (Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System)
Trennungskontrolle: Trennung von Entwicklungs-, Test- und Produktivumgebung; personenbezogene Daten dürfen nicht für Testzwecke verwendet werden.
Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage

2. Integrität

Die Integrität personenbezogener Daten ist dann gewahrt, wenn sie richtig, unverändert und vollständig sind.

Weitergabekontrolle: Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP), Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips; personenbezogene Daten werden nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfen; wo möglich, wird E-Mailverschlüsselung eingesetzt; wo möglich, werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt; Dokumentation der Weitergabe von physischen Speichermedien; Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag.
Eingabekontrolle: Technische Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Kontrolle der Protokolle; Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen); rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte); Protokollierung von administrativen Änderungen

3. Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Einsatz von Hardware- und Softwarefirewalls; Intrusion Detection Systeme, Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag, Unterbrechungsfreie-Stromversorgung (USV), Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust.
Durchführung von Wiederherstellungstests; wo notwendig, Nutzung redundanter Systeme (z.B. RAID), regelmäßiger Test von Datensicherungen, externe Audits und Sicherheitstests.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Datenschutz-Management: Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt.
Etablierung einer Datenschutz- und Informationssicherheitsorganisation: Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen; Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert; neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten; ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt; Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert.
Auftragskontrolle: Daten, die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet. Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt; Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert; sofern erforderlich, werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen.
Datenschutzfreundliche Voreinstellungen: Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden; es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind.
Incident-Response-Management: Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten; dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten.

5. Besondere technische und organisatorische Maßnahmen für Rechenzentren

Alle Rechenzentren sind nach dem ISO 27001 Standard zertifiziert; elektronische Zutrittskontrollsysteme überwachen und gewährleisten den Zutritt zum jeweiligen Rechenzentrum nur für autorisierte Personen.
Sicherheitsschleuse: Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes.
Definierte Sicherheitszonen: Hochredundante Netzwerkinfrastruktur; Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr; Kühlsystem im Rechenzentrum / Serverraum; Serverraumüberwachung Temperatur und Feuchtigkeit; keine sanitären Anschlüsse im oder oberhalb von Rechenzentren; Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren.

6. Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung durchgeführt, gelten zusätzlich folgende Vereinbarungen:

1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch.
2) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen, Ausnahmen sind mit dem Auftraggeber abzustimmen.
3) Der Beginn der Fernwartung wird vom Auftragnehmer angekündigt, um dem Auftraggeber die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Die Mitarbeiter des Auftragnehmers verwenden nach

dem Stand der Technik hinreichend sichere Identifizierungs- und Einwahlverfahren. Die Fernwartung darf nur über nach dem Stand der Technik sichere Leitungen abgewickelt werden.

4) Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu protokollieren, die Protokolle zu überprüfen und eine angemessene Zeit aufzubewahren.
5) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, wenn der Auftragnehmer von den vereinbarten Sicherheitsmaßnahmen abweicht oder die Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten durchgeführt wird.

Anhang Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in der Leistungsvereinbarung gemäß Angebot an den Auftraggeber mit der hier auf Seite 1 genannten Angebotsnummer beschrieben.

(2) Kategorisierung der personenbezogenen Datenkategorien und der Datenarten
Es werden folgende personenbezogene Datenarten / Datenkategorien verarbeitet:

Datenarten:

- ☒ Kontaktdaten der Eigentümer (Name, Vorname, E-Mail-Adresse)
- ☒ Kontaktdaten von Bevollmächtigten (Name, Vorname, E-Mail-Adresse)
- ☒ Kontaktdaten von Gast-Teilnehmern (Name, Vorname, E-Mail-Adresse)
- ☒ Daten zur WEG (MEA, Teilnehmernummer)
- ☒ Daten zur jeweiligen Versammlung (Benutzername, Abstimmungsergebnisse)
- ☐ Sonstige: Bitte eintragen

Betroffene:

- ☒ Eigentümer
- ☒ Sonstige Teilnehmer an Versammlungen

Anhang Übersicht Unterauftragsverhältnisse

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Name	Rechtsform	Kontaktdaten	Art der Leistung
1&1 IONOS SE	Europäische Aktiengesellschaft	Elgendorfer Str. 57 56410 Montabaur 0721 170 5522 info@ionos.de	(Bare Metal) Server Hosting der Vote@Home Domain (Serverstandort D)

Salmacis.com GmbH	GmbH	Salmacis.com GmbH Wettersteinstrasse 9 82049 Pullach im Isartal 089 7456 46 63 info@salmacis.com	Server Hosting des Jitsi-Meet Conferencing (Serverstandort D)
Jochen Winzer softwein	Personengesellschaft	Weinbergstr. 41 01129 Dresden 0351 8401235 info@winzer-sw.de	Software Entwicklung Vote@Home