

## Sicherheits-Broschüre

Verwalter-Arbeitsplatz und beschluss.app ergeben eine Einheit zur Durchführung der digitalen oder hybriden WEG-Versammlung. Während der Verwalter-Arbeitsplatz zur Vorbereitung, Durchführung und Nachbearbeitung der WEG-Versammlungen durch den Verwalter dient, kann jeder Eigentümer anhand des Registrierungsschreibens die App im Google Play Store oder im Apple App Store herunterladen. Die Nutzungsbedingungen der App sind in der beschluss.app einsehbar.

Bei der Entwicklung beider Komponenten hatte stets die Datensicherheit und der Datenschutz höchste Priorität, da der Umgang mit personenbezogenen Daten unerlässlich für die Aufgabenstellung war. Auf eine reine Cloud-Lösung wurde verzichtet, da an den Versammlungsorten die dauerhafte Internet-Verbindung nicht garantiert werden kann. Diese Vorgabe wurde von Anfang an sowohl beim Verwalter-Arbeitsplatz als auch bei der App berücksichtigt.

Im Bereich der App könnte am Versammlungsort der Mobilfunk-Empfang gestört sein. Das hätte zur Folge, dass die Abstimmung mit der beschluss.app nicht möglich wäre. Aus diesem Grunde kann der Verwalter sog. Keypads verteilen, mit der die Abstimmung aufgrund eines eigenen Senders/Empfängers im Versammlungsraum doch möglich ist. Die Datenversorgung der App mit Beschlussbuch und Niederschrift erfolgt, sobald es wieder Empfang gibt. Bei der Abstimmung mit der App aus der Ferne ist dieses Problem durch Standort-Änderung meistens schnell zu lösen.

Aber auch beim Verwalterplatz hätte man ein großes Problem bei einer reinen Cloud-Lösung, wenn im Versammlungsraum kein Internet verfügbar wäre. Daher wird das Programm lokal auf mehreren Rechnern installiert, zum Beispiel auf einem Notebook oder Tablet, die bei der Versammlung verwendet werden sollen. Die Daten hingegen werden in der Cloud gehalten. Somit kann der Verwalter bei der Vorbereitung der Versammlung den benötigten Datenbestand schon zum Beispiel im Büro laden. Sollte es dann zu einer nicht stabilen Internet-Verbindung am Versammlungsort kommen, kann mit der Software und einer temporären Datenspeicherung auf dem Rechner gearbeitet werden.

Der Verwalter-Arbeitsplatz verfügt über eine eigene Offline-Datenbank. Dadurch ist der Verwalter vor einer schlechten WLAN-Verbindung geschützt, denn die geladenen Daten stehen auch dann noch zur Verfügung, wenn es keine Internet-Verbindung gibt oder die Anwendung zwischendurch einmal geschlossen wurde. Beim Neustart der Anwendung werden die beiden Datenstände synchronisiert. Durch dieses Verfahren wird Server-Traffic gespart und die Ladezeiten werden verbessert. Die lokale Datenbank ist nach dem XXTEA-Verfahren verschlüsselt.

Der XXTEA (auch Corrected Block Tiny Encryption Algorithm) ist die von den Briten David Wheeler und Roger Needham 1998 an der Universität Cambridge vorgenommene Weiterentwicklung von Block TEA, einer TEA-Variante mit variabler Blocklänge. Auch XXTEA ist eine einfache symmetrische Blockchiffre. XXTEA basiert auf einem Feistel-Netzwerk und benutzt variabel große Blöcke und einen 128-Bit-Schlüssel (16 Zeichen). XXTEA stellt eine Korrektur der Schwächen des ursprünglich zeitgleich mit TEA publizierten Block TEA dar. XXTEA ist wie auch seine Vorgänger TEA und XTEA frei von Patenten.

Für jede Installation wird ein individuelles Passwort verwendet. **Das Passwort wird automatisch generiert.**

Damit ist ein Konzept entstanden, wie auch ohne Internet- und Mobilfunk-Empfang die digitale oder hybride WEG-Versammlung mit elektronischer Abstimmung durchgeführt werden kann.

Bei den technischen Komponenten wurde auf die Sicherheit und den Datenschutz größten Wert gelegt. Diese Komponenten werden in der Folge besprochen:

1. Hosting bei AWS (Weltmarktführer) mit Serverstandort in Frankfurt am Main
2. Verschlüsselung aller Verbindungen über HTTPS und SSL
3. Verschlüsselung der Daten auf dem Server
4. Automatisiertes Backup aller Daten
5. DSGVO-konforme Speicherung der Nutzerdaten

Mit den Themen Serverstandort, Verschlüsselung von Daten und Verbindungen, Automatisches Backup und DSGVO-konforme Speicherung der Daten werden die wichtigsten Umsetzungen nachfolgend ausführlich beschrieben. Als Anlage sind die Nutzungsbedingungen für Verwalter-Arbeitsplatz und App beigefügt.

## **1. Cloud Computing mit Serverstandort in Frankfurt am Main**

Cloud Computing ist eine IT-Infrastruktur, die beispielsweise über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung.

Die Datenspeicherung in der Cloud erfolgt bei Amazon Web Services (AWS), dem mit 45% Marktanteil Weltmarktführer für Cloud-Lösungen.

Die Datensicherheit hat bei AWS höchste Priorität. In über 190 Ländern erbringt AWS Services für hunderttausende Einrichtungen, einschließlich Großunternehmen, Bildungseinrichtungen und Regierungsbehörden. AWS-Kunden, darunter auch Finanzdienstleister und Dienstleister aus dem Gesundheitswesen, vertrauen AWS ihre sensibelsten Informationen an.

AWS ist so konzipiert, dass Kunden Kontrolle über ihre Inhalte haben, einschließlich wo und wie sie gespeichert werden, sowie wer Zugriff darauf hat. Daraus ergeben sich folgende Vorteile:

- Sichere Skalierung mit hervorragender Sichtbarkeit und Kontrolle
- Automatisieren und Reduzieren von Risiken mit tief integrierten Services
- Entwicklung mit den höchsten Standards für Datenschutz und Datensicherheit
- Größtes Ökosystem von Sicherheitspartnern und -lösungen
- Die umfassendsten Sicherheits- und Compliance-Kontrollen

So werden alle Daten, die über das AWS Global Network fließen, das die AWS- Rechenzentren und Regionen verbindet, automatisch auf der physischen Ebene verschlüsselt, bevor sie die abgesicherten Standorte verlassen. Um die Compliance-Aktivitäten zu unterstützen, erstellt AWS regelmäßig eine Drittanbieter-Validierung für Tausende von globalen Compliance-Anforderungen, die AWS kontinuierlich überwacht.

Neben der Deutschen Bahn oder Siemens nutzten auch viele Start-ups und Firmen wie MyTaxi, Zalando oder Airbnb die Dienste des Unternehmens im Rechenzentrum Frankfurt/Main. 25 Terabyte an Daten werden in den AWS-Zentren pro Sekunde bewegt.

Diese Fakten haben uns dazu bewegt, die Daten der Eigentümerversammlungen und der personenbezogenen Daten der Eigentümer (siehe auch § 28 DSGVO in Punkt 5) AWS anzuvertrauen.

## 2. Verschlüsselung aller Verbindungen über HTTPS und SSL

Hypertext Transfer Protocol Secure (HTTPS, englisch für „sicheres Hypertext-Übertragungsprotokoll“) ist ein Kommunikationsprotokoll im World Wide Web, mit dem Daten abhörsicher übertragen werden können. Es stellt eine Transportverschlüsselung dar. SSL steht für Secure Sockets Layer, die alte Bezeichnung für Transport Layer Security, ein Netzwerkprotokoll zur sicheren Übertragung von Daten.

Wie in Punkt 1 beschrieben, sind die Daten im Rechenzentrum verschlüsselt und werden auch für den Transport verschlüsselt. Wichtig ist, dass der Übertragungsweg zur Software auch den Sicherheitsanforderungen entspricht.

Zunächst sollen die beiden wichtigsten Abkürzungen erläutert werden:

**SSL:** Secure Socket Layer. Hierbei handelt es sich in erster Linie um eine Möglichkeit, einen Server zu authentifizieren.

**HTTPS:** Hypertext Transfer Protocol Secure. Hierbei handelt es sich um ein Protokoll, welches die Verschlüsselung durchführt.

Ein SSL-Zertifikat ermöglicht es dem Computer eines Seitenbesuchers die Identität des Seitenservers zu identifizieren und zu bestätigen. Bevor eine eigentliche Verbindung zwischen einem Browser und dem Server der Website hergestellt wird, findet ein „Handshake“ statt: Der Browser überprüft, ob er auch wirklich mit dem richtigen Server in Kontakt steht und ermittelt anschließend einen Schlüssel, mit welchem die Daten der Sitzung enkodiert werden. Die Nutzung dieser Technik ist an der URL einer Seite erkennbar: Diese beginnt bei Einbindung eines SSL-Zertifikats mit „HTTPS“. Die Sicherheit dieser Seiten ist deutlich größer als bei unverschlüsselten Websites. In Sachen Datenschutz ist das HTTPS-Protokoll empfehlenswert.

Was für Webseiten gilt, gilt auch entsprechend für die Übertragungswege von Daten. SSL ist die Standardtechnologie für die Absicherung von Internetverbindungen und den Schutz sensibler Daten, die zwischen zwei Systemen übertragen werden. So wird verhindert, dass Kriminelle übertragene Informationen, einschließlich potenzieller persönlicher Daten, lesen und verändern. Bei diesen beiden Systemen kann es sich um einen Server und einen Client

oder um eine Übertragung von einem Server auf einen anderen handeln. Die oben genannten Sicherheitsvorteile - Authentifizierung des Servers, Verschlüsselung der Datenübertragung und Schutz des Austauschs vor Manipulation - sind die Hauptvorteile des Einsatzes von HTTPS für die Datenübertragung.

### **3. Verschlüsselung der Daten auf dem Server**

Verschlüsselung ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.

Back4App ist eine Backend-Lösung, die sich ideal für Entwickler eignet, für die Benutzerfreundlichkeit, relationalen Abfragen und GraphQL-APIs wichtig sind. Es ist vor allem für die Skalierbarkeit und Benutzerfreundlichkeit für Entwickler bekannt. Back4App wird häufig für die Entwicklung, das Hosting und die Verwaltung von Anwendungen auf einer einzigen Plattform genutzt. Es eignet sich hervorragend zum Hosten von APIs für Web-, Mobil- und Internet of Things-Anwendungen (IoT).

Diese Anwendungen verwenden eine bestimmte Infrastruktur, die in einem AWS-Rechenzentrum gehostet wird. Die Verschlüsselung wird angewendet auf:

- EFS volumes mit KMS
- EBS volumes
- Buckets S3 (serverseitig), mit SSE-S3

In diesen Fällen verwaltet AWS die Verschlüsselungs-Schlüssel. Die Verschlüsselung wird auch auf MongoDB- und Konfigurationsdateien angewendet, wobei das Verschlüsselungssystem im Ruhezustand verwendet wird. Der gesamte Datenverkehr zwischen Servern und Clients erfolgt über HTTPS und SSL.

Die Verwaltung der Verschlüsselungsschlüssel erfolgt auf zwei Arten, je nachdem, wer für die Verschlüsselung verantwortlich ist. Von AWS generierte Schlüssel werden mithilfe von AWS KMS verwaltet, das von Back4App gemäß den unter „Konfigurationsverfahren für GDPR-Schutzmaßnahmen“ beschriebenen Verfahren konfiguriert wird. Schlüssel, die bei der Verschlüsselung von MongoDB- und Konfigurationsdateien generiert werden, werden von Back4App DPO verwaltet. In beiden Fällen läuft das Verfahren unter den gleichen Einstellungen maximal 90 Tage.

#### 4. Automatisiertes Backup aller Daten

Datensicherung (englisch backup) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können. Somit ist Datensicherung eine elementare Maßnahme zur Datensicherheit.

Wie sieht die Back4App-Infrastruktur aus? Die Server befinden sich bei Amazon AWS und die Einrichtung der Back4app-Infrastruktur berücksichtigt die folgenden Faktoren:

- Skalierbares Design - Die bei Back4app gehosteten Anwendungen werden automatisch skaliert.
- Redundanz - Vollständig redundante Serverstruktur, die Ausfallzeiten minimiert.
- Datensicherung - Die in Back4app gespeicherten Daten sind sicher und eine automatisierte Sicherungsroutine ist vorhanden.
- Leistung - Die Back4app-Serverarchitektur wurde eingerichtet, um die Leistung von Apps zu maximieren und Verzögerungen zu vermeiden.

Die bei Back4app gespeicherten Daten sind sicher und es gibt eine tägliche automatisierte Sicherungsroutine. Back4App führt automatische Backups einmal pro Stunde durch, die 7 Tage gespeichert werden. Einmal am Tag erfolgt eine Datensicherung, die 30 Tage gespeichert wird. Eine Restore-Routine ist verfügbar.

#### 5. DSGVO-konforme Speicherung der Nutzerdaten

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Je nach Geschäftsbeziehung kommen bestimmte Kapitel und Artikel der DSGVO bei unserem Software-Leistungsumfang in Frage. Für alle Fälle halten wir bestimmte Musterverträge vor, die zwischen Auftraggeber und Auftragnehmer abgeschlossen werden können.

Wir verarbeiten folgende Daten:

**Liegenschaft:** Referenz-ID der Liegenschaft, Name der Liegenschaft, Adresszusatz, Land der Liegenschaft, Ort der Liegenschaft, PLZ der Liegenschaft, Anmerkung bzgl. der Liegenschaft

**Daten zur Eigentümerversammlung:** Summe Eigentumsanteile der Liegenschaft, Abstimmungsverfahren (nach Köpfen, Einheiten oder MEA), Kontaktpräferenz (Online, per Brief), Miteigentumsanteil des Eigentümers

**Daten zur Einheit:** Referenz-ID der Einheit, Name der Einheit, Adresse der Einheit, Adresszusatz, Anmerkung bzgl. der Einheit

**Daten zum Eigentümer:** Referenz-ID des Kontakts, Anrede, Titel, Vorname, Nachname, Unternehmen, Unternehmensrolle, E-Mail, Telefon (Festnetz), Handy, Fax, Straße und Hausnummer, Adresszusatz, PLZ, Ort, Land, Notiz bzgl. des Kontakts, Vertragsart (immer Eigentümer), Vertragsbeginn, Vertragsende, Vertragsnummer

Diese Daten werden uns über unsere eigene API (verfügbar ab KW 13/2021) oder den Partner-API's zur Verfügung gestellt. Ein Import über MS-EXCEL und CSV sollte nur die Ausnahme sein, da eine genaue Prüfung der Daten erforderlich wird (aus PLZ 04435 darf nicht 4435 werden).

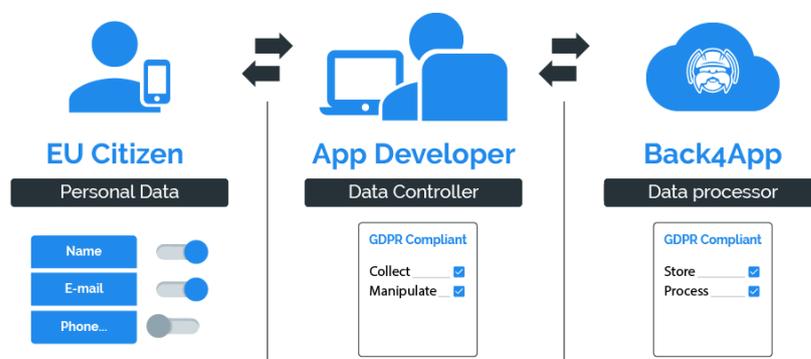
Auch die Programmierumgebung berücksichtigt die DSGVO-Vorgaben. Dazu sind zunächst zwei Begriffsdefinitionen notwendig:

Was ist ein Datencontroller?

Eine Organisation, die Daten von EU-Bürgern sammelt. bezeichnet die natürliche oder juristische Person, Behörde, Agentur oder andere Einrichtung, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt; Wenn die Zwecke und Mittel einer solchen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten bestimmt sind, kann der für die Verarbeitung Verantwortliche oder die spezifischen Kriterien für seine Ernennung durch das Recht der Union oder der Mitgliedstaaten festgelegt werden. Back4App-Clients fungieren normalerweise als Datencontroller für alle persönlichen Daten, die Back4App zur Verfügung gestellt werden.

Was ist ein Datenprozessor?

Eine Organisation, die Daten im Auftrag eines Datencontrollers wie Cloud-Dienstleister verarbeitet. Unter Verarbeitung sind alle Vorgänge oder Vorgänge zu verstehen, die mit personenbezogenen Daten oder mit personenbezogenen Daten durchgeführt werden, unabhängig davon, ob diese automatisiert erfolgen oder nicht, wie z. B. Erfassung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, Abruf, Konsultation, Verwendung, Offenlegung durch Übertragung, Verbreitung oder anderweitige Bereitstellung, Ausrichtung oder Kombination, Einschränkung, Löschung oder Zerstörung. Back4App fungiert normalerweise als Datenverarbeiter für alle Personendaten, die von unseren Kunden zur Verfügung gestellt werden.



## **Back4App als Datencontroller**

Back4App fungiert als Datenverantwortlicher, wenn es die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.

Einige Beispiele sind:

- Wenn Daten bezüglich Kontoregistrierung, Verwaltung und Zugriff auf Dienste gespeichert werden.
- Wann wurden Daten zu Supportaktivitäten gespeichert?

## **Data Processing Agreement (DPA)**

Ein Data Processing Agreement (DPA), (deutsch: Auftragsverarbeitungsvertrag (AVV, ehemals: Auftragsdatenverarbeitungsvertrag) wird von Unternehmen (Datencontroller, Datenverantwortlicher) abgeschlossen, wenn personenbezogene Daten durch einen weisungsabhängigen Dienstleister (Datenprozessor, Datenverarbeiter) verarbeitet werden. Der DPA sichert beide Parteien ab und regelt für beide Seiten die Besonderheiten im Umgang mit personenbezogenen Daten. Dazu zählen zum Beispiel Umfang und Zweck der Speicherung und Datenverarbeitung. Zusätzlich gewährleistet der DPA die durch die EU-Datenschutzgrundverordnung (DSGVO) erforderlichen Datenschutzmaßnahmen.

Back4App arbeitet mit folgenden Drittfirmen zusammen: AWS – Amazon Web Services, Inc und Cloudflare, Inc. Amazon Web Services bietet zuverlässige, skalierbare und kostengünstige Cloud-Computerdienste. Cloudflare bietet CDN, DNS, DDoS Datenschutz- und Datensicherheits-Dienste.

Um der EU-DSGVO zu entsprechen, hat Back4App ein Sicherheitsprogramm entwickelt, das auf fünf Elementen basiert:

- Nutzung der DSGVO-konformen Infrastruktur;
- Interne Richtlinien;
- Aufzeichnung der Verarbeitungsaktivitäten;
- Regelmäßige Überprüfung der Schutzmaßnahmen;
- Einhaltung des festgelegten Verhaltenskodex.

Das Back4-App-Handbuch mit Sicherheitsinformationen ist unter <https://www.back4app.com/product/parse-gdpr/gdpr-security-manual> abrufbar.

Die WEG-Verwaltung Pergolenviertel UG (haftungsbeschränkt), Geschäftsbereich Hausverwalter-Service, hat mit Back4App einen DPA/AVV-Vertrag abgeschlossen. Er kann auf Anfrage eingesehen werden.

Die Einhaltung der Datenschutz-Maßnahmen und sonstigen Sicherheitsmaßnahmen setzen voraus, dass auch die Nutzungsbedingungen, die in App und Verwalter-Arbeitsplatz abrufbar sind, vom Verwalter und Eigentümer eingehalten werden. Die Nutzungsbedingungen sind deshalb Anlage dieser Sicherheitsbroschüre.

## Anlage 1:

### Nutzungsbedingungen

#### 1. Geltungsbereich

1.1. Die WEG-Verwaltung Pergolenviertel UG (haftungsbeschränkt), Hamburg, HRB 158099 (nachfolgend „Anbieter“ genannt), ist Betreiber der Internetpräsenzen „*beschluss.app*“ und „*hausverwalter-service.de*“. Der Anbieter stellt über seine Internetseiten und in den einschlägigen App-Stores eine App (im Folgenden „*beschluss.app*“ genannt) zur Verfügung, mit dessen Hilfe Wohnungseigentümer (im Folgenden „Nutzer“ genannt) über Beschlüsse ihrer Wohnungseigentümergeinschaft abstimmen können, die durch die Wohnungsverwaltung (im Folgenden „Wohnungsverwalter“ genannt) auf einer Eigentümerversammlung, einer Online-Versammlung oder mittels Umlaufbeschluss vorgestellt werden. Der Wohnungsverwalter verfügt über eine Desktop-Anwendung, um u. a. die Tagesordnung zu verwalten sowie die Stimmen auszuwerten. Die nachfolgenden Bedingungen regeln die entgeltliche Nutzung des Verwalter-Arbeitsplatzes durch den Wohnungsverwalter, aber auch die unentgeltliche Nutzung der *beschluss.app* durch den Nutzer. Im Falle der Lizenzübertragung an den Wohnungsverwalter treffen Bestimmungen, die den Anbieter betreffen, auch teilweise auf den Wohnungsverwalter zu. Dies ist in den Nutzungsbedingungen an den entsprechenden Stellen kenntlich gemacht.

1.2. Die nachfolgenden Nutzungsbedingungen gelten für sämtliche Geschäftsbeziehungen zwischen dem Anbieter und dem Nutzer der *beschluss.app* sowie zwischen dem Anbieter und dem Wohnungsverwalter.

1.3. Es gelten ausschließlich die Nutzungsbedingungen des Anbieters. Von diesen Nutzungsbedingungen abweichende Bedingungen des Nutzers oder des Wohnungsverwalters werden, selbst bei Kenntnis, nicht Vertragsbestandteil, es sei denn, ihre Geltung wird durch bevollmächtigte Vertreter ausdrücklich schriftlich zugestimmt.

#### 2. Leistungen des Anbieters

2.1. Die *beschluss.app* setzt einen lizenzierten Verwalter-Arbeitsplatz voraus. Der Wohnungsverwalter nutzt diesen Arbeitsplatz zur Erstellung der Tagesordnung, zur Einladung, zur Durchführung der Eigentümerversammlung und zur Nachbearbeitung der Versammlung. Auch die Kommunikation mit den Abstimmungsgeräten erfolgt über den Verwalter-Arbeitsplatz.

2.2. Der Anbieter stellt entgeltlich den Verwalter-Arbeitsplatz zur Verfügung, der es Wohnungsverwaltern ermöglicht, ihre Versammlungen über die zur Verfügung gestellte *beschluss.app* und dazugehörige Tools (Registrierung, E-Post-Dienste, Einbindung TED-Systeme und ähnliche) zu verwalten, zu organisieren und inhaltlich zu gestalten. Den Nutzern wird ermöglicht, auf die *beschluss.app* über einen Link zuzugreifen, und über die *beschluss.app* die Teilnahme zu verwalten und Informationen über die Veranstaltung zu bekommen. Der Wohnungsverwalter kontrolliert selbstständig und eigenverantwortlich die Inhalte der *beschluss.app* und des Verwalter-Arbeitsplatzes. Auf diesem Weg unterstützt der Anbieter einerseits die digitale Kommunikation zwischen den verschiedenen Interessensgruppen einer

Wohnanlage und fördert andererseits die vollständige Digitalisierung der Vorbereitung, Durchführung und Nachbearbeitung der Eigentümerversammlungen.

2.3. Im Rahmen der Datenverarbeitung mit dem Verwalter-Arbeitsplatz werden externe Dienste genutzt.

Die Versand-API ist Teil der E-POSTBUSINESS API, das die REST-Schnittstelle des E-POST Systems für Anbieter von Software darstellt. Die E-POSTBUSINESS API ermöglicht die Integration bzw. Anbindung der E-POST Funktionalitäten in den Verwalter-Arbeitsplatz. Mit der E-POSTBUSINESS API wird das Versenden von E-POSTBRIEFEN ermöglicht. Die Einladungen zur Eigentümerversammlung werden optional als E-POSTBRIEF versandt. Nähere Informationen sind dem Integrationsleitfaden zu entnehmen:

[https://www.deutschepost.de/content/dam/dpag/images/E\\_e/epost/partnerportal/Downloads/api\\_send\\_documentation.pdf](https://www.deutschepost.de/content/dam/dpag/images/E_e/epost/partnerportal/Downloads/api_send_documentation.pdf)

Es wird nicht immer möglich sein, dass alle Nutzer in einer Eigentümerversammlung über die *beschluss.app* verfügen. Aus diesem Grund werden TED-Abstimmgeräte am Verwalter-Arbeitsplatz eingebunden. TED-Systeme der Firma SunVote sind kleine Abstimmgeräte, die der Wohnungsverwalter auf einer Eigentümerversammlung verteilen kann. Sie können gemietet oder gekauft werden.

Für die unmittelbare Erstellung der Niederschrift werden Unterschrift-Pads der Firma StepOver GmbH eingesetzt.

2.4. Der Anbieter ist jederzeit berechtigt, die zur Verfügung gestellten Dienste teilweise oder insgesamt zu ändern oder zu ergänzen oder zu beenden. Alle Komponenten sind in die Anwendung integriert und nicht ohne weitere Software-Entwicklung austauschbar.

### **3. Registrierung, Mitgliedschaft und Zusicherungen bei der Registrierung**

3.1. Die Nutzung des Dienstes setzt die Registrierung und Anlage eines Benutzerkontos des Nutzers voraus. Die Registrierung ist nur volljährigen und voll geschäftsfähigen Nutzern erlaubt. Durch den Abschluss der Registrierung gibt der Nutzer ein Angebot zum Abschluss eines Vertrages über die Nutzung des Dienstes ab. Der Anbieter nimmt dieses Angebot des Nutzers durch Bereitstellung der entsprechenden Dienste an. Erst durch diese Annahme kommt der Vertrag zwischen dem Nutzer und dem Anbieter zu Stande. Der Anbieter ist nicht zum Vertragsschluss verpflichtet.

3.2. Der Nutzer sichert zu, dass alle von ihm angegebenen Daten vollständig und wahr sind. Der Nutzer ist verpflichtet, die Daten hinsichtlich aller von ihm genutzten Anwendungen während der gesamten Vertragslaufzeit wahr und vollständig zu halten.

3.3. Für den Fall, dass der Nutzer für eine juristische Person tätig wird, sichert er zu, bevollmächtigt zu sein, um im Namen der juristischen Person tätig zu werden. Der Nutzer wird auf Anfrage des Anbieters die gemäß dieser Ziffer zugesicherten Angaben entsprechend nachweisen.

3.4. Der Nutzer ist damit einverstanden, dass ihm unter Verwendung der angegebenen E-Mail-Adresse zu Zwecken der Kommunikationsunterstützung zwischen Nutzer und

Wohnungsverwalter, Benachrichtigungen, insbesondere auch zu Neuerungen und Leistungen des Dienstes übermittelt werden.

3.5. Der Nutzer erklärt sich damit einverstanden, dass der Wohnungsverwalter die angegebene E-Mail- Adresse sowie bestimmte Daten aus dem Verwaltungssystem (Postadresse, Rufnummer des Smartphones etc.) für die Begründung, Durchführung und ggf. Beendigung des Vertrages verwenden darf.

3.6. Der Anbieter oder Wohnungsverwalter kann technisch nicht feststellen, ob ein registrierter Nutzer tatsächlich diejenige Person darstellt, die er vorgibt zu sein. Der Anbieter oder Wohnungsverwalter leistet daher keine Gewähr für die tatsächliche Identität des Nutzers.

3.7. Für den Erwerb einer Mitgliedschaft ist eine Registrierung erforderlich, bei der der Nutzer unter anderem ein Passwort zu wählen hat. Der Nutzer ist verpflichtet, das von ihm gewählte Passwort geheim zu halten. Sollten Dritte von dem Passwort des Nutzers Kenntnis erlangen, so kann der Nutzer das Passwort in der App ändern. Der Anbieter wird seinerseits das Passwort nicht an Dritte weitergeben und dieses nur für den Anmeldevorgang nutzen. Aus Sicherheitsgründen und zur Vorbeugung eines Missbrauches wird dem Nutzer empfohlen, sein Passwort in regelmäßigen Abständen zu ändern. Die Sicherung und Aufbewahrung der Zugangsdaten zur Nutzung des Dienstes fällt in den ausschließlichen Verantwortungsbereich des Nutzers.

3.8. Jeder Nutzer ist berechtigt, ein Nutzerprofil anzulegen. Es ist dem Nutzer jedoch nicht gestattet, das eigene Nutzerprofil Dritten zur Verfügung zu stellen.

#### **4. Allgemeine Pflichten des Nutzers**

4.1. Der Nutzer ist verpflichtet, ausschließlich wahre und nicht irreführende Angaben zu machen, sowie seinen vollständigen Namen und kein Pseudonym oder Künstlernamen zu verwenden.

4.2. Der Nutzer verpflichtet sich bei der Nutzung des Dienstes geltendes Recht, sowie alle Rechte Dritter zu beachten. Der Nutzer ist verpflichtet, belästigende Handlungen zu unterlassen, auch wenn diese nicht gegen gesetzliche Vorgaben verstoßen sollten. Dem Nutzer ist weiter jede Handlung untersagt, die geeignet ist, die Funktionalität des Dienstes zu beeinträchtigen.

4.3. Der Nutzer verpflichtet sich, den Anbieter von sämtlichen Ansprüchen Dritter schadlos und klaglos zu halten, die auf einer rechtswidrigen Nutzung der zur Verfügung gestellten Dienste beruhen oder mit seiner Zustimmung erfolgen oder sich insbesondere aus datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die durch ein rechtswidriges Handeln des Nutzers im Rahmen der Nutzung des Dienstes hervorgerufen worden sind. Erkennt der Nutzer oder muss er erkennen, dass ein solcher Verstoß droht, wird der Hausverwalter unverzüglich hiervon unterrichten.

4.4. Der Anbieter oder der Hausverwalter ist berechtigt, bei schwerwiegenden Verstößen gegen sich aus diesen Nutzungsbedingungen ergebenden Pflichten des Nutzers sowie bei begründeten erheblichen Verdachtsmomenten für eine entsprechende Pflichtverletzung das Benutzerkonto des Nutzers zu sperren.

4.5. Der Nutzer ist nicht berechtigt, irgendeinen Teil der zur Verfügung gestellten Dienste oder der darin enthaltenen Software zu vervielfältigen, zu verändern, zu verbreiten, zu verkaufen oder zu vermieten, es sei denn, der Nutzer verfügt über eine schriftliche Einwilligung des Anbieters.

## **5. Verfügbarkeit**

5.1. Der Anbieter ist berechtigt, die zur Verfügung gestellten Dienste zu ändern, auszusetzen oder zu beenden.

5.2. Der Nutzer erkennt an, dass eine hundertprozentige Verfügbarkeit des Dienstes technisch nicht durchführbar ist. Der Anbieter ist bemüht, den Dienst möglichst konstant verfügbar zu halten. Anpassungen, Änderungen und Ergänzungen des Verwalter-Arbeitsplatzes beziehungsweise der zur Verfügung gestellten Dienste sowie Maßnahmen, die der Feststellung und Behebung von Funktionsstörungen dienen, letztlich Ereignisse, die nicht im Einflussbereich des Anbieters stehen, können zu Störungen oder zur vorübergehenden Einstellung der Dienste führen.

## **6. Data-Hosting**

6.1. Der Anbieter ist verpflichtet, geeignete Vorkehrungen gegen Datenverlust und zur Verhinderung unbefugten Zugriff Dritter auf die Daten des Nutzers zu treffen.

6.2. Der Anbieter verwendet in wirtschaftlich angemessenem Umfang die jeweils dem Stand der Technik entsprechenden Sicherheitstechnologien (Bsp. Verschlüsselungen, Kennwort- und Firewall-Schutz) bei der Bereitstellung der Services. Der Nutzer verpflichtet sich, die gültigen Sicherheits-Richtlinien und –verfahren entsprechend zu beachten, die ihm im Rahmen dieser Vereinbarung mitgeteilt werden.

## **7. Nutzungsrechte**

7.1. Der Anbieter räumt dem Nutzer das nicht ausschließliche, nicht übertragbare Recht ein, die *beschluss.app* auf den Smartphones des Nutzers und den Smartphones der Mitbewohner der Wohneinheit zu nutzen. Für Abstimmungen sind die Stimmrechte der Versammlung maßgeblich. Darüber hinaus gehende Rechte erhält der Nutzer nicht. Sämtliche über die *beschluss.app* angebotenen Dienste, insbesondere zur Verfügung gestellte Informationen, Daten, Texte, Bilder, Grafiken etc. dürfen ausschließlich nur zum privaten Gebrauch des Nutzers verwendet werden. Eine kommerzielle Nutzung, auf welche Art diese auch immer erfolgt, ist unzulässig.

7.2. Der Nutzer ist nicht berechtigt, die *beschluss.app* über die nach Maßgabe dieses Vertrages erlaubte Nutzung hinaus zu nutzen oder von Dritten nutzen zu lassen oder Dritten zugänglich zu machen. In weiteren Programmständen ist geplant, die App mit einem QR-Code der Versammlung zu versehen. Dieser QR-Code soll dann zur Einlasskontrolle bei der Eigentümerversammlung verwendet werden.

7.3. Der Nutzer verpflichtet sich, jede wie auch immer geartete Verwertung oder Nutzung der über die *beschluss.app* angebotenen Dienste zu unterlassen, insbesondere jede Vervielfältigung, das Speichern, die Verbreitung, die Veröffentlichung oder die Bearbeitung, insbesondere von Informationen, Texten, Grafiken und Dateien.

## **8. Gewährleistung / Haftung**

8.1. Die vom Anbieter zur Verfügung gestellten Dienste werden nicht für die individuellen Anforderungen und Bedürfnisse einer einzelnen Person, sondern für die Allgemeinheit erstellt. Der Anbieter wird die angebotenen Dienste sorgfältig auswählen, übernimmt jedoch keine Gewähr und/oder Haftung für die inhaltliche Richtigkeit, Aktualität, Fehlerfreiheit oder Vollständigkeit der angebotenen Dienste sowie für eine bestimmte Verwend- oder Verwertbarkeit derselben.

8.2. Der Anbieter bietet den Nutzern auch Dienste an, die von Dritten vermittelt, erstellt oder zur Verfügung gestellt werden. Der Anbieter wird darauf achten, durch den Betrieb der *beschluss.app* keine Rechte Dritter, insbesondere Urheber-, Verwertungs-, Marken- oder sonstige Nutzungsrechte, zu verletzen. Der Anbieter übernimmt keine Gewähr dafür, dass die von Nutzern in Anspruch genommenen Dienste frei von Rechten Dritter sind. Eine Haftung für allenfalls daraus resultierende Schäden ist ausgeschlossen. Insoweit Dritte Angebote vorhalten oder bestimmte Waren und/oder Leistungen vertreiben oder zum Abruf bereithalten, so handelt es sich hierbei nicht um Leistungen des Anbieters. Diese Angebote werden von dem jeweiligen Unternehmen in eigener Verantwortung vorgehalten.

8.3. Außerhalb des Produkthaftungsgesetzes beschränkt sich die Haftung des Anbieters auf Vorsatz oder grobe Fahrlässigkeit. Die Haftung des Anbieters für leichte Fahrlässigkeit, der Ersatz von Folgeschäden, Vermögensschäden, entgangenem Gewinn, Handlungen seiner Erfüllungsgehilfen und für Schäden aus Ansprüchen Dritter gegen den Nutzer ist ausgeschlossen. Diese Haftungsbeschränkungen gelten nicht bei Personenschäden, bei Schäden an Sachen, die dem Anbieter zur Bearbeitung übergeben wurden und bei atypischen Schäden.

8.4. Die verschuldensunabhängige Haftung des Anbieters auf Schadenersatz (§ 536a BGB) für bei Vertragsabschluss vorhandene Mängel ist ausgeschlossen.

8.5. Nach derzeitigem Stand der Technik ist es nicht möglich, alle Risiken im Zusammenhang mit der Nutzung des Mediums Internet auszuschließen. Aus diesem Grund ist eine Haftung des Anbieters für durch technisch bedingte Ausfälle verursachte Datenverluste, abgebrochene Datenübertragungen oder sonstiges, in diesem Zusammenhang entstandenen Probleme, die nicht im Einflussbereich des Anbieters liegen (höhere Gewalt, Verschulden Dritter) ausgeschlossen. Dieser Haftungsausschluss gilt auch dann, wenn das schadensverursachende Ereignis auf Übertragungswegen des Telekommunikationsdienstleisters oder durch Störungen innerhalb des Internets eingetreten ist (zum Beispiel kein Funk- oder WLAN-Empfang etc.).

8.6. Die vorstehenden Haftungsregelungen gelten auch in Hinsicht auf Mitarbeiter, Vertreter und Erfüllungshilfen des Anbieters.

## **9. Datenschutz / Lizenzen**

9.1. Der Anbieter verweist auf seine Datenschutzerklärung, welche jederzeit abrufbar ist unter <https://hausverwalter-service.de/datenschutzerklärung/>.

9.2. Der Anbieter erklärt, dass es alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen

auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Anbieter aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

9.3. Der Anbieter erklärt, ausreichende Sicherheitsmaßnahmen ergriffen zu haben, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

9.4. Der Anbieter kann ein anderes Unternehmen, auch ohne Zustimmung des Nutzers, zur Durchführung von Verarbeitungen heranziehen.

9.5. Die verwendeten Bibliotheken sind über den Link „Lizenzen“ einzusehen.

## **10. Laufzeit, Beendigung**

10.1. Sowohl der Wohnungsverwalter als auch der Nutzer können das Vertragsverhältnis jederzeit und ohne Angabe von Gründen kündigen. Die Kündigung erfolgt durch den Nutzer durch Löschung seines gesamten Accounts oder durch schriftliche Erklärung (per Brief oder E-Mail) gegenüber dem Wohnungsverwalter. Die Kündigung ist mit Löschung oder Zugang der schriftlichen Kündigungserklärung wirksam. Der Wohnungsverwalter erklärt die Kündigung durch Versendung einer E-Mail an die von dem Nutzer hinterlegte E-Mail-Adresse. Die erklärte Kündigung ist mit Absendung der E-Mail wirksam. Der Account des Nutzers wird drei Tage nach Absendung der E-Mail gelöscht.

10.2. Der Anbieter ist ungeachtet der Regelung in Ziffer 10.1 berechtigt, den Nutzer statt einer Kündigung bei einer Verletzung seiner in Ziffer 4 benannten Verpflichtungen ohne weitere Vorankündigung zunächst zu sperren. Der Nutzer wird über die erfolgte Sperrung per E-Mail informiert. Die Sperre wird aufgehoben, wenn der Nutzer den Nachweis erbringen kann, dass er der entsprechenden Verpflichtung nachkommt. Bringt der Nutzer nicht innerhalb von einem Monat entsprechende Nachweise bei, so ist der Wohnungsverwalter zur Kündigung berechtigt.

10.3. Zum Zwecke des Schutzes des Nutzers gegen unbefugte Löschung seines Benutzerprofils durch Dritte, kann der Anbieter bei der Kündigung eine Identitätsfeststellung durchführen, z. B. durch Abfrage des Benutzernamens und einer registrierten E-Mail-Adresse.

10.4. Bei Beendigung dieses Vertrages ist der Anbieter oder Hausverwalter nicht weiter berechtigt, die Daten des Nutzers für diesen Dienst zu nutzen.

10.5. Die App muss im Falle der Kündigung von allen Smartphones, auf denen die *beschluss.app* installiert ist, deinstalliert werden.

## **11. Gerichtsstand**

11.1. Sollte eine Bestimmung dieses Vertrages rechtlich unwirksam sein, hat dies nicht die Unwirksamkeit des ganzen Vertrages zur Folge. Vielmehr ist die unwirksame Bestimmung durch eine ihrem wirtschaftlichen Zweck entsprechende wirksame Bestimmung zu ersetzen. Gleiches gilt für etwaige Lücken dieses Vertrages.

11.2. Der Anbieter behält sich vor, diese Nutzungsbedingungen für künftige Geschäfte anzupassen. Ausgenommen hiervon sind unzumutbare Änderungen, insbesondere von

wesentlichen Vertragsbestandteilen, wie der geschuldeten Hauptleistungen, die Gegenstand eines Änderungsvertrages wären.

11.3. Ausschließlicher Gerichtsstand für alle Ansprüche aus und aufgrund dieses Vertrages sowie sämtliche zwischen den Parteien sich ergebenden Streitigkeiten über das Zustandekommen, die Abwicklung oder die Beendigung des Vertrages ist, wenn der Partner Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, der jeweilige Sitz des Anbieters, zurzeit Hamburg.

11.4. Auf die Vertragsbeziehungen zwischen den Parteien findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung. Es wird die Anwendung deutschen Rechts unter Ausschluss der Normen des internationalen Privatrechts und des ins deutsche Recht übernommenen UN-Kaufrechts vereinbart.