# Datenschutzkonzept

## des Bezirksverbandes der Kleingärtner Celle e. V.

### 1 Grundsätzliches

#### 1.1 Beachtung der DS-GVO

Der Bezirksverband der Kleingärtner Celle e.V. (BV) hält sich an die geltenden Datenschutzbestimmungen der ab dem 25.05.2018 geltenden Datenschutz-Grundverordnung (DS-GVO). Aus diesem Grund hat der Vorstand des BV ein Datenschutzkonzept beschlossen, das bei Bedarf angepasst werden kann. Anpassungen aufgrund gesetzlicher Änderungen, fehlerhafter Regelungen und redaktioneller Änderungen können ohne neuen Vorstandsbeschluss vorgenommen werden. Das Datenschutzkonzept wird ständig fortgeschrieben.

#### 1.2 Erhebung personenbezogener Daten

Der BV verarbeitet personenbezogene Daten (z. B. Namen, Adressen, Kommunikationsverbindungen, Geburtsdaten, Bankverbindungen), soweit dies aufgrund einer Rechtsgrundlage erlaubt ist, oder die betroffene Person ihre Einwilligung zur Datenerhebung abgegeben hat. Rechtsgrundlage für den BV ist die Satzung des BV, da bestimmte personenbezogene Daten zum Erreichen des Satzungszweckes benötigt werden.

#### 1.3 Weitergabe von Daten

Der BV gibt bestimmte personenbezogene Daten an den Landesverband Niedersächsischer Gartenfreunde e.V. (LNG) weiter, wenn dies zur Aufgabenerfüllung notwendig ist.

#### 1.4 Verzeichnis der Verarbeitungstätigkeiten

Der BV führt ein Verzeichnis der Verarbeitungstätigkeiten und hält dieses aktuell. Aus dem Verzeichnis ist u. a. ersichtlich, auf welche Daten Vorstandsmitglieder des BV zur Erfüllung ihrer Aufgaben zugreifen dürfen.

### 2 Verpflichtungen

#### 2.1 Geheimhaltungspflicht

Die Vorstandsmitglieder des BV sind zur Geheimhaltung verpflichtet. Die Verpflichtung besteht auch nach dem Ausscheiden aus dem BV Vorstand weiter.

#### 2.2 Kenntnisse über den Datenschutz

Der Vorstand des BV trägt Sorge dafür, dass neue Vorstandsmitglieder über die notwendigen Kenntnisse zum Datenschutz verfügen. Hierzu zählen insbesondere Kenntnisse über,

- die sichere Aufbewahrung von schriftlichen und elektronischen Daten,
- die ggf. erforderliche verschlüsselte E-Mail-Korrespondenz,
- die ggf. notwendige sichere Vernichtung von schriftlichen und elektronischen Daten,
- technisch-organisatorische Maßnahmen.

## 3 Verarbeitung personenbezogener Daten

### 3.1 Aufbewahrung und Zugang
Schriftliche Unterlagen und Sicherheitskopien elektronisch verarbeiteter Daten werden grundsätzlich in der Geschäftsstelle des BV, Hannoversche Straße 9 in 29221 Celle aufbewahrt. Der Zugang zu den aufbewahrten Unterlagen ist ausschließlich den Vorstandsmitgliedern des BV gestattet.

### 3.2 Verschluss der Geschäftsstelle des BV
Die Geschäftsstelle ist nach dem Verlassen abzuschließen. Der Zugang darf Dritten nur möglich sein, wenn sich ein Vorstandsmitglied in der Geschäftsstelle befindet. Vorstandsmitglieder erhalten einen Schlüssel für die Geschäftsstelle. Der Verlust eines Schlüssels ist unverzüglich anzuzeigen.

### 3.3 Heimarbeit durch Vorstandsmitglieder des BV
Vorstandsmitglieder verarbeiten personenbezogene Daten auch zu Hause. Dies gilt für schriftliche Unterlagen und elektronische Daten gleichermaßen. Die Vorstandsmitglieder stellen sicher, dass die Daten von anderen Personen (z. B. Familienmitglieder, Besucher usw.) nicht eingesehen werden können.

### 3.4 Zeitnahe Verarbeitung
Vorstandsmitglieder erledigen Vorgänge möglichst zeitnah.

### 3.5 Besondere Sorgfalt beim Umgang mit Akten in der Geschäftsstelle des BV
Unterlagen dürfen nicht offen liegen gelassen werden, wenn Besucher Einsicht nehmen könnten. Nach Abschluss der Bearbeitung müssen die entnommenen Vorgänge wieder in die Aktenschränke zurückgelegt werden.

### 3.6 Dokumentation der Aktenbearbeitung
Wenn Vorgänge aus der Geschäftsstelle mitgenommen werden (z. B. Ordner, Papierunterlagen, elektronische Datenträger) muss dies in einer Entnahmeliste dokumentiert werden. Eingetragen werden das Datum der Entnahme, die Bezeichnung der entnommenen Vorgänge sowie der Name des Entnehmenden. Die Entnahme, ist durch eigenhändige Unterschrift zu bestätigen. Nach der Hineingabe der entnommenen Vorgänge ist das Datum der Hineingabe zu erfassen.

### 3.7 Vernichtung personenbezogener Daten
Alle Daten, die zu Hause elektronisch verarbeitet werden, müssen nach dem Ausscheiden aus dem Vorstand unverzüglich vernichtet werden. Relevante Papierunterlagen müssen dem Vorstand unverzüglich in der Geschäftsstelle übergeben werden, nicht relevante Unterlagen sind unverzüglich zu vernichten. Die Vernichtung der Daten muss ggf. mit einem dem Stand der Technik entsprechenden Hilfsmittel (z. B. Papierschredder, Dateischredder) erfolgen.

## 4 Umgang mit personenbezogenen Daten im Todesfall

### 4.1 Schriftliche Unterlagen und externe Speichermedien
Stirbt ein Vorstandsmitglied des BV, hat der BV Anspruch auf Herausgabe der dem BV gehörenden Unterlagen und Daten. Elektronisch verarbeitete Daten und solche in Papierform dürfen Rechtsnachfolger nicht einsehen, die Daten müssen dem Vorstand unverzüglich übergeben oder vernichtet werden. Die Vorstandsmitglieder sollten ihre möglichen Rechtsnachfolger vorsorglich darüber informieren.

### 4.2 Verpflichtung des Vorstands
Der Vorstand des BV verpflichtet sich dazu, keinerlei persönliche Dateien auf den Speichermedien oder anderer Hardware der/des Verstorbenen einzusehen. Von den Rechtsnachfolgern zum Zweck der Datensicherung freiwillig übergebene Speichermedien gibt der Vorstand nach Erledigung unverzüglich zurück.

## 5 Elektronische Datenverarbeitung

### 5.1 Erfassung personenbezogener Daten mit Privatgeräten
Soweit personenbezogene Daten mit privaten Geräten verarbeitet oder auf privaten Datenträgern gespeichert werden, ist in geeigneter Weise Sorge dafür zu tragen, dass Dritte keinen Zugriff auf die Daten haben. Eine Verpflichtung zur Verschlüsselung der Daten mit einem dem Stand der Technik entsprechenden Verschlüsselungsverfahren ist nur vorgeschrieben, wenn es sich um besonders schutzwürdige oder sensible Daten handelt. Da der BV solche Daten in der Regel nicht erfasst, dürfte dies eher die Ausnahme sein. Jedes Vorstandsmitglied entscheidet eigenverantwortlich, ob die von ihm elektronisch erfassten Daten verschlüsselt werden müssen.

### 5.2 Wiederherstellbarkeit der personenbezogenen Daten
Die Wiederherstellbarkeit personenbezogener Daten ist eine rechtliche Verpflichtung nach der DS-GVO, die unbedingt erfüllbar sein muss. Deshalb müssen Vorstandsmitglieder, die personenbezogene Daten verarbeiten, regelmäßig Sicherungskopien auf mindestens einem USB-Stick oder einer Speicherkarte erstellen. Die Sicherungskopien müssen nicht verschlüsselt werden, da sie in der Geschäftsstelle des BV unter Verschluss gehalten werden. Im Falle einer Verschlüsselung muss das Verschlüsselungsverfahren und das Passwort mindestens einem weiteren Vorstandsmitglied bekannt sein.

### 5.3 Zugriff auf die in der Geschäftsstelle des BV aufbewahrten Sicherungskopien
Auf die Sicherungskopien dürfen andere Vorstandsmitglieder nur zugreifen, wenn dies zur Wiederherstellung von Daten erforderlich ist. Bei einer Neubesetzung von Vorstandsämtern, darf das neue Vorstandsmitglied auf die Sicherungskopien des Vorgängers zugreifen.

## 6 Aufbewahrungsfristen
Die Daten werden nur so lange aufbewahrt, wie es zur Erfüllung der satzungsgemäßen Zwecke des BV oder geltender Rechtsvorschriften erforderlich ist. Sie werden zum frühestmöglichen Zeitpunkt vernichtet. Dabei müssen die gesetzlichen Aufbewahrungsfristen beachtet werden:

- Kassenbelege: 10 Jahre
- Kassenbücher: 10 Jahre
- Buchhaltungsunterlagen: 10 Jahre
- Protokolle: unbegrenzt

## 7 E-Mail

### 7.1 Allgemeines
Über das Internet versandte E-Mails können von Dritten abgefangen und mitgelesen werden. Soweit E-Mails besonders schutzwürdige oder sensible Daten enthalten oder geeignet sind, Personen zu identifizieren, muss in geeigneter Weise Sorge dafür getragen werden, dass das Mitlesen der E-Mails und Anhänge nicht möglich ist, zumindest aber erheblich erschwert wird. Dabei geht es nicht um die Verschlüsselung des Transportweges (SSL, TLS), sondern um die inhaltliche Verschlüsselung der E-Mails (z. B. PGP-Verschlüsselung). Denn auch gesichert übertragene E-Mails können an den Knotenpunkten (Servern der Provider) abgefangen und mitgelesen werden. Das Mitlesen inhaltlich verschlüsselter E-Mails ist hingegen nicht ohne weiteres möglich. Zwar können auch inhaltlich verschlüsselte E-Mails abgefangen werden, dass Lesen der E-Mails ist aber nur möglich, wenn der Abfangende (Hacker) den privaten Schlüssel des Empfängers der E-Mail besitzt. Für das Versenden verschlüsselter E-Mails benötigt der Versender den öffentlichen Schlüssel des Empfängers der E-Mail, damit verschließt der Versender die E-Mail. Der eigene öffentliche Schlüssel dient also dem Verschließen von E-Mails durch den Versender und darf deshalb an Dritte weitergegeben werden. Mit dem privaten Schlüssel werden die vom Versender verschlossenen E-Mails vom Empfänger der E-Mails aufgeschlossen und damit lesbar gemacht. Deshalb darf der eigene „private Schlüssel“ auf keinen Fall an Dritte weitergegeben werden!

**7.2 E-Mails ohne Inhaltsverschlüsselung von Dritten an den BV**
Erhält der Vorstand unverschlüsselte E-Mails von Dritten (z. B. Privatpersonen, Firmen), ist eine Verschlüsselung bei Antworten oder Weiterleitungen nicht erforderlich, da die E-Mails bereits durch die Dritten unverschlüsselt versandt wurden. Es darf davon ausgegangen werden, dass die übermittelnden Dritten die Risiken kennen und mit dem unverschlüsselten Versand einverstanden sind. Dies gilt aber nicht für E-Mails, die der BV von anderen Vereinen erhält. Je nach Inhalt der E-Mails müssen die Vorstandsmitglieder entscheiden, ob bei einer Antwort oder Weiterleitung der E-Mails eine Inhaltsverschlüsselung erforderlich ist.

**7.3 E-Mails von Vorstandmitgliedern des BV**
Versenden Vorstandsmitglieder E-Mails mit besonders schutzwürdigen oder sensiblen Daten, oder mit Daten, die eine eindeutige Identifizierung von Personen ermöglichen, ist ein dem Stand der Technik entsprechender Schutz (z. B. Inhaltsverschlüsselung) gegen unberechtigtes Mitlesen der E-Mails erforderlich. Dies gilt nicht, wenn Nr. 7.2 Satz 1 und 2 zutreffen.

**Der Schutz von E-Mails kann wie folgt gewährleistet werden:**

**Variante 1 (Abkürzungen, Passwort zum Öffnen von Dokumenten)**
Es ist darauf zu achten, dass der Text der E-Mail keine Identifizierung von Personen ermöglicht. Dies kann z. B. durch Abkürzungen oder anstelle von Namen durch Angabe der Parzellennummern erfolgen. Zu beachten ist dabei, dass dies auch für die Betreffzeile der E-Mail gilt. Eventuelle Anlagen müssen mit einem sicheren Passwort zur Berechtigung zum Öffnen der Anlagen geschützt werden. Das Passwort darf den E-Mail-Empfängern nicht mit derselben E-Mail mitgeteilt werden, es ist ihnen gesondert mitzuteilen. Die so versandten E-Mails bieten einen geringen Schutz, der von Hackern leicht umgangen werden kann. Gegen das Mitlesen der Anlagen durch normale Anwender bietet diese Möglichkeit aber einen ausreichenden Schutz.

**Variante 2 (Kein Text, Passwort zum Öffnen von Dokumenten)**
In der Betreffzeile ist der Betreff so zu formulieren, dass eine Identifizierung von Personen nicht möglich ist (z. B. alleinige Angabe der Parzellennummern). Im Textfenster der E-Mails wird kein Text erfasst, allgemeine Hinweise oder Grußworte sind aber möglich. Die eigentlichen E-Mail-Texte werden mit einem geeigneten Textverarbeitungsprogramm, einem geeigneten Tabellenkalkulationsprogramm oder einem geeigneten PDF-Programm erstellt und mit einem sicheren Passwort zur Berechtigung zum Öffnen geschützt. Die so geschützten Dateien werden dann den E-Mails als Anlagen hinzugefügt. Die Texte in den Anlagen dürfen ausführlich sein und es muss nicht mit Abkürzungen gearbeitet werden. Das Passwort darf den E-Mail-Empfängern nicht mit der derselben E-Mail mitgeteilt werden, es ist ihnen gesondert mitzuteilen. Die so versandten E-Mails bieten einen geringen Schutz, der von Hackern leicht umgangen werden kann. Gegen das Mitlesen der Anlagen durch normale Anwender bietet diese Möglichkeit aber einen ausreichenden Schutz.

**Variante 3 (Inhaltsverschlüsselung)**
Werden E-Mails mit ausführlichen Texten, die eine Identifizierung von Personen ermöglichen, mit oder ohne Anlagen versandt, müssen diese E-Mails mit einem dem Stand der Technik entsprechenden Verschlüsselungsverfahren (z. B. PGP-Verschlüsselung) verschlüsselt werden. Ein Passwort zur Berechtigung zum Öffnen von Anlagen ist in diesem Fall nicht erforderlich, da die Anlagen ebenfalls verschlüsselt übertragen werden. Die so versandten E-Mails bieten einen starken Schutz, der von Hackern nur mit sehr großem Aufwand ausgehebelt werden kann. Normale Anwender hingegen haben keine Chance, eventuell abgefangene oder falsch zugestellte E-Mails mitzulesen.

**7.4 Entscheidung über die Anwendung einer Verschlüsselung**
Jedes Vorstandsmitglied entscheidet nach eigenem Ermessen, ob E-Mails verschlüsselt werden müssen. Die unter Nr. 7.3 vorgestellten Varianten dienen als Entscheidungshilfe.

## 8 Onlinespeicher / Eigene Cloud (NAS) / Eigene Speichermedien

### 8.1 Onlinespeicher bei Speicheranbietern

Besonders schutzwürdige oder sensible Daten, die eine eindeutige Identifizierung von Personen ermöglichen, dürfen grundsätzlich nicht unverschlüsselt im Onlinespeicher (Cloud) gespeichert werden. Dies gilt insbesondere, wenn sich die Serverstandorte der Onlinespeicheranbieter außerhalb der Europäischen Union befinden. Dies ist beispielsweise bei OneDrive von Microsoft, Drive von Google, DropBox, Amazon Web Services usw. der Fall. Zwar haben diese Firmen auch Serverstandorte in Europa (u. a. auch direkt in Deutschland), ungewiss ist aber, ob Daten durch die Infrastruktur der Anbieter auch auf Server außerhalb der Europäischen Union gelangen können. Zu den Firmen, die eine sichere Speicherung von Daten ausschließlich in Deutschland garantieren, gehören beispielsweise die Deutsche Telekom GmbH, 1&1, Web.de, Strato-AG und GMX (1&1 Mail & Media GmbH). Aber auch bei diesen Anbietern dürfen die vorgenannten Daten grundsätzlich nur verschlüsselt gespeichert oder in einem Cloud-Safe abgelegt werden. Die Verschlüsselung kann mit Programmen wie z. B. BoxCryptor oder Cryptomator bewerkstelligt werden.

### 8.2 Onlinespeicher in einer eigenen Cloud (NAS), andere Datenträger

Bei einem NAS (Network-Attached-Storage) handelt es sich um einen dedizierten Dateispeicher (File-Storage), der es mehreren Benutzern und heterogenen Client-Geräten ermöglicht, Daten von der zentralen Festplattenkapazität abzurufen. Das NAS ist kein Onlinespeicher im herkömmlichen Sinn. Der Standort des NAS ist in der Regel in einer Wohnung oder in einem Firmengebäude des Anwenders. Der Anwender ist in der Regel auch der Administrator (Admin) des NAS. Er allein entscheidet darüber, wer auf das NAS zugreifen und welche Daten der Zugreifende verwenden darf. Hinsichtlich des Erfordernisses zur Verschlüsselung von Daten ist nach Nr. 5.1 dieses Datenschutzkonzepts zu verfahren. Im Übrigen ist ein ausreichender Schutz der Daten, im Gegensatz zum herkömmlichen Onlinespeicher, durch die heimische Speicherung und Verwaltung der Daten sichergestellt.

### 8.3 Speichermedien (z. B. Festplatten, USB-Sticks, Speicherkarten, Smartphone usw.)

Für die Speicherung von personenbezogenen Daten auf Speichermedien der Vorstandsmitglieder gilt Nr. 8.2 entsprechend.

## 9 Technisch-organisatorische Maßnahmen

Jeder Verantwortliche muss geeignete technische und organisatorische Maßnahmen treffen, um für Daten ein Schutzniveau zu gewährleisten, das dem Risiko der konkreten Verarbeitung angemessen ist. Es sollten also stets aktuelle Betriebssysteme und Anwendungen verwendet werden. Außerdem sollten regelmäßige Backups durchgeführt und aktuelle Virenscanner verwendet werden. Ein effektiver Passwortschutz muss selbstverständlich sein.

## 10 Internetseite des BV (Homepage)

Der BV betreibt eine Internetseite über den Hostinganbieter Gartenbund.de mit Sitz in Deutschland. Der Hostinganbieter gewährleistet die Einhaltung der Vorschriften der DS-GVO. Die Regelungen zum Datenschutz sind auf der Homepage des BV nachlesbar. Insoweit wird auf die Homepage des BV verwiesen.

**Angaben zum Hostinganbieter:**

20Media GmbH
Eiswerderstr. 14
13585 Berlin
Deutschland
Telefon: +49 178 790 57 48
Homepage: https://www.20media.de/
E-Mail: info@20media.de

## 11 Haftung der Vorstandsmitglieder des BV

### 11.1 Grundsatz der Einzelhaftung
Alle Vorstandsmitglieder haften bei Verstößen gegen das Datenschutzrecht persönlich. Die Mithaftung anderer Vorstandsmitglieder ist, vorbehaltlich abweichender gesetzlicher Regelungen, ausgeschlossen.

### 11.2 Haftung bei Verstößen gegen das Datenschutzkonzept des BV
Bei der Verhängung von Strafen und Bußgeldern sowie dem Eintritt von Vermögensschäden oder sonstigen Schadenersatzforderungen gegen den Verein können die Vorstandsmitglieder persönlich in Regress genommen werden, wenn sie grob fahrlässig oder vorsätzlich gehandelt haben. Die Entscheidung darüber obliegt der Mitgliederversammlung des BV.

### 11.3 Schadensersatz
Für einen Datenschutzverstoß verantwortliche Vorstandsmitglieder haben den anderen Vorstandsmitgliedern, vorbehaltlich abweichender gesetzlicher Regelungen, ggf. entstandene Schäden zu ersetzen. Dies gilt insbesondere für durch die Datenschutzaufsichtsbehörde an den gesamten Vorstand verhängte Strafen und Bußgelder.

## 12 Meldung von Vorfällen an die Datenschutzaufsichtsbehörde
Verletzungen gegen den Schutz besonders schutzwürdiger oder sensibler Daten sind vom Vorstand gemäß § 33 DS-GVO binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Dies gilt jedoch nicht, wenn die Verletzung des Schutzes voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten des Betroffenen führt. Der Vorstand hat vor einer Meldung an die Aufsichtsbehörde eine schriftliche Risikobewertung vorzunehmen. Erfolgt eine nach dem Ergebnis der Risikobewertung erforderliche Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist der Meldung eine schriftliche Begründung für die Verzögerung beizufügen.

**Zuständige Aufsichtsbehörde ist:**

Die Landesbeauftragte
für den Datenschutz in Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon: 0511 - 120 4500
Fax: 0511 - 120 4599
E-Mail: poststelle@lfd.niedersachsen.de

## 13 Salvatorische Klausel
Sollten einzelne Regelungen/Bestimmungen dieses Datenschutzkonzeptes aus irgendwelchen Gründen unwirksam sein oder nachträglich unwirksam werden, bleibt davon die Wirksamkeit des Datenschutzkonzeptes im Übrigen unberührt. An die Stelle der unwirksamen Regelungen/ Bestimmungen, soll diejenige wirksame und durchführbare Regelung/Bestimmung treten, deren Wirkung dem beabsichtigten Zweck am nächsten kommt, welchen der BV mit der unwirksamen Regelung/Bestimmung verfolgt hat.

## 14 Inkrafttreten
Das vorstehende Datenschutzkonzept des Bezirksverbands der Kleingärtner Celle e.V. tritt mit Genehmigung des Vorstandes am 13.07.2021 in Kraft. Gleichzeitig tritt das Datenschutzkonzept vom 01.12.2020 außer Kraft.

Celle, den 13.07.2021

Bezirksverband der
Kleingärtner Celle e.V.
Der Vorstand

## Links:

**Die Landesbeauftragte für den Datenschutz Niedersachsen:**
https://lfd.niedersachsen.de/startseite/wir_uber_uns/die_landesbeauftragte/die-landesbeauftragte-fuer-den-datenschutz-niedersachsen-130186.html

**Datenschutz im Verein:**
https://lfd.niedersachsen.de/themen/vereine/datenschutz-im-verein-56043.html

**Verzeichnis von Verarbeitungstätigkeiten:**
https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/verzeichnis_von_verarbeitungstatigkeiten/verzeichnis-von-verarbeitungstatigkeiten-179665.html

**Meldung von Datenschutzverstößen**
https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/faq/meldung-von-datenschutz-verstoeen-167312.html

**Meldung von Datenschutzverletzungen nach Artikel 33 DS-GVO**
https://lfd.niedersachsen.de/startseite/fortbildung_service/meldung_einer_datenpanne_art_33_dsgvo/meldung-von-datenschutzverletzungen-nach-artikel-33-ds-gvo-164616.html

**Fehlerhaften Link bitte per E-Mail melden an:**
bv-kleingaertner-celle@web.de