

Datenschutzrichtlinie des Bürgerforums Wangen im Allgäu e.V.

Grundsatz

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Vereinsmitglieder, Kunden sowie Geschäftspartner in Übereinstimmung mit den jeweils gültigen Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

Zweck

Diese Richtlinie soll Mitglieder, ehrenamtliche Mitarbeiter und Beschäftigte des Vereins mit den wesentlichen Bestimmungen des Datenschutzes vertraut machen. Darüber hinaus werden einige Empfehlungen gegeben, wie Sie im Umfang mit personenbezogenen Daten Verstöße gegen Datenschutzgesetze und interne Regelungen vermeiden können.

Zielgruppe

Alle Mitglieder und Mitarbeiter des Bürgerforums Wangen im Allgäu e.V., insbesondere die ehrenamtlichen Mitarbeiter, sofern sie im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten (Funktionsträger).

1 Datenschutz

Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person, z.B. Name, Vorname, Geburtsdatum und Ort, Wohnanschrift, Rufnummer, eMailadressen, Bankverbindung oder Vereinstätigkeiten. Das Datenschutzrecht kennt keine frei verwendbaren, personenbezogenen Daten.

Personenbezogene Daten unterliegen hohen Sicherheitsanforderungen. Das Bürgerforum Wangen im Allgäu e.V. verfolgt einen einheitlichen hohen Datenschutz durch den Beschluss die Umsetzung dieser Datenschutzrichtlinie. Diese bieten die Grundlage hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen.

1.1 Grundsätze des Datenschutzes

Personenbezogene Daten müssen

- nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

- für festgelegte eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden;
- den Zwecken entsprechen, für die sie erhoben und / oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;
- sachlich richtig und aktuell sein;
- nach Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, gelöscht oder anonymisiert werden.

1.2 Zulässigkeit der Verarbeitung und Nutzung personenbezogener Daten

Beim Bürgerforum Wangen im Allgäu e.V. ergibt sich die Zulässigkeit aus dem jeweiligen Vertragsverhältnis. Ist dies nichtzutreffend, dann muss eine ausdrückliche Einverständniserklärung eingeholt werden.

Die Empfänger von personenbezogenen Daten dürfen sie nur für den Zweck verarbeiten oder nutzen, für den sie ihnen von der verantwortlichen Stelle zur Verfügung gestellt wurden.

Die Daten dürfen nur satzungsgemäß zweckgebunden verwendet werden und sind nach Zweckerfüllung oder nach Ablauf der Aufbewahrungsfrist zu löschen.

1.3 Übermittlung von Daten

Eine Weitergabe von personenbezogenen Daten ist nur in folgenden Fällen zulässig:

- *Weitergabe an andere Mitglieder*
Dies ist nur im Sinne eines Minderheitenbegehrens nach § 37 BGB zur Einberufung einer Mitgliederversammlung zulässig. Hierfür wäre dann der Vorstand zuständig. Damit ist eine Weitergabe von personenbezogenen Daten an andere Mitglieder grundsätzlich untersagt.
- *Weitergabe an Funktionsträger*
Bei Funktionsträgern gilt: jeder Funktionsträger darf nur die für die Erfüllung seiner Aufgaben erforderlichen Mitgliederdaten kennen, verarbeiten oder nutzen. Dabei dürfen die Daten grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern genutzt werden.
- *Veröffentlichung von Daten*
Im Rahmen der Öffentlichkeitsarbeit über Vereinsaktivitäten dürfen personenbezogene Daten in Aushängen und in Internetauftritten veröffentlicht werden sowie an die Presse weitergegeben werden.
Die Veröffentlichung von Fotos und Videos, die außerhalb öffentlicher Veranstaltungen gemacht wurden, erfolgt ausschließlich auf Grundlage einer Einwilligung der abgebildeten Personen.

Auf der Internetseite des Vereins werden die Daten der Mitglieder der Vorstandschaft, der Gruppenleiter*innen und der Übungsleiter*innen mit Vorname, Nachname, Funktion, eMail-Adresse und/oder Telefonnummer veröffentlicht.

Diesem kann widersprochen werden.

- *Weitergabe zu Werbezwecken (z.B. Sponsor)*
Dies darf nur mit Zustimmung des jeweiligen Mitglieds erfolgen.
- *Persönliche Nachrichten*
Persönliche Nachrichten sind zum Beispiel Spenden, Geburtstage und Jubiläen und dürfen veröffentlicht werden.
Die betroffene Person kann der Veröffentlichung widersprechen.

1.4 Maßnahmen zur Gewährleistung des Datenschutzes

Das Bürgerforum Wangen im Allgäu e.V. ist verpflichtet, angemessene technische und organisatorische Maßnahmen zu treffen, um den Schutz der Daten zu gewährleisten.

Grundsätzlich sind alle personenbezogenen Daten vor Verlust, Manipulation, aber auch vor unbefugter Einsichtnahme zu schützen. Speziell für die automatisierte Datenverarbeitung gibt es gesetzliche Anforderungen, die der Datensicherheit dienen (z. B. Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle).

Im Bereich der Zentralen Datenverarbeitung des Bürgerforum Wangen im Allgäu e.V. wurden umfangreiche Maßnahmen ergriffen, die den Anforderungen des Gesetzes Genüge tun.

Besondere Aufmerksamkeit erfordert der Einsatz von personalisierten IT-Geräten (wie Laptop, Tablet, Smartphone) bei der Verarbeitung personenbezogener Daten, da die Schutzmöglichkeiten für Daten hier im Allgemeinen geringer sind als bei zentralen IT-Anlagen. Die Verantwortung dafür tragen die jeweiligen Benutzer.

Erheben, verarbeiten und nutzen Sie so wenig personenbezogene Daten wie möglich.

Bearbeiten Sie für den Verein personenbezogene Daten in Ihrem Heimnetz, sollten Sie für eine ausreichende Datensicherheit sorgen.

Alle unter Zielgruppe genannten Mitarbeiter sind vom Verein auf das Datengeheimnis hin informiert und hierzu verpflichtet. Sie haben auf die Einhaltung der nationalen Vorschriften und Gesetze und der vereinsintern getroffenen Datenschutzregelungen zu achten. Die Mitarbeiter sind persönlich für die Einhaltung der Gesetze verantwortlich.

2 Empfehlungen

Alle Mitglieder, Mitarbeiterinnen und Mitarbeiter, die mit personenbezogenen Daten zu tun haben, sollten folgende Richtlinien beachten:

2.1 Zweckbindung

Erfassen und verarbeiten Sie nur personenbezogene Daten, die Sie zur Erfüllung der Ihnen übertragenen Aufgabe benötigen. Handeln Sie nach dem Prinzip der Datenvermeidung und Datensparsamkeit:

Vermeiden Sie die Erzeugung von Kopien in andere Systeme oder auf andere Datenträger, da für diese Kopien nicht mehr der umfassende Schutz des Originalsystems gewährleistet werden kann, insbesondere ist das Einhalten von Löschfristen nicht mehr kontrolliert möglich.

Löschen Sie personenbezogene Daten, sobald ihre Kenntnis für die Zweckerfüllung der Speicherung nicht mehr erforderlich ist. Löschen Sie insbesondere nach Ende der Aufbewahrungsfrist.

2.2 Datenqualität und Verhältnismäßigkeit

Halten Sie die Daten sachlich richtig und aktuell. Sie dürfen im Hinblick auf die Zweckbestimmung nicht exzessiv sein.

2.3 Transparenz

Erheben Sie nur Daten mit Kenntnis der Betroffenen oder wenn die Speicherung durch Gesetz oder Vertrag vorgesehen ist. Andernfalls sind die Betroffenen bei der erstmaligen Speicherung über die Art der Daten, den Zweck der Erhebung und die Identität der verantwortlichen Stelle zu benachrichtigen.

2.4 eMailverkehr

eMail-Adressen stellen personenbezogene Daten dar und dürfen nicht ohne schriftliche Einwilligung offengelegt werden.

Möchten Sie eine eMail an mehrere Empfänger senden, dann müssen die eMail-Adressen der Empfänger in „BCC“ eingetragen werden. Adressangaben in dem Feld „BCC“ werden nicht an die Empfänger der eMails durchgereicht. Die Empfängeradressen können daher vom Empfänger der eMail nicht gesehen werden.

Arbeits-/Projektgruppen des Vereins, die eng miteinander zusammenarbeiten, können aufgrund von Kommunikationstransparenz von dieser Regel abweichen.

Des Weiteren dürfen personenbezogene Daten nicht unverschlüsselt per eMail versendet werden, sondern verschlüsselt oder sind als eMail-Anhang, in einer passwortgeschützten Datei, wie 7z, Zip oder bei Office-Dateien mit Kennwortvergabe, zu verschlüsseln.

2.5 Sicherheit und Vertraulichkeit

- Ergreifen Sie Schutzvorkehrungen gegen die Risiken der Verarbeitung: Verhindern Sie jeglichen Missbrauch Ihres Benutzernamens. Verwenden Sie sichere Passworte und geben Sie diese auf keinen Fall weiter.

- Verlassen Sie Ihre IT-Geräte nicht ohne ordnungsgemäße Beendigung der Sitzung. Verwenden Sie Bildschirmschoner mit automatischem Passwort-Schutz nach kurzer Zeit.
- Wenn Ihr IT-Gerät auch anderen zugänglich ist: Stellen Sie sicher, dass auf der lokalen Festplatte keine personenbezogenen Daten gespeichert sind, z.B. durch Verwendung einer zentralen Ablage eines besonders geschützten IT-Gerätes (wie Server, NAS, Cloud). Prinzipiell müssen auch in solchen Fällen - soweit der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht - die Forderungen des Gesetzes erfüllt werden.
- Sorgen Sie dafür, dass nur Berechtigte Einblick in Ihre Unterlagen nehmen können. Halten Sie auch Datenträger mit personenbezogenen Daten wie vertrauliche Unterlagen unter Verschluss.
- Stellen Sie sicher, dass nicht mehr benötigte Unterlagen, soweit Sie sie nicht selbst vernichten können, kontrolliert entsorgt werden (Shredder, verschlossene Abfall-Container).
- Kopieren Sie keine personenbezogenen Daten aus dem Netzwerksystem auf eigene Datenträger über Download, Copy & Paste, Screenshots usw., wenn es nicht ausdrücklich im Verarbeitungsprozess vorgesehen ist.
- Nutzen Sie bei der internen und externen Kommunikation von Daten mit hohem Vertraulichkeitsgrad (Geschäftsgeheimnisse oder sensible personenbezogene Daten) sichere Medien. Unverschlüsselte E-Mails, offene Hauspost oder Faxverkehr sind nicht dafür geeignet.

2.6 Recht auf Auskunft, Berichtigung, Löschung und Widerspruch

Betroffene Personen haben das Recht, Auskunft über ihre Daten zu verlangen und sachlich unrichtige Daten berichtigen, sperren oder löschen zu lassen.

Wenden Sie sich bei allen Auskunftersuchen von Betroffenen, die über die an Ihrem Arbeitsplatz üblichen Routineanfragen hinausgehen an den Vorstand oder dafür autorisierte Personen. Diese werden veranlassen, dass die Auskunft dem Gesetz entsprechend gegeben wird.

2.7 Beschränkung der mündlichen Weiterübermittlung

Geben Sie an Stellen außerhalb des Vereins auch keine mündlichen Auskünfte über Daten einzelner Personen, es sei denn, es bestehen besondere Anweisungen hierzu.

Geben Sie aus Ihren Unterlagen nur eindeutig Berechtigten innerhalb des Vereins oder einer berechtigten Behörde Auskünfte.

3 Meldung von Verletzungen des Schutzes personenbezogener Daten

Ein jeder, der merkt, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat sich unverzüglich an den Vorstand zu wenden.

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss dieser Vorfall binnen 72 Stunden gemäß Artikel 55 DSGVO der zuständigen Aufsichtsbehörde von autorisierten Personen mit entsprechendem Vordruck (der jeweils gültige Vordruck ist über das Internet herunter ladbar) gemeldet werden.

4 Bußgeldvorschriften

Bitte beachten Sie, dass Verletzungen des Datenschutzes abhängig von nationalen Gesetzen zu Ordnungswidrigkeiten oder gar Straftatbeständen führen können.

Wangen, den 18.10.2018

Ulrich Mayr, Vorstand