

# Datenschutzordnung

## Bürger-Schützenverein Oberlohberg e. V. 1907

Gültig ab März 2019



## Inhalt

§ 1 Geltungsbereich

§ 2 Allgemein

§ 3 Datenschutzbeauftragter

§ 4 Speicherung, Nutzung und Verarbeitung personenbezogener Daten

§ 5 Recht auf Löschung gespeicherter personenbezogener Daten

§ 6 Recht auf Auskunft über personenbezogene Daten

§ 7 Zugriff auf personenbezogene Daten

§ 8 Übermittlung von personenbezogenen Daten

§ 9 Speicherung personenbezogener Daten

§ 10 Datenpanne

§ 11 Datenschutz auf Vereinshomepage

§ 12 Änderungen

§ 13 Salvatorische Klausel

§ 14 Inkrafttreten

Anhang 1: Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Datenschutz-Grundverordnung

Anhang 2: Verpflichtungserklärung zum „Datenschutz für das Ehrenamt im BSV Oberlohberg 1907 e.V.“

Anhang 3: Mitteilung einer unrechtmäßigen Datenübermittlung bzw. unrechtmäßigen Kenntniserlangung von Daten durch Dritte („Datenpanne“) gemäß Art. 33 Abs. 1 DSGVO oder § 15a TMG i. V. m. § 42a BDSG

## **Vorwort:**

Im „**Bürger-Schützenverein Oberlohberg e.V. 1907**“ sind weibliche und männliche Personen gleichberechtigt. Zur besseren Lesbarkeit wird eine geschlechtsneutrale Sprachform im Folgenden verwendet.

## **§ 1 Geltungsbereich**

1.1. Der „Bürger-Schützenverein Oberlohberg e.V. 1907“ (folgend Verein) erlässt entsprechend seiner Satzung (§ 14 Vereinsordnungen) zur Regelung des Datenschutzes und dessen Umsetzung im Verein diese Datenschutzordnung.

1.2. Die Datenschutzordnung gilt für alle Mitglieder des Vereins (Bestandsmitglieder und neue Mitglieder) und die in der Satzung bezeichneten Organe und Ausschüsse. Die Vorschriften der Datenschutzordnung sind grundsätzlich verbindlich.

1.3. Mit der Datenschutzordnung werden § 18 der Satzung und § 8 der Sportordnung konkretisiert und ergänzt.

## **§ 2 Allgemein**

2.1. Der Verantwortliche im Sinne der Datenschutz-Grundverordnung und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist der:

**Vorstand des BSV Oberlohberg e.V. 1907 - Bergerstraße 354 - 46539 Dinslaken**

2.2. Dem Verein obliegt hier ein besonderer respekt- und würdevoller Umgang zur Berücksichtigung der schutzbedürftigen/persönlichen Interessen jedes Mitgliedes.

## **§ 3 Datenschutzbeauftragter**

Ein Datenschutzbeauftragter muss z. Z. nicht bestellt werden weil nicht mehr als 10 Personen mit der Bearbeitung datenschutzwürdiger Belange betraut sind. Sollte zukünftig die Verpflichtung eintreten, wird dem unverzüglich entsprochen.

## § 4 Speicherung, Nutzung und Verarbeitung personenbezogener Daten

4.1. Mit dem Beitritt eines Mitglieds nimmt der Verein personenbezogene Daten zum Mitglied auf. Dabei handelt es sich unter anderem um folgende Angaben: Name, Kontaktdaten, Bankverbindung, ggf. Familienstand (sofern für Familien-/Eheleutebeitrag erforderlich) und weitere dem Vereinszweck dienende Daten. Sonstige Informationen zu den Mitgliedern und Informationen über Nichtmitglieder werden von dem Verein grundsätzlich nur verarbeitet oder genutzt, wenn sie zur Förderung des satzungsgemäßen Vereinszweckes nützlich sind und keine Anhaltspunkte bestehen, dass die betroffene Person ein schutzwürdiges Interesse hat, das der Verarbeitung oder Nutzung entgegensteht.

Die personenbezogenen Daten werden grundsätzlich im Rahmen des Erwerbs der Mitgliedschaft erhoben. Details sind im Verzeichnis von Verarbeitungstätigkeiten beschrieben **(s. Anhang 1)**.

4.2. Mit dem Beitritt erklärt sich das Mitglied einverstanden, dass die im Zusammenhang mit der Mitgliedschaft erhobenen und benötigten personenbezogenen Daten unter Berücksichtigung der Maßgaben des BDSG und der ab 25. Mai 2018 nach EU Recht geltenden DSGVO per EDV für den Verein auf vereinseigenen Systemen gespeichert, genutzt und verarbeitet werden.

Dieses Einverständnis ist Grundlage einer Mitgliedschaft im Verein. Mit der Angabe seiner Telefonnummer/n und der E-Mail-Adresse/n erkennt das Mitglied an, dass vorrangig diese Medien für die Kommunikation an die und mit den Mitgliedern genutzt wird. Weiterhin erklärt sich das Mitglied ausdrücklich damit einverstanden, dass im Rahmen von Meisterschaften und Wettkämpfen von ihm sowohl auf Vereins- als auch auf Verbandsebene erzielte Ergebnisse in den hierfür vom Verein genutzten Medien mit Nennung seines Namens ggf. auch mit Bild veröffentlicht werden dürfen.

4.3. Mitgliederdaten (siehe Punkt 4.1) werden nur Vorstandsmitgliedern sowie weiteren ausgesuchten Mitgliedern (z.B. Mannschaftsführern) zugänglich gemacht, die im Verein eine besondere Funktion außerhalb des Vorstandes ausüben, für welche die Kenntnis spezifischer Daten (z.B. Kontaktdaten für Mannschaftsführer) für die Ausübung ihrer Tätigkeit zwingend erforderlich sind. Die Mitglieder mit Zugriff auf die personenbezogenen Daten, verpflichten sich durch Unterzeichnung der Verpflichtungserklärung zum Datenschutz für das Ehrenamt im Verein alle Punkte dieser Ordnung sowie die geltenden Datenschutzbestimmungen einzuhalten **(s. Anhang 2)**.

4.4. Macht ein Mitglied geltend, dass es die Mitgliederliste zur Wahrnehmung seiner satzungsgemäßen Rechte benötigt, wird diese auf die dazu notwendigen Informationen reduzierte Liste nur gegen eine schriftliche Versicherung ausgehändigt, dass die Daten ausschließlich für die Ausübung dieses Rechtes genutzt werden. Die Versicherung muss ebenfalls beinhalten, dass Daten nicht an Dritte weitergegeben werden, sofern dies zur Ausübung des Rechts nicht zwingend erforderlich ist.

## § 5 Recht auf Löschung personenbezogener Daten / Widerruf

Mitglieder haben jederzeit das Recht, dieses Einverständnis in Gänze oder teilweise zu widerrufen. Sofern dieser Widerruf einer ordentlichen Ausübung der satzungsgemäßen Zwecke entgegensteht, verweist der Verein auf mögliche, sich daraus ergebende Konsequenzen. Diese werden dann unmittelbar fallbezogen dem widersprechenden Mitglied aufgezeigt.

## § 6 Recht auf Auskunft über personenbezogene Daten

Jedes Mitglied hat zu jeder Zeit das Recht auf unentgeltliche Auskunft über die von ihm gespeicherten personenbezogenen Daten, die Berichtigung seiner gespeicherten Daten im Falle der Unrichtigkeit und Sperrung seiner Daten sowie Löschung seiner freiwillig angegebenen Daten.

## § 7 Zugriff auf personenbezogene Daten

7.1 Die personenbezogenen Daten werden für die Dauer der Mitgliedschaft im Verein gespeichert. Mit Beendigung der Mitgliedschaft werden die Datenkategorien gemäß den gesetzlichen Aufbewahrungsfristen weitere zehn Jahre vorgehalten und dann gelöscht. In der Zeit zwischen Beendigung der Mitgliedschaft und der Löschung wird die Verarbeitung dieser Daten eingeschränkt. Bestimmte Datenkategorien werden zum Zweck der Vereinschronik im Vereinsarchiv gespeichert. Hierbei handelt es sich um die Kategorien Vorname, Nachname, Zugehörigkeit zu einer Mannschaft, besondere sportliche Erfolge oder Ereignisse, an denen die betroffene Person mitgewirkt hat. Der Speicherung liegt ein berechtigtes Interesse des Vereins an der zeitgeschichtlichen Dokumentation von sportlichen Ereignissen und Erfolgen und der jeweiligen Zusammensetzung der Mannschaften zugrunde.

7.2 Die Beendigung von Mitgliedschaften von Waffenbesitzkarteninhabern im Verein werden der Kreispolizeibehörde Wesel gem. den gesetzlichen Vorgaben gemeldet. Personenbezogene Daten des ausgetretenen Mitglieds, die Kassenverwaltung betreffend, werden gemäß den steuerrechtlichen Bestimmungen bis zu 10 Jahren ab Wirksamwerden des Austritts aufbewahrt.

## § 8 Übermittlung von personenbezogenen Daten

8.1. Als Mitglied des Rheinischen Schützenbundes e.V. sowie des Deutschen Schützenbundes e.V. ist der Verein verpflichtet, seine Mitglieder an den übergeordneten Verband zu melden. Übermittelt werden in der Regel Name, Vorname, Geburtsdatum, Adresse, Telefonnummer, Eintrittsdatum und im Falle des Austritts auch das Austrittsdatum. Die Meldung erfolgt über ein internetgestütztes Verwaltungssystem. Bei Bedarf und zur Erlangung eines angemessenen Versicherungsschutzes ist es möglich, dass die hierzu erforderlichen Daten auch an die ausgewählte Versicherungsgesellschaft weitergegeben werden.

8.2. Die Daten der Bankverbindung der Mitglieder werden zum Zwecke des Beitragseinzuges an das jeweilige Bankinstitut des Vereins - z. Z. an die Niederrheinische Sparkasse Wesel (Nispa) - weitergeleitet.

8.3. Eine anderweitige Verarbeitung oder Nutzung (z. B. Übermittlung an Dritte) ist - mit Ausnahme der erforderlichen Weitergabe von Angaben zur namentlichen Mitgliedermeldung von Startberechtigungen an entsprechende Verbände (Kreis/Bezirk 012 sowie RSB/DSB) - nicht zulässig.

## § 9 Speicherung personenbezogener Daten / Datensicherheit

Der Verein setzt technische und organisatorische Sicherheitsmaßnahmen ein, um zu gewährleisten, dass die persönlichen Daten der Mitglieder vor Verlust, unrichtigen Veränderungen oder unberechtigten Zugriffen Dritter geschützt sind. In jedem Fall haben auf Seiten des Vereins nur berechtigte Personen Zutritt zu den persönlichen Daten, und dies auch nur insoweit, als es im Rahmen der oben genannten Zwecke erforderlich ist. Die Sicherheitsmaßnahmen werden ständig den verbesserten technischen Möglichkeiten angepasst.

## § 10 Datenpanne

Gem. Art. 33 Abs. 1 DSGVO oder § 15a TMG i. V. m. § 42a BDSG muss der Verein als verantwortliche Stelle die zuständige Datenschutzaufsichtsbehörde und die betroffenen Personen innerhalb von 72 Stunden nach Bekanntwerden des Verstoßes informieren. Hierzu wird das Formblatt „Mitteilung einer unrechtmäßigen Datenübermittlung bzw. unrechtmäßigen Kenntniserlangung von Daten durch Dritte („Datenpanne“) gemäß Art. 33 Abs. 1 DSGVO oder § 15a TMG i. V. m. § 42a BDSG“ verwendet (**s. Anhang 3**).

## § 11 Datenschutz auf Vereinshomepage

Der Verein als Websitebetreiber nimmt den Datenschutz sehr ernst und behandelt personenbezogene Daten vertraulich und entsprechend den gesetzlichen Vorschriften. Damit durch neue Technologien und die ständige Weiterentwicklung dieser Vereins-Website Änderungen / Anpassungen vorgenommen werden können, hat der Verein eine Datenschutzerklärung auf der Website niedergelegt. Diese Datenschutzerklärung soll die Nutzer dieser Vereins-Website über die Art, den Umfang und den Zweck der Erhebung und Verwendung personenbezogener Daten durch den Websitebetreiber informieren.

Diese hinterlegte Datenschutzerklärung ist in ihrer jeweils gültigen Fassung Bestandteil dieser Datenschutzordnung.

**Der Verein empfiehlt seinen Mitgliedern, sich die auf der Website hinterlegte Datenschutzerklärung in regelmäßigen Abständen wieder durchzulesen.**

## § 12 Änderungen

Der Verein behält sich vor, bei technischen und/oder rechtlichen Änderungen diese Datenschutzordnung anzupassen. Den jeweils aktuellen Stand der Datenschutz-Ordnung kann jederzeit auf der Homepage einsehen werden.

Änderungen dieser Datenschutzordnung sind von der Mitgliederversammlung gemäß § 14 der Satzung zu beschließen.

## § 13 Salvatorische Klausel

Sollten einzelne Punkte in dieser Ordnung nicht rechtskonform sein, so bleiben alle anderen Punkte der Ordnung hiervon unberührt. Die rechtsungültigen Inhalte sind durch rechtskonforme Inhalte zu ersetzen. Die Anfechtung der Ordnung nach BGB bleibt unberührt.

## § 14 Inkrafttreten

Die Datenschutzordnung ist gemäß Beschluss der Mitgliederversammlung in der vorliegenden Fassung am 10.03.2019 verabschiedet worden und tritt mit sofortiger Wirkung in Kraft.



## Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Datenschutz-Grundverordnung – DSGVO

### 1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit <i>Erfassung, Speicherung und Übermittlung von Mitgliederdaten</i>		Dokumenten Stand: <i>Datum 30.12.2018</i>
Vereinsname und Postanschrift, E-Mail-Adresse, Telefonnummer <i>BSV Oberlohnberg e.V. 1907, Bergerstraße 354 - 46539 Dinslaken</i>		
Name und Kontaktdaten des Datenschutzbeauftragten (Postanschrift, E-Mail-Adresse, Telefonnummer) <i>keiner erforderlich</i>		

### 2. Zwecke der Datenverarbeitung

*Organisation des Vereins, des vereinsinternen Sportbetriebs und des gemeinschaftlichen Vereinslebens sowie Übermittlung der Daten an hierarchisch übergeordnete Fach- und Sportverbände zu deren Organisation ihres Verbandes und ihrer Sportbetriebe*

### 3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten
1	<i>Titel, Name, Vorname</i>
2	<i>Anschrift</i>
3	<i>Geburtsdatum</i>
4	<i>Kommunikationsdaten (Telefon, Mobilnummer, Fax, E-Mail)</i>
5	<i>Bankverbindung</i>
6	<i>Lizenzen (z.B. Lizenzausbildung RSB/DSchB und waffenrechtliche Lizenzen (Waffenbesitzkarte, Befürwortungen, usw.)</i>
7	<i>Zusätzliche Daten zur Organisation des Sportbetriebes (Staatsangehörigkeit, Behindertenklasse, Wettkampfergebnisse, Zugehörigkeit zu Mannschaften, Startrechte, ausgeübte Wettbewerbe, En- und Austrittsdatum</i>
8	<i>Ehrungen</i>
9	<i>Zusätzliche Daten zur Organisation des Vereins (Funktionen im Verein / Abteilungen, Zugehörigkeit zu Arbeitsgruppen)</i>
10	<i>Einzelfotos</i>

### 4. Kategorien der betroffenen Personen

Lfd. Nr.	Lfd. Nr. von Ziffer 3	Bezeichnung der Daten
1	<i>alle</i>	<i>Mitglieder</i>
2	<i>1,2,3,4,6,7,</i>	<i>Aktive Sportler</i>

### 5. Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

Lfd. Nr.	Lfd. Nr. von Ziffer 3	Lfd. Nr. von Ziffer 4	Empfänger	Anlass der Offenlegung

1	1,3,6,7,8,9	1,2	Kreis/Bezirksverband (Bezirk 012 Dinslaken	Organisation und Entwicklung des Verbandes und des Sportbetriebs
2	1,2,3,4,6,7, 8,9	1,2	Landesverband (RSB	Organisation und Entwicklung des Verbandes und des Sportbetriebs
3	1,2,3,4, 6,7,8,9	1,2	Bundesverband (DSchB)	Organisation und Entwicklung des Verbandes und des Sportbetriebs
4	1,3,7,9	1,2	Schützenverband Dinslaken	Organisation und Entwicklung des Verbandes und des Sportbetriebs
5	Ausschl. statistische Daten	1,2	Stadtverwaltung Dinslaken	Wahrung und Zuteilung von Zuschüssen für die Jugendabteilung
6	Ausschl. statistische Daten	1,2	Landessportbund (lsb-nrw)	Organisation und Entwicklung des Verbandes und des Sportbetriebs
7	1,2,7 (nur Austrittsdat um)	1,2	Kreispolizeibehörde	Gesetzliche Vorgaben

## 6. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr. von Ziffer 3	Löschungsfrist
1	Titel, Name, Vorname für Chronik dürfen Informationen noch gespeichert bleiben
2	Mit Ausscheiden des Mitgliedes sofern keine offenen Forderungen mehr bestehen
3	Mit Ausscheiden des Mitgliedes
4	Mit Ausscheiden des Mitgliedes sofern keine offenen Forderungen mehr bestehen
5	10 Jahre nach Ausscheiden, sofern keine offenen Forderungen mehr bestehen
6	Mit Ausscheiden des Mitgliedes
7	Aus der Datenbank: Mit Ausscheiden des Mitgliedes; Aus den online verfügbaren Medien (Facebook, Internet...) ist eine Löschung aus veröffentlichten Startlisten, Ergebnislisten praktisch nicht möglich. für Chronik dürfen Informationen (z.B. Bestenlisten, Teilnahme an olympischen Spielen...) noch gespeichert bleiben
8	Mit Ausscheiden des Mitgliedes; für Chronik dürfen Informationen noch gespeichert bleiben
9	Mit Ausscheiden des Mitgliedes
10	Einzelfotos aus der Datenbank: Mit Ausscheiden des Mitgliedes; Aus den online verfügbaren Medien (Facebook, Internet...) ist dies praktisch nicht möglich.

## 7. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO

Lfd. Nr.	Maßnahme	Umsetzung der Maßnahme
1	<b>Zutrittskontrolle</b> Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Daten liegen in einem vom Verein beauftragten Rechenzentrum. Die internen Arbeitsplätze vom Auftragnehmer sind in abschließbaren Büroräumen ohne Internetzugang.
2	<b>Zugangskontrolle</b>	

	<i>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.</i>	<ul style="list-style-type: none"> <li>- Passwortschutz</li> <li>- Firewall</li> <li>- Anti-Viren-Software</li> <li>- Bildschirmsperre</li> </ul>
3	<p><b>Zugriffskontrolle</b></p> <p><i>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.</i></p>	<p>Reduzierte Zahl der Zugriffsberechtigten.</p> <p>Berechtigungskonzept für unterschiedliche Rollen in dem System selbst.</p>
4	<p><b>Weitergabekontrolle</b></p> <p><i>Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Überarbeitung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stelle und in welcher Form eine Übermittlung personenbezogener Daten vorgesehen erfolgen kann.</i></p>	<ul style="list-style-type: none"> <li>- HTTPS-Verschlüsselung</li> <li>- Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen</li> <li>- Übermittlung möglich durch (zugriffsgeschützte): Datenbank, Applikation, Export, Schnittstellen, Druckfunktion</li> </ul>
5	<p><b>Eingabekontrolle</b></p> <p><i>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.</i></p>	<ul style="list-style-type: none"> <li>- Logging über Software</li> </ul>
6	<p><b>Auftragskontrolle</b></p> <p><i>Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.</i></p>	<ul style="list-style-type: none"> <li>- Weisung laut Vereinbarung zur Auftragsdatenverarbeitung</li> </ul>
7	<p><b>Verfügbarkeitskontrolle</b></p> <p><i>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.</i></p>	<p>Daten liegen in einem vom Verein beauftragten Rechenzentrum.</p> <ul style="list-style-type: none"> <li>- Backup</li> <li>- Sicherheitstests der Software werden vom Anbieter garantiert.</li> </ul>
8	<p><b>Trennungskontrolle</b></p> <p><i>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.</i></p>	<ul style="list-style-type: none"> <li>- Logische Trennung der Daten über Tabellen und Mandate</li> </ul>



## Verpflichtungserklärung zum Datenschutz für das Ehrenamt

Ich, \_\_\_\_\_  
 wohnhaft in \_\_\_\_\_  
 verpflichte mich,

1. Die Datenschutzerklärung – DSGVO und BDSG – des BSV Oberlohberg e.V.1907 sowie die anderen für meine Tätigkeit geltenden Datenschutzbestimmungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen des Datenschutzes hingewiesen wurde. Mir ist bewusst, dass sich die Pflicht zur Geheimhaltung nicht nur auf das erstreckt, was mir anvertraut wird, sondern auch auf das bezieht, was mir sonst bekannt wird;
2. Daten nicht unbefugt zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen;
3. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten;

Ich bin weiterhin darüber belehrt worden, dass

1. Daten nur zu dem Zweck und in dem Umfang erhoben und verwendet werden dürfen, der zur rechtmäßigen Aufgabenerfüllung erforderlich ist,
2. personenbezogene Daten (z. B. Angaben über persönliche und finanzielle Verhältnisse, Krankengeschichten, Gutachten etc.) und einrichtungsbezogene Daten, Angaben oder Informationen der Geheimhaltung unterliegen,
3. sich die Pflicht zur Geheimhaltung nicht nur auf das erstreckt, was mir anvertraut wird, sondern auch auf das bezieht, was mir anderweitig bekannt wird,
4. ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der strafrechtliche und / oder zivilrechtliche Folgen haben kann sowie zu einer Beendigung der ehrenamtlichen Tätigkeit führen kann,
5. die Texte der für meine Tätigkeit geltenden Datenschutzvorschriften in der Geschäftsstelle eingesehen und auch für kurze Zeit ausgeliehen werden können.

Diese Erklärung wird zu den Akten genommen.

\_\_\_\_\_, den \_\_\_\_\_

Ort, Datum

\_\_\_\_\_

Unterschrift



**Mitteilung einer unrechtmäßigen Datenübermittlung bzw.  
unrechtmäßigen Kenntniserlangung von Daten durch Dritte  
(„Datenpanne“) gemäß Art. 33 Abs. 1 DSGVO  
oder § 15a TMG i. V. m. §42a BDSG**

**Hinweise:**

Bei bestimmten Datenschutzverstößen und Datenschutzpannen müssen die Sie als verantwortliche Stelle die zuständige Datenschutzaufsichtsbehörde in Nordrhein-Westfalen oder Rheinland Pfalz ([www.datenschutz-wiki.de/Aufsichtsbehörden\\_und\\_Landesdatenschutzbeauftragte](http://www.datenschutz-wiki.de/Aufsichtsbehörden_und_Landesdatenschutzbeauftragte) LINK) und die betroffenen Personen innerhalb von 72 Stunden nach Bekanntwerden des Verstoßes gem. Art. 33 Abs. 1 DSGVO oder § 15a TMG i.V.m. §42a BDSG informieren. (Hinweis: In der Regel werden hier auch beschreibbare PDFs auf den Seiten der Landesdatenschutzbeauftragten vorgehalten.)

Eine solche „Verpflichtung zur Selbstanzeige“ besteht, wenn Dritte unrechtmäßig von bestimmten sensiblen Daten Kenntnis erlangt haben und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen.

Voraussetzungen für die Informationspflicht

Die Informationspflicht tritt ein, wenn folgende in der Datenschutzgrundverordnung abschließend genannten Arten personenbezogener Daten von einem Datenschutzverstoß bzw. einer Datenpanne betroffen sind:

- besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, z.B. Gesundheitsdaten oder Religionszugehörigkeit,
- personenbezogene Daten, die z.B. bei Ärzten, Apothekern, Rechtsanwälten, Steuerberatern oder Personenversicherern einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder auf einen Verdacht hierauf beziehen,
- personenbezogene Daten zu Bank- und Kreditkartenkonten, z.B. Kontonummern mit Bankleitzahl oder Kreditkartennummern und
- Bestands- und Nutzungsdaten im Bereich der Telemedien (Internet), z.B. Benutzerkennungen, Passworte.

Die unrechtmäßige Kenntniserlangung von Daten durch Dritte kann auf einer unrechtmäßigen Übermittlung von Daten beruhen (z.B. Fehl-Versendungen, illegale Datenweitergaben oder Datenabrufe). Die Daten können aber auch auf sonstige Weise dritten Personen unrechtmäßig zur Kenntnis gelangen, insbesondere beim Verlust von Datenträgern durch Einbrüche, Diebstähle und Fundunterschlagungen oder beim Internet-Datenhacking.

Es muss nicht im Einzelfall schon belegt sein, dass dritte Personen von den Daten tatsächlich Kenntnis erlangt haben, z.B. durch bereits eingetretene Schadensfälle wie illegale Lastschriftinzüge von Bankkonten oder Internetbestellungen auf Kosten der Geschädigten. Es reicht aus, dass aufgrund der Lebenserfahrung eine hohe Wahrscheinlichkeit dafür besteht, dass die Daten von einem Dritten zur Kenntnis genommen wurden bzw. werden. Dies ist insbesondere gegeben, wenn Daten durch eine kriminelle Handlung in den Verfügungsbereich Dritter gelangt sind. Denn dann besteht eine hohe Wahrscheinlichkeit dafür, dass z.B. Diebe, Cyberkriminelle oder ihre Abnehmer die gespeicherten Daten für rechtswidrige Zwecke nutzen, womit für die Betroffenen eine konkrete Gefahr droht.

Bei der Frage, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen, ist eine Prognoseentscheidung zu treffen, ob eine schwerwiegende Beeinträchtigung in eine bedrohliche Nähe gerückt ist. Dabei ist zu berücksichtigen, um welche Art von Daten es geht, wer - vermutlich - in den Besitz der Daten gelangt ist ("vertrauenswürdige Umgebung" oder kriminelle Personen) und welche potentiellen Auswirkungen sich für die betroffenen Personen ergeben können, z.B. finanzielle Schäden, Identitätsbetrug, soziale Nachteile, Bloßstellung, Erpressbarkeit.

### **Umsetzung der Informationspflicht**

Die verantwortliche Stelle muss innerhalb von 72 Stunden nach Bekanntwerden des Datenschutzverstoßes gem. Art. 33 Abs. 1 DSGVO oder § 15a TMG i.V. m. §42a BDSG die zuständige Datenschutzaufsichtsbehörde und unverzüglich die betroffenen Personen, um deren Daten es geht, gem. Art. 34 Abs. 1 DSGVO informieren, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen durch den Verstoß vorliegt. Dabei muss sie mitteilen, was konkret geschehen ist, welche Maßnahmen zur Abhilfe inzwischen getroffen wurden und was die betroffenen Personen selbst für ihren Schutz noch tun können.

Die zuständige Datenschutzaufsichtsbehörde kann nach der Information prüfen, ob die meldende Stelle die möglichen bzw. gebotenen Abhilfe-, Schutz- und Sicherheitsmaßnahmen schon getroffen hat und bei Bedarf weitere Maßnahmen einfordern.

Die Information der betroffenen Personen muss folgenden Inhalt haben:

- Name der verantwortlichen Stelle mit Ansprechpartnern und Kontaktdaten,
- Datum/Zeitraum des Vorfalles sowie Ursache der Datenpanne (kurze Beschreibung des Sachverhalts) mit Beschreibung der betroffenen personenbezogenen Daten,
- Nennung der (möglichen) Dritten, die Kenntnis erlangt haben bzw. die eine Möglichkeit zur Kenntnisnahme hatten,
- mögliche Folgen bzw. nachteilige Auswirkungen der Datenpanne (z.B. finanzieller Schaden, Ruf-/Imageschädigung, Bloßstellung) mit Hinweisen auf mögliche Vorkehrungen der betroffenen Personen dazu, und
- infolge der Datenpanne durch die verantwortliche Stelle ergriffene Maßnahmen.

Aufgrund der Information sollen die betroffenen Personen die Möglichkeit haben, Schaden von sich abzuwenden oder Schutzmaßnahmen zu treffen.

Ein Verstoß gegen die Informationsverpflichtung gegenüber der Datenschutzaufsichtsbehörde oder den betroffenen Personen ist bußgeldbewehrt (Art. 83 Abs. 4a DSGVO).

Für den Fall bekannt-werdender Datenpannen sollte die verantwortliche Stelle organisatorisch gerüstet sein und ein geeignetes Prüfungs- und Meldesystem vorbereitet haben.

## § 1 Meldebogen für Datenschutz- und Sicherheitsereignisse

Ereignisnummer:	Vertraulichkeitskennzeichnung	gemeldet am:	Status:
Ereignisdatum:	gemeldet von:		Priorität hoch
verantwortlicher Bearbeiter:		Kategorie: <ul style="list-style-type: none"> <li><input type="checkbox"/> Datenschutz</li> <li><input type="checkbox"/> Informationssicherheit</li> <li><input type="checkbox"/> IT-Sicherheit</li> <li><input type="checkbox"/> Andere:</li> </ul>	
Ausführliche Beschreibung:			
betroffene Komponenten:	System:	Standort:	verantwortliche Abteilung:
Sofortmaßnahmen:		Effekt in Prozent:	Einführungsdatum:
Fehlerursachen:  Ursachen:		Effekt in Prozent:	Einführungsdatum:

geplante Korrektivmaßnahmen:  Maßnahmen:	kontrolliert durch:	Kontrolldatum:
Information an Betroffene  <input type="checkbox"/> nötig <input type="checkbox"/> nicht nötig.  Begründung:  Art (E-Mail/Fax/Brief): Datum:		
<input type="checkbox"/> <b>Datenschutzbeauftragte/r eingebunden</b> <b>Begründung:</b>	<input type="checkbox"/> <b>Behörde eingebunden</b> <b>Begründung:</b>	

## § 2 Priorisierungstabelle

Mit der Priorisierungstabelle erfolgt die Festlegung der Priorität. Für eine einfache und übersichtliche Priorisierung wird mit vier Prioritäten gearbeitet (Auswirkung/Schaden): katastrophal und existenzbedrohlich (1), großer Schaden (2), mittlerer Schaden (3), geringer Schaden (4).

Durch die Bestimmung der Kategorie und deren Auswirkung wird eine Priorisierung des Datenschutzereignisses gemäß nachfolgender Tabelle abgeleitet:

<b>Kategorie</b>	<b>geringe Auswirkung/ Schaden</b>	<b>mittlere Auswirkung/ Schaden</b>	<b>große Auswirkung/ Schaden</b>	<b>katastrophal e Auswirkung/ Schaden</b>
Diebstahl von Kundendaten				
Verletzung des Datenschutzes				
Verstoß gegen Gesetze				

Hackerangriff				
---------------	--	--	--	--

Um die Priorisierung und die damit zusammenhängenden Ereignisse zuordnen zu können, ist das Arbeiten mit entsprechenden tabellarischen Übersichten geeignet. Beispielhaft sind nachfolgend die Ereignisse aus der oben dargestellten Tabelle beschrieben.

### **Diebstahl von personenbezogenen Daten**

<i>Auswirkung</i>		<i>Priorität</i>
gering	nicht klassifizierte Personendaten wurden unautorisiert kopiert	
mittel	vertrauliche Personendaten wurden unautorisiert kopiert	
groß	vertrauliche Personendaten werden veröffentlicht; Schadensersatzforderungen von Betroffenen möglich; Mitteilung nach § 42 a BDSG notwendig;	
katastrophal	<b>sensible Personendaten werden veröffentlicht; sehr hohe Schadensersatzforderungen von Betroffenen möglich; Meldung nach § 42 a BDSG notwendig; Imageschaden für das Unternehmen</b>	

### **Verletzung des Datenschutzes**

<i>Auswirkung</i>		<i>Priorität</i>
gering	versehentliche Weitergabe von personenbezogenen Daten innerhalb des Unternehmens	
mittel	unbeabsichtigte personenbezogene Daten in Auswertungen; personenbezogene Daten ohne Zweckbindung in Log-Dateien	
groß	grob fahrlässige Offenbarung personenbezogener Daten gegenüber Dritten, Verletzung des Trennungsgebots; Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	Veröffentlichungen von personenbezogenen Daten; Zweckmissbrauch Diebstahl von personenbezogenen Daten; Unerlaubte Nutzung von personenbezogenen Daten zur Verhaltenskontrolle Informationspflicht nach § 42 a BDSG notwendig	

### **Verstoß gegen Gesetze**

<i>Auswirkung</i>		<i>Priorität</i>
gering	geringfügiger Verstoß gegen den Datenschutz ohne erkennbaren Vorsatz keine Außenwirkung Vorfall kann intern (ggf. mit disziplinarischen Mitteln) geregelt werden	
mittel	Ordnungswidrigkeit mittelschwerer Verstoß gegen den Datenschutz	

	Einsatz zwingender disziplinarischer Mittel erforderlich Prüfung der Hinzuziehung der entsprechenden Behörden notwendig möglicherweise Informationspflicht nach § 42 a BDSG notwendig	
groß	Rechtsverstoß Hinzuziehung der entsprechenden Behörden notwendig Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	strafrechtliche Relevanz mit eindeutig erkennbarem Vorsatz Einschaltung der Strafermittlungsbehörden zwingend erforderlich hohe Außenwirkung mit Imageverlust für das Unternehmen Informationspflicht nach § 42 a BDSG notwendig	
<b>Hackerangriff</b>		
<i>Auswirkung</i>		<i>Priorität</i>
gering	Angriff auf IT-Systeme mit personenbezogenen Daten Angriff ohne nachweislichen Schaden (z. B. Versuch eines Hackereintruchs wird rechtzeitig erkannt und vereitelt)	
mittel	Angriff mit geringfügiger Verschlechterung der Verfügbarkeit Angriff auf die IT-Infrastruktur wird durch entsprechende technische Frühwarnsysteme erkannt und führt zur vorübergehenden Sicherheitsabschaltung dezidierter Systeme oder Segmente	
groß	Hackerzugriff auf zentrale Verarbeitungssysteme Diebstahl von Passwortdateien massive Beeinträchtigungen der Dienste Hinzuziehung der entsprechenden Behörden notwendig Informationspflicht nach § 42 a BDSG notwendig	
katastrophal	Ausfall von Systemen durch Hackerangriffe Verlust von Daten durch Hacker Diebstahl von personenbezogenen Daten Offenlegung von personenbezogenen Daten durch Hacker hohe Außenwirkung mit Imageverlust für das Unternehmen Einschaltung der Strafermittlungsbehörden zwingend erforderlich Informationspflicht nach § 42 a BDSG notwendig	

### Ablaufprozess bei einer Datenpanne im BSV Oberlohberg e.V.

<u>Prozessschritt</u>	<u>Betroffener/Erlediger</u>
<b>1. Kenntnisnahme einer Datenpanne</b>	<b>Vorstandsmitglieder</b>
<b>2. Unverzügliche Information des gesamten Vorstandes</b>	<b>Vorstandsmitglieder</b>
<b>3. Einschätzung des vermutlichen Schadens gemäß vorstehender Priorisierungstabelle</b>	<b>Vorstandsmitglieder</b>
<b>4. Unverzügliche schriftliche Information an die zuständige Aufsichtsbehörde</b>	<b>1. Vorsitzender</b>



# BSV Oberlohberg e.V. 1907

Bergerstr. 354 - 46539 Dinslaken

www.bsv-oberlohberg1907.de



## AUFNAHMEANTRAG

Hiermit beantrage ich meine Aufnahme in den Bürgerschützenverein Oberlohberg e.V. 1907

Name : \_\_\_\_\_ Vorname : \_\_\_\_\_

Wohnort: \_\_\_\_\_ Straße : \_\_\_\_\_

Geb. am : \_\_\_\_\_  Kind  Jugendliche  Azubi  Student/in

Email : \_\_\_\_\_

Der Jahresbeitrag beträgt derzeit für Erwachsene 46,- €, Kinder bis 11 Jahre 0,- €, Kinder / Jugendliche 12 bis 18 Jahre, Auszubildende und Studenten 18 bis 25 Jahre 16,- €, Eheleute 69,- € und wird halbjährlich eingezogen. Als Aufnahmespende bin ich bereit, 100,- € zu zahlen.

Ich bestätige, die Regelungen zum Datenschutz in der Vereinssatzung (§ 18) und in der Sportordnung (§ 8) zur Kenntnis genommen zu haben und willige ein, dass der BSV Oberlohberg die aufgeführten Daten für vereinsinterne Zwecke und zu Zwecken der Mitgliedermeldung an den Rheinischen Schützenbund und übergeordnete Verbände in einer EDV-gestützten Mitgliederverwaltungssoftware gespeichert, verarbeitet und genutzt werden. (Vereinsatzung und Vereinsordnungen unter [www.bsv-oberlohberg1907.de](http://www.bsv-oberlohberg1907.de)) Ich bin damit einverstanden, dass der Verein im Zusammenhang mit dem Vereinszweck, der Vereinswerbung sowie satzungsgemäßen Veranstaltungen personenbezogene Daten und Fotos von mir z.B. in der Vereinszeitung und auf der Homepage des Vereins veröffentlicht, für Werbezwecke nutzt und diese ggf. an Print- und andere Medien übermittelt. Dieses Einverständnis betrifft insbesondere folgende Veröffentlichungen: Ergebnislisten, Mannschaftslisten und Kontaktdaten von Vereinsfunktionären, Berichte über Ehrungen und Geburtstage. Veröffentlicht werden ggf. Fotos, der Name, die Vereins- und Abteilungszugehörigkeit, die Funktion im Verein, ggf. die Einteilung in Wettkampf- oder andere Klassen inklusive Alter und Geburtsjahrgang und die Platzierung bei Wettkämpfen. Mir ist bekannt, dass ich jederzeit gegenüber dem Vorstand der Veröffentlichung von Einzelfotos und persönlichen Daten widersprechen kann. In diesem Fall wird die Übermittlung/Veröffentlichung unverzüglich für die Zukunft eingestellt. Etwa bereits auf der Homepage des Vereins veröffentlichte Fotos und Daten werden dann unverzüglich entfernt.

\_\_\_\_\_  
(Ort, Datum)

\_\_\_\_\_  
(Unterschrift/bei Jugendlichen die des Erziehungsberechtigten)

BSV Oberlohberg e.V. 1907, Bergerstr. 354, 46539 Dinslaken

Gläubiger Identifikationsnummer: DE8511100000372374, Mandatsreferenz: wird separat mitgeteilt

## SEPA - LASTSCHRIFTMANDAT

Hiermit ermächtige ich den BSV Oberlohberg e.V. 1907 Zahlungen von meinem Konto mittels Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die vom BSV Oberlohberg e.V. 1907 auf mein Konto gezogenen Lastschriften einzulösen.

Hinweis: Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

IBAN.: \_\_\_\_\_ BIC: \_\_\_\_\_

Bank : \_\_\_\_\_

Name und Anschrift des Kontoinhabers:

Name : \_\_\_\_\_ Vorname : \_\_\_\_\_

Wohnort: \_\_\_\_\_ Straße : \_\_\_\_\_

\_\_\_\_\_  
(Ort, Datum)

\_\_\_\_\_  
(Unterschrift des Kontoinhabers)

Anschrift: BSV Oberlohberg e.V. 1907 - Vorstand - Bergerstr. 354 - 46539 Dinslaken

Email: [vorstand@bsv-oberlohberg1907.de](mailto:vorstand@bsv-oberlohberg1907.de) - Internet: [www.bsv-oberlohberg1907.de](http://www.bsv-oberlohberg1907.de)

Bankverbindung: IBAN: DE51 3565 0000 0000 1363 17 BIC: WELADED1WES Niederrh. Sparkasse Rhein Lippe