Bogenschützen RSG Düren e. V.

(Rollstuhl-Sport-Gemeinschaft)

Mitglied des Behinderten-Sportverbandes Nordrhein-Westfalen e.V. und des Deutschen Schützenbundes e.V.

Homepage: www.rsg-dueren.de

Werner Eismar
Auf dem Horstert 10
D-52353 Düren

Tel. 0 24 21/3 52 02
Email eismar@gmx.net

Richtlinie zur Datenschutzgrundorganisation der Bogenschützen RSG Düren e.V.

(25.05.2018)

1. Grundsätze

Der Schutz personenbezogener Daten ist Bogenschützen RSG Düren e.V. (RSG) ein wichtiges Anliegen. Deshalb verarbeitet die Bogenschützen RSG Düren e.V. die personenbezogenen Daten unserer Mitglieder sowie Bürger in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.
In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten durch den RSG erhoben werden, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem wird beschrieben, mit welchen Maßnahmen die Sicherheit der Daten gewährleistet werden und wie betroffene Personen Kontakt mit der RSG aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.
Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei der RSG bestehenden Verantwortlichkeiten. Alle iun irgendeiner Form Verantwortliche sind zur Einhaltung der Richtlinie verpflichtet.
Sie richtet sich an

- die Personen oder Bereiche, die über den Einsatz/die Bereitstellung von Verarbeitungsprozessen mit personenbezogenen Daten und eines entsprechenden Anwendungssystems entscheiden (Vorstand)
- haupt- und ehrenamtliche Mitarbeiter bzw. Benutzer, d.h. derjenige, der personenbezogene Daten für die Erledigung ihrer Vereinsaufgaben nutzen;

- die/der betriebliche Datenschutzbeauftragte (DSB), die ihre Umsetzung beratend und kontrollierend begleitet und die ihr/ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Dabei gelten folgende Grundsätze:

- Die DV-Hard- und Software sind für Vereinsaufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.
- Jeder verantwortliche Funktionsträger ist in seinem Aufgabenbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Der/Die Datenschutzbeauftragte berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem Datenschutzbeauftragen gegenüber auskunftspflichtig.

2. Beschaffung/Hard- und Software

2.1 Die Beschaffung von Hard-und Software erfolgt grundsätzlich aufgrund eines Vorstandsbeschlusses der Bogenschützen RSG Düren e.V. Bereits bei der Auswahl von Hard-und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

2.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist die/der Datenschutzbeauftragte rechtzeitig vorab zu informieren (siehe hierzu Näheres in Ziff. 5.2). Sollten sensible Daten gemäß Art. 9 DS-GVO verarbeitet werden, müssen alle Verfahren und Systeme, die personenbezogene Daten verarbeiten, einer Risikoanalyse unterzogen werden und verpflichtend ist eine Datenschutzfolgenabschätzung gemäß Art. 35 Abs. 3 a).

2.4 Die Bogenschützen RSG Düren e.V. führen ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme.

2.5 Bei Verdacht des Diebstahls von Hard-und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind der Vorstand und die/der Datenschutzbeauftrage unverzüglich zu informieren. Näheres regelt die Verfahrensanweisung „Verhaltensmaßnahmen bei einer Datenpanne“ (Anlage 1).

3. Verpflichtung/Schulung der Funktionsträger

3.1 Jeder verantwortliche Funktionsträger, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

3.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars

4. Transparenz der Datenverarbeitung

4.1 Der Vorstand führt über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, ein Verzeichnis. Der für ein Verfahren Verantwortliche meldet dieses zeitnah der/dem Datenschutzbeauftragten. Gleiches gilt für Veränderungen.

4.2 Unabhängig von dieser Meldung ist die/der Datenschutzbeauftragte bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren (vgl. Ziff. 6.3).

4.3 Sollte gem. Art. 9 eine Verarbeitung besonderer Kategorien personenbezogener Daten erfolgen, ist bei jeder Einführung bzw. Veränderung bestehender Verfahren eine Datenschutz-Folgenabschätzung erforderlich. Zum Verfahren siehe Ziffer 3.2.

4.4 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur-oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die Bearbeitung durch den 1. Vorsitzenden oder in Streitfällen durch die/der Datenschutzbeauftragte.

4.5 Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

5. Erhebung/Verarbeitung von personenbezogenen Daten

5.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen und insbesondere im Rahmen der Satzung der Bogenschützen RSG Düren e.V. erfolgen. Bei der Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO sind auch die besonderen Voraussetzungen zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

5.2 Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

5.3 Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.
Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und

Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

5.4 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der/die Datenschutzbeauftragte zu kontaktieren.

6. Datenhaltung/Versand/Löschung

6.1 Die Speicherung von Daten erfolgt grundsätzlich auf privaten Speichermedien (Notebook, Desktop-PC) der jeweiligen Funktionsträger bei den Bogenschützen RSG Düren e.V.

6.2 Der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal monatlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

6.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Der Vorstand der Bogenschützen RSG Düren e.V. ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

6.4 Bei der Weiter-oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht oder entsprechend zertifizierte Dienstleister mit der Löschung beauftragt wurden.

7. Externe Dienstleister/Auftragsverarbeitung/Wartung

Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist die/der Datenschutzbeauftragte vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

8. Sicherheit der Verarbeitung

8.1 Für jedes Verfahren ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

8.3 Neben dieser Richtlinie bestehen ergänzende Regelungen, die

insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen.

9. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

10. Die betriebliche Datenschutzbeauftragte

10.1 Die Bogenschützen RSG Düren e.V. hat nach Maßgabe des Artikels 37 DS-GVO eine/n Datenschutzbeauftragte/n bestellt. Die Kontaktdaten der/s Datenschutzbeauftragten werden auf der Homepage des RSB und den offiziellen Printmedien veröffentlicht.
Die/Der Datenschutzbeauftragte nimmt die ihr/ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung ihres/seines Fachwissens sowie ihrer/seiner datenschutzrechtlichen Qualifikation wahr.

10.2 Die/Der Datenschutzbeauftragte unterrichtet und berät den hinsichtlich ihrer Datenschutzpflichten. Ihr/Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.
Im Falle risikoreicher Datenverarbeitungen steht die/der Datenschutzbeauftragte dem Verantwortlichem beratend bei der Abschätzung des Risikos zur Seite.

10.3 Die/Der Datenschutzbeauftragte berichtet unmittelbar dem 1. Vorsitzenden.

10.4 Die/Der Datenschutzbeauftragte wird frühzeitig in allen Datenschutzfragen eingebunden und wird vom Vorstand bei der Erfüllung ihrer/seiner Aufgaben unterstützt.

10.5 Das Verzeichnis über die Verarbeitungstätigkeiten (Art. 30 DS-GVO) und des Erteilens von Auskünften (Art. 15 DS-GVO) auf die/den Datenschutzbeauftragten. Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden liegt die bearbeitende Zuständigkeit bei der/dem Datenschutzbeauftragten. Die Bereiche stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen Betroffener (vgl. Ziff. 5.4).

10.6 Jedes Vereinsmitglied kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an der/die Datenschutzbeauftragte wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

10.7 Die/Der Datenschutzbeauftragte berichtet dem 1. Vorsitzenden Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Soweit der Bericht die Verarbeitung von Personaldaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Vorstand zugänglich gemacht.

Anlage 1

Verfahrensanweisung „Verhaltensmaßnahmen bei einer Datenpanne“

Die Bogenschützen RSG Düren e.V. sind verpflichtet, den Aufsichtsbehörden nach Art. 33 Abs. 1 DSGVO eine Datenpanne zu melden, wenn dadurch der Schutz der sensiblen Daten gem. Art. 9 Abs. 1 DSGVO verletzt wurde.
Solche Daten enthalten zumeist Informationen zu sehr privaten Lebensbereichen der Betroffenen. Bei einer Offenbarung an Unbefugte oder einer Veröffentlichung sind die Betroffenen einem erhöhten Risiko für Bloßstellungen bzw. Diskriminierungen ausgesetzt, oder es wird z.B. das Recht auf Resozialisierung gefährdet. Nicht ohne Grund sind diese Daten größtenteils unter einen besonderen gesetzlichen Schutz gestellt, so z.B. besondere Kategorien personenbezogener Daten.
Auf einen Vorsatz, anderes eigenes unrechtmäßiges Verhalten oder eigene Fehler kommt es hier nicht an. Meldepflichtig ist jede Verletzung der Sicherheit, die zu Vernichtung, Verlust, Veränderung zu unbefugter Offenlegung oder zu unbefugtem Zugang zu diesen persönlichen Daten führt.
Es ist dabei ausreichend, wenn es entweder offensichtlich ist, dass Dritte Kenntnis erlangt haben, oder wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann.
Eine Informationspflicht kommt auch in Fällen des Datenverlusts in Betracht, wenn Laptops, Smartphones usw. an Orten verloren gehen, wo sie Dritten zugänglich sind und die Daten nicht verschlüsselt sind. Gleiches gilt, wenn Daten gestohlen oder illegal aus IT-Systemen abgerufen werden.
Eine Zugangssperre, etwa in Form des Windows-Login, reicht nicht aus. Diese kann technisch leicht umgangen werden. Auf ein etwaiges Verschulden beim Datenverlust, auf eine selbst initiierte Weitergaben oder auf eine sonstige Mitwirkung der betroffenen Stelle kommt es insgesamt nicht an.
Als Datenpanne wird auch gesehen, wenn Mitarbeiter etwa Daten unbefugt an private eigene E-Mail-Adressen versenden oder auf externen Medien speichern und diese mitnehmen. In solchen Fällen erhält der Mitarbeiter die Daten nicht im Rahmen seiner festgelegten Aufgabenbereiche, sondern als Privatperson. Damit ist er nicht mehr Teil der Organisation, sondern steht außerhalb der betroffenen Stelle und wird mithin zum Dritten. Die Daten, die er mitgenommen hat, sind damit einem Dritten unrechtmäßig zur Kenntnis gelangt.
Nach dem Bekanntwerden einer solchen Verletzung muss die Meldung an die Aufsichtsbehörde unverzüglich, spätestens jedoch nach 72 Stunden nach dem Bekanntwerden, erfolgen. Eine spätere Meldung muss eine Begründung für die Verzögerung beigelegt werden.
Weiterhin sind auch die Betroffenen selber zu informieren. Die Regelungen hierzu enthält Art. 34 DSGVO.
Aus diesem Grunde sind alle datenschutzrelevanten Vorfälle sofort der Datenschutzbeauftragten sowie dem Geschäftsführer des RSB zu melden.
Diese entscheiden dann, welche weiteren Maßnahmen ergriffen werden müssen.

Anlage 2

Umgang mit personenbezogenen Daten bei den Bogenschützen RSG Düren e.V.

Der Datenschutz soll vor Missbrauch und unbefugtem Zugriff bewahren. Die wesentliche Idee ist es, den sogenannten „gläsernen Menschen“ zu verhindern. Jeder Mensch soll grundsätzlich selbst entscheiden können, wem wann welche seiner persönlichen Daten zugänglich sein sollen.
Die entsprechenden Datenschutzbestimmungen finden sich in der europäischen Datenschutz-Grundverordnung (DS-GVO). Diese wird ab dem25.05.2018 für alle EU-Mitgliedstaaten verbindlich.
Durch die DS-GVO werden personenbezogene Daten geschützt.
Grundsätzlich sind alle Daten, die sich einer bestimmten oder bestimmbaren natürlichen Person zuordnen lassen zu schützen. Natürliche Person ist ein jeder Mensch in seiner Funktion als Träger von bestimmten Rechten und Pflichten.
Die DSGVO erweitert diese allgemeine Definition noch ein wenig:
Personenbezogene Daten sind hiernach Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke ermöglichen in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität (Artikel 4 Ziffer 1 DSGVO).

Welche personenbezogenen Daten gibt es im Einzelnen?

Die Arten personenbezogener bzw. auf Personen beziehbarer Daten sind zahlreich. Eine abschließende Zusammenfassung lässt sich kaum bewältigen. Im Folgenden wird eine Liste mit den Daten aufgeführt, die für die Aufgaben der Bogenschützen RSG Düren e.V. relevant ist, aufgeführt:

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummern, Geschlecht, Nationalität usw.)
- Bankdaten

Daneben existieren auch noch besondere personenbezogene Daten, die eines erhöhten Schutzes bedürfen. Die Vorschriften zur Sammlung und Verarbeitung solcher Daten sind wesentlich strenger. Solche besonders sensible personenbezogene Daten sind nach Art. 9 DS-GVO:

- Gesundheitsdaten (Behinderungen, Medikamentierung hinsichtlich Doping)

Verarbeitung von besonderen Kategorien personenbezogener Daten durch die Bogenschützen RSG Düren e.V.

Bei den Bogenschützen RSG Düren e.V. können folgende besonderes zu schützenden Daten verarbeitet:
- Gesundheitsdaten (für die Klassifizierung gem. der Sportordnung des DSB)

Das bedeutet, dass nach Art. 9 Abs. 2 d) die Daten mittelbarer Mitglieder nur auf der

Grundlage geeigneter Garantien im Rahmen unserer rechtmäßigen Tätigkeit und unter der Voraussetzung verarbeitet werden, dass sich die Verarbeitung ausschließlich auf die mittelbaren Mitglieder oder ehemalige mittelbare Mitglieder der Bogenschützen RSG Düren e.V., verarbeitet werden dürfen. Diese Daten dürfen nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden. Ansonsten dürfen diese besonderen personenbezogenen Daten nur mit Einwilligung der betroffenen Person verarbeitet werden.
Zudem müssen diese Daten besonders geschützt werden, da nach dem Gesetz die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bedeutet.
Deshalb bedarf es beim Umgang mit diesen personenbezogenen Daten einer erhöhten Sorgsamkeit. Es gilt insbesondere:

- Sie sind dem Datengeheimnis verpflichtet und dürfen weder außenstehenden Dritten noch Mitarbeitern, die nicht direkt mit dem jeweiligen Vorgang befasst sind, personenbezogene Informationen geben oder diesen entsprechende Daten zugänglich machen oder weiterleiten.
- Personenbezogene Mitgliederdaten müssen getrennt gespeichert und bearbeitet werden. Sie haben Sorge dafür zu tragen, dass es nicht zu einer Vermengung der unterschiedlichen Datenbestände kommt.
- Personenbezogene Daten sind gegen unautorisierte Zugriffe zu schützen. Speichern Sie personenbezogene Daten daher nur in kennwortgeschützten Bereichen und sorgen Sie dafür, dass Ihre Benutzerdaten keinem Dritten und auch keinem anderen Mitarbeiter bekannt werden.
- Das Speichern und/oder Kopieren vertraulicher und/oder personenbezogener Daten ist nur auf den dafür vorgesehenen und entsprechend gesicherten Massenspeichern gestattet.
- Das Speichern und/oder Kopieren vertraulicher und/oder personenbezogener Daten auf Wechseldatenträgern ist ausdrücklich verboten.
- Beachten Sie, dass Sie personenbezogene Daten nur für aktuelle Dienstvorgänge erheben, speichern, verarbeiten und nutzen dürfen, soweit es für Ihre Tätigkeit erforderlich ist.
- Beachten Sie, dass Sie ohne die Zustimmung der betroffenen Personen keine personenbezogenen Daten sammeln und speichern dürfen.
- Dokumentieren Sie den Umgang mit personenbezogenen Daten so, dass nachvollziehbar ist, wann und warum Sie mit bestimmten personenbezogenen Daten gearbeitet und wo Sie diese gespeichert haben.
- Beachten Sie, dass betroffene Personen einen Anspruch darauf haben, Auskunft der über sie gespeicherten Daten zu erhalten, und seien Sie darauf vorbereitet, derartige Auskünfte zu erteilen.
- Die Weitergabe personenbezogener Daten an Dritte ist regelmäßig – und ohne Zustimmung des Betroffenen – nicht zulässig. Ist es in Ausnahmefällen gestattet, muss die Übermittlung verschlüsselt sein und die Daten müssen abgetrennt voneinander übermittelt werden. So soll am Ende

zunächst das unrechtmäßige Abgreifen verhindert, zum anderen aber auch unterbunden werden, dass Datensammlungen zu einer Person zu viele Informationen über den Betroffenen preisgeben.

- Die Speicherung personenbezogener Daten bedarf erhöhter Sicherheitsmaßnahmen. Das meint nicht nur passwortgeschützte Arbeitsplätze und Datenbänke, sondern vor allem auch angemessene Verschlüsselungsprogramme und höchstwirksame Maßnahmen zur Unterbindung einer Infiltrierung durch Schadsoftware (Antivirenprogramme, Firewall usf.). Unter Umständen müssen personenbezogene Daten auch anonymisiert werden, d. h. der Bezug zu einer bestimmten oder bestimmbaren Person wird aufgehoben.
- Die Verarbeitung personenbezogener Daten muss immer zweckgebunden erfolgen. Ist der Zweck erfüllt, müssen die Angaben gelöscht oder vor einem weiteren Zugriff geschützt werden. Diesem Zweck muss der Betroffene zudem eindeutig zugestimmt haben.
- Die Pflicht zur Löschung personenbezogener Daten besteht regelmäßig, sobald die Daten nicht mehr benötigt werden bzw. die Zweckgebundenheit aufgelöst ist. Auch unrechtmäßig gespeicherte Daten müssen umgehend sicher gelöscht werden.

Rechte der Betroffenen

Da die personenbezogenen Daten als Eigentum der jeweils betroffenen Person anzusehen sind, haben die Betroffene, deren Daten gesammelt, gespeichert und verarbeitet werden, zahlreiche Rechte. Die wichtigsten Rechte betreffen das Recht auf Berichtigung, das Recht auf Löschung („Recht auf Vergessenwerden“), den Auskunftsanspruch, Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Recht auf Widerspruch.
Wenn eine betroffene Person von ihrem Auskunftsrecht Gebrauch macht, informieren Sie bitte unverzüglich die Datenschutzbeauftragte. Die Datenschutzbeauftragte übernimmt die zentrale Bearbeitung und stellt die zu erteilenden Informationen gemäß Art. 12 Abs. 3 DSGVO zur Verfügung. Das Gesetzt sieht vor, dass diese Auskunft innerhalb eines Monats nach Eingang des Antrags erfolgen muss. Diese Frist kann in komplexen Fällen um zwei Monate verlängert werden. Über Fristverlängerungen ist die betroffene Person unter Angabe der für die Verzögerung verantwortlichen Gründe innerhalb eines Monats nach Eingang ihres Antrags zu informieren. Deshalb unsere Bitte: Handeln Sie rasch!
Ein Betroffener kann bei einer Verletzung seiner Rechte Anspruch auf Schadensersatz geltend machen und jederzeit die zuständige Aufsichtsbehörde einschalten.

Anlage 3

Richtlinie zum Umgang mit Passwörtern

1. Die bei den Funktionsträgern geführten personenbezogenen Daten sind besonders zu schützen. Aus diesem Grunde müssen die Anforderungen an die Sicherheit der Passwörter dementsprechend hoch sein. Um diesen Sicherheitsansprüchen zu genügen, sollte ein Passwort aus mindestens acht Zeichen bestehen. Je länger das Passwort, desto schwerer ist es zu knacken. Neben Buchstaben und Ziffern sollten im Passwort auch Sonderzeichen verwendet werden. Bei den Buchstaben sollten in jedem Fall Groß- und Kleinbuchstaben benutzt werden.

2. Auf keinen Fall dürfen dabei Namen oder sonstige reale Wörter aus welchen Sprachen auch immer verwendet werden, da diese zu leicht zu erraten sind und bei ernsthaften Angriffen stets zuerst ausprobiert werden. Auch nebeneinander liegende Tasten (qwertz, yxcvb) bieten keinerlei Sicherheit.

3. Begriffe oder Namen aus dem persönlichen Umfeld des Nutzers sollten in keinem Fall verwendet werden, auch nicht in abgewandelter Form, etwa indem diese Namen durch vor- oder nachgestellte Zahlen erweitert werden (etwa Julia87, 31_Klaus).

4. Um sich komplexe Passwörter besser zu merken, kann man auf bestimmte Eselsbrücken, zurückgreifen. So kann man z.B. Passwörter aus Gedichtzeilen, Liedtexten oder Buchtiteln herleiten, indem man zunächst die Anfangsbuchstaben hintereinander notiert und diese dann zusätzlich noch durch weitere Maßnahmen verfremdet. Ausgehend von WrssdNuW? (Wer reitet so spät durch Nacht und Wind?) könnte man z.B. bestimmte Buchstaben durch Ziffern ersetzen (etwa alle Vokale in ihrer Reihenfolge durch 1,2, 3 etc., was hier dann zum Passwort WrssdN1W? führt. Es sind aber auch beliebige andere Variationen möglich (Weglassen von Vokalen, Versetzen der Buchstaben um eine Stelle im Alphabet etc.). Anstelle eines komplizierten Passworts muss man sich hier nur noch die Konstruktionsregel merken, was wesentlich leichter sein dürfte.

5. Ein und dasselbe Passwort sollte nicht für unterschiedliche Einsatzbereiche verwendet werden. So angenehm es ist, sich nur ein Passwort merken zu müssen, so groß sind hier die Missbrauchsmöglichkeiten, wenn dieses Passwort in die falschen Hände gerät.

6. Passwörter dürfen in keinem Fall an unberechtigte Dritte weitergegeben werden. Um den Zugriff auf wichtige Bereiche oder Ressourcen anderen Berechtigten zu ermöglichen, können die Passwörter an sicherer Stelle hinterlegt werden.

7. Eine schriftliche Fixierung der Passwörter ist nach Möglichkeit zu vermeiden. Sollte sich dies als nicht praktikabel erweisen, sollten die Passwörter in jedem Fall an einem sicheren Ort verwahrt und niemals öffentlich zugänglich

sein. Besteht der Verdacht, dass unberechtigte Personen ein Passwort in Erfahrung gebracht haben könnten, ist dieses unverzüglich zu ändern bzw. bei den jeweiligen Administratoren ein neues Passwort anzufordern.

8. Passwörter sollten regelmäßig gewechselt werden. Je sensitiver die hierüber geschützten Daten sind, desto kürzer sollte die Nutzungsdauer eines Passworts sein.

Anlage 4

Merkblatt zur E-Mail-Nutzung

Beim Empfang von E-Mails ist auf Folgendes zu achten:

- Im Microsoft Explorer sollte die Anzeige aller Dateitypen aktiviert sein.
- Der elektronische Briefkasten muss regelmäßig (zumindest mehrmals täglich) hinsichtlich des Eingangs elektronischer Post überprüft werden.
- Offensichtlich unsinnige E-Mails von unbekannten Absendern sollten ungeöffnet gelöscht werden. Gleiches gilt für die Anhänge von Mails aus nicht zuverlässigen oder unbekannten Quellen.
- E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sind hinsichtlich des Inhalts zu überprüfen (zweifelhafter Text, fehlender Bezug zu konkreten Vorgängen etc.).
- Bei mehreren E-Mails mit gleich lautendem Betreff ist Vorsicht geboten.
- Nur vertrauenswürdige Dateianhänge (Attachments) dürfen geöffnet werden.
- Kein Doppelklick bei ausführbaren Programmen (z. B. *.COM, *.EXE) oder Script-Sprachen (z. B. *.VBS, *.BAT) sowie Bildschirmschonern (*.SCR).
- Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT).
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.
- Die Weiterleitung von Nachrichten im Vertretungsfall ist zu gewährleisten.
- Personenbezogene und vertrauliche Nachrichten sind physikalisch zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist.
- Elektronische Irrläufer sind nach Möglichkeit an den richtigen Adressaten weiterzuleiten. Ist dieser nicht zu ermitteln, muss die E-Mail an den Absender zurückgeschickt werden.

Beim Versenden von E-Mails ist zu beachten:

- Sensible personenbezogene oder sonstige vertrauliche Informationen dürfen nur unter Einsatz geeigneter Verschlüsselungsverfahren elektronisch übertragen werden. Das Gleiche gilt für beigefügte Anlagen.
- Auch die E-Mail-Adresse ist ein personenbezogenes Datum. Die Weitergabe – insbesondere bei unseren Mitgliedern – bedarf der Einwilligung der Betroffenen. Aus diesem Grunde dürfen die E-Mail-Adressen niemals Dritten übermittelt werden. Somit ist z. B. bei einem Massenversand sicherzustellen, dass die Adressen für die Empfänger nicht sichtbar sind. Verwenden Sie daher die Funktion „bcc“.

- Soweit möglich sollte von der Digitalen Signatur Gebrauch gemacht werden.
- Unnötige E-Mails dürfen nicht versandt werden.
- Der Versand von Kettenbriefen und Mails, deren Inhalt Anstoß erregen könnte, ist verboten. Ebenso das Abonnieren von Mailinglisten.
- Ausführbare Programme dürfen grundsätzlich nicht übermittelt werden.
- E-Mails sollten nicht im HTML-Format versendet werden.
- Aktive Inhalte (ActiveX, Java, JavaScript) in E-Mails sind zu vermeiden.
- Ein elektronisch zu versendendes Dokument muss den internen Vorschriften und Regelungen hinsichtlich äußerer Form und Gestaltung entsprechen. Außerdem muss es die erforderlichen Angaben zum Absender enthalten und im Betreff der E-Mail eine möglichst aussagekräftige Beschreibung des Nachrichteninhaltes angegeben sein.
- Zur Vermeidung einer fehlerhaften Zustellung müssen E-Mails eindeutig adressiert werden.
- Alle Dateien sind vor dem Versand explizit auf Virenbefall zu überprüfen.
- Grundsätzlich darf keiner Aufforderung zur Weiterleitung von Mails oder Anhängen ohne strenge Prüfung gefolgt werden.
- Gelegentlich ist zu prüfen, ob sich E-Mails im Postausgangskorb befinden, die nicht vom Benutzer selbst verfasst wurden.

Anlage 5

Richtlinien / Handlungsanweisungen bei der Nutzung eines privaten PC´s oder anderen mobilen Endgeräten

1. Die wichtigste Schutzvorkehrung auf einem Rechner am Heimarbeitsplatz ist die Installation und Nutzung eines Antivirenprogramms. Das Antivirenprogramm sollte regelmäßig (mindestens einmal pro Woche) aktualisiert werden, um seine Schutzfunktion aufrechterhalten zu können. Neben dem permanenten Betrieb (On-Access-Modus) sind regelmäßige Komplettscans des Systems notwendig, um mögliche Schädlinge noch rechtzeitig zu erkennen und zu bekämpfen.
2. Auf Windows-PCs sollten die hier enthaltenen und standardmäßig aktivierten Sicherheitsoptionen in jedem Fall beibehalten werden. Dazu gehört insbesondere das automatische Windows-Update, durch das das Betriebssystem und weitere Microsoft-Programme auf dem jeweils neuesten Stand gehalten werden. Auch die Windows-Firewall sollte eingeschaltet bleiben. Darüber hinaus sollten auch alle anderen verwendeten Programme wie Media-Player oder PDF-Software auf dem neuesten Stand gehalten werden, um das Risiko von Angriffen über diese Anwendungen zu minimieren.
3. Weitere Sicherheitsprogramme wie spezialisierte Antispyware-Programme, Browser-Erweiterungen mit Phishing-Filtern können zusätzliche Sicherheit bieten.
4. Zusätzlichen Schutz bietet die Verwendung eines Routers für den Internetzugang, da über die NAT-Funktion (Network Adress Translation) des Routers und die hier integrierten Firewall-Komponenten ein zusätzlicher Schutz realisiert wird.
5. Erfolgt die Verbindung zum Router über die WLAN-Funktechnik, so ist unbedingt eine Verschlüsselung des WLANs über die WPA2-Technik zu verwenden. Ältere Verfahren, insbesondere WEP, bieten dagegen keinen ausreichenden Schutz. Das Passwort für die WLAN-Verschlüsselung sollte möglichst komplex und von ausreichender Länge (mind. 12 Zeichen) sein.
6. Der Zugang zum Heim-PC sollte ausschließlich dem jeweiligen Nutzer möglich sein. Zugangsdaten wie Benutzername und Passwörter dürfen nicht an andere Personen weitergegeben werden. Passwörter, die als Gedächtnisstütze niedergeschrieben wurden, dürfen nicht in der Nähe des PCs aufbewahrt werden. Der Rechner darf nicht mit anderen Privat-PCs zu einem Netzwerk verbunden werden.
7. Beim Austausch von E-Mails mit sensiblen Informationen über das Internet müssen die Nachrichten über geeignete Kryptographie-Anwendungen verschlüsselt werden, um das mögliche Mitlesen dieser Daten zu verhindern.
9. Sensible Daten des Vereins dürfen nur in verschlüsselter Form auf dem Rechner gespeichert werden, damit diese auch im Falle eines Diebstahls des PCs oder Fremdzugriffs auf den Rechner geschützt bleiben.

10. Internet-Anwendungen dürfen nur mit höchstmöglichen Sicherheitseinstellungen genutzt werden, Downloads und Installation von Software aus potenziell gefährlichen Quellen sind untersagt und ein vorsichtiger Umgang mit E-Mail-Attachments ist Pflicht.

Mit der Unterschrift bestätigen Sie, dass Sie sämtliche Regelungen verstanden haben und sich an die hier ausgeführten Richtlinien halten werden.