Sicherheitskonzept

Dieses Dokument beschreibt die im MRRC e.V. einheitlich umgesetzten technischen und organisatorischen Maßnahmen zur Erfüllung gesetzlicher Datenschutzanforderungen nach Art. 32 EU-DSGVO. Es dient gleichzeitig als Sicherheitskonzept für Geschäftsstelle und die im Verein eingesetzten IT-Systeme. Das Dokument ist regelmäßig fortzuschreiben.

Dokumentation

In der Nextcloud liegt die Datei MRRC_Datenschutz/MRRC_Übersicht_Zugänge.ods.

Darin sind alle nicht persönlichen Zugänge zu hinterlegen und wer diese kennt.

Physische Zutrittskontrolle

Maßnahmen zur Kontrolle des Zutritts zu Gebäuden und Räumlichkeiten des Vereins.

Die Räume des Vereins sowie die Einrichtungen für die Aufbewahrung von Daten sind durch die in den folgenden Abschnitten beschrieben physischen Schutzmaßnahmen vor unbefugtem Zutritt geschützt.

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Alle Datenverarbeitungssysteme sind mit einem sicheren Authentifizierungsmechanismus (Passwortschutz, teilweise Mehrfaktor-Authentifizierung) ausgestattet.

Alle Zugangsrechte (sowohl für den Zugriff auf IT-Systeme und Daten als auch für den Zutritt zu Gebäuden und Räumen) werden nach dem Prinzip vergeben, dass Benutzer nur das Maß an Zugang erhalten, das sie für die Ausübung ihrer Tätigkeiten benötigen (Minimalprinzip).

Zugangsrechte werden nach definierten (rollenbasierten) Berechtigungsprofilen vergeben. Die erteilten Zugangsrechte werden regelmäßig überprüft. Nicht mehr benötigte Rechte werden zeitnah entzogen.

Eine generelle Überprüfung von Zugangsrechten erfolgt bei jedem Vorstandswechsel.

Akten sind im verschlossenen Schrank zu hinterlegen.

Schlüssel sind im verschließbaren Schlüsselschrank zu hinterlegen.

Bargeld und kleine sensible Dinge sind im Tresor zu hinterlegen.

Das Notebook auf dem Schreibtisch ist mit einer Diebstahlsicherung gesichert werden. Das zweite Notebook liegt im abschließbaren Aktenschrank.

Umgang mit Kennwörtern

Zur Authentifizierung an IT-Systemen sollen sichere Passwörter verwendet werden, die nach dem Stand der Technik über eine ausreichende Komplexität verfügen, um robust gegen Wörterbuchangriffe zu sein (z.B. Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, keine Zeichenketten aus aufeinanderfolgenden Buchstaben oder Ziffern) und nicht leicht erraten werden können. Für Regelungen zur Änderung der Passwörter siehe die folgenden Abschnitte.

Kennwörter dürfen nicht ohne Sicherheitsschutz zu übertragen. Bei einer E-Mail ist ein Verschlüsselung notwendig. Ansonsten ist noch der Versand per SMS erlaubt.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es ist sicherzustellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben werden, in ihrer Verarbeitung nicht vermischt werden. Dies ist insbesondere beim Export und ggf. lokaler Verarbeitung von Daten (z.B. als EXCEL-Datei) zu beachten.

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Dateiablage

Personenbezogene Daten sollten nach Möglichkeit nur innerhalb der entsprechenden IT-Systeme bearbeitet werden (z.B. Mitgliedsdaten in Sewobe). Ist eine darüber hinausgehende Verarbeitung notwendig, sollen die Daten in der MRRC Cloud abgelegt werden. Der Zugriff auf die Daten ist entsprechend durch Zugriffsberechtigungen zu regeln. Eine lokale Ablage von Daten z.B. auf privaten Rechnern, E-Mail-Accounts, USB-Laufwerken etc. ist generell nicht erwünscht.

Elektronische Kommunikation

- Es ist auf sichere Kommunikation zu achten:
- Beim Versand von E-Mails nur vertrauensvolle E-Mail-Dienstleister verwenden. Der MRRC nutzt HostEurope.
- Bei der Konfiguration von einem E-Mail-Client wie z.B. Thunderbird muss beim E-Mail Versand die Transportverschlüsselung sichergestellt werden (z.B. STARTTLS)

- Damit E-Mails verschlüsselt werden können, muss dem Versender der öffentliche Schlüssel des Empfängers bekannt sein. Dieser Schlüssel kann unverschlüsselt per E-Mail verschickt werden. Es muss aber auf einem weiteren Weg (z.B. Telefon, Fax) geprüft werden, ob der öffentliche Schüssel wirklich der Person gehört.
- „Offene“ E-Mail-Verteiler sollten vermieden werden. Stattdessen soll die BCC-Funktionalität geeignet eingesetzt werden. Eine Ausnahme gilt nur in Fällen, wo die Mitglieder des Verteilers ausdrücklich ihre E-Mail-Adresse der Gruppe veröffentlicht haben. So eine Ausnahme kann z.B. der Arbeitskreis zu Organisation einer Veranstaltung sein
- E-Mail-Signatur. Für vereinsbezogene E-Mails ist eine Signatur nach folgendem Schema an jede E-Mail anzuhängen:

Grußformel Vor- und Nachname MRRC München e.V. Amt / Funktion E-Mail-Adresse: vorname.nachmame@mrrc.de Web-Adresse: http://www.mrrc.de

Papierunterlagen

Es müssen nur sensible Papierdaten geschreddert werden (die personenbezogene Daten enthalten).

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, sind im erforderlichen Umfang umgesetzt. Die Integrität der Loginformationen wird durch technische und organisatorische Maßnahmen gewährleistet.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Mit allen externen Dienstleistern die Zugriff auf personenbezogene Daten des Vereins erhalten, sind Verträge zur Auftragsverarbeitung abzuschließen.

Aktuell liegen folgende Verträge vor:

- Sewobe (Software zur Vereins- und Mitgliederverwaltung)
- HostEurope (Web-Hosting)

Datenschutz

Regelungen zur Erarbeitung, Umsetzung und Nachhaltung von Datenschutz-Maßnahmen im Verein.

m Verein sind weniger als zehn Personen ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt. Ein Datenschutzbeauftragter gemäß DSGVO wird daher nicht benannt. Die Verantwortung für das Thema Datenschutz liegt beim Vorstand. Alle Mitglieder und Mitarbeiter des Vereins, die mit Themen des Datenschutzes im Verein betraut sind können unter der Adresse datenschutz@mrrc.de erreicht werden.

Verzeichnis der Verarbeitungsprozesse

Alle Verarbeitungsprozesse sind in der folgenden Datei hinterlegt.