Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der Organisation
SV Energie Berlin e. V.

Inhalt

1. Allgemeines

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

2. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen.

2.1.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um den Zutritt Unbefugter zu Gebäuden und Räumlichkeiten der Rechenzentren und den darin enthaltenen Serveräumen und Servern zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucherbuch / Protokoll der Besucher
☒ Manuelles Schließsystem	☒ Mitarbeiter- / Besucherausweise
☒ Sicherheitsschlösser	☒ Besucher in Begleitung durch Mitarbeiter
☒ Schließsystem mit Codesperre	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	
☒ Türen mit Knauf Außenseite	
☒ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge	

2.1.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um den Zutritt Unbefugter zum Bootshaus und den Räumlichkeiten darin zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Manuelles Schließsystem	☒ Schlüsselregelung / Liste
☒ Sicherheitsschlösser	☒ Besucherbuch / Protokoll der Besucher
☒ Türen mit Knauf Außenseite	☒ Besucher in Begleitung durch Vereinsmitglieder
☒ ABUS-Transpondersystem	☒ Zugtrittsberechtigungskonzept

2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

2.2.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um den Zugang Unbefugter zu IT-Systemen in den Rechenzentren/ auf den Servern zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Virus-Software Clients	☒ Erstellen von Benutzerprofilen
☐ Anti-Virus-Software mobile Geräte	☒ Zentrale Passwortvergabe
☒ Firewall	☒ Richtlinie „Sicheres Passwort" oder einfach: 8-stellig mit Buchstaben, Ziffern und Sonderzeichen. Vergabe durch Geschäftsführer de Fa. Internetworx, Kopie des Passwortes an 1. Vorsitzenden des SV Energie Berlin e.V.
☒ Intrusion Detection Systeme	☐ Richtlinie „Löschen / Vernichten"
☒ Mobile Device Management: Nutzung nur von Apps, die verschlüsselte und sichere Übertragung der Daten gewährleisten	☐ Allg. Richtlinie Datenschutzordnung des SV Energie Berlin e. V.
☒ Einsatz VPN bei Remote-Zugriffen	☐
☒ Verschlüsselung von Datenträgern Clients für Remote Zugriff auf Server	☐
☒ Gehäuseverriegelung, Serverschränke	☐

☒ Verschlüsselung von Notebooks / Tablet für Remote Zugriff auf Server	☐
☐ Login mit Zertifikatsverfahren an Clients	

2.2.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um den Zugang Unbefugter zu IT-Systemen im Bootshaus und auf mobilen Geräten zu verhindern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Login mit Benutzername + sicheres Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Virus-Software Clients	☒ Erstellen von Benutzerprofilen
☒ Firewall	☒ Datenschutzordnung des SV Energie Berlin e. V.
☒ Mobile Device Management: Nutzung nur von Apps, die verschlüsselte und sichere Übertragung der Daten gewährleisten	☒ sicheres Passwort zum Aufheben der Sperre
☐ BIOS Schutz (separates Passwort)	☐
☒ Automatische Desktopsperre	☒

2.3 Zugriffskontrolle

Maßnahmen, die 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 der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

2.3.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um den unbefugten Zugriff auf personenbezogene Daten auf den IT-Systemen der Server zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Physische Löschung von Datenträgern	☒ Einsatz Berechtigungskonzepte
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Minimale Anzahl an Administratoren
	☒ Verwaltung Benutzerrechte durch Administratoren

2.3.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um den unbefugten Zugriff zu IT-Systemen im Bootshaus und auf mobilen Geräten zu verhindern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☒ Für ABUS-Transpondersystem: Protokollierung von Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch Administratoren

2.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

2.4.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auf den Servern getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Ersatz-Umgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	

2.4.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auf den IT-Systemen im Bootshaus und auf mobilen Geräten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Steuerung über Berechtigungskonzept

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

***Ma**ßnahmen, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.*

Der SV Energie ergreift die folgenden Maßnahmen, um den unbefugten Zugriff auf personenbezogene Daten bei Übertragung, Transport oder Speicherung auf Datenträger zu verhindern und zu gewährleisten, dass überprüfbar ist, an wen eine Übermittlung personenbezogener Daten vorgesehen ist.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Email-Verschlüsselung (Anlagen)	☒ Dokumentation der Datenempfänger
☒ Nutzung von Apps mit Verschlüsselung	☒ Sorgfalt bei Auswahl der Apps
☒ Protokollierung der Zugriffe und Abrufe (nur für Serverdaten)	☐
☒ Bereitstellung der Webseiten-Daten über verschlüsselte Verbindungen wie sftp, https	☒ Passwort für Mitgliederbereich
☒ Nutzung von Signatur- und Zertifikatsverfahren	☐
☒ Protokollierung der Web-Accounts und Logins	☒ WP-Cerber-App
☒ Protokollierung von unberechtigten Login-Versuchen und anderer Atacken auch per Bots	☒ WP-Cerber-App

3.2 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Der SV Energie ergreift die folgenden Maßnahmen, um die Überprüfbarkeit von Eingaben, Änderungen und Löschungen personenbezogener Daten in IT-Systemen zu gewährleisten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten, nur für Server.	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☒ Für ABUS-Transpondersystem: Technische Protokollierung der Eingabe, Änderung und Löschung von Daten, nur für Server.	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können (VVZ)
☐	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden.
☐	☒ Klare Zuständigkeiten für Löschungen.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

4.1.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um personenbezogene Daten auf den Servern gegen zufällige Zerstörung oder Verlust zu schützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Serverstandort ist Berlin
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert) für Clients
☒ Feuerlöscher	☒ Kontrolle des Sicherungsvorgangs auf Servern
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums, Hot-StandBy-Server an einem zweiten Standort
☒ Serverraum klimatisiert	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ USV	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4/ 200-4) für Serverraum
☒ Schutzsteckdosenleisten	☒ Getrennte Partitionen für Betriebs-systeme und Daten
☒ Videoüberwachung	☒ Separate Partition oder Benutzerzugang auf Client-PC's mit Benutzername/ PW ausschließlich für Daten des Vereins
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☒ Zwei Serverstandorte mit jeweils 3 Servern in Berlin, Deutschland, geographisch getrennt,
☒ Daten werden auf 6 Servern mit 96 Festplatten verteilt.	☒ Daten werden auf den Servern 4-fach gespiegelt
	☒ Backup auf zusätzlichen Server

4.1.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um personenbezogene Daten auf IT-Systemen im Bootshaus und mobilen Geräten gegen zufällige Zerstörung oder Verlust zu schützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuerlöscher	☒ Elektronisches Schließsystem
	☒ Backup auf externen Datenträgern

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitglieder nach Bedarf / Berechtigung	☒ Mitglieder und Funktionsträger sind geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	☒ DS-Ordnung des SV Energie Berlin e. V. und Anlagen
	☒ Regelmäßige Sensibilisierung der Mitglieder Mindestens jährlich
	☒ Interner DS-Ansprechpartner ist im Verfahrensverzeichnis dokumentiert
	☒ Der Verein kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach.
	☒ Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.

5.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

5.2.1 Für Rechenzentrum und Serverraum/ Server

Der SV Energie ergreift die folgenden Maßnahmen, um bei der Reaktion auf Sicherheitsverletzungen bezüglich der IT-Systeme in den Rechenzentren/ der Servern zu unterstützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (ggf. SW-Lösung, auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☐ Intrusion Detection System (IDS)	
☐ Intrusion Prevention System (IPS)	

5.2.2 Für das Bootshaus

Der SV Energie ergreift die folgenden Maßnahmen, um den Zugang Unbefugter zu IT-Systemen im Bootshaus zu verhindern.

☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten- Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Der SV Energie ergreift die folgenden Maßnahmen, um sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Datenschutzordnung des SV Energie Berlin e. V.
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☒, Einwilligungserklärung des SV Energie Berlin e. V.
☒ Fernwartungszugänge für Server sind per Default deaktiviert und werden nur auf Anforderung freigegeben. Mit Mario abstimmen	☒ Berechtigungskonzept des SVE (ggf noch zu erstellen)
☒ Für den Ausnahmefall der Übertragung von personenbezogenen Daten erhalten nur die Personen Zugang, die dazu berechtigt sind.	☐

☒ Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Ausgefüllt für den SV Energie Berlin e. V. **durch**

Name Dunsing/ Rothe
Funktion Ansprechpartner für Datenschutz
Rufnummer 030 64387509
Email datenschutz@sv-energie-berlin.de

Ort, Datum Berlin, 03.09.2021

Vom Auftraggeber auszufüllen:

Geprüft am 13.08.2021 durch Ernst Peter, Gerhard Nuck.

Ergebnis(se):

☐ Es besteht noch Klärungsbedarf zu

☒ TOMs sind für den angestrebten Schutzzweck ausreichend

Hinweis: Diese Vorlage verwendet durchaus noch Begrifflichkeiten des BDSG a.F. Inhaltlich unterscheiden sich die technischen und organisatorischen Maßnahmen nicht von denen, die in der DSGVO gefordert werden!