Datenschutzrichtlinien

Datenschutzrichtlinien (nachfolgend „Richtlinien“ genannt) der Organisation _____

1. Einleitung

Datenschutz geht uns alle an. Nur wenn Datenschutz von allen Mitarbeitern eines Unternehmens beachtet wird und ein stetes Unternehmensziel darstellt, kann er gelebt werden.

Die vorliegende Richtlinie soll die **datenschutzkonforme Informationsverarbeitung** zusichern, **Datenverarbeitungsprozesse** beschreiben und **Verantwortlichkeiten** klären. Alle Mitarbeiter sind zur Einhaltung der Richtlinien verpflichtet. Bitte melden Sie sich daher, falls Sie etwas nicht verstehen sollten.

2. Grundsätze

Innerhalb des Geschäftsbetriebs der VHS gelten folgende Grundsätze:

- Die Hard- und Software der Organisation sind **nur für betriebliche Aufgaben** zu verwenden und entsprechend ihrem Zweck einzusetzen. Es muss eine Sicherung gegen Verlust und Manipulation bestehen. Eine Nutzung für private Zwecke bedarf der vorherigen ausdrücklichen Genehmigung der Organisation.
- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die **Umsetzung der Richtlinien** verantwortlich. Der Mitarbeiter muss die Einhaltung der Vorgaben regelmäßig kontrollieren.
- Die jeweiligen **Vorgesetzten** der Mitarbeiter stellen sicher, dass ihre Mitarbeiter über diese Richtlinien informiert werden und die Kenntnisnahme durch Unterschrift bestätigen. Das gilt auch für nur eine bestimmte Zeit Tätige (z.B. Praktikanten, Auszubildende, Berater).
- Der Datenschutzbeauftragte („DSB“) berät bei der Umsetzung der Richtlinien und prüft deren Einhaltung. Die Mitarbeiter haben dem DSB auf Anfrage entsprechende Auskünfte zu erteilen, damit er dieser Prüfungspflicht auch nachkommen kann.

3. Verpflichtung und Schulung der Mitarbeiter

- Jeder Mitarbeiter ist zu verpflichten, personenbezogene Daten vertraulich zu behandeln. Dies kann durch eine gesonderte Klausel innerhalb des Arbeitsvertrags geschehen.
- Die Mitarbeiter sind im Datenschutz zu schulen. Dies kann extern oder durch den Datenschutzbeauftragten geschehen. Die Mitarbeiter sind für Schulungstermine freizustellen.

4. Datenschutzbeauftragte(r)

- Die Organisation hat eine(n) Datenschutzbeauftragten bestellt. Er unterrichtet und berät die Unternehmensleitung und alle Mitarbeiter in **sämtlichen Fragen des Datenschutzes**. Er ist berechtigt, im Bereich des Datenschutzes Zuständigkeiten von Mitarbeitern zu bestimmen. Er schätzt ferner das Risiko sensibler Datenverarbeitungen ab.
- Der DSB ist frühzeitig in alle Fragen des Datenschutzes einzubinden und wird von allen Mitarbeitern bei der Erfüllung seiner Aufgabe unterstützt.
- Dem DSB obliegt das Erstellen und Führen des **Verarbeitungsverzeichnisses** nach Art. 30 DS-GVO. Dazu zählt auch das Einpflegen von Änderungen. Mitarbeiter, denen eine Änderung eines Datenverarbeitungsprozesses bekannt wird, haben den DSB zu unterrichten. Der DSB bearbeitet ferner die Anfragen auf Erteilung von Auskünften (Art. 15 DS-GVO).
- Die Beantwortung von **Anfragen der Datenaufsichtsbehörde** obliegt der Unternehmensleitung. Der DSB wie auch alle Mitarbeiter werden die Unternehmensleitung hierbei insbesondere mit der Mitteilung von Informationen und Übergabe von Unterlagen unterstützen.
- Jeder Mitarbeiter kann den DSB bei Fragen und mit Anliegen zum Datenschutz konsultieren. Der DSB ist auf Wunsch zur **Vertraulichkeit** verpflichtet.
- Der DSB erstellt einen **Jahresbericht** über seine Tätigkeiten. Hierin sind vorgekommene Datenschutzverstöße sowie Beschwerden zu dokumentieren.
- Unabhängig von dieser Meldung ist der DSB 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. Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Website etc.) ist der Erhebungsbogen etc. dem DSB zur Abstimmung vorzulegen.
- Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer **Datenschutz-Folgenabschätzung** unterliegt, teilt er dies umgehend mit. Das Verfahren darf dann erst nach Zustimmung des DSB durchgeführt werden.

5. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus diesen Richtlinien ergeben, muss jederzeit nachweisbar sein („**Accountability**“). Maßnahmen und Abwägungen zu personenbezogenen Daten sind daher stets zu dokumentieren.

6. Beschaffung Hard- und Software

- Der Erwerb und/oder Einsatz von Hard- und/oder Software ist stets mit dem IT-Dienstleister abzustimmen. Bei Erwerb und Programmierung sind auf **datenschutzfreundliche Einstellungen** zu achten.
- Wird mit der Hard- und/oder Software ein neues Verfahren zur Bearbeitung personenbezogener Daten eingeführt, ist der DSB vorab zu informieren. Insbesondere wird geklärt, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

- Private Hard- und Software (z.B. auch Smartphone / Handy) darf nicht für dienstliche Zwecke nicht verwendet werden. Ausnahmegenehmigungen müssen vor dem Einsatz der Hard- oder Software eingeholt werden und bedürfen der Textform.
- Der IT-Dienstleister führt eine Liste der eingesetzten Hard- und Software. Der DSB erhält hiervon eine Kopie.
- Bei Diebstahl von Hard- oder Software oder anderen Datenschutzverstößen ist der **Krisenplan** einzuhalten.

7. Verarbeitung personenbezogener Daten

- Die Erhebung und Verarbeitung personenbezogener Daten muss zulässig sein. Bei sensiblen Daten, z.B. Gesundheitsdaten, gelten gesonderte Anforderungen.
- Es dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in **unmittelbarem Zusammenhang** mit dem Verarbeitungszweck stehen.
- Natürliche Personen dürfen keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich dem Betroffenen gegenüber einer rechtlichen Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (**z.B. Profiling**).
- Eine Zweckänderung setzt voraus, dass die neue Verarbeitung auch mit dem alten Zweck vereinbar ist. Hierfür herangezogene Abwägungskritierien sind einer Prüfung zu unterziehen. Die gesamte Prüfung ist zu dokumentieren.
- Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person eingeholt wird.
- Vor jeder Erhebung und Speicherung von Daten ist zu prüfen, ob der Verein erpflichtet ist, den Betroffenen hierüber zu **benachrichtigen.**
- 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 Anfragenden besteht. Zudem muss die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der DSB zu kontaktieren.

8. Speichermedien und Löschung ihrer Daten

- Die Speicherung von Daten erfolgt grundsätzlich auf den zur Verfügung gestellten **Netzlaufwerken**. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch den DSB.
- Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Endgerät), ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook oder Tablet mit WLAN), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu kopieren. Die gewählten Datensicherungsmaßnahmen sind in dem **Verfahrensverzeichnis** zu dokumentieren.
- Die Löschregeln gemäß **Löschkonzept** sind von dem über die Daten wachenden Mitarbeiter zu beachten.

- Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten sind sämtliche Daten durch den vorherigen Benutzer unwiderruflich zu löschen.

9. Datenanfragen, Datenpannen

- Macht ein Betroffener von seinem Auskunfts-, Berichtigungs-, Widerspruchs-, Löschungs- oder einem anderweitigen Recht auf Datenschutz Gebrauch, ist die Anfrage unverzüglich an den DSB zur Beantwortung weiterzuleiten. Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.
- Gleiches gilt für Anfragen von Datenschutzbehörden.
- Datenpannen (z.B. Offenlegung von Daten Dritter) sind dem DSB unverzüglich zu eskalieren.

10. Dienstleister, Auftragsverarbeitung und Wartung

- Werden externe Dienstleister mit der Verarbeitung von personenbezogenen Daten beauftragt, z.B. mit dem Versend eines E-Mailnewsletters oder dem Hosten der Webseite der Organisation, ist ein Auftragsverarbeitungsvertrag zu schließen. Hierfür ist der DSB zu kontaktieren.
- Gleiches gilt, soweit Dienstleister bei Ausübung ihrer Tätigkeit, z.B. bei Wartung eines Servers, Einblick in personenbezogene Daten haben.

11. Datensicherheit

- Für jedes Verfahren muss der **Schutzbedarf** festgestellt und dokumentiert werden. Mögliche Risiken für den Betroffenen sind zu eruieren. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.
- Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse.
- Neben diesen Richtlinien bestehen ergänzende Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffenden Maßnahmen betreffen.
  Hierzu gehören u. a.:

- Arbeitsanweisung zum datenschutzgerechten Versand von Datenträgern und zur Verschlüsselung von Daten,
- Arbeitsanweisung zum Passwortverfahren,
- Arbeitsanweisung zur Erteilung von Auskünften im Personalbereich,
- Arbeitsanweisung zur PC- und Laptop-Nutzung und
- Arbeitsanweisung Telearbeit/Home-Office.

Ferner ist die Verarbeitung von Personaldaten in einer Anzahl von Betriebsvereinbarungen näher festgelegt. Hierzu gehört u. a. die Vereinbarung

- über die Nutzung von Telekommunikation (Telefon, E-Mail, Internet) und
- die Vergabe von Telearbeit/Homeoffice