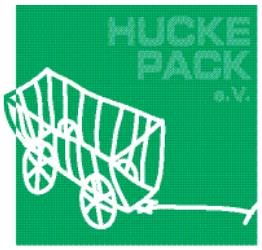
Betriebliche Datenschutzrichtlinie

Richtlinie zur Datenschutz-Organisation Huckepack e.V.
Herausgegeben durch den Datenschutzbeauftragten im Auftrag der Geschäftsleitung



Grundsätze

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung im Verein gem. DSGVO und BDSG-neu und die insoweit bestehenden Verantwortlichkeiten. Alle Mitarbeiter und Mitarbeiterinnen sind zur Einhaltung der Richtlinie verpflichtet. Sie richtet sich an

- die Personen oder Abteilungen, welche den Einsatz eines Anwendungssystems entscheiden;
- die Personen oder Abteilungen, die über die Verarbeitungen des Systems für ihre Aufgaben betroffen sind;
- Benutzer, d. h. diejenigen, die das zur Verfügung gestellte System für die Erledigung ihrer betrieblichen Aufgaben nutzen;
- den betrieblichen Datenschutzbeauftragten (DSB), der die Umsetzung der Richtlinien beratend und kontrollierend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Dabei gelten folgende Grundsätze:

- Die IT-Komponenten sind für betriebliche Aufgaben und zwar für die jeweils vorgesehenen Zwecke zu verwenden und gegen Verlust und Manipulation zu sichern.
  Eine Nutzung für private Zwecke ist nicht gestattet.
- Jeder Mitarbeiter mit Personalverantwortung ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter und Mitarbeiterinnen (Benutzer) über diese Richtlinie informiert werden; dies gilt auch für temporär Beschäftigte.
- Der Datenschutzbeauftragte und der Abwesenheitsvertreter beraten bei der Umsetzung der Richtlinie und prüfen deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB auskunftspflichtig.
- Die Mitwirkungsrechte der Personalvertretung bleiben unberührt

1 Der betriebliche Datenschutzbeauftragte und seine Vertretung

1.1 Die Geschäftsführung des Vereins hat nach Maßgabe des Art. 37 DSGVO und § 38 BDSG-neu Herrn Steve Vetter, Vetter Consulting Datenschutzberatung zum betrieblichen Datenschutzbeauftragten (bDSB) bestellt. Der DSB nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.
Der DSB hat auf die Einhaltung des Datenschutzes gemäß DSGVO und BDSG-neu hinzuwirken. Diese Aufgabe ist von allen Mitarbeitenden des Vereins tatkräftig zu unterstützen.

1.2 Abwesenheitsvertretung (DS-Koordinator) für den Datenschutzbeauftragten des Vereins ist Frau Viktoria Zumpe oder der Amtsinhaber zum jeweiligen Zeitpunkt. Die Vertretung des DSB ist dem DSB fachlich zugewiesen und ist bei der Beratung zur Einhaltung der DSGVO und des BDSG-neu sowie der Umsetzung der Richtlinie unterstützend zuständig. Sie informiert den DSB über vor Ort aufgetretene Datenschutzfragen. Sie erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren und gibt die Meldung an den DSB weiter.

1.3 Für Meldungen und Auskünfte gegenüber den Datenschutzaufsichtsbehörden liegt die bearbeitende Zuständigkeit grundsätzlich bei dem DSB. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung.

1.4 Jeder Mitarbeiter und jede Mitarbeiterin kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSB oder die Vertretung wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

1.5 Der DSB berichtet jährlich in einem Tätigkeitsbericht der 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 Betriebsrat zugänglich gemacht.

2 Beschaffung Hard- und Software

2.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung durch die über die Verarbeitungen entscheidende Person/Abteilung.

2.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab von der anfordernden Stelle zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des DSB.

2.3 Private Hard- und Software darf nicht zur Verarbeitung oder Nutzung personenbezogener Daten Verwendung finden. Die dienstliche Nutzung privater Hard- und Soft-

ware im heimischen und außerbetrieblichen Bereich (z. B. private Laptops) bedarf der Genehmigung durch die Geschäftsführung im Einzelfall.

2.4 Die Vertretung des Datenschutzbeauftragten im Verein führt und pflegt in Zusammenarbeit mit der IT-Abteilung einen Netzwerkplan sowie ein Inventarverzeichnis der im Organisationsbereich eingesetzten Hardware (einschl. Seriennummern) und der verwendeten Anwendungsprogramme. Eine Kopie ist im Datenschutzordner einzufügen.

2.5 Da Verletzungen des Schutzes personenbezogener Daten Meldeverpflichtungen des Arbeitgebers/Verantwortlichen an die Aufsichtsbehörde und den Betroffenen nach sich ziehen, stehen alle Mitarbeiter und insbesondere die Mitarbeiter der Fachabteilung IT in der Pflicht, den vermuteten oder tatsächlichen Missbrauch oder Missbrauchsversuche der Datenverarbeitungs- und Kommunikationssysteme (dazu gehören auch der Verdacht auf Diebstahls von Hard-/Software, der unbefugten Zugriff auf personenbezogene Daten, Sabotage etc.) der GF und dem bDSB mitzuteilen.

3 Verpflichtung / Schulung der Mitarbeiter

3.1 Jeder Mitarbeiter und jede Mitarbeiterin, der/die Umgang mit personenbezogenen Daten hat, ist gem. Art. 5 in Verbindung mit Art. 24, 29 und 32 DSGVO und gem. § 35 SGB I in Verbindung mit § 80 SGB X und § 3 Abs. TDDDG auf die Vertraulichkeit im Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten. Alle Vorgesetzten haben ihre Mitarbeiter und Mitarbeiterinnen darüber hinaus auf die besonderen Datenschutzanforderungen ihres Arbeitsbereiches hinzuweisen.

3.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars durch die Personalverwaltung. Die Verpflichtung ist gegenzuzeichnen und in der Personalakte sowie als Kopie im Datenschutzordner abzulegen.

3.3 Der DSB schult die Mitarbeiter und Mitarbeiterinnen in datenschutzrechtlichen Belangen und kontrolliert die Umsetzung an deren Arbeitsplatz. Die Teilnahme der Mitarbeiter ist Pflicht. Für die in Abstimmung mit der Geschäftsführung angesetzten Schulungstermine sind die betroffenen Mitarbeiter und Mitarbeiterinnen freizustellen.

4 Transparenz der Datenverarbeitung

4.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt die Geschäftsführung in Zusammenarbeit mit der Vertretung des Datenschutzbeauftragten gem. Art. 30 Abs. 1 DSGVO ein ‚Verzeichnis der Verarbeitungstätigkeiten VVT' (vormals ‚Internes Verfahrensverzeichnis'). Entsprechende Verfahren werden durch die Vertretung des DSB zeitnah und gemäß den vom DSB definierten Vorgaben dokumentiert. Gleiches gilt für Veränderungen. Das VVT unterliegt der permanenten Risikoabschätzung für die Datensicherheit durch die Fachabteilung IT.

4.2 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 (vgl. Ziffer 5.2). Bei allen standardisierten Erhebungen (z. B. Fragebögen oder Eingabefelder auf der Internethomepage etc.) ist der Erhebungsbogen dem DSB zur Abstimmung vorzulegen.

4.3 Soweit der Verantwortliche feststellt, dass die beabsichtigte Verarbeitung seiner Pflicht zur Datenschutz-Folgeabschätzung/Vorabkontrolle (DSFA gem. Art 35 DSGVO) unterliegt, hat er diese in Delegation durch die Fachabteilung IT unter Einbeziehung des DSB durchzuführen. Das Verfahren darf erst nach Zustimmung des DSB durchgeführt werden.

4.4 Alle Mitarbeiter werden gemäß Transparenzgebot der EU-DSGVO (Art. 12 ff) umfassend und proaktiv über die Be- und Verarbeitung ihrer personenbezogenen Daten sowie über ihr Beschwerderecht informiert.

4.5 Macht ein Betroffener von seinem Auskunftsrecht oder seinen Rechten auf Berichtigung, Löschung und Einschränkung der Verarbeitung sowie Widerspruch gegen die Verarbeitung seiner Daten Gebrauch, so erfolgt die zentrale Bearbeitung in der Einführungsphase durch den DSB. Ein regelmäßiges Auskunftsbegehren wird durch die Abwesenheitsvertretung des DSB in Zusammenarbeit mit der entsprechenden Abteilung bearbeitet. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Abwesenheitsvertretung in Zusammenarbeit mit der Personalverwaltung erfüllt.

4.6 Das Verein stellt das Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO sicher. Jeder Betroffene hat das Recht eine Kopie seiner pb-Daten in einem üblichen maschinenlesbaren Dateiformat zu erhalten.

5 Erhebung / Verarbeitung und Nutzung von personenbezogenen Daten

5.1 Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen gem. Art. 5 und 6 DSGVO sowie nach den Vorgaben für die ‚Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses' gem. § 26 BDSG-neu erfolgen. Werden personenbezogene Daten bei der betroffenen Person erhoben, so steht der betroffenen Person gem. Art 12 ff DSGVO das Recht auf transparente Information zu.
Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Hierbei sind die besonderen Voraussetzungen für die Erhebung, Verarbeitung, Nutzung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO und den § 22 ff zu beachten. Die Be- und Verarbeitung sensibler Daten ist gem. DSGVO ausschließlich unter dem Grundsatz des Erlaubnisvorbehaltes oder bei Vorlage einer gesetzlichen Grundlage gestattet.

5.2 Vor neuen Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den Betreiber schriftlich zu dokumentieren. 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.

5.3 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 Vereins besteht, die Identität des Anfragenden zweifelsfrei feststeht und kein schutzwürdiges Interesse des Betroffenen der Weitergabe entgegensteht. Im Zweifel ist der DSB zu kontaktieren.

6 Datenhaltung / Versand / Löschung

6.1 Die Speicherung von personenbezogenen Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern (z. B. Disketten, USB-Stick, CD, DVD) bedarf der Genehmigung durch die Geschäftsführung und der Registrierung durch die den Träger einsetzenden Benutzer.

6.2 Soweit technisch oder funktional bedingt ein anderer Speicherort erforderlich ist (z. B. Notebook, stand-alone-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z. B. bei Notebook mit Netzwerk-Karte), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerke zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

6.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über Verarbeitung der Daten Entscheidenden in seiner Verantwortlichkeit zu beachten. Die Datenbestände sind durch die verantwortlichen Mitarbeiter und Mitarbeiterinnen regelmäßig zu sichten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren. Daten sind zu löschen, wenn der Zweck für Ihre Speicherung entfällt und keine Rechtsnorm, Aufbewahrungsfrist oder ein unternehmerischer Zweck die Beibehaltung der Daten vorsieht. Es gelten die Vorgaben des Art. 17 DSGVO in Verbindung mit § 35 BDSG-neu. Die Verfahrensanweisung ‚Datenschutzkonformes Löschkonzept' ist zu beachten.

7 Externe Dienstleister / Auftragsdatenverwaltung / Wartung

7.1 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 der DSB vor der Beauftragung unter Vorlage des den Anforderungen der Art. 28 und 32 DSGVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

8 Ergänzende Regelungen

Neben dieser Richtlinie bestehen ergänzende Regelungen zur Realisierung der Datensicherungsgebote gem. Art. 32 DSGVO.
Ergänzend zu den nachfolgend aufgeführten Einzelmaßnahmen gelten folgende Ausführungsbestimmungen in der jeweils gültigen Fassung:

- IT-Sicherheits-Richtlinie
- Konzept zur Datensicherheit personenbezogener Daten
- Verpflichtung auf die Vertraulichkeit personenbezogener Daten
- Zusätzliche Verpflichtungserklärung für Systemadministratoren
- Zusätzliche Verpflichtungserklärung für Mitarbeiter/-innen) in der Personalverwaltung
- Dienstanweisung mobile Telearbeit oder Homeoffice (betroffene Mitarbeiter/-innen)
- Nutzungsvereinbarung Smartphones (betroffene Mitarbeiter/-innen)

Einwahl in das vereinsinterne Datennetz von extern (von Zuhause oder Dienstreise)
In Abhängigkeit der betrieblichen Erfordernisse kann der Verein ausgewählten Mitarbeitern und Mitarbeiterinnen einen Zugriff auf das Datennetz des Vereins via Internet mit VPN-client (Terminal-Server-Struktur) zur Verfügung stellen. Die Nutzung ist nur gestattet, wenn auf dem externen Rechner oder Notebook eine Antivirensoftware installiert und diese auch aktiviert ist. **Werden personenbezogene Daten auf externen Medien gespeichert, so sind diese zu verschlüsseln.** Zu beachten sind die Nutzungsvereinbarungen zur mobilen Telearbeit und Homeoffice.
Die persönlichen Zugangsdaten sind sorgfältig zu schützen und eine Weitergabe an Dritte ist nicht gestattet. Alle Remote-Zugriffe werden systemtechnisch protokolliert.

Vernichtung personenbezogener Daten
Elektronische Dokumente (Dateien), die personenbezogene Daten enthalten, sind vorschriftsmäßig und sicher zu vernichten. Es gelten die Vorgaben des Art. 17 DSGVO in Verbindung mit den § 35 BDSG-neu. Die Verfahrensanweisung ‚Datenschutzkonformes Löschkonzept' ist zu beachten. Nach dem Löschen der betroffenen Datei(en) ist der elektronische Papierkorb unverzüglich zu leeren.
Papierdokumente sind durch die Benutzung des Aktenvernichters und/oder Entsorgung durch ein zertifiziertes Unternehmen zu vernichten. Bei größeren Mengen sind die dafür vorgesehenen abgeschlossenen Dokumentenbehälter zu verwenden.

Umgang mit Betriebsschlüsseln und Mitarbeiterkarten
Alle Mitarbeitenden sind verpflichtet, sorgfältig mit Schlüsseln des Vereins umzugehen. Die Schlüssel dürfen nicht an Betriebsfremde ausgeliehen werden. Bei Verlust ist die Geschäftsführung unmittelbar darüber zu informieren.

Weitere Maßnahmen in Organisation der Geschäftsführung
- Verschluss und Zutrittsregelung des Serverraumes
- regelmäßiges Wechseln der Sicherungsbänder des Servers (intern) entsprechend eines festgelegten Backupverfahrens
- unverzügliches Sperren von Systemnutzern nach Beendigung des Vertragsverhältnisses
- Verwaltung der Schlüssel (beinhaltet auch die Kontrolle der Schlüsselrückgabe nach Ausscheiden eines Mitarbeiters)

Kontaktdaten des betrieblichen Datenschutzbeauftragten

Steve Vetter, Vetter Consulting Datenschutzberatung
Oschatzer Str. 46, 01127 Dresden
Tel.: 0173 8947506
Mail: steve.vetter@vc-datenschutz.de
Internet: www.vc-datenschutz.de

Dresden, den 01.07.2024

Harry Vahle	Steve Vetter
Geschäftsführer Huckepack e.V.	Betrieblicher Datenschutzbeauftragter